

Hálózatbiztonság

Kerecsendi András

MÉDLAINFORMATIKAI KIADVÁNYOK

Hálózatbiztonság

Kerecsendi András



Eger, 2013



Korszerű információtechnológiai szakok magyarországi adaptációja

TÁMOP-4.1.2-A/1-11/1-2011-0021

Nemzeti Fejlesztési Ügynökség
www.ujsechenyiterv.gov.hu
06 40 638 638



A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Lektorálta:

Nyugat-magyarországi Egyetem Regionális Pedagógiai Szolgáltató és
Kutató Központ

Felelős kiadó: dr. Kis-Tóth Lajos

Készült: az Eszterházy Károly Főiskola nyomdájában, Egerben

Vezető: Kérészy László

Műszaki szerkesztő: Nagy Sándorné

Tartalom

1	Bevezetés	11
	1.1. Célkitűzések, kompetenciák a tantárgy teljesítésének feltételei....	11
	1.1.1. Célkitűzés.....	11
	1.1.2. Kompetenciák.....	11
	1.1.3. A tantárgy teljesítésének feltételei	12
	1.2. A kurzus tartalma	12
	1.2.1. Tanulási tanácsok, tudnivalók	12
2	Bevezetés a hálózatok biztonsági problémáiba	15
	2.1. Célkitűzések és kompetenciák	15
	2.2. Tananyag	15
	2.2.1. A hálózati rendszerek biztonsága	15
	2.2.2. A hálózat biztonságának jelentősége	16
	2.2.3. A biztonság alapszabályai	17
	2.2.4. Biztonság a hálózati rétegekben	17
	2.2.5. Védelem a felsőbb rétegekben	18
	2.2.6. Veszélyek a hálózati kommunikációban.....	18
	2.2.7. Az AAA protokoll jelentősége	20
	2.2.8. Védekezést segítő szoftverek	20
	2.3. Összefoglalás, kérdések	21
	2.3.1. Összefoglalás	21
3	Hálózati operációs rendszerek biztonsága.....	23
	3.1. Célkitűzések és kompetenciák	23
	3.2. Tananyag	23
	3.2.1. Védelmi alapsmegoldások	24
	3.2.2. Felhasználói fiókok szerepe	24
	3.2.3. Felhasználói fiókok adminisztrációja	25
	3.2.4. Felhasználók tárhelykorlátozása	26
	3.2.5. Mappák, állományok tikosítása.....	27
	3.1.6. BitLocker meghajtótitkosítás.....	28
	3.2.7. BitLocker szolgáltatás használata	29
	3.2.8. Biztonsági házirend	31
	3.2.9. Biztonsági mentés funkció.....	32
	3.2.10.Távoli asztali hozzáférés	32
	3.3. Összefoglalás, kérdések	33

3.3.1. Összefoglalás	33
4 Tűzfalak működése	35
4.1. Célkitűzések és kompetenciák	35
4.2. Tananyag	35
4.2.1. A tűzfal szerepe	35
4.2.2. Tűzfalak típusai	36
4.2.3. Hardveres tűzfalak jellemzői	37
4.2.4. Szoftveres tűzfalak jellemzői	37
4.2.5. Állapottartó tűzfalak	38
4.2.6. Proxy tűzfalak	39
4.2.7. Microsoft operációs rendszerek tűzfalának jellemzése	39
4.2.8. Fokozott biztonságú Windows tűzfal kezelőfelülete	40
4.2.9. Fokozott biztonságú Windows tűzfal bemutatása	41
4.2.10. Tűzfal beállítások testreszabása és a naplózás	43
4.2.11. Tűzfalszabályok kezelése	44
4.2.12. Tűzfalszabály létrehozása	45
4.3. Összefoglalás, kérdések	47
4.3.1. Összefoglalás	47
5 Kriptográfiai alapismeretek	49
5.1. Célkitűzések és kompetenciák	49
5.2. Tananyag	49
5.2.1. A kriptográfia fogalma	49
5.2.2. A kriptográfia története	50
5.2.3. Behelyettesítéses módszer	51
5.2.4. Az elektronikus eszközök megjelenése	52
5.2.5. Modern kriptográfia	53
5.2.6. Kriptográfiai alapfogalmak	54
5.2.7. A kriptográfia részterületei	54
5.2.8. Szimmetrikus kriptográfia	55
5.2.9. Aszimmetrikus kriptográfia	56
5.2.10. Szteganográfia napjainkban	57
5.3. Összefoglalás, kérdések	58
5.3.1. Összefoglalás	58
6 Titkosító algoritmusok	59
6.1. Célkitűzések és kompetenciák	59
6.2. Tananyag	59

6.2.1. Bevezetés a titkosítási módszerekbe	59
6.2.2. Egyszer használatos bitminta	60
6.2.3. Data Encryption Standard – DES	61
6.2.4. Háromszoros DES	61
6.2.5. Advanced Encryption Standard – AES	62
6.2.6. Rijndael kódolás	62
6.2.7. International Data Encryption Algorithm – IDEA	63
6.2.8. Egyéb szimmetrikus kódolási eljárások	63
6.2.9. Nyilvános kulcsú algoritmusok	64
6.2.10. Az RSA algoritmus alapjai	64
6.2.11. Az RSA algoritmus	65
6.2.12. Példa az RSA működésére	66
6.2.13. Egyéb aszimmetrikus kódolási megoldások	66
6.3. Összefoglalás, kérdések	67
6.3.1. Összefoglalás	67
7 Digitális azonosítók	69
7.1. Célkitűzések és kompetenciák	69
7.2. Tananyag	69
7.2.1. Digitális aláírások jelentősége	69
7.2.2. Digitális lenyomatok	70
7.2.3. MD5 hash függvény	71
7.2.4. SHA-1 hash függvény	71
7.2.5. Digitális aláírás fogalma	72
7.2.6. Az időbélyegzés	73
7.2.7. Tanúsítványok szerepe	73
7.2.8. Nyilvános kulcsú infrastruktúra	74
7.2.9. Tanúsítványok kezelése	75
7.2.10. Tanúsítványok használata	76
7.2.11. Tanúsítványok kezelése Microsoft operációs rendszerekben	76
7.2.12. Tanúsítványkezelő modul használata	77
7.2.13. Tanúsítványok exportálása	79
7.2.14. Tanúsítványok kezelése az Internet Explorerben	81
7.2.15. Tanúsítványok kezelése az Outlookban	81
7.2.17. A digitális aláírás törvényi háttere	83
7.3. Összefoglalás, kérdések	83
7.3.1. Összefoglalás	83
8 Hálózati támadások típusai	85

8.1 Célkitűzések és kompetenciák.....	85
8.2. Tananyag.....	85
8.2.1. Hálózati fenyegetettség	85
8.2.2. Social engineering	86
8.2.3. A hálózati támadás folyamata.....	87
8.2.4. Szolgáltatásmegtagadásos támadás (DoS).....	88
8.2.5. Szolgáltatásmegtagadásos támadás: SYN flooding	88
8.2.6. Szolgáltatásmegtagadásos támadás: PoD.....	89
8.2.7. Elosztott szolgáltatásmegtagadásos támadás (DDoS)	89
8.2.8. Hamis megszemélyesítés	90
8.2.9. Sebezhetőségek kihasználása	91
8.2.10. Kártékony programok	91
8.2.11. Hálózati eszközök támadása	92
8.3. Összefoglalás, kérdések	93
8.3.1. Összefoglalás	93
9 Kommunikációs szolgáltatások biztonsága.....	95
9.1. Célkitűzések és kompetenciák.....	95
9.2. Tananyag.....	95
9.2.1. Kommunikációs szolgáltatások biztonsága	96
9.2.2. Internetbiztonság	96
9.2.3. Az IPsec.....	97
9.2.4. Az IPsec használati módjai	97
9.2.5. IPsec használata Microsoft környezetben	98
9.2.6. Virtuális magánhálózat (VPN)	99
9.2.7. Virtuális magánhálózat a gyakorlatban.....	100
9.2.8. Hálózatvédelem Microsoft környezetben.....	104
9.2.9. DirectAccess szolgáltatás	105
9.2.10. Biztonságos csatlakozórétteg	106
9.3. Összefoglalás, kérdések	107
9.3.1. Összefoglalás	107
10 Autentikációs protokollok	109
10.1. Célkitűzések és kompetenciák	109
10.2. Tananyag.....	109
10.2.1. Hitelességvizsgálat	110
10.2.2. A hitelességvizsgálat általános modellje	110
10.2.3. Hitelességvizsgálat nyilvános kulcsú titkosítással	111
10.2.4. Hitelességvizsgálat CHAP alkalmazásával	112

10.2.5. Hitelességvizsgálat EAP alkalmazásával	112
10.2.6. Azonosítók átadása – Pass thru módszer	113
10.2.7. Hitelességvizsgálat Kerberos alkalmazásával	113
10.2.8. Active Directory szolgáltatás	114
10.2.9. LDAP alapú hitelesítés	115
10.2.10. RADIUS alapú hitelesítés	115
10.2.11. RADIUS a gyakorlatban.....	117
10.2.12. A TACACS alapú hitelesítés.....	119
10.2. Összefoglalás, kérdések	119
10.2.1. Összefoglalás	119
11 E-mail és web biztonság.....	121
11.1. Célkitűzések és kompetenciák	121
11.2. Tananyag	121
11.2.1. Elektronikus levelek biztonsága	121
11.2.2. A PGP (Pretty Good Privacy) protokoll	122
11.2.3. S/MIME szabvány	123
11.2.4. Vírusok elleni védelem	124
11.2.5. Spamek elleni védelem	126
11.2.6. Adathalászat – phishing.....	126
11.2.7. Védekezés beállítása Outlookban	127
11.2.8. Webbiztonság.....	129
11.2.9. Biztonságos névkezelés	130
11.2.10. Biztonságos összeköttetés.....	131
11.2.11. Az SSL működése	132
11.2.12. Hordozható kódok biztonsága.....	133
11.2.13. Védelmi beállítások IIS kiszolgálóban.....	135
11.3. Összefoglalás, kérdések	138
11.3.1. Összefoglalás	138
12 Vezeték nélküli hálózatok biztonsága	139
12.1. Célkitűzések és kompetenciák	139
12.2. Tananyag	139
12.2.1. Vezeték nélküli hálózatok alaptulajdonságai	139
12.2.2. Vezeték nélküli hálózatok biztonsága	140
12.2.3. Vezeték nélküli hálózatok egyszerű védelme.....	140
12.2.4. Wired Equipment Privacy – WEP.....	141
12.2.5. Wi-Fi Protected Access – WPA	142
12.2.6. A WPA továbbfejlesztett verziója.....	142

12.2.7. 802.1X rendszerű hitelesítés	143
12.2.8. Vezeték nélküli kapcsolat biztonsági beállításai a gyakorlatban.....	144
12.2.9. Vezeték nélküli hálózatok tulajdonságai.....	145
12.2.10. Adattitkosítási szabványok.....	147
12.2.11. 802.1X alapú hitelesítés beállítása	148
12.3. Összefoglalás, kérdések	150
12.3.1. Összefoglalás	150
13 Összefoglalás	151
13.1. Tartalmi összefoglalás	151
13.2. Zárás	151
13. Kiegészítések	153
13.2. Irodalomjegyzék	153

1 BEVEZETÉS

1.1. CÉLKITŰZÉSEK, KOMPETENCIÁK A TANTÁRGY TELJESÍTÉSÉNEK FELTÉTELEI

1.1.1. Célkitűzés

A tantárgy keretein belül a hallgatók átfogó elméleti és gyakorlati ismereteket szereznek a modern hálózatok biztonsága körében. Megismerik azon eszközök, módszerek elméletét és gyakorlatát, amelyek segítségével egy hálózat vagy hálózati szolgáltatás biztonságossá tehető. Elsajátítják a kommunikáció titkosítására, hitelesítésre, integritásvédelemre, valamint az eszközök és hálózati szolgáltatások esetén a hamisítás megakadályozására, hozzáférés- és szolgáltatmegtagadás elleni védelemre kidolgozott módszereket, lehetőségeket. Képesek lesznek felismerni egy működő rendszer gyenge pontjait és megfelelő javaslatokat tenni a veszélyeztetettség megszüntetésére. Fontos, hogy a hallgatók felkészültek legyenek a legújabb technológiák alkalmazásában is, így például a vezetékek nélküli hálózatokban használt biztonsági architektúrákkal és protokollokkal is megismerkednek.

1.1.2. Kompetenciák

- A hallgató legyen képes a megszerzett tudás hatékony használatára hálózati környezetben.
- Biztonsági megoldások teljes körű használata, nyitottság az új megoldásokra.
- Legyen képes gyakorlatias feladatértelmezésre a hálózatok biztonsági kérdéseinek megoldásához.
- Ismerje a hálózati kommunikáció veszélyeit, azok fontosabb jellemzőit tudja megnevezni!
- Képes lesz hatékony biztonsági megoldásokat tervezni, alkalmazni.
- Megismeri a különböző védelmi szolgáltatásokat, képes lesz beállítani, konfigurálni működésüket.
- Munkájában, későbbi tanulmányai során hasznosítani tudja a megszerzett ismereteket.

- Absztrakt gondolkodás kialakítása a biztonsági problémák megelőzésére, megoldására.
- A problémaelemzés segít a veszélyhelyzetek gyors elhárításában

1.1.3. A tantárgy teljesítésének feltételei

A tananyag megismerése, befogadása, a bemutatott eljárások, módszerek, funkciók gyakorlása után a hallgató képes lesz önállóan ellenőrizni hálózati rendszereket, azok biztonsági tulajdonságait és elvégezni alapvető beállításokat.

A hálózati operációs rendszereken belül létre tudja hozni a felhasználói fiókokat, a szervezeti igényeknek megfelelően el tudja végezni a felhasználói jogosultságok beállítását, meg tudja határozni az erőforrásokhoz való hozzáférési szinteket. Megismeri a hálózatra, a hálózati kommunikációra leselkedő veszélyeket, illetve az azokra adható válaszokat, képes lesz például a tűzfal szabályainak meghatározására.

Napjainkban fontos a cégek, szervezetek számára az interneten való megjelenés és ennek biztonságossá tétele. A kurzus végére a hallgató tisztában lesz azokkal a kriptográfiai alapismeretekkel, eljárásokkal, amelyek a biztonságos kommunikációt, hitelesítést teszik lehetővé. Megismerkednek a digitális aláírás jellemzőivel, használatának, működésének tulajdonságaival, előnyeivel, a különböző, elterjedten használt titkosítási algoritmusokkal, illetve az ezekre épülő biztonsági protokollokkal. Külön fejezeteket szenteltünk a leggyakrabban használt, internetalapú kommunikációs szolgáltatások, az elektronikus levelezésnek és a web biztonságának, illetve a nagyon elterjedt vezeték nélküli hálózati megoldásoknak.

A tananyag elolvasása, áttanulmányozása önmagában nem elég a témakör megértéséhez, az elméleti, gyakorlati bemutatók mellett fontos, hogy elvégezzük azokat a műveleteket, gyakorlati feladatokat, amelyek segítik a hálózatok biztonságosabbá tételét. A tananyag a Microsoft operációs rendszerein keresztül mutatja be az alkalmazásokat, szolgáltatásokat, így valószínűleg mindenkinek lesz lehetősége ezeket kipróbálni, végrehajtani.

1.2. A KURZUS TARTALMA

1.2.1. Tanulási tanácsok, tudnivalók

A tananyag a Microsoft szoftverein keresztül mutatja be a hálózati biztonsággal kapcsolatos alkalmazások, szolgáltatások, funkciók működését, kezelését, alkalmazási lehetőségeit. Fontos megemlíteni, hogy a többi operációs rend-

szerben is hasonlóan működnek ezek a megoldások, így azt itt megszerzett tudás nagy valószínűséggel hasznosítható más programok esetén is.

Fontos, ahogy már említettük, hogy minél több leírt, bemutatott módszert, szolgáltatást, funkciót próbáljanak ki a gyakorlatban is, hiszen legkönnyebben így lehet megtanulni az informatikai rendszerek működését.

A tananyag a jelenleg elérhető megoldásokat, algoritmusokat, programokat mutatja be, amelyek pár éven belül könnyen elavulttá válhatnak, de valószínűleg az alapvető jellemzők nem fognak változni, új rendszerek esetén csak az újdonságokat, a továbbfejlesztett szolgáltatásokat, funkciókat kell megismernünk. Ne feledjük, tökéletes biztonság nincs!

2 BEVEZETÉS A HÁLÓZATOK BIZTONSÁGI PROBLÉMÁIBA

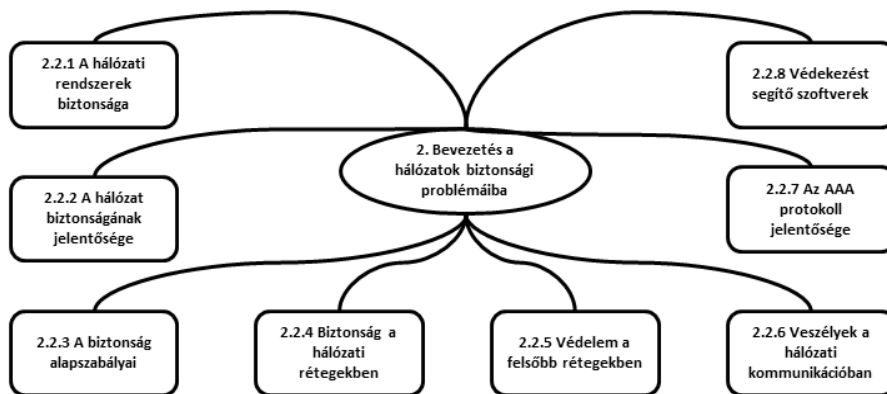
2.1. CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

A fejezet célja, hogy a hallgatók megismerkedjenek a hálózati rendszerek alapvető biztonsági problémáival, illetve az alkalmazható védekezési módszerekkel.

Tisztázni fogjuk, hogy milyen feltételek teljesülése esetén beszélhetünk biztonságos kommunikációról, milyen alapszabályok szem előtt tartása fontos a biztonsági rendszerek alkalmazása esetén.

Bemutatjuk, hogy hol és hogyan lehet védekezni a hálózati kommunikáció különböző rétegeiben, illetve az AAA protokollokat általánosságban.

2.2. TANANYAG



2.2.1. A hálózati rendszerek biztonsága

A hálózati rendszerek biztonságával kezdetben nem foglalkoztak túl sokat, hiszen nagyon szűk szakmai kör tudott egyáltalán hozzáférni a számítógépekhez, hálózati rendszerekhez, és az ott tárolt adatokhoz, információkhoz. Később, ahogy bővült a felhasználói kör, és már nemcsak elhivatott szakemberek fértek hozzá az informatikai rendszerekhez, megjelentek olyan személyek is, akik sajnos felismerték és kihasználták a számítógépes hálózatok védtelenségét.

Emellett nem szabad elfeledkezni arról a tényről sem, hogy a hagyományos kommunikációs csatornák helyett egyre többen veszik igénybe a számítógépes hálózatok által nyújtott szolgáltatásokat, viszont katonai, üzleti vagy érzékeny céges adatoknál elengedhetetlenek a megfelelő biztonsági megoldások. Mindezen okok következményeként szükséges a rendszerek, a kommunikáció, az adatokhoz, erőforrásokhoz való hozzáférés biztonságossá tétele.

Létrehoztak olyan szabványos megoldásokat, titkosítási eljárásokat, biztonsági funkciókat, amelyek megfelelnek az elvárásoknak. Ezeket már az újabb fejlesztett rendszerek is át tudják venni, alkalmazhatják. Ennek olyan előnye is van, azon kívül, hogy nem kell időt, erőforrásokat áldozni ezek kidolgozására, hogy a különböző fejlesztésű rendszerek is képesek együttműködni: ma már nem okoz problémát például egy UNIX alapú és egy Windows-t futtató számítógép között biztonságos adatátvitelt, kommunikációt biztosítani.

A Microsoft operációs rendszereit úgy készítették, hogy az elfogadott, használt szabványokat alkalmazza, felkészült a hálózati támadásokra, rendelkezik az azok kivédésére szolgáló eszközökkel.

2.2.2. A hálózat biztonságának jelentősége

Napjainkban a biztonság a legfontosabb szempontok közé tartozik, amikor egy cég, egy szervezet az informatikai, hálózati infrastruktúráját tervezi, működteti. A globalizálódás folyamata arra kényszerít mindenkit, hogy ne csak a munkatársakkal, hanem a partnerekkel is számítógépen, illetve számítógépes hálózaton keresztül, minél egyszerűbben, gyorsabban és biztonságosabban tudjon kommunikálni. Ennek a nagymértékű használatnak sajnos az a hátránya, hogy az ártó szándékú tevékenységet folytatók előtt is nagyobb lehetőségek nyílnak.

A biztonság több részből tevődik össze: egyrészt védeni kell a hálózati erőforrásokat, hogy azokhoz csak a megfelelő felhasználók és a megfelelő jogosultsággal férjenek hozzá. Másrészt biztosítani kell két fél között a biztonságos kommunikációt. Ez utóbbiról akkor beszélhetünk, ha a következő feltételek teljesülnek:

- bizalmas kezelés, vagyis a két félén kívül más nem képes elolvasni az átküldött üzenetet
- hitelesítés, vagyis az üzenet fogadója tudja azonosítani a küldőt
- az adat sérthetetlensége, vagyis az üzenet tartalma nem változtatható meg észrevétlenül a kommunikációs folyamat során
- letagadhatatlanság, vagyis a küldő nem tudja letagadni az üzenet elküldését, harmadik fél előtt sem

2.2.3. A biztonság alapszabályai

A hálózati támadások elleni védekezés esetén ne felejtkezzünk meg három fontos alapszabályról!

A biztonság nem egy termék, hanem sokkal inkább egy eljárás, egy módszer. A hamis biztonságérzet a legrosszabb eset, hiszen ha azt hisszük, hogy teljes biztonságban vagyunk, és nem teszünk semmit a védekezés érdekében, akkor bizony könnyen érhet meglepetés. Hasonló probléma lehet, ha úgy gondoljuk, miért pont a mi adatainkra, kommunikációnkra, erőforrásainkra lenne kíváncsi bárki is?

Mindezek alapján ne csak a biztonsági programokban lássunk megoldást a problémákra, hanem a szoftvereket megfelelően alkalmazó elvi elgondolásokban is, és célszerű ezeket az elveket időnként átgondolni, felülvizsgálni. Ez egy folyamatosan végzett művelet, mert mint már tudjuk, tökéletes biztonság nincs, legfeljebb csak tudatos kockázatvállalás.

Alapelveként mondhatjuk azt is, hogy a hálózatot védő biztonsági rendszerek kialakítása akkor tekinthető megfelelőnek, ha egy esetlegesen előforduló támadás során – amennyiben a támadó már el is jutott valameddig a rendszer feltörésében – a továbbjutáshoz újabb (és lehetőleg addig még nem használt) módszerek, műveletek használatára is szükség legyen. Vagyis egy összetett, komplex védelmi rendszer nagyobb biztonságot nyújt!

2.2.4. Biztonság a hálózati rétegekben

A hálózat biztonságossá tétele, védelme a hálózati kommunikáció minden területére kiterjedhet, nincs egy egységes, jól bevált eljárás, ami egyszerűen használható és anyagilag sem megterhelő. Ebből következik, hogy a védelmi rendszer a felhasználóktól, a küldött adatok minőségétől, a használt szolgáltatásoktól függően kerül kialakításra.

Melyik hálózati rétegbe célszerű elhelyezni a biztonsági megoldásokat? Könnyen belátható, hogy nem helyezhető egyetlen helyre, hiszen minden réteg hozzájárulhat valamilyen formában a biztonságos adatátvitelhez.

A fizikai rétegben védhetőek a vezetékek, kábelek, például egy gázzal töltött csőbe elhelyezve azokat, így támadás során a nyomáscsökkenés riasztást okozhat. Természetesen ez költséges megoldás, de katonai rendszereknél alkalmazzák. Az adatkapcsolati réteg két végpont között haladó keretekben található adatokat képes titkosítani, a felsőbb rétegek tudta nélkül. Ennek hátránya, hogy a közbeeső hálózati eszközökön vissza kell fejteni, majd újra kódolni az adatokat, illetve eközben támadható is a kommunikáció. Ráadásul az ilyen típu-

sú védelem esetén nem szabályozható, hogy milyen kapcsolatokat akarunk védeni (például on-line banki műveletek), és milyeneket nem. Ezt a védekezési módot egyébként adatkapcsolati titkosításnak nevezzük, könnyen és hatékonyan használható, ha erre van szükség.

2.2.5. Védelem a felsőbb rétegekben

Sokkal gyakrabban használunk a gyakorlatban olyan védelmi megoldásokat, amelyeket a felsőbb rétegekben (esetleg azok között) helyezünk el.

Elég csak a valószínűleg mindenki által hallott tűzfalra gondolni, amelyeket azért telepítünk, hogy képesek legyünk minden egyes csomagot megvizsgálni. Szintén a hálózati rétegben találhatóak az IP-hez köthető egyéb biztonsági funkciók.

A szállítási réteg feladata a végponttól végpontig terjedő összeköttetés biztosítása, természetes, hogy ezen a szinten tudunk a leghatékonyabban biztonsági eljárásokat alkalmazni.

Végül gondoljunk az olyan kérdésekre, mint a felhasználók azonosítása, vagy a letagadhatatlanság, ezek kezelése csak a viszony-, illetve az alkalmazási rétegben oldható meg.

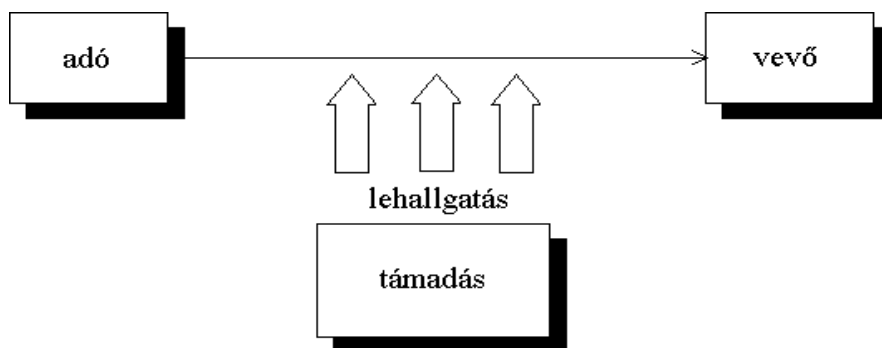
A tananyag ezekkel, a felsőbb rétegekben használatos megoldásokkal foglalkozni, hiszen jellemzően ezeket használjuk a leggyakrabban.

2.2.6. Veszélyek a hálózati kommunikációban

A hálózati kommunikációra a fő veszélyforrások lehetnek az üzenetek meghamisítása, törlése, hamis adatok, információk átvitele. A hálózati szolgáltatások használata során bebizonyosodott, hogy önmagában a hozzáférés-védelem nem nyújt kellő biztonságot, ennek következtében ajánlott olyan kriptográfiai módszereket (például a hitelesítést) is igénybe venni a kommunikáció során, amelyekkel biztosítható és ellenőrizhető üzeneteink változatlansága, sértetlensége.

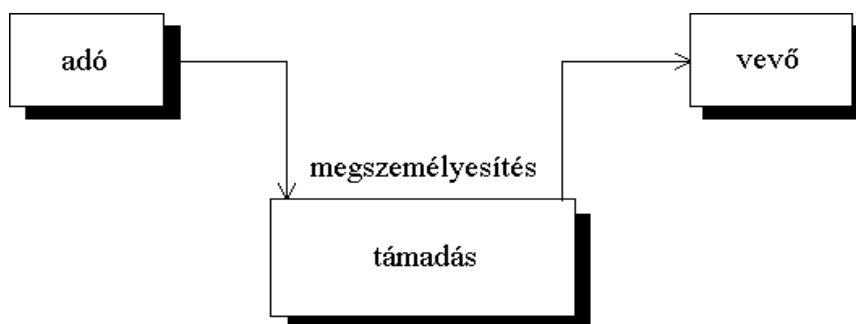
A hálózati kommunikáció nem megfelelő védelme okozhatja a másik veszélyforrást, amikor tárolt adatainkhoz – ezek lehetnek dokumentumok, állományok, elektronikus levelek, adatbázisok stb. – illetéktelenül férnek hozzá.

A kommunikációs folyamat közben maga az átviteli csatorna is lehet problémaforrás a védelmi rendszeren belül. Nézzük meg a két jellegzetes támadási formát, a lehallgatást és a megszemélyesítést!



1. ábra: Lehallgatás

A lehallgatás során a támadó rákapcsolódik az átviteli közegre, és az ott folyó adatforgalmat rögzíti, figyeli, sok esetben automatizálva, programok segítségével. Ezzel a módszerrel, az adatok összegyűjtésével, a kommunikáció figyélésével akár teljes informatikai rendszerünk ellen támadást intézhet a rosszindulatú személy.



2. ábra: Megszemélyesítés

A megszemélyesítés abban különbözik a lehallgatástól, hogy a támadó nemcsak passzív módon figyeli az adatcserét, hanem része lesz a kommunikációs folyamatnak, amit úgy ér el, hogy az üzeneteket átvitel közben elnyeli, majd ő válaszol azokra, akár mindkét irányban. „Különös veszélyforrás lehet, ha a támadó az egymással kommunikáló állomásokat sorozatos ismétlésre kényszeríti, esetleg ugyanazon üzenet két különböző rejtjelezett variációját szerzi meg, vagy valamelyik állomásról ismert választ kényszerít ki, amellyel megszerzi annak rejtjelezett változatát”¹.

¹ http://www.itb.hu/ajanlasok/a8/html/a8_m3_1.htm, 2012.06.28.

2.2.7. Az AAA protokoll jelentősége

Az informatikai biztonság témakörének egyik fontos eljárásmodja az úgynevezett AAA protokoll, amely három angol kifejezés kezdőbetűiből áll: ezek az authentication, authorization és az accounting szavak. Magyarul hitelesítésről, jogosultságkezelésről és könyvelésről beszélhetünk. Ez egy általános eljárás, mai hálózati rendszereink gyakorlatilag ezt a három biztonsági műveletet oldják meg különböző módszerek, algoritmusok segítségével.

Tekintsük át röviden, mit is jelent ez a három fogalom!

A hitelesítés az a folyamat, amelyen keresztül egy objektum azonosításra kerül, vagyis bizonyítja, hogy rendelkezik megfelelő hitelesítő adatokkal. Többféle hitelesítő adat létezik, a legegyszerűbbek a felhasználónevek, jelszavak, de beszélhetünk digitális aláírásokról, biometria azonosítókra is. A hitelesítés nemcsak személyekre vonatkozhat, hanem számítógépekre, hálózati eszközökre is!

A jogosultságkezelés a sikeres hitelesítés után kap szerepet, amikor a hálózati rendszer szabályozza, hogy az objektumnak mely erőforrásokhoz és milyen hozzáférési jogai vannak.

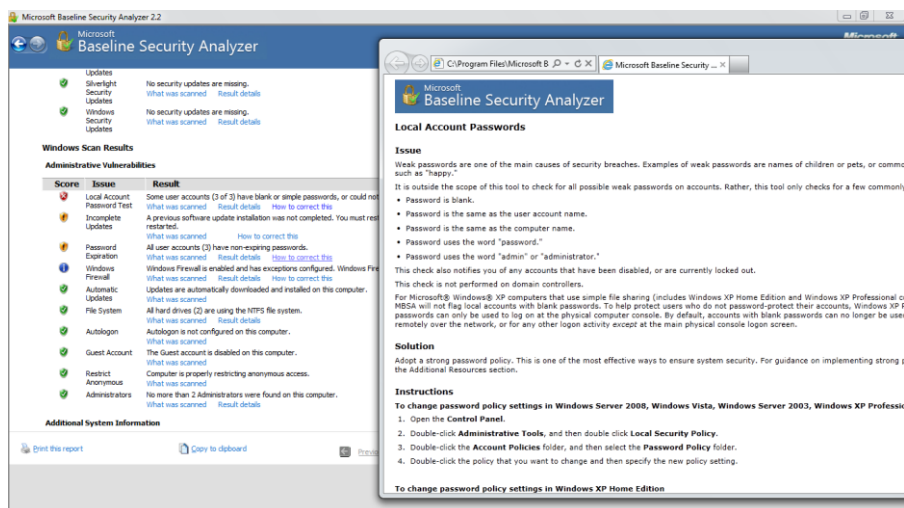
A könyvelés egy viszonylag ritkán emlegetett funkció, nem is igazán a biztonsághoz tartozik. Arra szolgál, hogy nyomon kövesse, az objektum milyen erőforrásokat, mennyi ideig használ, elsősorban azért, hogy ki lehessen számlázni a tevékenységek árát a felhasználónak.

2.2.8. Védekezést segítő szoftverek

Napjaink hálózati rendszerei már beépítve tartalmazznak rengeteg olyan funkciót, amelyek azt a célt szolgálják, hogy minél biztonságosabban tudjunk kommunikálni, tudjuk használni a hálózati erőforrásokat. Ehhez a védelemhez hozzátartozik az elterjedt biztonsági eljárások, algoritmusok, szabványok használata, ami azt is eredményezi, hogy különböző platformon dolgozó felhasználók, illetve az általuk használt alkalmazások is tudnak egymással biztonságos körülmények között együttműködni.

Emellett a különböző rendszerek gyártói egyéb kiegészítő alkalmazásokkal is segítik a felhasználókat, illetve rendszergazdák munkáját. Így például a Microsoft ingyenesen elérhetővé tesz egy vírusok és kémprogramok elleni védelmet biztosító programot, amit Microsoft Security Essentials néven adnak közre. A másik ilyen szoftver az MBSA (Microsoft Baseline Security Analyzer), amelynek alkalmazásával feltérképezhetjük, hogy hol vannak hibák vagy gyengeségek a rendszerünkben. Az MBSA használata természetesen nem pótolja a biztonsági

beállítások finomhangolását, de egy ellenőrzés után felhívja a figyelmet a lehetséges védelmi hiányosságokra!



3. ábra: MBSA ellenőrzés eredménye

Ahogy a képen is látszik, az ellenőrzés végén egy listát kapunk az adott, valamelyik Windows verziót használó számítógép állapotáról (tehát nemcsak a saját számítógépünkről, hanem megfelelő jogosultsággal egyéb, hálózaton elérhető eszközről is), illetve egy linken keresztül a veszély elhárításáról is olvashatunk. Egyetlen apró nehezítő tényezője a program használatának, hogy nincs magyar nyelvű felülete, így az angol nyelv ismerete szükséges a hatékony ellenőrzéshez.

2.3. ÖSSZEFOGLALÁS, KÉRDÉSEK

2.3.1. Összefoglalás

A fejezet általánosságban foglalkozott a számítógépes hálózatok biztonsági problémáival, meghatároztuk, hogy milyen kritériumok teljesülése esetén beszélhetünk biztonságos kommunikációról hálózati környezetben.

Összefoglaltuk, hogy a hálózati rétegekben milyen módon lehet védekezni az esetleges támadások ellen, melyek a leggyakrabban alkalmazott támadási formák.

A biztonság megvalósításához gyakran használjuk az AAA protokollt, ennek rövid bemutatására is sor került.

3 HÁLÓZATI OPERÁCIÓS RENDSZEREK BIZTONSÁGA

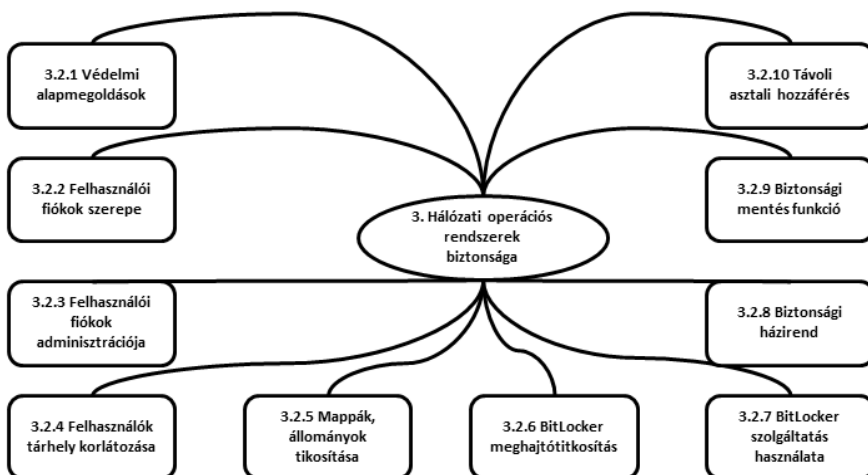
3.1. CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

A fejezet célja bemutatni azokat az alapvető biztonsági megoldásokat, amelyeket a Microsoft operációs rendszerei használnak annak érdekében, hogy a felhasználó biztonságban tudhassa adatait, erőforrásait, szolgáltatásait.

A hallgatók megismerik a hálózati biztonsághoz tartozó fogalmakat, eljárásokat, célokat, majd azokat a konkrét megoldásokat, amelyeket az operációs rendszer biztosít. Áttekintik a fájl- és meghajtótitkosítási szolgáltatásokat, azok engedélyezését, használatát, beállításait, megismerik a biztonsági mentés funkciót.

A hálózati védelem egyik fontos szegmensét, a Microsoft rendszerek egyik legfontosabb szabályozó rendszerének, a házirendek használatának módját, jelentőségét szintén megismertetjük a hallgatókkal, hogy hatékonyan tudják majd védeni a rájuk bízott operációs rendszereket.

3.2. TANANYAG



3.2.1. Védelmi alapmegoldások

Minden Microsoft operációs rendszer védi magát és erőforrásait, így a rendszer használatához minden esetben felhasználói név és jelszó szükséges, kiszolgáló esetén a jelszavakra vonatkozóan is alapértelmezetten meg kell felelni erős biztonsági követelményeknek, így például a jelszó hosszára, a tartalmazott karakterek típusára vonatkozóan.

A felhasználói azonosításon túl, belépve a rendszerbe, az erőforrásokhoz való hozzáférést a jogosultságok, engedélyek szabályozzák. Az operációs rendszer fog figyelni arra, hogy egy adott erőforráshoz a felhasználónak szabad-e hozzáférnie, illetve milyen műveleteket végezhet. Ezt egy rugalmasan szabályozható jogosultsági rendszer segítségével tehetjük meg, amelyet alapvetően a rendszergazda fog kezelni.

Alapvető megoldásnak számít hálózati rendszereknél a felhasználók kvótázása, vagyis limitáljuk, hogy az egyes felhasználók a közös háttértáron mekkora helyet foglalhatnak el az állományaikkal.

A Microsoft az úgynevezett házirendek (policy) segítségével biztosítja az operációs rendszereinek bővebb szabályozhatóságát, amellyel egyes funkciókhoz, szolgáltatásokhoz adhatunk meg tulajdonságokat, illetve hozzárendelhetünk felhasználókat, akik kezelhetik azokat.

Az előzőleg említett funkciókról a további alfejezetekben bővebben is szólunk majd.

3.2.2. Felhasználói fiókok szerepe

A hálózati operációs rendszerek megkövetelik a felhasználó azonosítását, minden erőforrás elérése, minden program futtatása, minden folyamat (említjük még processz néven is) valamely felhasználói fiókhoz kapcsolódik. Fiókról (vagy account-ról) azért beszélünk, mert nem csak azonosítóadatok, hanem az erőforrásokhoz való hozzáférések, jogosultságok, esetleg tárhely, postafiók információk is itt, ebben a komplex objektumban kerülnek tárolásra. Léteznek úgynevezett rendszer szintű fiókok, ezek telepítéskor jönnek létre, a rendszer-folyamatok ezeknek a fiókoknak a nevében futnak. Ilyen rendszerfiók például a SYSTEM vagy a HÁLÓZATI SZOLGÁLTATÁS.

Ahogy már volt szó róla, az operációs rendszer telepítésekor a Rendszergazda fiók jön létre, illetve Windows 7 esetén egy általunk megadott nevű, rendszergazdai jogosultságokkal rendelkező felhasználó. A további felhasználók létrehozása, adminisztrálása a rendszergazda joga és felelőssége lesz. Sokan elfelejtik, hogy a rendszergazdának nemcsak mindenre kiterjedő jogköre van,

hanem az övé a felelősség is a hálózat, a rendszer, a szolgáltatások, az erőforrások működtetése során!

Miért is szükséges adminisztrálni a felhasználókat? Gondoljuk végig az eddigiek alapján! Létre kell hozni a felhasználói fiókot, megadni a rendszerben a felhasználó alapadatait, be kell állítanunk a jogosultságait, hozzáférési szintjeit a különböző erőforrásokhoz, szolgáltatásokhoz, mindezt természetesen úgy, hogy egyrészt megfeleljünk a szervezetünk belső szabályainak, másrészt pedig megpróbálva figyelembe venni a felhasználó kéréseit, igényeit is.

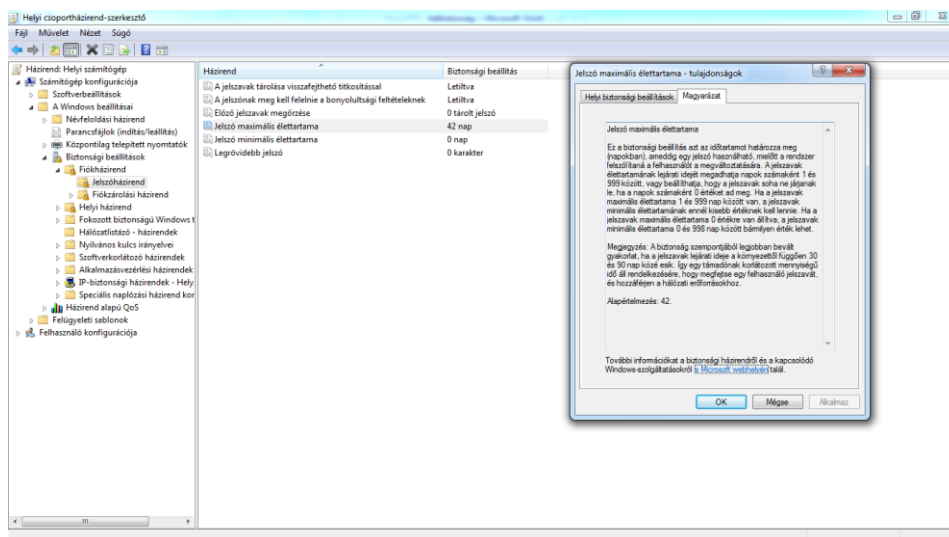
3.2.3. Felhasználói fiókok adminisztrációja

A Rendszereszközök között található a Helyi felhasználók és csoportok ág, amelyet ha megnyitunk, akkor két almappát látunk, a Felhasználók-at és a Csoportok-at. Nézzük meg először a Felhasználók mappát! Kattintásra megjelennek az operációs rendszerünkben létező felhasználói fiókok. Már vizuálisan is látszik, hogy alapesetben a Rendszergazda fiók nem használható, erre utal a kis ikonon látható, lefelé mutató nyíl szimbólum (ugyanígy az automatikusan létrejövő Vendég fiók is inaktív).

Mielőtt hozzáadnánk egy új fiókot a rendszerünkhöz, nézzünk meg pár szabályt, amit be kell tartanunk! A felhasználói fiókok nevére vonatkozóan a következő megszorításokat alkalmazza az operációs rendszerünk:

- nem lehet ugyanolyan név a felhasználók, illetve a csoportok között
- a név hossza maximum 20 karakter lehet
- tartalmazhat kis- és nagybetűket, de azonosításkor nem tesz különbséget
- nem tartalmazhat speciális karaktereket, így: o „ / \ [] : ; | = , + * ? < > @, nem állhat csupa pontból (.) illetve szóközből.

A jelszavakra vonatkozóan annyit kell betartanunk, hogy legfeljebb 14 karakter lehet a hossz, illetve ne felejtjük el, hogy hitelesítéskor az operációs rendszer különbséget fog tenni a kis- és a nagybetűk között. Szerver esetén a jelszavaknál követelmény a minimum 8 karakter hosszúság, legalább két darab kis- és nagybetűt, illetve számjegyet kell tartalmaznia.



4. ábra: Jelszó maximális élettartamának beállítása

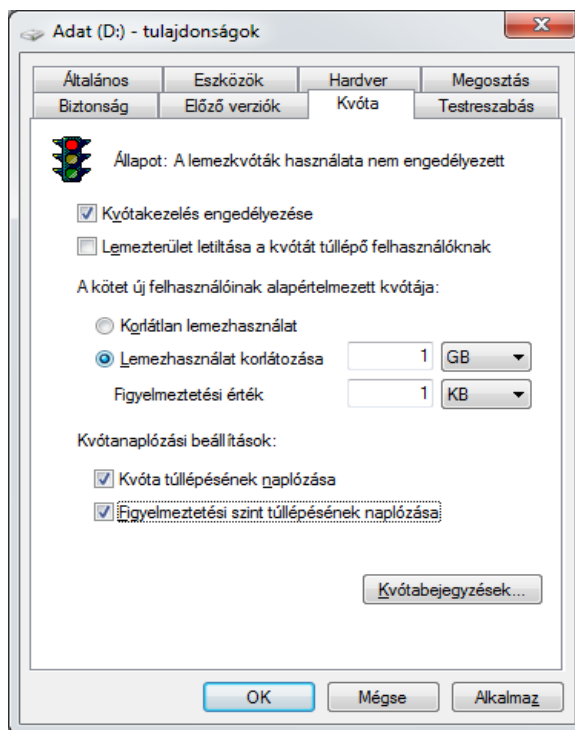
A jelszavakra még egyéb megkötéseket is lehet tenni (például kötelező időszakos változtatás), ezt a háztartásban belül tehetjük meg, amelyről a későbbiekben lesz szó.

3.2.4. Felhasználók tárhelykorlátozása

Az operációs rendszer által kezelt köteteken (természetesen ahol van értelme) beállítható, hogy egyes felhasználók mennyi tárhelyet foglalhatnak el állományaikkal. Ez fontos abból a szempontból, hogy a közösen használt tárhelyek ne teljenek meg pl. egy felelőtlen felhasználó miatt.

A kötetek helyi menüjében található a Tulajdonságok menüpont, ahol a kötetről további információkat jeleníthetünk meg, illetve egyéb funkciókat, szolgáltatásokat engedélyezhetünk, vagy tilthatunk meg.

A Kvóta fülön állíthatjuk be a szolgáltatást. Alapesetben ez a funkció nincs engedélyezve, de kötetenként beállítható a használata.



5. ábra: Kvótakezelés

Megadható az új felhasználókra vonatkozó kvóta, illetve a Kvótabejegyzések... gombra kattintva akár felhasználónként beállíthatóak a korlátozások. Ha használat közben engedélyezzük a funkciót, akkor ott már lehetnek állományok, így a rendszer ebben az esetben összegzi a felhasználók tulajdonában lévő fájlok méretét, ez is látható lesz a listában.

3.2.5. Mappák, állományok titkosítása

A titkosított fájlrendszer (Encrypting File System – EFS) egy olyan Windows-szolgáltatás, amely lehetővé teszi, hogy a merevlemezünkön titkosított formában tároljuk az adatinkat.

A titkosítási művelet elvégzése nagyon egyszerű: a fájl vagy mappa tulajdonságainak lapján kattintsunk a Speciális... gombra, majd a speciális attribútumok között jelöljük be a jelölőnégyzetet a Tartalom titkosítása az adatvédelem érdekében opció előtt. Ha egy fájlt szeretnénk titkosítani, akkor az operációs rendszer feltesz egy kérdést, hogy csak a fájlt, vagy az egész mappát szeretnénk-e titkosítani, amiben az állomány is található? Így kiválaszthatjuk, hogy titkosítsa a szülőmappát is, vagy csak az állomány titkosítása történjen meg.

Amennyiben egy mappát titkosítottunk, akkor minden a mappában létrejövő (vagy oda másolt, áthelyezett) fájl is automatikusan titkosítva lesz. Ha kipipáljuk a Mindig csak a fájl titkosítása opciót, akkor erre nem kérdez rá többet az operációs rendszer.

A titkosítás után az állományunkat ugyanúgy használhatjuk mint eddig, nem veszünk észre változást (kivéve, hogy a fájlkezelőben zöld betűkkel jelenik meg a neve), mert a Windows automatikusan elvégzi a visszafejtést és az esetleges titkosítást, ha megváltoztattuk a fájl tartalmát. Más felhasználók azonban nem fognak hozzáférni, illetve mi magunk sem, ha újrategybeépítjük a rendszerünket, vagy esetleg a fizikai lemezt egy másik számítógépbe helyezük át. De van megoldás ezekre az esetekre is, ha előre felkészülünk rájuk!

A mappák, állományok tulajdonság lapjára visszatérve, a speciális attribútumok között most már lesz egy Részletek gomb, amelyre rákattintva bővebben is szabályozhatjuk a titkosítást. Meghatározhatjuk, hogy ki férhet hozzá a fájlokhoz, illetve Kulcsok biztonsági másolata... gombra kattintva egy varázsló segítségével exportálhatjuk a tanúsítványt, amely szükséges a titkosított adatok visszafejtéséhez. Ezt a kiexportált kulcsot kell biztonságos helyre elhelyezni, és akkor bárhol, bármikor vissza tudjuk kapni eredeti formájában az adatainkat. Ha fel szeretnénk oldani egy fájl titkosítását, akkor egyszerűen csak töröljük a jelet a jelölőnégyzetből a fájl tulajdonságainak lapján.

A fájlrendszer titkosítása funkció nem teljesen támogatott a Windows 7 Starter, Windows 7 Home Basic és a Windows 7 Home Premium kiadásban.

3.1.6. BitLocker meghajtótitkosítás

Az előző alfejezetben megismert titkosított fájlrendszerrel ellentétben, amellyel egyes fájlok titkosíthatóak, a BitLocker szolgáltatás a teljes meghajtót titkosítja. Továbbra is ugyanúgy jelentkezhetünk be a rendszerbe, és úgy dolgozhatunk a fájljainkkal, mint eddig, de a BitLocker szolgáltatás képes megakadályozni, hogy támadók férjenek hozzá a rendszerfájlokhoz, vagy a számítógépből eltávolított merevlemezhez úgy, hogy azt egy másik számítógépbe helyezik át. A szolgáltatást kiszolgáló esetén külön kell hozzáadni a Kiszolgálókezelőben, alapértelmezetten nem lesz engedélyezve.

A BitLocker meghajtótitkosítás biztosítja minden, a Windows rendszert tartalmazó meghajtón (vagyis a rendszer-meghajtón) és a beépített adattároló meghajtókon tárolt fájl védelmét. A BitLocker To Go szolgáltatás segítségével a cserélhető adattároló meghajtókon (például külső merevlemezeken vagy USB flash meghajtókon) tárolt fájlok védhetőek.

Amennyiben új fájlokat helyezünk el egy, a BitLocker segítségével titkosított meghajtón, akkor a szolgáltatás automatikusan titkosítja az új fájlokat is. Egyéb tulajdonságok:

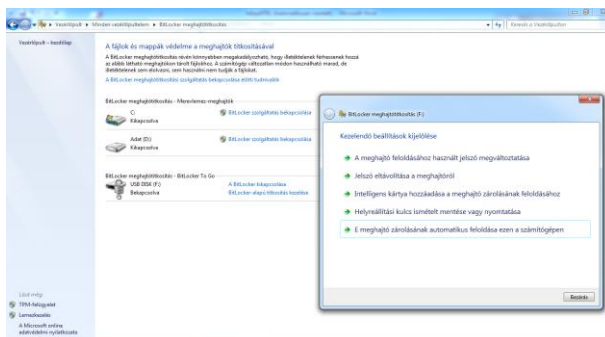
- A fájlok csak addig maradnak titkosítva, amíg a titkosított meghajtón tárolódnak.
- A fájlok másik meghajtóra vagy számítógépre történő másolása esetén a titkosítatlan fájlok kerülnek használatra.
- Amennyiben más felhasználókkal osztunk meg fájlokat, például a hálózaton keresztül, akkor ezek az állományok a titkosított meghajtón titkosított állapotban maradnak, de jogosult felhasználók szokásos módon hozzáférhetnek.

A rendszer-meghajtó titkosítása esetén a BitLocker szolgáltatás ellenőrzi a számítógép elindításakor, hogy fennáll-e bármilyen, biztonsági kockázatot képviselő állapot (ilyen lehet például valamely indítófájl megváltozása vagy a BIOS módosulása). Amennyiben a szolgáltatás biztonsági kockázatot észlel, zárolja a rendszer-meghajtót, és a speciális BitLocker helyreállítási kulcsot kéri a zárolás feloldásához. Feltétlenül hozzuk létre ezt a helyreállítási kulcsot a szolgáltatás bekapcsolásakor, ellenkező esetben a hozzáférés lehetőségének megszűnésével véglegesen elveszíthetjük a fájlokat.

3.2.7. BitLocker szolgáltatás használata

A szolgáltatás igénybevételéhez a Vezérlőpulton belül található BitLocker meghajtótitkosítás alkalmazást indítsuk el, amelyben láthatjuk az egyes partícióinkat, illetve azok állapotát a titkosításra vonatkozóan. A szolgáltatás elindításához kattintsunk a titkosítandó meghajtó melletti BitLocker szolgáltatás bekapcsolása linkre, ennek hatására elindul egy varázsló, amely segít a művelet elvégzésében. Meg kell adnunk a zárolás feloldásának módját, ez a beépített és a cserélhető adattároló meghajtók titkosítása esetén lehet jelszóval vagy intelligens kártyával, illetve beállítható, hogy automatikusan feloldódjon a zárolás a számítógépre való bejelentkezéskor. Utóbbi opció csak abban az esetben választható, ha a rendszer-meghajtó titkosítása is védett a BitLocker szolgáltatással.

A következő ablakban a helyreállítási kulcsot menthetjük el megfelelő helyre, majd utolsó lépésként elkezdhetjük a titkosítást, ez a meghajtó méretétől függően több percig is eltarthat, de a folyamat végeztével titkosítottak lesznek adatink, állományaink. Ezt a BitLocker kezelőfelületén láthatjuk is:

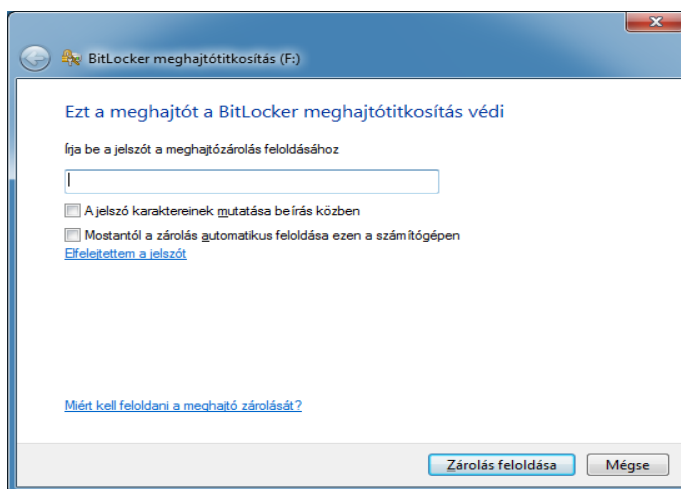


6. ábra: BitLocker szolgáltatás használata

Bármikor kikapcsolhatjuk a BitLocker szolgáltatást, ebben az esetben az operációs rendszer visszafejti a meghajtót, titkosítatlan állapotba kerülnek állományaink.

A meghajtó melletti BitLocker-alapú titkosítás kezelése linkre kattintva a zárolás feloldására vonatkozóan végezhetünk beállításokat, megváltoztathatjuk a jelszót, vagy akár a zárolás módszerét is.

Végül nézzük a szolgáltatás működését: hogyan tudjuk a BitLocker szolgáltatással titkosított meghajtót használni? Nézzük egy példát! Ebben az esetben egy pendrive-on tárolt állományokat szeretnénk megnézni.



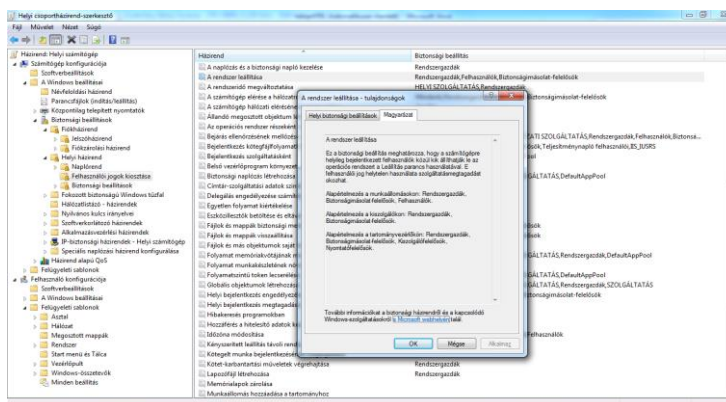
7. ábra: BitLocker jelszó megadása

3.2.8. Biztonsági házirend

A Microsoft operációs rendszereinek egyik fontos védelmi és szabályozó összetevője a házirend funkció (angolul policy-ként említik), amelyről a legtöbb felhasználó nem is tud, mert nincs rá különösebben szüksége. A házirend határozza meg az operációs rendszer működésének szabályait, számos beállítási lehetőséggel, amelyek egyrészt meghatározzák bizonyos műveletek végrehajtási feltételeit, másrészt itt lehet megadni, hogy a rendszerszintű műveleteket melyik felhasználó, vagy felhasználói csoport tagjai végezhetik el.

A házirend nagyon részletes beállítási lehetőségeket biztosít, többféle kategóriában szabályozza az operációs rendszer működését, biztonsági beállításait. Egyrészt szabályozható a számítógép konfigurációja, biztonsági beállításai, illetve megadhatóak a felhasználókra vonatkozó korlátozások.

A házirend eléréséhez a gpedit.msc parancsot adjuk ki parancssorból, ennek hatására fog elindulni a grafikus felületű házirend kezelő program. A bal oldali keretben egy faszervezeten keresztül érhetőek el az egyes ágak, a jobb oldalon találhatóak a házirend bejegyzések, melyekre kattintva kapjuk meg azt a párbeszéd ablakot, ahol a tulajdonságok értékeit meg tudjuk változtatni, illetve egy bővebb magyarázatot olvashatunk a házirendről.



8. ábra: Házirend bejegyzések tulajdonságlapja

Mivel nagyon fontos rendszerezeszközzel van szó, csak rendszergazdai jogosultsággal lehet a házirendeket szerkeszteni.

Hálózati környezetben ki lehet terjeszteni a házirend hatókörét, vagyis egy kiszolgálón használt házirendet az ügyfél gépeken is kötelezővé tehetünk, így biztosítva egységes tulajdonságokat, beállításokat a teljes gépparkra.

3.2.9. Biztonsági mentés funkció

Adatainkkal kapcsolatban nagyon fontos szempont, hogy védve legyünk azok sérülése ellen. Az adatvesztések, sérülések keletkezhetnek hardver hiba okán, esetleg valamilyen szándékos, vagy véletlen adatmanipuláló művelet eredményeként. Amennyiben ilyen esemény történik, akkor a biztonsági mentésekből tudunk hozzájutni az eredeti adatokhoz, vagy legalábbis azok nagy részéhez. Az operációs rendszerek már önmagukban képesek megvalósítani ezt a funkciót, és hatékony eszközt adnak a kezünkbe adataink biztonsági mentésére és visszaállítására.

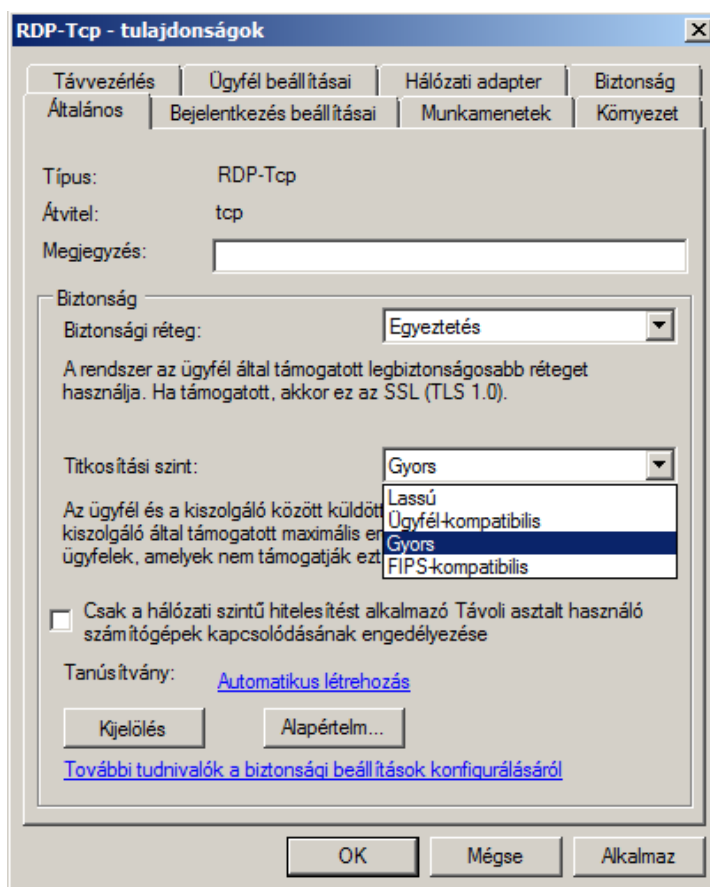
A Vezérlőpulton belül a Rendszer és biztonság lap Biztonsági mentés és visszaállítás parancsára kattintva tudjuk elindítani a funkciót. Ha korábban nem használtuk a Windows biztonságimásolat-készítő eszközét, akkor kattintsunk a Biztonsági mentés beállítása lehetőségre, majd kövessük a varázsló lépéseit. Előfordulhat, hogy a rendszer rendszergazdai jelszót vagy megerősítést kér, ekkor írjuk be a jelszót. Meg kell adnunk a folyamat során a biztonsági másolat helyét (célszerű nem azt a meghajtót, ahonnan mentünk), aztán azokat az állományokat, amelyeket szeretnénk menteni. Itt rábízhatnánk magunkat akár az operációs rendszerre is, de adjuk meg inkább mi a fájlokat. Ezután már csak az ütemezést kell beállítanunk, hiszen a Windows alapértelmezésben hetente automatikusan elvégzi a mentési folyamatot, vagyis újabb másolatot készít a kijelölt állományokról. Természetesen az ütemezés konfigurálható: megadható kisebb, vagy nagyobb időtartam is.

A Varázsló a folyamat végén el is készíti az első mentést, így adataink biztonságban lesznek.

3.2.10. Távoli asztali hozzáférés

A Microsoft operációs rendszereiben nagyon hasznos szolgáltatás a Távoli asztal hozzáférés biztosítása. Ennek keretében egy kliensprogram segítségével úgy tudunk csatlakozni a kiszolgálóhoz, hogy át tudjuk venni a vezérlést a távoli gép felett, alkalmazásokat telepíthetünk, futtathatunk, hozzáférhetünk az erőforrásokhoz, mintha csak az adott számítógép előtt ülnénk.

Természetesen nagyon fontos, hogy a szolgáltatás biztonságos körülmények között menjen végbe, ezt biztosítja a szolgáltatáshoz használt RDP (Remote Desktop Protocol), amelynél szabályozhatóak a biztonsági beállítások.



9. ábra: Távoli asztali kapcsolat biztonsága

Választhatunk szerver hitelesítési megoldást, RDP, SSL (TLS) vagy éppen Egyeztetés-t. Az utóbbi az alapértelmezés, amelynek a lényege, hogy mindkét oldal a TLS-t használja majd. Egyéb esetben attól függ a kapcsolódás létrejötte, hogy a kliensben a titkosítási szint miként kerül beállításra.

3.3. ÖSSZEFOGLALÁS, KÉRDÉSEK

3.3.1. Összefoglalás

Ez a fejezet az operációs rendszerek által nyújtott biztonsági szolgáltatásokba engedett betekintést, amelynek során a hallgatók megismertkedtek a fájl- és meghajtótíkosítási megoldásokkal. Megnézték ezeknek a funkcióknak a használatát, beállítási lehetőségeit, így képesek lesznek megvédeni a rájuk bízott állományokat.

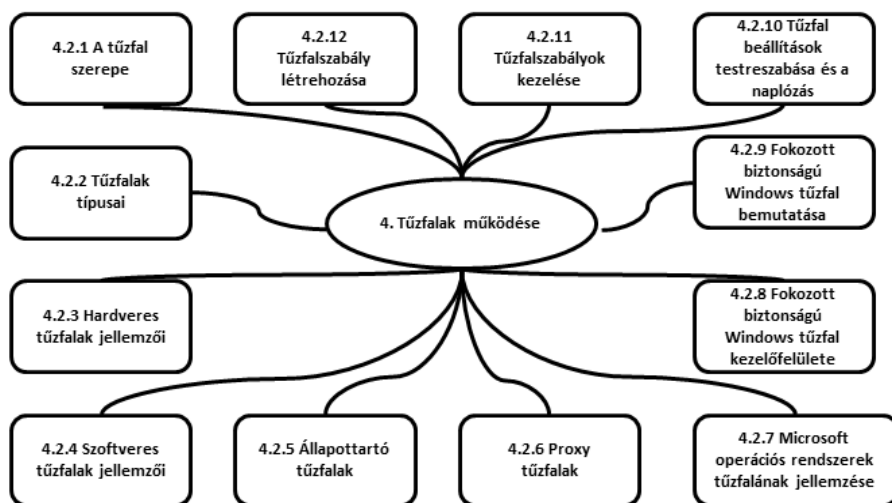
A hallgatók a Microsoft operációs rendszerek egyik különleges szolgáltatásával, a házirenddel is megismerkedtek, amely segítségével az operációs rendszer működése hatékonyan szabályozható. Bemutattuk a tárhelykorlátozási lehetőséget, illetve a távoli asztal kapcsolat biztonsági beállításait.

4 TŰZFALAK MŰKÖDÉSE

4.1. CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

A fejezet célja, hogy bemutassa a hálózati védelem egyik legfontosabb összetevőjét, a tűzfal szolgáltatást. A hallgatók megismerik a szolgáltatás jelentőségét, főbb típusait, működésének tulajdonságait. Fontos, hogy ezeket a tulajdonságokat pontosan megismerjék a hallgatók, mert a további alfejezetekben bemutatásra kerülnek a Microsoft tűzfalprogramjának beállítási lehetőségei, így képesek lesznek akár önállóan is létrehozni olyan tűzfalszabályokat, amelyekkel hatékonyan tudják védeni a rájuk bízott hálózatok, rendszerek biztonságát.

4.2. TANANYAG



4.2.1. A tűzfal szerepe

A hálózati támadások elleni védelem egyik legfontosabb és leghatékonyabb eszköze a tűzfal (elterjedt angol elnevezése: firewall). De pontosan mit is jelent ez a fogalom az informatikában?

 **Tűzfal alatt olyan biztonsági rendszert értünk, amely a számítógépes hálózatok kapcsolódási pontján helyezkedik el,**

és minden átmenő (kimenő és bejövő) hálózati forgalom figyelésével, szűrésével nyújt védelmet.

A tűzfal tehát a teljes hálózati forgalmat képes figyelni, akár csomagonként átvizsgálva azt, hogy átengedje-e azokat, vagy veszélyesnek minősítse, és megakadályozza a továbbításukat. Fontos kiemelni, hogy a legtöbb esetben kétirányú tűzfalról beszélhetünk. Sokan azt hiszik, csak a bejövő adatok ellenőrzése történhet meg. Ezzel szemben a kimenő csomagok ellenőrzésére is sor kerülhet, így egyszerűen lehet megakadályozni a belső hálózatunkból induló támadásokat, vagy a nem kívánt hálózati helyek elérését (vállalati környezetben például ilyen módon nagyon egyszerűen megakadályozható a teljes belső hálózatból a közösségi oldalak használata.).

Mi alapján dönti el a tűzfal, hogy egy csomag átjuthat-e rajta, vagy megakadályozza a továbbítását? Ennek meghatározására többféle lehetőség áll rendelkezésre, alapvetően az előre megadott szabályok fogják irányítani a működést, de erről a későbbiekben lesz még szó.

4.2.2. Tűzfalak típusai

A hálózati technológia fejlődése magával hozta a tűzfalak fejlődését is, röviden tekintsük át, hogy milyen típusú megoldásokról beszélhetünk, vagyis milyen tűzfal típusokat különböztethetünk meg.

Első megoldásként adódott, hogy a külső és a belső hálózat határán lévő eszköz, a router lássa el a védelmi feladatokat is, ez mai napig nagyon hatékony megoldás lehet. Ebben az esetben nem egy számítógépen fut a szolgáltatás, hanem egy speciális hardveren, ezért ezt a módszert hívjuk hardveres tűzfal szolgáltatásnak is. Alapvetően ezzel a megoldással a teljes belső hálózatunk védhetjük.

Az egyedi számítógépekre is telepíthető tűzfal alkalmazás, amely szoftveresen fog védeni, de csak azt az egy gépet. Miért van szükség erre, hiszen a router védi az egész hálózatot? Ajánlatos használni ezt a funkciót, hiszen nem tudhatjuk, hogy a hálózatunkon belül található-e már fertőzött, feltört számítógép, esetleg rosszindulatú felhasználó, aki belülről támadna. Ebben az esetben a központi tűzfal nem nyújt védelmet!

Kezdetben a routerek a hálózati forgalom csomagszűrését látták el, vagyis a meghatározott feltételek szerinti csomagokat engedték át. Ez viszont nem felelt meg minden esetben az elvárásoknak, hiszen gondoljunk csak bele, akár webhasználat közben is új és új hálózatokhoz, számítógépekhez akarunk kapcsolódni, nem lehet hatékonyan szabályozni a forgalmat, mindig új szabályokat beállítani. Erre a problémára adtak megoldást az állapottartó tűzfalak, ame-

lyekben már nemcsak legalsó szinten kerülnek ellenőrzésre a csomagok, hanem a kapcsolatok egésze, az azok közti összefüggések alapján van lehetőség az ellenőrzésre.

A továbbiakban részletesebben megnézzük az egyes típusokat.

4.2.3. Hardveres tűzfalak jellemzői

A tűzfal funkciót akár több eszköz kombinációja is biztosíthatja. Léteznek nagyobb teljesítményű, hardver alapú eszközök, ezeket általában nagyobb cégek, szervezetek, intézmények használják belső hálózatuk védelmére.

A hardver alapú tűzfalak leggyakrabban egy routerrel egybeépítve kerülnek forgalomba, nézzük, milyen előnyei és hátrányai vannak ennek a megoldásnak.

Előnyök:

- A router ára mellett a tűzfal funkció már nem okoz jelentős költség-többletet, illetve nincs szükség újabb eszközre.
- A router szokásos beállításai mellett egyszerű a tűzfal funkciót is konfigurálni, ráadásul ugyanazon a felületen, nincs szükség külön képzésre a rendszergazdák számára.
- Egyszerűbb hálózati topológia, egyszerűbb hálózatmenedzsment
- A router naplózási funkciója tartalmazza a tűzfalra vonatkozó bejegyzéseket is.
- Hátrányok:
- Általában korlátozottabb funkcionalitást biztosítanak, csak a nagyobb teljesítményű routerek támogatják a komolyabb tűzfal funkciókat.
- Legtöbb esetben csak csomagszűrés és alkalmazásengedélyezés állítható be.
- Az útválasztó teljesítménye romlik.
- A naplózási funkció lassabb lesz, ez utóbbi két jellemző a teljes hálózati forgalmat lassítja.

4.2.4. Szoftveres tűzfalak jellemzői

Sokkal gyakoribb a szoftveres megoldás, amikor egy program ellenőrzi a hálózati forgalmat. Mivel gyakran a végfelhasználó számítógépére telepítjük ezeket a programokat, ezért personal, vagyis személyes tűzfalnak hívjuk ezeket az alkalmazásokat. Jelenleg már az operációs rendszerek is tartalmazznak ilyen programot, így előfordulhat, hogy nem is kell külön beszereznünk.

Szoftveres tűzfalak előnyei:

- Alacsonyabb ár.
 - Az alkalmazott operációs rendszer részeként funkcionálnak.
 - Léteznek ingyenesen letölthető, telepíthető programok, természetesen kisebb funkcionalitással, mint a nem ingyenesek.
- Könnyen konfigurálhatóak.
- Alapbeállítások mellett is hatékonyan képesek működni.

Hátrányai:

- Központi kezelhetőség hiánya.
- Minden számítógépen külön-külön kell elvégezni a beállításokat.
- Korlátozott teljesítmény, egy számítógép védelmére készültek, így például egy kisebb hálózatot routerként kiszolgáló gépen komoly terhelést és teljesítmény visszaesést okoznak.

4.2.5. Állapottartó tűzfalak

A csomagszűrés tehát például az elektronikus kereskedelem igényeire nem jelentett megoldást. Olyan tűzfalra volt szükség, ami az ismeretlen, nem szabályozott hálózatokkal, számítógépekkel történő kommunikációt is képes volt biztonságosabbá tenni.

Első lépésként szükség volt arra, hogy a tűzfal azonosítani tudja egy kapcsolat kezdetét és végét, valamint a kettő között zajló adatforgalmat. Ha erre már képes, akkor következő lépésben ki tudja szűrni a kapcsolat közben érkező, nem oda illő csomagokat, amik könnyen veszélyesek lehetnek. Ehhez a beérkező csomagokat tárolni kell átmenetileg, amíg a szolgáltatás a döntéshez szükséges adatokat össze nem gyűjti. A csomagok vizsgálata között nincs különbség, csupán az azokból nyert információ feldolgozásában, a kapcsolatot képes vizsgálni a csomagokban található fejlécek adataiból. Ez a módszer alapvetően a kapcsolatorientált protokollok esetén nyújt újabb lehetőségeket és nagyobb védelmet, biztonságot, így az internet protokollra, a TCP-re vonatkozóan is.

A kapcsolatoknak a típusa alapján is engedélyezhető, illetve tiltható egy-egy kommunikációs folyamat, amit szintén egy szabályrendszer felállításával tudunk befolyásolni. Például egyszerűen blokkolható bármilyen FTP kapcsolat.

Bizonyos esetekben elfogadható, ha az egyszerűbb, nem állapotartó tűzfalat alkalmazzuk, bár a mai technológiák nagy része állapotartó elv alapján működik. Milyen előnyei lehetnek egy ilyen tűzfal alkalmazásának?

- Jóval kisebb erőforrásokat igényel.

- Gyorsabb, nincs szükség munkamenetek azonosítására, csak csomag-szűrésre.
- A nem kapcsolatorientált protokollok esetén jól használható.

4.2.6. Proxy tűzfalak

A nem csomagszűrő típusú tűzfalak fejlődésében a proxy tűzfalak jelentik az első jelentős lépést. A proxy megoldások azzal a céllal készültek, hogy kiküszöböljék a felhasználók kiszolgálókra való bejelentkezésből adódó kényelmetlenségeket, illetve az ebből fakadó veszélyeket.

„A proxy tűzfalak működési elve nagyon egyszerű. A kliensek és a kiszolgálók között nem épül fel közvetlen kapcsolat, hanem mindketten a tűzfalon futó proxy alkalmazással kommunikálnak. A proxy egyik hálózati csatolójával az ismeretlen hálózat kiszolgálóihoz kapcsolódik, a másikkal pedig a belső hálózatban található kliensekhez. A kapcsolat kettősségéből kifolyólag a proxy tűzfalak minden különösebb beállítás nélkül képesek kivédeni a csomagszintű támadásokat.

Bár a proxy-k kifejlesztésében elsősorban használhatósági szempontok jelentették a fő motívumot, a kialakult új architektúra képessé tette a tűzfalakat arra is, hogy alkalmazásszinten ellenőrizzék a rajtuk áthaladó információáramot. A proxy alkalmazások már nem csupán a csomagok fejlécét vizsgálták, hanem azok adatairészebe is belenéztek, és akár módosításokat is végrehajtottak. Már most le kell azonban szögezni, hogy a cél alapvetően nem a mély protokollelemzés volt, így bár architektúráisan megoldható lett volna, a proxy tűzfalak első generációja nem értelmezte a protokollok összes utasítását, csupán azok elenyésző részét.”²

4.2.7. Microsoft operációs rendszerek tűzfalának jellemzése

A Microsoft operációs rendszerei tartalmaznak beépített tűzfal szolgáltatást, mely alapértelmezetten bekapcsolt állapotban lesz telepítés után, figyel a biztonságunkra. Mire képes ez a tűzfal szolgáltatás?

- Állapottartó csomagszűrő tűzfalként védi számítógépünket.
- Segíti megelőzni a számítógépes vírusok és férgek terjedését, megakadályozza, hogy elérjék a védett operációs rendszert.

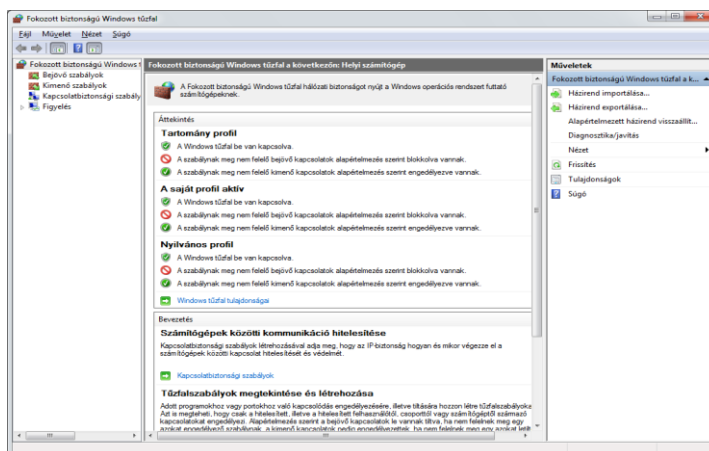
² ILLÉS Márton – BÁNFI Tamás: *Tűzfalak evolúciója*. Budapest, BalaBit White Papers, 2003. 7. o.

- Lehetőséget ad a felhasználónak, hogy engedélyezzen vagy tiltsa kapcsolatokat, erre annak létrejötte előtt rákérdez.
- Naplózást képes végezni, amelyben a sikeres és sikertelen kapcsolódási kísérletek kerülnek rögzítésre, így hasznos eszközt kapunk a hibaelhárításhoz, megelőzéshez, elemzéshez.
- Fontos tudni, hogy mire nem képes a program:
- Ha a számítógép már megfertőződött, akkor az ott található vírust vagy férget nem képes kiirtani, legfeljebb a további terjedést megakadályozni.
- Nem tudja megakadályozni a felhasználót, hogyha e-mail csatolmányként akar vírusos állományt megnyitni.
- Spamnek, kéretlen levelek szűrésére.

A Fokozott biztonságú Windows tűzfal kezelését segítő program a Felügyeleti eszközök között található meg. Indítsuk el, és nézzük meg részletesebben a működését.

4.2.8. Fokozott biztonságú Windows tűzfal kezelőfelülete

A tűzfal program kezelése egy MMC (Microsoft Management Console) felületen keresztül végezhető el, mint szinte minden rendszerszintű szolgáltatás konfigurálása. A kezelőprogram elindítása után az alábbihoz hasonló képernyőt látunk:



10. ábra: Fokozott biztonságú Windows tűzfal

Az operációs rendszerben a hálózati kapcsolatunk besorolható három kategóriába, ennek jelentősége itt jön elő, hiszen a tűzfal szabályait erre a három kategóriára, profilra lehet finomhangolni. Röviden tisztázzuk, mit is jelent ez a három profil:

„Tartomány: Alkalmazása akkor indokolt a hálózati adapterre, amikor az olyan hálózatra kapcsolódik, amelyen érzékeli azon tartomány tartományvezérlőjét, amelyhez a számítógép csatlakozik.

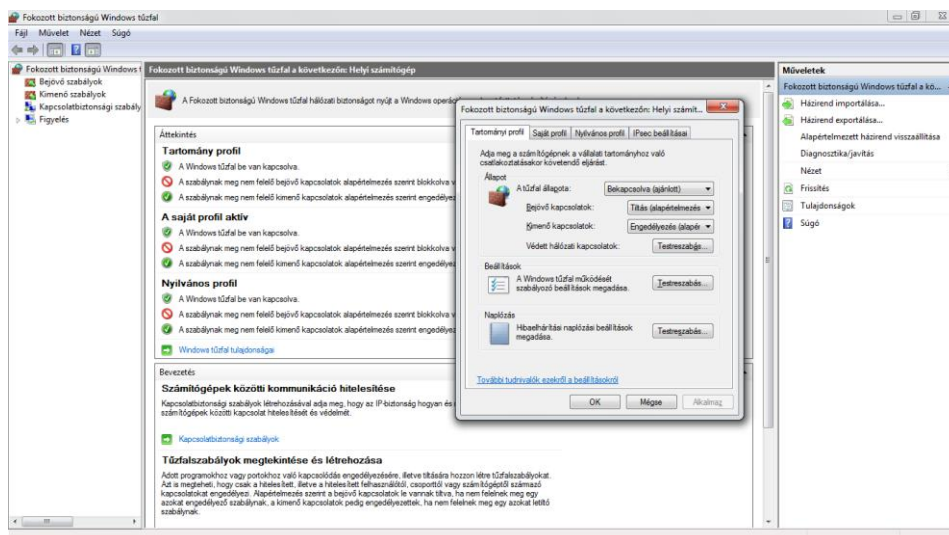
Személyes (saját): Alkalmazása akkor indokolt a hálózati adapterre, amikor az olyan hálózathoz kapcsolódik, amelyet a rendszergazda magánhálózatként azonosít. A magánhálózat olyan hálózat, amely nem kapcsolódik közvetlenül az internetre, hanem valamilyen biztonsági eszköz, például hálózati címfordító útválasztó vagy hardveres tűzfal mögött van. A személyes profil beállításainak szigorúbbnak kell lenniük, mint a tartományi profil beállításainak.

Nyilvános: Alkalmazása a hálózati adapterre akkor indokolt, ha nyilvános hálózathoz kapcsolódik, például a repülőtereken és kávézókban elérhető hálózatokon. A nyilvános hálózat olyan hálózat, ahol semmilyen biztonsági eszköz nincs a felhasználó és az internet között. A nyilvános profilbeállításoknak kell a legszigorúbbnak lenniük, mert a számítógép nyilvános hálózathoz kapcsolódik, ahol a biztonság nem ellenőrizhető.”³

4.2.9. Fokozott biztonságú Windows tűzfal bemutatása

Az áttekintő ablakban láthatjuk a legfontosabb tulajdonságokat, ha ezeken szeretnénk változtatni, vagy bővebben megnézni, akkor kattintsunk a Tulajdonságok műveletre, amelynek hatására egy párbeszédablakban elvégezhetőek a főbb beállítások. Profilonként ki- vagy bekapcsolhatjuk a tűzfal funkciót, meghatározhatjuk a kapcsolatokra vonatkozó szabályok működési szintjét, megadhatjuk a naplózási opciókat.

³ Windows 7 Help



11. ábra: Tűzfal tulajdonságlapja

Ahogy a képen is látható, minden profilhoz külön fül tartozik, amelyeken aztán ugyanazokat a beállításokat tudjuk elvégezni. A tűzfal állapota lehet Bekapcsolva, illetve Kikapcsolva, vagyis engedélyezhetjük a szolgáltatást, vagy letilthatjuk az adott profilra. A Bejövő kapcsolatok értékei a következők lehetnek, és a jelentésük:

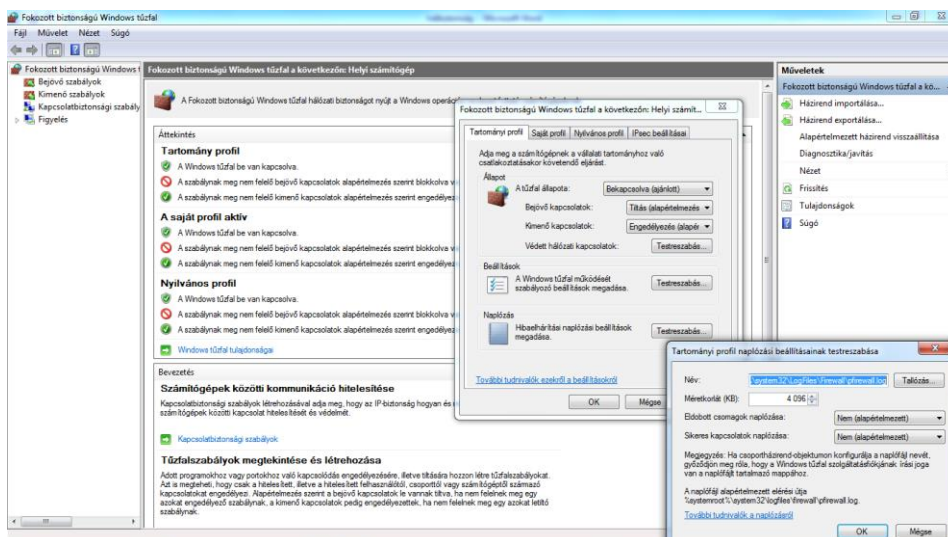
- **Tiltás:** Minden kapcsolat letiltása abban az esetben, ha nincs olyan tűzfalszabály, amely engedélyezi a kapcsolatot.
- **Minden kapcsolat letiltása:** Minden kapcsolat letiltása, még akkor is, ha létezik szabály, amely engedélyezné.
- **Engedélyezés:** A kapcsolat engedélyezése abban az esetben, ha nincs olyan tűzfalszabály, amely tiltja a kapcsolatot.
- **A Kimenő kapcsolatok értékei a következők lehetnek, és a jelentésük:**
- **Tiltás:** Minden kapcsolat letiltása, ha nincs olyan tűzfalszabály, amely engedélyezi a kapcsolatot.
- **Engedélyezés:** A kapcsolat engedélyezése, ha nincs olyan tűzfalszabály, amely tiltja a kapcsolatot.

A Védett hálózati kapcsolatok beállításával meghatározhatjuk, hogy a profil konfigurációjának hatálya alá mely hálózati adapterek tartoznak.

4.2.10. Tűzfal beállítások testreszabása és a naplózás

A Beállítások blokkon belül konfigurálhatjuk az értesítéseket (küldjön-e az operációs rendszer üzenetet, ha letilt kapcsolatot), a csoportos küldésre vagy szórásos forgalomra adott egyedi küldéses válaszokat, valamint a csoportházi-rend szabályegyesítésének állapotát tudjuk megnézni, mert ez utóbbi a Csoportházi-renden belül szerkeszthető.

A Naplózás testreszabása is elvégezhető, nézzük, milyen opciókat állíthatunk be:



12. ábra: Tűzfal naplózási beállítások

Megadható a naplózási fájl neve, elérési útvonala, ha bele akarunk nézni, akkor ezt az állományt kell keresnünk a fájlrendszerünkben. Ez egyébként egy egyszerű szöveges állomány, bármilyen szövegszerkesztővel megtekinthető a tartalma.

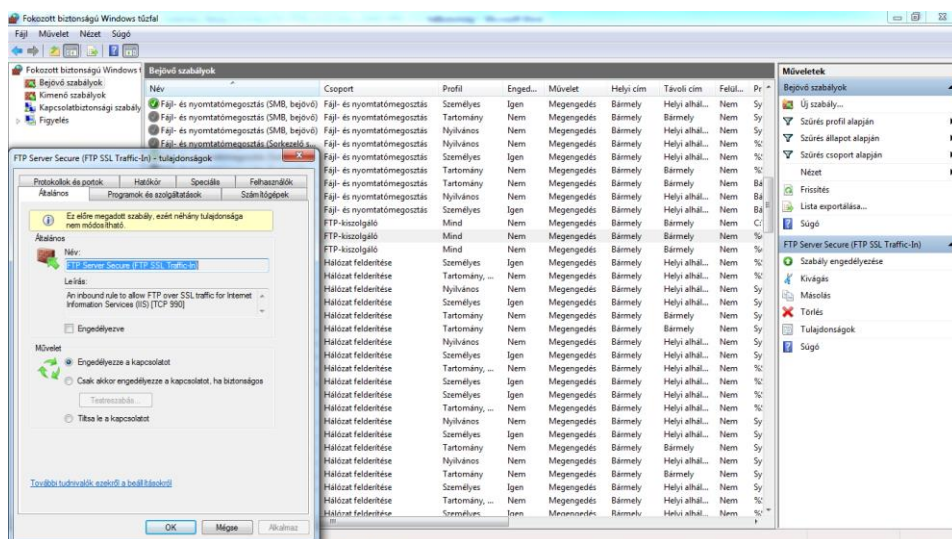
A méretkorlát a naplózási fájl maximális méretét határozza meg, ez fontos lehet egy nagyobb forgalmat bonyolító gép esetén, hiszen a naplófájl növekedése akár tárhely problémákat is okozhat. Természetesen a korlát elérésekor továbbra is rögzíti az adatokat a rendszer, csak az időben legkorábbiakat elkezd törölni.

A következő két opcióval adható meg, hogy a naplózás során milyen adatok kerüljenek be a naplófájlba, külön az eldobott csomagok, illetve a sikeres kapcsolatok szabályozhatóak. Alapértelmezésben mindkettő kikapcsolt állapot-

ban lesz, vagyis nem rögzít adatot a szolgáltatás, ha használni szeretnénk ezt a funkciót, akkor itt be kell állítanunk az engedélyezést.

4.2.11. Tűzfalszabályok kezelése

A tűzfalszabályok fogják alapvetően meghatározni a tűzfal működését, a csomagok átjutását, a kapcsolatok létrejöttét. Szabályok kezelésére a Bejövő szabályok, vagy a Kimenő szabályok ágon belül van lehetőség.



13. ábra: Tűzfalszabályok kezelése

A listában soronként látjuk a szabályokat, illetve azok legfontosabb tulajdonságait. Meglévő szabály szerkesztéséhez kattintsunk duplán a szabályra, vagy kijelölés után a jobb oldali keretben a Tulajdonságok-ra. Ahogy az ábrán is látható, egy párbeszédablakban állíthatóak be a szabályhoz tartozó tulajdonságok. Ezt most nem néznénk meg, hanem egy új szabályt definiálunk, azon keresztül mutatjuk be az opciókat:

A jobb oldali keretben az Új szabály... műveletre kattintva egy varázsló segíti a beállítási folyamatot, melynek során megadhatjuk a megfelelő opciókat. Érdekes megemlíteni, hogy a varázsló gyakorlatilag ugyanazokat az opciókat veszi végig a bejövő és a kimenő szabályok esetén, ezért elég csak az egyiket végignéznünk, a másik teljesen hasonló, csak éppen az ellenőrzés iránya lesz más.

Készítsünk egy olyan szabályt, amely megakadályozza egy adott hálózathoz, hogy elérjék a számítógépünkön működő webszerverünket.

4.2.12. Tűzfalszabály létrehozása

A Bejövő szabályokon belül a varázsló elindítása után első lépésben meg kell adnunk a szabály típusát: válasszuk az Egyénit, ezen keresztül az összes tulajdonságot látni fogjuk. A következő ablakban beállítható az a program, amelyre vonatkozik a szabály. Mi most nem konkrét programra állítjuk be a szabályt, hagyjuk az alapértelmezett Minden program opciót. Tovább lépve adhatjuk meg a szabályozandó protokollok és portok értékeit.

Új bejövő szabály varázsló

Protokoll és portok

Adja meg azokat a protokollokat és portokat, amelyekre a szabály vonatkozik.

Lépések:

- Szabály típusa
- Program
- Protokoll és portok
- Hatókör
- Művelet
- Profil
- Név

Mely portokra és protokollokra vonatkozik a szabály?

Protokoll típus: TCP

Protokollszám: 6

Helyi port: Adott portok

80

Példa: 80, 443, 5000-5010

Távoli port: Minden port

Példa: 80, 443, 5000-5010

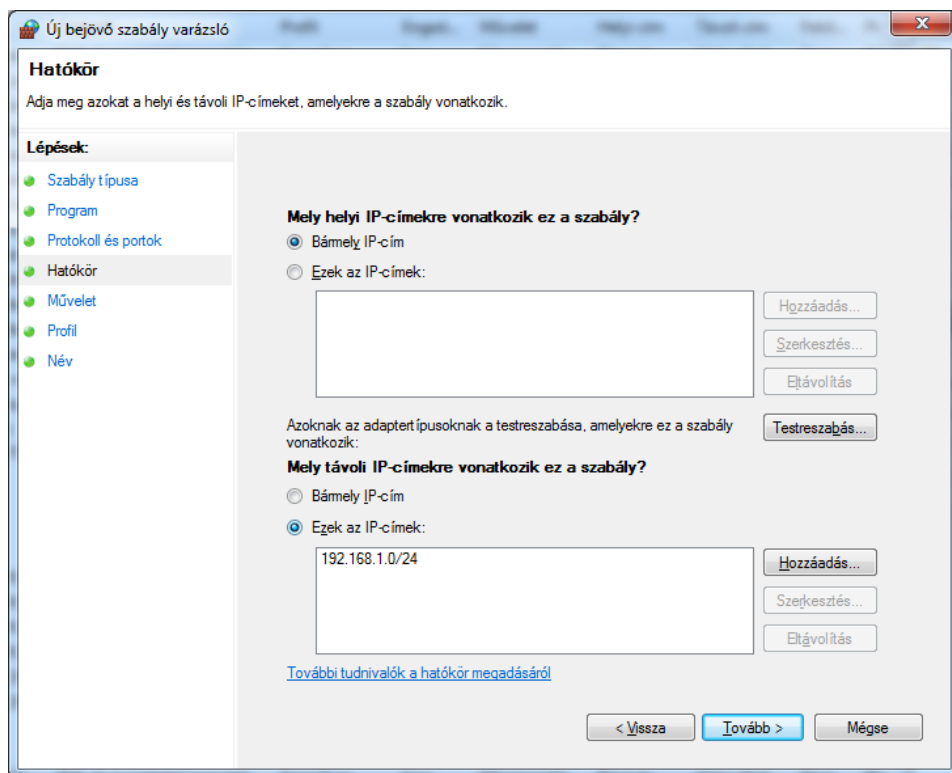
ICMP-beállítások: Testreszabás...

[További tudnivalók a protokollokról és a portokról](#)

< Vissza Tovább > Mégse

14. ábra: Protokoll és portok szabályozása

Válasszuk ki a TCP protokollt a legördülő menüből, a Helyi portoknál pedig az Adott portok elemet, majd írjuk be a 80 értéket, mert ezt használja a webszerverünk. A következő ablakban megadhatjuk a hatókört:



15. ábra: Hatókör beállítása

Nekünk most a távoli címekre kell feltételt megadni, ezt a Hozzáadás... gombra kattintva megtehetjük. Következő lépésben a műveletet kell megadni, válasszuk a Tiltsa le a kapcsolatot értéket. Továbbá beállíthatjuk, hogy melyik profilhoz rendeljük a szabályt, majd utolsó lépésként egy nevet adhatunk a most létrehozott szabálynak és menthetjük azt.

Talán nem tűnt bonyolultnak a folyamat, nem is az. Természetesen egy nagyobb rendszer esetén át kell gondolni pontosan, hogy hogyan is alakuljanak a korlátozások, engedélyek; illetve sokat segítenek az operációs rendszerben előre definiált szabályok.

4.3. ÖSSZEFOGLALÁS, KÉRDÉSEK

4.3.1. Összefoglalás

A fejezet bemutatta a hálózati védelem egyik legfontosabb összetevőjét, a tűzfal szolgáltatást.

Megismertettük a szolgáltatás jelentőségét, különböző típusait, működésének tulajdonságait. Bemutatásra kerültek a Microsoft tűzfalprogramjának beállítási lehetőségei, a kezelőfelület sajátosságai, a működés alapvető tulajdonságai. A jobb megértés érdekében példán keresztül megtörtént tűzfalszabályok létrehozása, kezelése.

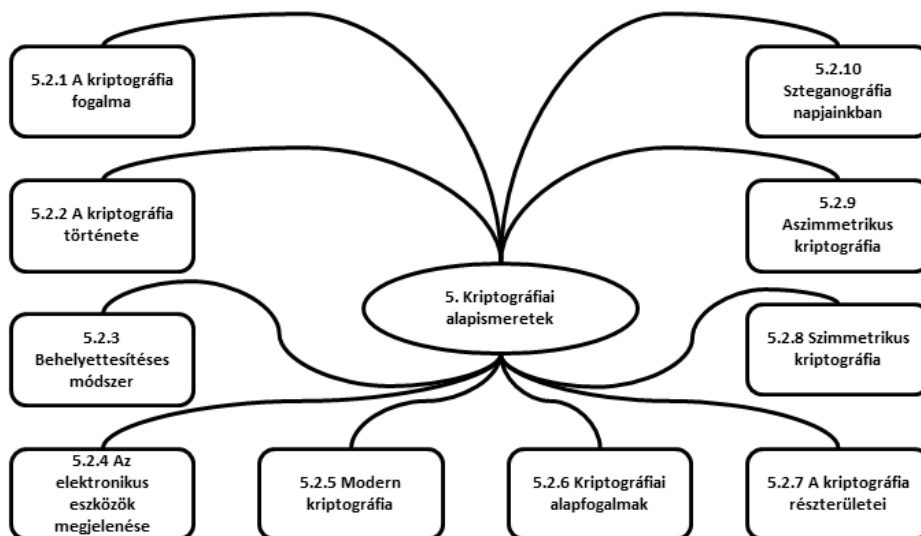
5 KRIPTOGRÁFIAI ALAPISMERETEK

5.1. CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

A számítógépes hálózatokon zajló kommunikáció biztonságáért különböző eljárások, algoritmusok felelnek, amelyeket a megfelelő alkalmazások használatával tudunk igénybe venni. Ezeknek az eljárásoknak a megismertetése a cél ebben a fejezetben.

Bemutatásra kerül a kriptográfia, a tudományág rövid története, definiáljuk az alapfogalmakat, illetve a két, legelterjedtebb módszert, amelyet a jelenlegi megoldások is használnak, a szimmetrikus és az aszimmetrikus kriptográfiai módszert.

5.2. TANANYAG



5.2.1. A kriptográfia fogalma

? Mielőtt belekezdenénk, gondolja át, Ön mit ért kriptográfia alatt?

📖 A kriptográfia ma már tudományágnak tekintendő, amelynek a rejtjelezett, titkosított kommunikáció a szakterülete.

A kriptográfia tehát a rejtjelezésnél tágabb fogalom, minden olyan elmélet, technikát magában foglal, amely a kódolás, titkosítás módszereit felhasználva védelmet nyújt adatainknak, biztonságos kommunikációt garantál. Amivel több a rejtjelezésnél, azok a kódolás melletti tényezők, így például a digitális aláírás, vagy a felhasználó-azonosításra szolgáló protokollok.

A kriptográfia mellett fontos megemlíteni a vele „párban járó” kriptanalízist, amely kódszövegek kulcs ismerete nélküli megfejtésének tudománya⁴, vagyis kriptográfiai eljárások megbízhatóságát, erősségét vizsgáló módszerek összessége, ahol különböző támadásokkal tesztelik a kriptográfiai megoldásokat, hogy meggyőződjenek a védelem mértékéről.

Jelenleg is folyik a kriptográfia módszereinek fejlesztése, hiszen egyre nagyobb szükségünk van arra, hogy adatainkat, üzeneteinket biztonságban tudhassuk. Fontos viszont tisztázni, hogy sajnos sohasem lehetünk teljesen nyugodtak, a technológiai fejlődés, a számítógépek kapacitásának növekedése azzal is jár, hogy a biztonsági megoldások is gyorsabban avulnak el.

5.2.2. A kriptográfia története

A történelem korábbi szakaszában, ismert módon már az ókori civilizációknál, például görögöknél, rómaiaknál fellépett az igény a féltett információ, egy adott üzenet elrejtésére, majd az üzenet cseréjére a megfelelő felek között. Ennek megoldására kezdetben olyan eszközök álltak rendelkezésre, amelyek lényege még nem a titkosítás, hanem az üzenet elrejtése volt.

? Tudna mondani ilyen módszert, eljárást?

Ilyen eljárás volt a viasszal fedett palatábla, vagy a küldönc hajának levágása, majd a fejre írt üzenetet az újra kinőtt haj rejtette el. De szinte mindenki által ismert a pitypang tejével írás is, amely láthatatlanná válik, amíg meg nem melegítjük a papírt.

A szteganográfiával egy időben alakult ki a kriptográfia, aminek a célja már nem magának az üzenetnek, hanem annak a tartalmának, jelentésének elrejtése, titkolása.

Szintén az ókorból ismertek már ilyen módszerek is.

Az egyik ilyen ismert módszer az úgynevezett Caesar-rejtjel, amelyet Julius Caesar írt le egyik művében. Lényege, hogy az ábécé betűit egy bizonyos értékkel eltolta, és így állította elő a titkosított szöveget. Természetesen az üzenet

⁴ Lengyelne Molnár Tünde: *Digitális jogok kezelése*. Eger, Eszterházy Károly Főiskola, 2011. 42. o.

fogadójának tudnia kellett azt az értéket, amellyel betűnként vissza kellett számolnia, és megkapta a helyes betűket, illetve üzenetet.

 Nézzünk egy egyszerű példát, az eltolás értéke négy.

1. Caesar-rejtjel

Betűk megfeleltetése												Kódolás	
Eredeti:	a	b	c	d	e	...	v	w	x	y	z	Üzenet:	magyarok
Kódolva:	E	F	G	H	I	...	Z	A	B	C	D	Kódolva:	QEKEVSO

5.2.3. Behelyettesítéses módszer

A behelyettesítéses módszer egy eljárás, ahol a szöveg minden elemét egy szabályos rendszer alapján átalakítjuk rejtjelezett szöveggé. A rejtjelek lehetnek betűk, betűpárok, számjegyek, vagy ezek valamilyen kombinációja. A behelyettesítéses módszer tehát az elemeket a helyükön hagyja, de megváltoztatja azokat. Ettől eltérő módszer az átrendezés (transzpozíció), amikor az eredeti szöveg elemeit összekeverjük (akár nagyon bonyolult sorrendben), de a szöveg egyes elemei érintetlenül maradnak.

A behelyettesítéses rejtjelezés sokfajta módon használható, megkülönböztetünk három csoportot, amelyeket az idők során használtak:

Monoalfabetikus behelyettesítés: a legegyszerűbb, a betűnek ugyanaz lesz a kódolt változata minden előfordulásánál.

Polialfabetikus behelyettesítés: nehezebben feltörhető, egy betűnek az üzeneten belül akár többféle kódolt változata is lehet.

Poligrafikus behelyettesítés: karaktersorozatokat helyettesítünk másik karaktersorozatokkal.

Ez a sorrend gyakorlatilag történeti is, egyre bonyolultabb módszereket próbáltak létrehozni, viszont a történelem során kiderült, hogy az eljárások aránylag könnyen feltörhetőek, elsősorban az egyes betűk, betűcsoportok ismert szövegbéli gyakoriságát felhasználva.

Bár önmagában a behelyettesítéses módszert ma már nem használjuk, a modern titkosító algoritmusokban is szerepet kapnak.

5.2.4. Az elektronikus eszközök megjelenése

Az előzőleg ismertetett módszereket használták gyakorlatilag a 20. század elejéig, amikor még sem a kódoláshoz, sem annak megfejtéséhez nem nagyon használták gépeket, eszközöket. A technikai fejlődés (és sajnos a háborúk) viszont lehetővé és később szinte kötelezővé tették az elektronikus eszközök, számítógépek használatát.

Az egyik leghíresebb ilyen eszköz az I. világháború végén kifejlesztett Enigma volt, amelyet a német Albert Scherbius alkotott meg, majd folyamatosan fejlesztették, egészen a II. világháborúig, amikor úgymond fénykorát élte.



16. ábra: Az Enigma katonai, háromtárcsás változata⁵

Az Enigma gyorsan és hatékonyan dolgozott, a begépett szöveget különböző tárcsák segítségével kódolta, lámpák felvillanása mutatta a kódszöveget. A németek teljesen megbíztak a feltörhetetlennek tartott gépben, nem számoltak azonban az angol tudósokkal, akik Alan Turing (aki jelentős személye az informatika történetének is) vezetésével feltörték és el tudták olvasni az üzeneteket. Szintén ennek a csapatnak volt köszönhető a világ első, mai értelemben is számítógépnek tekinthető eszközének elkészítése, amely a Colossus nevet kapta,

⁵ http://hu.wikipedia.org/wiki/A_kriptogr%C3%A1fia_t%C3%B6rt%C3%A9nete 2012. május 16.

és kódfeltörésre használták. Sajnos mivel hadi célokra használták, a háború után megsemmisítették, mindent titkosítottak, sokáig semmit sem lehetett erről a gépről tudni, még a létezéséről sem.

- ✿ A modern eszközök mellett érdemes megemlíteni a találékonytságot is. Keressen leírást az egyik leghatékonyabb katonai titkosításról, ami a navahó indiánokhoz kapcsolódik!

5.2.5. Modern kriptográfia

Az elektronikus számítógépek megjelenése egyszerűsítette a titkosítást, hiszen a programok és az algoritmusok képesek gyorsan, automatikusan elvégezni a feladatot, viszont felgyorsította a kódok feltörését is. Az addig használt módszerek nem voltak megfelelőek, újabbakat kellett kitalálni, amelyek az egyre nagyobb számítókapacitással rendelkező számítógépek mellett is képesek biztosítani, hogy az üzenet csak az érintettek számára legyen érthető.

Mivel az üzenetek is számítógépes környezetben születtek, illetve használták azokat, ezért megváltozott a titkosítás módja: nem karakterenként történt, hanem a karakterek számítógépes kódjait vették alapul. Ezek a kódok gyakorlatilag kettes számrendszerbeli számok, így a kódolás bitenként, vagy bitek csoportjaival, blokkonként történik.

Az egyértelmű katonai célok mellett hamarosan megjelent az igény az egyéb szervezetek részéről is, akik szintén kezdtek számítógépes rendszereket, hálózati megoldásokat alkalmazni a mindennapokban, gondoljunk csak a banki, kereskedelmi szektorra. Ebben az esetben is szükséges a biztonságos kommunikáció a felek között.

Az 1970-es évek elejétől kezdődött meg egyfajta szabványosítás, az addigi különböző megoldások helyett. Ennek eredményeként született meg az első jelentős szabvány, a DES (Data Encryption Standard), amely az Amerikai Szabványügyi Hivatal 1973-ban kiírt pályázatán nyert és vált később elfogadott kódolási rendszerré.

Szinte ugyanebben az időszakban készítették el az RSA névre keresztelt titkosítási módszert, amely már más elven működik, mint a DES, és megfelelően használva egyelőre feltörhetetlennek tűnik.

A következő fejezetben bővebben is foglalkozunk a titkosító algoritmusokkal.

5.2.6. Kriptográfiai alapfogalmak

A kriptográfiai eljárások leírásakor számos olyan szakszóval, fogalommal találkozunk, amelyeknek pontos jelentését fontos tudni, éppen ezért most értelmezzünk közülük néhányat, feltüntetve az angol megnevezéseket is:

- Nyílt szöveg (angolul: plaintext): az eredeti, mindenki által értelmezhető információ.
- Titkosított szöveg (ciphertext): a titkosított információ.
- Titkosítás (encryption): egy olyan eljárás, amely során egy információt a birtokosa titkossá minősít, alapvetően adatvédelmi fogalomnak tekinthető. Ebben az értelemben a titkosítás független az alkalmazott technikai megoldástól, gondolhatunk akár az ókori megoldásokra, vagy a számítógépes hálózatoknál használtakra.
- Visszafejtés (decryption): az az eljárás, amelynek során a titkosított információból visszaállítjuk az eredetit.
- Rejtjelezés: valamilyen módszerrel egy nyílt szöveg olyan módú kódolása, hogy annak visszafejtéséhez szükséges információ nélkül a kódolt adatokból az eredeti információt ne, vagy csak nagyon nehezen lehessen kikövetkeztetni.
- Kulcs (key): az az információ, amelynek segítségével történik a rejtjelezés, illetve adott esetben a visszafejtés is. A kulcs hiányában sem a rejtjelezés, sem a visszafejtés nem valósítható meg. A kulcsoknak két típusát különböztetjük meg, így létezik:
 - Nyilvános kulcs (public key): az az információ, amelynek segítségével, a rejtjelezést végezzük.
 - Titkos kulcs (private key): az az információ, amelynek segítségével, adott esetben a visszafejtést tudjuk elvégezni.
- ábécé (alphabet): egy olyan véges elemszámú halmaz, amelynek elemei különböző szimbólumok lehetnek. A nyílt szöveg, illetve a titkos szöveg elemei csak az alkalmazott ábécé szimbólumai közül vehetnek fel értékeket. A rejtjelezésnél alkalmazott ábécé így például lehet a 0 és az 1, az angol ábécé betűinek halmaza, vagy valamelyik karakterkódolási táblázat értékei.

5.2.7. A kriptográfia részterületei

A kriptográfián belül jó pár olyan részterületet különböztethetünk meg (köszönhetően az informatikai megoldásoknak is), amelyek már önmagukban is tudományágnak tekinthetőek. Nézzük meg ezek közül is a legfontosabbakat!

A titkos kulcsú vagy szimmetrikus kriptográfia, amelynek lényege, hogy olyan titkosítási algoritmusok, megoldások leírásával foglalkozzon, ahol a küldő és az üzenetet fogadó fél ugyanazt a kulcsot használja az információ titkosítására, illetve visszafejtésére. Így működik a már említett DES.

A nyilvános kulcsú vagy aszimmetrikus kriptográfia, amelynek lényege, hogy olyan titkosítási algoritmusok, megoldások leírásával foglalkozzon, ahol a küldő az információ titkosítására nem ugyanazt a kulcsot használja, mint az üzenet fogadója a visszafejtésre. Így működik a már említett RSA.

A létező kriptográfiai algoritmusok gyakorlati alkalmazásának módját határozzuk meg a kriptográfiai protokollok segítségével, így például az elektronikus kommunikációt, a digitális aláírást, a biztonságos adattárolást stb.

A kriptográfiai primitíveknek nevezzük azokat az alapvető kriptográfiai algoritmusokat, amelyeken a létező kriptográfiai megoldások biztonsága alapszik. Ilyenek a hash függvények, digitális aláírások, stb.

A kriptográfiai technikák alatt azt értjük, hogy a nyílt szöveg feldolgozásának módját hogyan határozzuk meg, vagyis hogy bitenként vagy bitek sorozataként, blokkonként végezzük a titkosítást. Utóbbi esetben a nyílt szöveget előre meghatározott hosszúságú bitsorozatokra, blokkokra osztjuk, majd ezekkel végezzük el a titkosítási eljárást.

A kriptoanalízis létező kriptográfiai rendszerek gyenge pontjait, a titkosítás feltörését, a titkosított információ nem legális úton való visszafejtését próbálja meg végrehajtani, alapvetően tesztelési, javítási céllal.

A kriptográfia és a kriptoanalízist együttesen hívjuk kriptológiának.

Napjainkban, az elektronikus kommunikáció világában a kriptográfia további problémák megoldására is alkalmas, mint például a kommunikáló felek azonosítása, üzenetek sértetlenségének az ellenőrzése, dokumentumok elektronikus úton való hitelesítése stb.

5.2.8. Szimmetrikus kriptográfia

A szimmetrikus kulcsú titkosítás azon titkosításokat takarja, melynél a kódolás és dekódolás folyamatához szükséges kulcs egyforma⁶.

A cél tehát olyan algoritmusok létrehozása, amelyek esetében a küldő fél a titkos kulcsával kódolja a nyílt szöveget, amelyet aztán a fogadó fél szintén a titkos kulcs segítségével vissza tud fejteni. A módszer lényege a titkos kulcs, hiszen a titkosítást végző algoritmus nyilvános, az esetleges támadó is ismeri

⁶ Lengyelne Molnár Tünde: *Digitális jogok kezelése*. Eger, Eszterházy Károly Főiskola, 2011. 75. o.

azt, így feltöréskor gyakorlatilag „csak” ezt a kulcsot kell kitalálnia, meghatároznia.

A módszer gyengesége is egyben a titkos kulcs, hiszen azt mindkét félnek ismernie kell még az üzenetváltás előtt. Két fél esetében ez még megoldható, hogy akár hagyományos úton eljusson a kulcs a másik félhez. Viszont gondolkunk egy bankra, vagy kereskedelmi cégre, akiknek minden ügyfélhez el kellene juttatni biztonságosan az egyedi kulcsot.

A másik probléma a feltörhetőség. A „brute force” (nyers erő) támadás lényege, hogy az összes lehetséges kulcsot kipróbálják, így nyilvánvalóan a helyes kulcsot is megtalálják, csak éppen észlelni kell, hogy az a helyes kulcs. Természetesen minél hosszabb a kulcs, annál tovább tart a törés. Jelenlegi számítási kapacitások mellett a 128 bites kulcs már biztonságosnak tűnik, annak teljes átvizsgálásához 2^{128} kulcsváltozatot kellene ellenőrizni, ami tovább tartana, mint az univerzum eddigi kora, viszont a DES-nél alkalmazott 56 bites kulcs már gyengének tekinthető!

5.2.9. Aszimmetrikus kriptográfia

Az előző alfejezetben már láttuk, hogy a szimmetrikus kriptográfiai algoritmusok esetén az egyik fő probléma a titkos kulcsok kiosztása, a fogadó felekhez való eljuttatása. Így hiába nagyon erős egyébként a titkosító rendszer, ha elég megszerezni a kulcsot a támadónak. Sokáig viszont ez volt az elfogadott (és egyetlen megvalósíthatónak vélt) módszer.

1976-ban viszont Diffie és Hellmann, két amerikai kutató jelentkezett egy új elmélettel, amelynek lényege, hogy nem ugyanazt a kulcsot kell használni a titkosításhoz, mint a visszafejtéshez. A módszerrel szemben 3 követelményt támasztottak:

- A kódolás és visszafejtés után teljes egészében álljon elő az eredeti üzenet.
- A kódoló és a visszafejtő algoritmus és az azokban használt kulcsok egymástól függetlenek.
- A kódolás feltörhetetlen legyen választott nyílt szöveg típusú támadással.

„A módszer a következőképp működik. Tegyük fel, hogy Aliz titkos üzeneteket szeretne fogadni, ezért először kifejleszt két olyan algoritmust, melyek megfelelnek a fenti követelményeknek. Ezek után a kódoló algoritmust, illetve a titkosító kulcsot nyilvánosságra hozza, innen ered a nyilvános kulcsú titkosítás (public-key cryptography) elnevezés is. Aliz felrakhatja például a nyilvános kul-

csát a webes honlapjára.”⁷ Ezek után bárki, aki titkosított üzenete akar küldeni, egyszerűen a nyilvános kulccsal titkosítja azt, de visszafejteni csak Aliz tudja majd a saját titkos kulcsával.

A módszer előnyös tulajdonságokkal rendelkezik, csak éppen nem volt gyakorlati megvalósítása, ezt az elmélet megalkotóinak nem sikerült létrehozni. Viszont más szakembereknek igen, így ma már több ilyen alapokon nyugvó algoritmus is használható.

5.2.10. Szteganográfia napjainkban

? A fejezet elején volt szó a szteganográfiáról, emlékszik, hogy mit is jelent?

Mára már elavultnak tűnik a módszer, pedig jól lehet használni napjaink technikai megoldásai mellett is. Hogy hogyan? Gondoljunk csak bele, ma már nem csak tisztán szöveges információkat tudunk küldeni a számítógépes hálózatokon, hanem egyéb formátumokat is, így képeket, mozgóképeket. Miért ne lehetne elrejtetni információkat ezekben az állományokban?

Egy átlagosnak tekinthető 1024x768-as felbontású, 24 bites színmélységű képállományban, ha minden színkód (8 bit) legalsó bitjét a titkos adatainknak szánjuk, akkor máris $1024 \cdot 768 \cdot 3$ bit, azaz 294912 bájt áll rendelkezésünkre. Ráadásul ez nem okoz problémát a kép megjelenítésében, a szemünk nem tud különbséget tenni a 21 vagy 24 bites színmélységű képek között.

Természetesen ebben az esetben a fogadónak tudnia kell, hogy mit és hol keressen, de így akár egy családi nyaralásról készült (és manipulált) kép is hordozhat magában titkokat.

A módszer gyakorlati hasznát például a szerzői jogoknál lehet érvényesíteni, akár a weben elhelyezett képállományok is tartalmazhatnak a tulajdonosra utaló adatokat, így illetéktelen felhasználás esetén peres úton lehet bizonyítani a tulajdonjogot.

⁷ TANENBAUM, S. Andrew: *Számítógép-hálózatok*. Budapest, Panem kft., 2004. 804. o.

5.3. ÖSSZEFOGLALÁS, KÉRDÉSEK

5.3.1. Összefoglalás

A fejezet a számítógépes hálózatokon zajló kommunikáció biztonságát is szavatoló kriptográfia mint tudományág általános bemutatását tartalmazza.

Definiáltuk a kriptográfia fogalmát, bemutattuk a tudományág rövid történetét, meghatároztuk az alapfogalmakat, illetve leírtuk a két legelterjedtebb módszert, amelyet a jelenlegi megoldások is használnak: a szimmetrikus és az aszimmetrikus kriptográfiai módszert. Röviden szóltunk a szteganográfiáról, annak jelentőségéről, használatáról napjainkban.

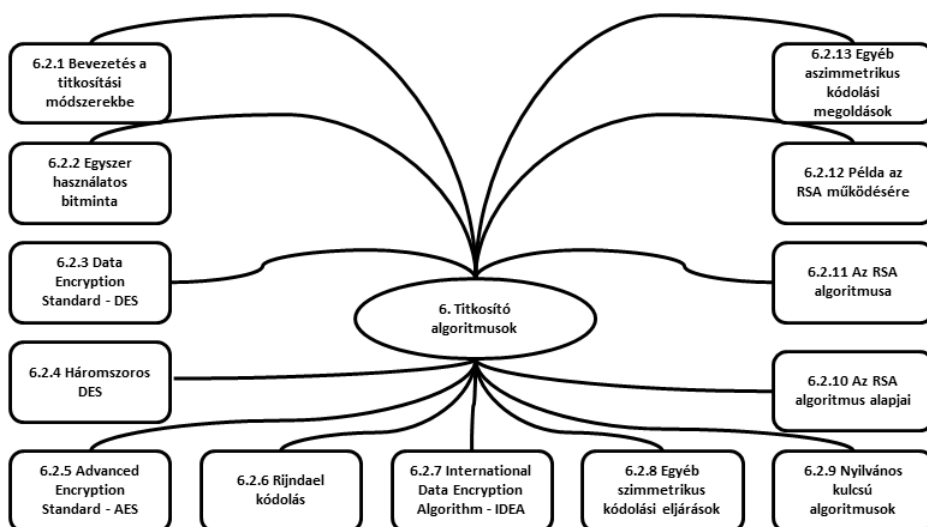
6 TITKOSÍTÓ ALGORITMUSOK

6.1. CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

Az előző fejezet folytatásaként, ahol általánosságban kerültek bemutatásra a módszerek, ebben a fejezetben a cél az, hogy a hallgatók megismerjék a napjainkban használt különböző titkosítási eljárásokat, algoritmusokat.

Bemutatásra kerülnek mind a szimmetrikus, mind az aszimmetrikus eljárások, a matematikai és informatikai leírások mellett megismerkednek a felhasználási lehetőségekkel is, így tisztában lesznek az egyes eljárások jelentőségével is.

6.2. TANANYAG



6.2.1. Bevezetés a titkosítási módszerekbe

A következő részekben a különböző, ma is használt titkosító eljárásokról, algoritmusokról lesz szó. Legtöbbjük értelmezéséhez, működésének megértéséhez nagyon komoly matematikai alapokra, tudásra lenne szükség, ezért ebben a fejezetben inkább csak az egyes módszerek elméletét foglaljuk össze, hogy ismerjék meg ezeket az eljárásokat, értsék meg, hogy hogyan működnek, de nem fogunk túlzottan mély matematikai, kriptográfiai ismeretekbe merülni.

A továbbiakban tehát az egyes, a gyakorlatban ma is használt megoldásokat nézzük át, szimmetrikus és aszimmetrikus eljárásokat is meg fogunk ismerni.

? Mi is a két eljárás között a fő különbség?

6.2.2. Egyszer használatos bitminta

A módszer nagyon egyszerű, és feltörhetetlen bármekkora számításteljesítmény mellett.

Válasszunk egy véletlenül generált bitsorozatot, ezt fogjuk kulcsként használni. A kódolandó üzenetet szintén bitsorozattá alakítva, és a kulccsal bitenként végezzünk kizáró vagy (xor) műveletet, ezzel kész is vagyunk. A fogadó oldalon ugyanazzal a kulccsal, szintén a kizáró vagy művelettel előáll az eredeti üzenet.

Az egyszer használatos bitminta (one-time pad) feltörhetetlen, mert az üzenet semmilyen információt nem hordoz, bármilyen, adott hosszúságú nyílt szöveg előfordulhat.

```

Nyílt szöveg: MAGYAR
Bitsorozat: 010011010100000101000111010110010100000101010010
Kulcs: 010010001000010100100010000101001000100001010010
Titkosított bitsorozat: 000001011100010001100101010011011100100100000000
  
```

17. ábra: Titkosítás egyszer használatos bitmintával

A kódtörő kipróbálhatja az összes lehetséges bitmintát, valójában minden X karakter hosszú nyílt szöveghez létezik egy azt előállító bitsorozat.

A módszer tehát nagyszerű, gyors, egyszerű, de a gyakorlatban nem igazán használatos.

? Gondolja át, mi a probléma a módszerrel?

Mivel a bitminta véletlenszerű, nehéz megjegyezni, ha pedig rögzítjük, akkor azt biztonsági szempontból nem tekinthetjük tökéletes megoldásnak. Másrészt, mindkét félnek ismernie kell a kulcsot, annak biztonságos eljuttatása újabb nehéz feladat lehet. A harmadik probléma, hogy csak a kulccsal azonos hosszúságú szöveget lehet titkosítani. Egyes alkalmazásokban mindezek ellené-

re előfordulhat a módszer használata, például egy teljes DVD-n lehet a kulcs maga.

6.2.3. Data Encryption Standard – DES

Az eljárást az IBM dolgozta ki, majd az amerikai kormányzat is elfogadta a 1970-es években szabványként, később ipari környezetben is elterjedté vált. Ma már eredeti formájában nem tekinthető biztonságosnak, de némi kiegészítéssel ma is használják bizonyos esetekben.

A nyílt szöveget 64 bites részekre kell bontani, ezekkel a blokkokkal történik a kódolás. A kulcs hossza 56 bit, maga a titkosítás 19 lépésből áll, a visszafejtés ugyanazzal a kulccsal történik, csak a lépések sorrendjét kell felcserélni.

Az első lépés egy kulcsfüggetlen keverés (a kezdeti 64 bit sorrendjét összekeverjük), az utolsó lépés ennek a keverésnek az inverze lesz, illetve előtte még az első 32 bitet felcseréljük a második 32 bittel. A módszer lényege a közbülső 16 lépés, amelyek mindegyikében a kulcs használatával és különböző függvények segítségével megtörténik a kódolás. A 16 lépés során a kulcs is változik, előre meghatározott algoritmus szerint, majd végül szintén a kizáró vagy műveletet végezzük el a kulcs és a kódolandó bitsorozat bitjei között.

A módszert eredetileg 128 bites kulccsal tervezték, amely jóval nagyobb biztonságot szavatolt volna, de a szabványba az 56 bites verzió került, nem keves bizonytalanságot hagyva a szakemberekben. Ma a DES feltörése kevesebb, mint egy napig tart megfelelő számítógépekkel.

6.2.4. Háromszoros DES

Nem sokkal a DES elterjedése után már szükségessé vált annak továbbfejlesztése, amit az IBM el is végzett, ennek eredményeként jött létre a háromszoros DES néven elterjedt módszer.

Az eljárás két kulcsot használ, és három menetben végzi el a titkosítást, innen származik az elnevezés is. Első lépésben az első kulccsal megtörténik a DES alapú kódolás, viszont második lépésben egy dekódolási folyamatot hajtunk végre a kódolt üzeneten, melyhez a második kulcsot használjuk. Utolsó lépésként pedig újra az első kulccsal végzünk kódolást, így előállítva a titkosított üzenetet.

Mi volt az előnye ennek a megoldásnak? Elvben kompatibilis az eredeti DES rendszerekkel, aránylag egyszerűen át lehet állítani a szoftvereket ennek a használatára, hiszen háromszor kell a DES eljárást alkalmazni. Másrészt a két használt kulcs összesen 112 bites hossza megnyugtatónak tűnt mindenki számára.

6.2.5. Advanced Encryption Standard – AES

A DES és a háromszoros DES megoldása felett azonban a számítógépek fejlődése miatt eljárt az idő, mert belátható időn belül visszafejthetők az üzenetek. Az amerikai National Institute of Standards and Technology (Nemzeti Szabványügyi és Technológiai Intézet) ezért kiírt egy pályázatot 1997-ben egy új titkosítási eljárás elkészítésére, amely Advanced Encryption Standard (AES) néven amerikai (majd világméretű) szabványként jelenne meg.

A pályázati kiírásban természetesen erős feltételeket fogalmaztak meg az eljárással szemben, ezek közül a legfontosabbak:

- Az algoritmusnak szimmetrikusnak és blokkok kódolásával kell működnie.
- A teljes eljárásnak nyilvánosnak kell lennie.
- A kulcsok hossza 128, 192 és 256 bit hosszú is lehessen.
- Az eljárás mind hardveresen, mind szoftveresen megvalósítható legyen.
- Az algoritmus legyen nyilvános és mindenki számára engedélyezett, ne védje szerzői jog.

Az első felhívásra érkezett javaslatok közül 15-öt választottak ki, melyeket többéves munkával, tesztelésekkel, konferenciákkal szűkítettek le előbb egy ötös csoportra, majd hivatalosan 2001-ben bejelentették, hogy az úgynevezett Rijndael kódolást fogadják el szabványként, bár a verseny többi résztvevője is használható és akár még ma is használt eljárást készített.

6.2.6. Rijndael kódolás

Az amerikai kormányzati szabványként elfogadott AES titkosítás tehát a Rijndael kódolás lett, amelyet két belga szakember, Vincent Rijmen és Joan Daemen készített el, az eljárás elnevezése is a készítőkre utal.

Az algoritmus 128-tól 256 bitig terjedő kulcsokat és szintén ekkora tartományba eső blokkokat támogat, de a kulcs és a blokk méretének nem kell egyforma hosszúságúnak lennie. Az AES specifikáció szerint a blokknak 128, a kulcsnak 128, 192 vagy 256 bitesnek kell lennie, a gyakorlatban a 128 és a 256 bites kulcsokat alkalmazzák.

A Rijndael a DES-hez hasonlóan helyettesítést és keverést alkalmaz az eljárás során, szintén több körben. Az ismétlések száma függ a kulcs és a titkosítandó blokk méretétől, így például 128 bites blokk- és kulcsméret mellett 10 körben történik a kódolás, nagyobb kulcsok és blokkok esetén több kör van, maximum 14. Létezik azonban egy nagy különbség is a DES-sel összehasonlítva,

a Rijndael ugyanis nem bitenként, hanem a könnyebb megvalósítás miatt bájtónként végzi a műveleteket.

Az eljárást teljes részletességben nem nézzük át, leírása, algoritmusa több helyen megtalálható, magyarul is.

A Rijndael kódolás is szimmetrikus, vagyis a kulcs ismeretében a visszafejtés gyakorlatilag az inverz műveletek végrehajtásából adódik.

6.2.7. International Data Encryption Algorithm – IDEA

Az IDEA (nemzetközi adattitkosító eljárás) Xuejia Lai és James Massey által kidolgozott titkosítási eljárás, amelyet Svájcban fejlesztettek ki 1991-ben. Egy ideig a DES ellenfeleként volt elkönyvelve. Bruce Schneier, elismert kriptográfus szerint a szimmetrikus blokktitkosítók közül az egyik legbiztonságosabb algoritmus.

Az IDEA blokktitkosító kriptorendszer, ahol egy bemeneti blokk hossza 64 bit. A rejtjelezés során létrejövő kimeneti blokk mérete is 64 bit. A kulcs 128 bit hosszúságú. A titkosítás és visszafejtés folyamata megegyezik, 8-szor végezzük el ugyanazt a számítási folyamatot, 8 különböző körkulccsal (a kulcs körönként változik, az előző lépésben használtból alakítjuk át matematikai módszerekkel). Az utolsó kör után a kimeneten még egy végső átalakítást végzünk.

A titkosítás három különböző matematikai művelet alkalmazásából áll, melyek hardver és szoftver megvalósításai egyszerűek, könnyen alkalmazhatóak. Az eljárás viszont szabadalmaztatott, így a gyakorlatban is működő rendszerben csak a jogdíjak megfizetése után használhatjuk, ezért elterjedtsége nem nagy, sokan inkább az ingyenesen használható algoritmusokat veszik igénybe.

6.2.8. Egyéb szimmetrikus kódolási eljárások

Az említetteken kívül természetesen egyéb eljárásokat is kifejlesztettek, illetve használnak, akár a mai napig. Néhányat közülük különböző termékekbe ágyazva találhatunk meg. Említsük meg ezeket az eljárásokat is, egy-két jellemzőjükkel együtt.

- Blowfish: Bruce Schreiner készítette, a kulcs hossza 1 és 488 bit között változhat, ma már elavultnak, lassúnak számít.
- Twofish: Szintén Bruce Schreiner által készített eljárás, a kulcs hossza 128 és 256 bit között lehet, nagyon erős titkosítást ad, széles körben alkalmazzák.
- RC5: Ronald Rivest nevéhez köthető eljárás, szintén 128 és 256 bit közötti kulcsokkal, erős titkosítást tesz lehetővé, de szabadalmaztatott.

- Serpent: A Rijndael egyik legerősebb ellenfele volt az AES kiválasztásánál, Andersen, Biham és Knudsen alkotta meg a módszert. Az AES felteteleinek megfelelően 128, 192 vagy 256 bites kulcsokkal tud titkosítani, 32 körben végzi el a feladatot, emiatt biztonságosabbnak minősül, mint akár a Rijndael, viszont lassabb és nehezkesebben megvalósítható.

6.2.9. Nyilvános kulcsú algoritmusok

A legtöbb titkosítási rendszer gyenge pontja a kulcskiosztás, hiszen bármilyen erős is az algoritmus, ha a kulcs nem megfelelő személy kezébe kerül, akkor a rendszer teljesen védtelen lesz. Sokáig egyértelmű volt, hogy ugyanazt a kulcsot használjuk a titkosításhoz és a visszafejtéshez, viszont (ahogy az előző fejezetben is említettük) az informatikai rendszerek egyre nagyobb használatával együtt felmerült egy új típusú megoldás lehetősége, először csak elméletben.

A módszer lényege, hogy két kulcsot használunk az eljárás során, lesz egy nyilvános (public) kulcs, amelyet akár mindenki ismerhet, szabadon hozzáférhet, ezzel történik az üzenetek titkosítása. A titkos (private) kulcsot viszont csak a felhasználó ismeri, aki az üzeneteket fogadja, és csak ennek a titkos kulcsnak a segítségével tudja elvégezni a visszafejtést. Nagyon nagy előny, hogy így olyan személyek is biztonságosan tudnak kommunikálni, akik nem ismerték előzőleg egymást, és nem kell a kulcsok elküldésének problémájával foglalkozni.

A módszer kitalálói viszont nem tudták gyakorlatban is bemutatni az algoritmust, mert nem tudták azt megvalósítani, de sok szakembert gondolkodásra és munkára készítettek, akik megpróbálták az elméletet gyakorlatba ültetni. Szerencsére sikerrel jártak, így ma is használhatunk ilyen típusú eljárásokat, amelyek közül a legismertebb az RSA-ként emlegetett algoritmus. Nézzük meg ennek működését, tulajdonságait!

6.2.10. Az RSA algoritmus alapjai

A módszer a nevét kidolgozó vezetőneveinek kezdőbetűjéből kapta, a három személy, aki 1978-ban megalkotta az eljárást: Ron Rivest, Adi Shamir és Leonard Adleman.

Az eljárás alapvetően a számelmélet tételeire épül, pontosabban arra, hogy egy kellően „nagy” számról még a mai számítógépek teljesítménye mellett is nehéz eldönteni, hogy milyen prímszámok szorzatából áll. A szorzótényezőkre bontást nevezzük faktorizálásnak, „... ha folytatódna is a számítógépek sebességének évtizedenkénti egy nagyságrenddel való növekedése, akkor is évszázadok

múlva kerül az 500 bites számok gyors faktorizálása elérhető közelségbe.”⁸, ráadásul ebben az esetben is csak növelni kell majd az alkalmazott számok nagyságát.

Az algoritmus a legelterjedtebb aszimmetrikus kódolás, rengeteg helyen használják a gyakorlatban is, bár tegyük hozzá, hogy a kódolási folyamat lassú, főleg, ha nagy mennyiségű adatot kell titkosítani. Gyakori megoldás, hogy egyéb szimmetrikus kódolás kulcsait titkosítják RSA-val, majd így küldik el a felhasználóknak.

Az eljárást már több mint 30 éve használják, de még nem sikerült feltörni. Bizonyos esetekben könnyebb lehet a törés, de ezek a problémás körülmények a módszer helyes paraméterezésével kiküszöbölhetőek.

6.2.11. Az RSA algoritmusa

Nézzük (természetesen leegyszerűsítve) az RSA algoritmust!

Első lépésben válasszunk két nagy (napjainkban jellemzően 512 bites) prímszámot, jelöljük ezeket a számokat p és q -val. A két prím szorzatát nevezzük az RSA modulusának, jelölése N , és $N=p*q$, N értéke 1024 bit lesz, ami decimálisan is több mint 300 számjegy. Számoljuk ki a $(p-1)*(q-1)$ értéket, jelöljük ezt z -vel, majd keressünk egy olyan d értéket, amely relatív prím z -hez viszonyítva. Az utolsó lépés egy olyan e szám meghatározása, amelyre igaz lesz, hogy $e*d \equiv 1 \pmod{z}$.

Az értékek kiszámítása, meghatározása után a titkosítási folyamat a következőképpen történik: a nyílt szöveget, mint bitsorozatot olyan blokkokra (jelöljük M -mel) osztjuk, amelyek rövidebbek az N hosszánál. Ezután kiszámítjuk a $C=M^e \pmod{N}$ értéket. Ez a C érték lesz a titkosított üzenet, míg a visszafejtéshez az $M=C^d \pmod{N}$ képletet kell használni.

Rendeljük össze az értékeket eddigi fogalmainkkal: mire is lesz szükség egy RSA kódoláshoz? A titkosítás elvégzéséhez az e és N értékeket kell ismernünk, gyakorlatilag ez a kettős adja a nyilvános kulcsot, míg a visszafejtés a d és N értékek ismeretében végezhető el, ez a páros adja a titkos kulcsot.

Talán kicsit sok volt a matematikai rész, nézzünk egy példát az RSA működésére!

⁸ TANENBAUM, S. Andrew: *Számítógép-hálózatok*. Budapest, Panem kft., 2004. 806. o.

6.2.12. Példa az RSA működésére

Az eljárás, mint az előző alfejezetben láttuk, a nagy számok faktorizálására épül, annak nehézségére. Mi természetesen az érthetőség kedvéért kisebb értékek mellett nézzük meg az algoritmus működését.

Válasszunk két kis értékű prímet, $p=3$ és $q=11$, amiből következik, hogy $N=33$ és $z=20$. Következő lépésben kiválasztunk egy relatív prímet a z értékéhez, legyen ez a 7, ez lesz a d értéke. Most már csak az e -t kell kiszámolni, az $e \cdot 7 = 1 \pmod{20}$ képletből, adódik, hogy $e=3$.

Nézzük a titkosítást adó számításokat az INFORMATIKA szóra:

Nyílt szöveg		Titkosított szöveg			Visszafejtett szöveg	
Jel	Kód	p^3	$p^3 \pmod{33}$	C^7	$C^7 \pmod{33}$	Jel
I	9	729	3	2187	9	I
N	14	2744	5	78125	14	N
F	6	216	18	612220032	6	F
O	15	3375	9	4782969	15	O
R	18	5832	24	4586471424	18	R
M	13	2197	19	893871739	13	M
A	1	1	1	1	1	A
T	20	8000	14	105413504	20	T
I	9	729	3	2187	9	I
K	11	1331	11	19487171	11	K
A	1	1	1	1	1	A

A küldő számítása
A fogadó számítása

18. ábra: RSA titkosítás

6.2.13. Egyéb aszimmetrikus kódolási megoldások

Bár messze az RSA a legelterjedtebb, leginkább használt megoldás, azért említsünk meg egyéb nyilvános kulcsú eljárásokat is. Az ilyen típusú eljárások alapvetően két csoportba sorolhatóak, vagy a nagy számok faktorizálásának nehézségét vagy a diszkrét logaritmusok nagy prímeikkel vett modulusának számítását veszik alapul.

Megemlíthető az első nyilvános kulcsú titkosítási eljárás, amelyet hátizsák (knapsack) módszernek neveztek el készítői, Merkle és Hellman 1978-ban. A módszer lényege, hogy nagyszámú különböző súlyú tárggyal rendelkezünk, és a titkosításhoz ezen tárgyak közül választunk ki néhányat, és tesszük egy hátizsákba. A zsák súlya és a használható tárgyak listája lehet a nyilvános kulcs, a kiválasztott tárgyak listája pedig a titkos kulcs. Ennek a listának az összeállítása algoritmikusan nehéz feladat, ezen a tényen alapul a módszer. Később bizonyították, hogy nem lehetetlen a törés, így a később bevezetett módosítások ellenére sem tekinthető biztonságosnak az algoritmus, ennek megfelelően nem is használják a gyakorlatban.

A diszkrét logaritmusok számításának nehézségeire alapuló algoritmusok közül megemlíthető Rabin, El Gamal és Schnorr erre az elvre épülő módszere.

6.3. ÖSSZEFOGLALÁS, KÉRDÉSEK

6.3.1. Összefoglalás

A fejezet bemutatta azokat az eljárásokat, algoritmusokat, amelyeket napjaink informatikai rendszerei használnak a kommunikáció titkosítására. Az előző fejezethez kapcsolódva a hallgatók megismerték a szimmetrikus és az aszimmetrikus kódolási eljárásokat. Kiemelésre került az is, hogy mely eljárások milyen területen hatékonyak, hol érdemes azokat használni.

7 DIGITÁLIS AZONOSÍTÓK

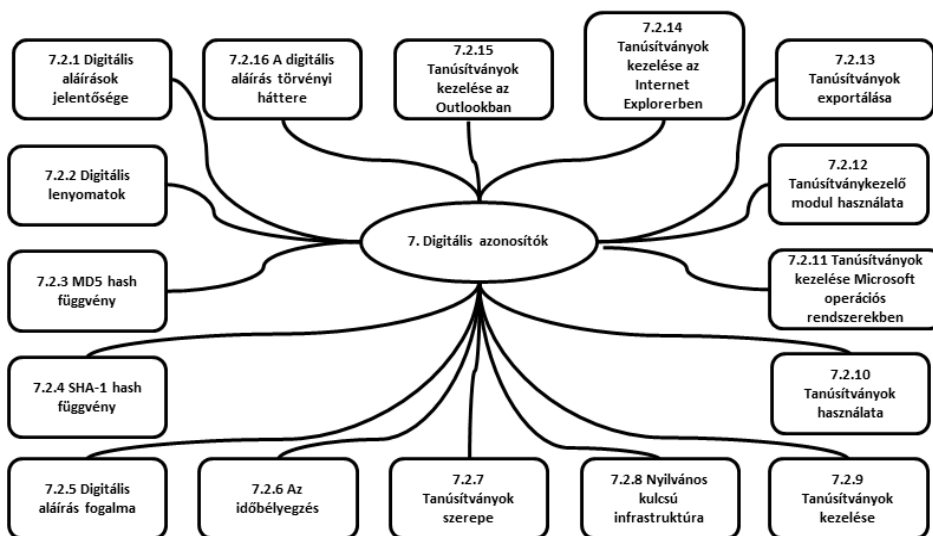
7.1. CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

A hálózati kommunikáció hitelesítésére, titkosítására az előző fejezetben megismert algoritmusok használhatóak. Ebben a fejezetben ezeknek a módszereknek az egyik legelterjedtebb alkalmazási területét mutatjuk be, a digitális (vagy másnéven elektronikus) aláírás jelentőségét, használatát.

Bemutatjuk az eljárás működését, az alkalmazott digitális lenyomat-készítő algoritmusokat, a nyilvános kulcsú infrastruktúra szerkezetét. A fejezet második része a gyakorlatban is, a Microsoft rendszerein keresztül mutatja be a tanúsítványok szerepét, kezelését.

Nem feledkezhetünk meg a digitális aláírások jogi szabályozásának tisztázásáról sem.

7.2. TANANYAG



7.2.1. Digitális aláírások jelentősége

Történelmünk utolsó néhány évszázadában, és még ma is a dokumentumok hitelességét egy kézzel írott aláírás bizonyította, bizonyítja. A számítógépes

rendszerekben is szeretnénk megoldani a hitelességvizsgálatot, amely a hagyományos iratokhoz hasonlóan egyértelműen azonosítaná az aláíró személyt.

Ez nem egyszerű feladat, alapvetően azt kell elérni, hogy elkészüljön egy olyan rendszer, amelynek segítségével a küldő fél úgy tud üzenetet küldeni egy másik félnek úgy, hogy az alábbi feltételek teljesüljenek:

- A fogadó fél ellenőrizhesse a küldő valódiságát.
- A küldő később ne tagadhassa le az üzenet elküldését.
- A fogadó ne tudja az üzenetet önmaga összeállítani.

Az első követelmény szükséges ahhoz, hogy egyértelműen tudja azonosítani a feladót a fogadó fél, ez nagyon fontos lehet például üzleti, diplomáciai kapcsolatoknál. Egy aránylag könnyen hamisítható e-mail hatására egy bank nem fog üzleti tranzakciókba kezdeni, ha nincs meggyőződve az üzenet küldőjének valódiságáról.

A második követelmény azért szükséges, mert tegyük fel, hogy olyan megbízás ad egy ügyfél a banknak, ami később káros számára, anyagi veszteséget okozna. Ekkor, ha nem tisztességes az ügyfél, akkor hivatkozhatna arra, hogy ő bizony nem adott semmilyen megbízást előzőleg. Fontos tehát, hogy ne lehessen letagadni az üzenet elküldését, annak semmilyen tulajdonságát, tartalmát.

A harmadik feltétellel pedig azért van szükség, mert nagy gondot okozhatna a bank is, ha a veszteséges tranzakciókat átháríthatná az ügyfelekre, hamisított dokumentumok alapján.

7.2.2. Digitális lenyomatok

Mielőtt definiálnánk a digitális aláírás fogalmát, nézzük át a digitális lenyomatok elméletét!

Az aláírásnak majd a dokumentum sértetlenségét is biztosítania kell, hogyan tehető ez meg? Az úgynevezett digitális lenyomatokkal, vagy ahogyan a szakirodalomban hivatkoznak rá: hash, message digest, üzenet pecsét segítségével.

A kriptográfiában a hash eljárások olyan egyirányú matematikai függvények, amelyek egy tetszőleges hosszúságú bitsorból generálnak egy rögzített hosszúságú bitsorozatot, amely jellemzően 128 vagy 160 bit, és amelyet hash értéknek nevezünk. Az informatikában számos protokoll során használunk hash függvényeket, elsősorban hitelesítés, digitális aláírások és üzenetsértetlenség ellenőrzésekor. A sértetlenség ellenőrzése azt jelenti, hogy két különböző időpontban, de ugyanarra az elektronikus dokumentumra kiszámolt hash értékek

összehasonlításával meg lehet állapítani, hogy a dokumentum tartalma a két időpont között (például üzenetküldés vagy letöltés közben) megváltozott-e.

A hash függvényekre vonatkozóan több fontos tulajdonságot tudunk megfogalmazni:

- Egy bitsorozathoz könnyen kiszámítható legyen a hash érték.
- A hash értékből gyakorlatilag lehetetlen az eredeti bitsorozat előállítása.
- Nincs olyan eljárás, amely egy bitsorozatot úgy alakítana át, hogy ugyanazt a lenyomatot kapjuk az eredeti és az átalakított bitsorozatra is.

Ezen feltételek teljesülése esetén nyilvánvalóvá válik, hogy a sértetlenség biztosításához nem lesz szükség a teljes üzenet, dokumentum ellenőrzésére, hanem elég lesz a digitális lenyomatot alapul venni.

Az évek során többféle hash algoritmust kidolgoztak, ezek közül a két legelterjedtebb eljárást mutatjuk be röviden.

7.2.3. MD5 hash függvény

Az MD5 (message digest) eljárást az RSA algoritmusnál megismert Ron Rivest tervezte, ez a jelenleg használt függvény egy sorozat ötödik tagja.

A függvény működése nem túl bonyolult, gyorsan elvégezhető a számítás. Első lépésben az eredeti bitsorozatot úgy alakítja át az algoritmus, hogy a hossza bitben számolva 512-vel osztva 448 legyen, ezt úgy éri el, hogyha nem ez az állapot, akkor feltölti plusz bitekkel. Ezután az eredeti bitsorozat méretét fűzi a dokumentum végére 64 bites számként ábrázolva, így a bemenet hossza végül 512 bit többszöröse lesz. Utolsó előkészületeként megtörténik egy előre megadott 128 bites érték betöltése a pufferbe.

A számítás során 512 bitenkénti beolvasás történik a dokumentumból, majd ennek a szeletnek a pufferrel való „összekeverése” egy algoritmus szerint. Minden szeletre négyszer kell végrehajtani ezt a keverést. Ez a folyamat ismétlődik, amíg nem érünk a bitsorozat végére. A lenyomatot a 128 bites puffer értéke adja.

7.2.4. SHA-1 hash függvény

Az SHA (Secure Hash Algorithm) az Egyesült Államok NSA (National Security Agency) szervezete fejlesztette ki, elfogadott és jellemzően használt az egyes verziója, de nagyobb biztonságot az SHA-256 tud adni, amely már 256 bites hash értéket generál.

Az algoritmus az MD5-höz hasonlóan 512 bites blokkokban dolgozza fel a bemenetet, viszont SHA esetén 160 bit hosszú lesz a hash értéke. Tehát első lépésben itt is az eredeti bitsorozatot ki kell egészíteni úgy, hogy 512 bit többszöröse legyen, ehhez egy darab 1-es bitet, illetve utána csupa 0 bitet illeszt a bemenet végére az algoritmus.

A számítás újra 512 bites egységenként fog történni, megint csak addig, amíg nem érünk a bemenet végére. Pufferként öt darab 32 bites változót használ az eljárás, az egyes bitszeletekkel elvégzett logikai és matematikai műveletek eredményeként az öt puffer tartalma folyamatosan változik. A teljes bemeneten elvégzett számítások hash eredményét végül az öt puffer fogja adni, így jön ki a 160 bites érték.

7.2.5. Digitális aláírás fogalma

 **Digitális aláírás alatt értjük azt az elektronikus lenyomatot, hash értéket, amely egy adott elektronikus dokumentumhoz – ami lehet akár e-mail, akár egy tetszőleges állomány – tartozik, és amelyet az üzenet feladója egy titkos kulcs segítségével titkosít.**

A titkosított lenyomatot a feladó eljuttatja a címzetthez, legtöbb esetben az eredeti dokumentummal együtt. Az üzenet címzettje, a feladó nyilvános kulcsának ismeretében képes ellenőrizni mind az eredeti elektronikus dokumentum sértetlenségét, mind az aláíró személy hitelességét, hiszen elvileg a titkos kulcsot csak az aláíró ismeri. Problémát okozhat, ha ez a titkos kulcs nyilvánosságra kerül, esetleg illetéktelen személy hozzáfér ahhoz a számítógéphez, ahol a titkosítás történik.

A digitális aláírás a dokumentum sértetlenségének ellenőrzésére és a feladó azonosítására egyaránt alkalmas, ezért használni lehet azokon a területeken, ahol ez a kettős confirmálás szükséges. Fontos azonban tisztázni, hogy önmagában a digitális aláírás alkalmatlan nyílt szöveg tartalmának a titkosítására.

Az egyik elterjedt digitális aláírás-eljárás a DSA (Digital Signature Algorithm), mely az El Gamal nyilvános kulcsú megoldáson alapszik, az erre épülő szabvány a DSS (Digital Signature Standard). A másik digitális aláírási rendszer az RSA aláírási séma, amelynek elméleti háttérében az RSA kriptorendszerrel bemutatott algoritmus áll.

7.2.6. Az időbélyegzés

Az időbélyegzés lényege annak bizonyítása, hogy egy adott elektronikus dokumentum egy meghatározott időpillanatban már biztosan létezett. Az időbélyegzéssel szemben három alapvető követelményt támaszthatunk:

- Az elektronikus dokumentumot magát kell időbélyeggel ellátni.
- Biztosítani kell, hogy az elektronikus dokumentumot ne lehessen megváltoztatni sehogyan sem a leleplezés veszélye nélkül.
- Ne lehessen egy elektronikus dokumentumot oly módon időbélyegezni, hogy a dátum és az időpont ne egyezzen meg a pillanatnyival.

Maga az időbélyegzési folyamat gyakorlatilag egy üzenetcsereből áll. Az első üzenetet az időbélyegzést kérelmező elküldi az időbélyegzést végző szervezetnek (amelyet időbélyegzés-szolgáltatónak is nevezünk), ez az üzenet az időbélyegzés-kérelem. Az időbélyeg-kérelem tartalmazza az időbélyeggel ellátni kívánt elektronikus dokumentum lenyomatát.

A válaszüzenet az időbélyegzés-szolgáltató válasza a kérelemre, ami maga az időbélyeg, ebben az időbélyeg-szolgáltató a lenyomathoz legalább két megbízható időforrásból vett referenciaidő adatot kapcsol, és ezeket az adatokat saját digitális aláírásával ellátva visszaküldi a kérelmezőnek.

Az ilyen időbélyeggel ellátott elektronikus dokumentumok a teljes bizonyító erejű magánokiratok súlyával igazolják, hogy az adott dokumentum a pecsét elhelyezésének időpontjában már létezett.

7.2.7. Tanúsítványok szerepe

A nyilvános kulcsok biztonságos szétosztása egy fontos tényezője a digitális aláírások kezelésének. Milyen esetben lehet probléma? Tegyük fel, hogy két, egymást nem ismerő személy szeretne biztonságos kommunikációt folytatni egymással. Legegyszerűbb esetben a nyilvános kulcsukat közzéteszik, például a weboldalukon. Tegyük fel, hogy Andrea meg akarja keresni Béla nyilvános kulcsát, meg is találja egy weboldalon, ami sajnos hamisított: Tamás lemásolta az oldalt, illetve kicserélte a saját nyilvános kulcsára. Andrea ezzel a kulccsal titkosítja az üzenetet és elküldi, amit Tamás elfog, vissza tudja fejteni a saját titkos kulcsával, és ezután küldi tovább Bélának most már a megfelelő nyilvános kulccsal kódolva az üzenetet, vagy akár annak módosított változatát. Sem Andrea, sem Béla nem fogja észrevenni, hogy más is olvasta az üzenetet.

A probléma megoldása első ránézésre az lehetne, ha lenne egy olyan központ, akiben mindenki megbízna, és ott tárolnánk a nyilvános kulcsokat, így nem lehetne hamisítani azokat. Ez viszont a hatalmas forgalom mellett nagy

terheltséget okozna bármilyen on-line rendszer esetén, nem beszélve arról, ha valamilyen okból meghibásodna, elérhetetlenné válna, akkor a teljes kommunikáció megszűnhetne.

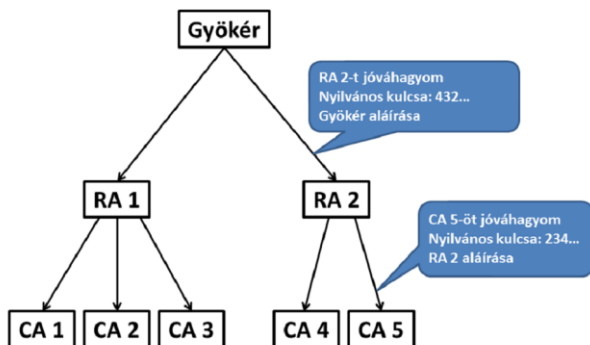
Ezen okok miatt egy másik megoldást fejlesztettek ki, amelyben a központnak nem kell on-line elérhetőnek lennie, hanem csak annyit tesz, hogy hitelesíti az egyes személyekhez, cégekhez, szervezetekhez tartozó nyilvános kulcsokat. Az ilyen központokat, szervezeteket nevezzük tanúsító hatóságnak, angolul Certification Authority-nek, vagy az elterjedt rövidítéssel CA-nak.

7.2.8. Nyilvános kulcsú infrastruktúra

Nyilvánvaló, hogy egyetlen CA működtetése nem elegendő, nem lehet rábízni az összes tanúsítvány kezelését. Ez a technikai feltételek hiánya mellett azért sem lenne szerencsés, mert ha egyetlen szervezetre bíznák a működést, akkor az aggodalmakra adhatna okot. A megoldást jelenleg a nyilvános kulcsú infrastruktúra, a PKI (Public Key Infrastructure) eljárás jelenti.

Az eljárásnak több összetevője van, így a felhasználók, a tanúsítványok, a CA-k, a könyvtárak. A PKI jelentősége, hogy lehetővé teszi az előbb említett elemek szervezetbe rendezését, illetve szabványos megoldásokat határoz meg különböző dokumentumok és protokollok számára.

A PKI a tanúsító hatóságok számára hierarchiát hoz létre, ahol a legfelső szintű CA, amit gyökérnek neveznek, hitelesíti az alsóbb szintű központokat, amelyeket ezek után RA-nak (Regional Authorities – regionális hatóságok) neveznek, mert gyakran egy földrajzi egységet fognak össze. Az RA-k aztán további, alsóbb rendű CA-kat hitelesítenek, amelyek már ténylegesen a felhasználók azonosítására szolgálnak.



19. ábra: PKI hierarchia

A hierarchián belül tehát a központok egymást képesek hitelesíteni, egy bizalmi láncot létrehozva. Amikor egy felhasználó egy másik tanúsítványát ellenőrzi, akkor ezen a láncon keresztül haladva tudja elfogadni a hitelesítést. Kérdésként merülhet fel, hogy honnan ismerjük a gyökérhatóság nyilvános kulcsát, vagyis mi alapján fogadjuk el annak hitelességét? Itt jön egy apró trükk: az eljárás kidolgozói feltételezik, hogy ezt a kulcsot mindenki ismeri. Ezt a gyakorlatban úgy a legegyszerűbb megoldani, hogy maguk a böngészők tartalmazzák a legfontosabbnak tekintett gyökér CA-k nyilvános kulcsát, a felhasználóknak nem kell keresgélniük ezeket, hanem automatikusan tudják használni azokat sokszor anélkül, hogy tudnának bármit is az egész eljárásról.

7.2.9. Tanúsítványok kezelése

A tanúsítványokat tehát elismert szervezetek bocsátják ki, akik igazolják a hozzátartozó tulajdonos valóságát. Milyen módon lehet hozzájutni ilyen tanúsítványhoz? El kell mennünk egy ilyen szervezethez, ahol valódi okiratokkal (például személyi igazolvány, jogosítvány vagy cégalapítási okirat) ténylegesen igazolnunk kell személyazonosságunkat, vagy cégünk valóságát. A CA ezután – és a szolgáltatás díjának befizetése után – állítja ki a tanúsítványt, amelyet saját kulcsával egy SHA pecséttel is ellát.

Maguk a tanúsítványok nem titkosítottak, tulajdonosuk nyilvánosan terjesztheti, akár a weboldalon is elhelyezheti. Az előző alfejezetben leírt támadás ezzel a megoldással kivédhető, hiszen a kicserélt nyilvános kulcs tanúsítványa nem az eredeti tulajdonosra utal, illetve ha azt is kicseréli a támadó, akkor az SHA pecsét értéke nem lesz helyes!

A tanúsítványok további jó tulajdonsága, hogy egyéb attribútumokat is tartalmazhat, így például azt is igazolhatja, hogy a tulajdonos nagykorú, betöltötte a 18. életévét, hozzáférhet szolgáltatásokhoz, tartalmakhoz anélkül, hogy esetleg a valódi személyazonosságát fel kellene fedni. A tanúsítványokat időkorlátozással is ellátják, csak az érvényességi időig használhatóak, ez az idő digitális aláírás esetén általában egy év, aztán meg kell újítani (amiért természetesen újra fizetnünk kell).

Magyarországon több ilyen tanúsító hatóság is működik, amelyek a közigazgatásban, oktatásban, üzleti életben megkövetelt tanúsítványokat (de akár digitális aláírásokat is) képesek kiállítani, a jogi környezetről pár gondolatot az utolsó alfejezetben találunk.

7.2.10. Tanúsítványok használata

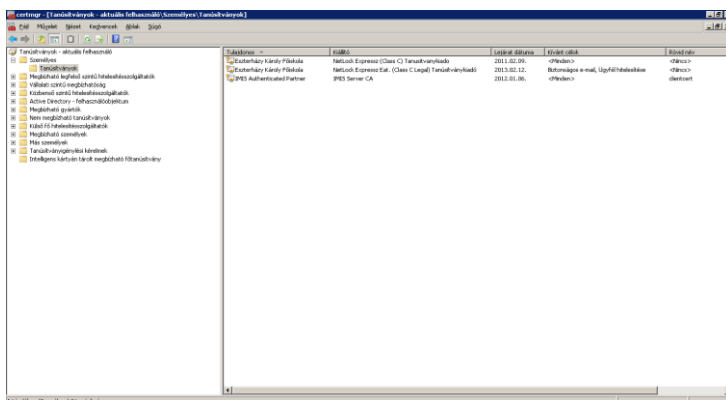
A tanúsítványokat, illetve annak privát részét beszerzésük után aránylag egyszerűen használhatjuk. De hogyan juthatunk hozzá, hogyan tárolhatjuk? Ha a legegyszerűbb esetet vesszük, akkor akár egy biztonságos weboldalról is letölthetjük a tanúsítványt, amelyet az operációs rendszerünkbe telepíthetünk, így az automatikusan képes lesz kezelni a tanúsítványt. Ez a megoldás csak akkor biztonságos, ha tudjuk, hogy más nem fér hozzá ehhez a számítógéphez, nem tudja használni az operációs rendszer szolgáltatásait, ellenkező esetben az automatizmus miatt bárki képes lesz igénybe venni a tanúsítványunkat.

Biztonságosabb megoldás, ha a tanúsítványt valamilyen hordozható eszközön tároljuk. Ez az eszköz napjainkban a chipkártya, amelyre feltöltik a tanúsítványt, és csak akkor használjuk egy kártyaolvasó segítségével, amikor szükségünk van rá, hasonló módon vigyázva rá, mint a bankkártyánkra. Még egy hasonlóság a bankkártyához, hogy a tanúsítvány használata előtt szintén pinkódot is meg kell adnunk.

Sajnos előfordulhat, hogy a privát kulccsal olyan esemény történik (elveszik, ellopják a chipkártyát, számítógépet), amely esetlegesen visszaélésre adna lehetőséget, ebben az esetben a CA-nál lehet kérni a tanúsítvány felfüggesztését.

7.2.11. Tanúsítványok kezelése Microsoft operációs rendszerekben

A Microsoft operációs rendszerei külön kezelőfelületet biztosítanak a tanúsítványok kezelésére, így a személyes tanúsítványok telepítése, használata leegyszerűsíthető.



20. ábra: Tanúsítványkezelő

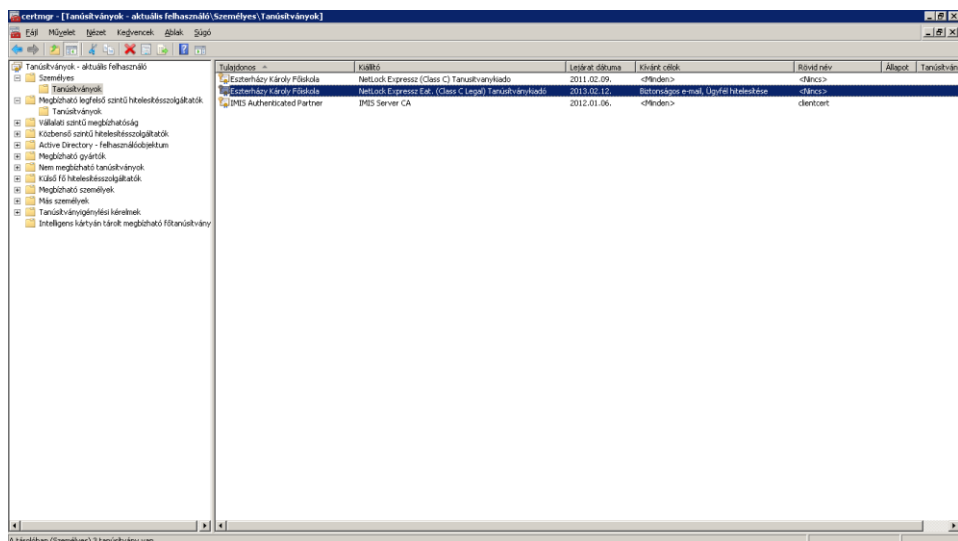
A Tanúsítványkezelő beépülő modul hozzáadható az MMC (Microsoft Management Console) konzolhoz, így a szokásos felületen keresztül végezhetőek el a műveletek. A modul felhasználók, számítógépek vagy szolgáltatások tanúsítványainak kezelését végzi, az ilyen tanúsítványok közötti váltáshoz a Tanúsítványkezelő modul különböző példányait szükséges a konzolhoz hozzáadnunk.

Nézzük meg, hogyan tehetjük meg ezt egy felhasználói fiók esetében! A művelet elvégzéséhez legalább Felhasználók vagy helyi Rendszergazdák csoporttagság szükséges.

- Kattintsunk a Start gombra, írjuk be az mmc kifejezést a Keresés programokban és fájlokban mezőbe, majd nyomjuk le az Enter billentyűt.
- A Felhasználói fiókok felülete ablakban az Igen-re kattintva engedélyezzük a hozzáférést!
- Kattintsunk a Fájl menü Beépülő modul hozzáadása/eltávolítása parancsára.
- Az Elérhető beépülő modulok listában kattintsunk duplán a Tanúsítványok elemre, majd:
 - Ha rendszergazdaként jelentkezünk be, akkor kattintsunk a Saját felhasználói fiókom elemre, végül a Befejezés gombra (gyakorlatilag itt választható ki, hogy felhasználó, számítógép vagy szolgáltatás tanúsítványát szeretnénk kezelni).
 - Ha felhasználóként jelentkezünk be, akkor automatikusan megnyílik a Tanúsítványkezelő beépülő modul.
- Ha nincs több hozzáadandó beépülő modul, kattintsunk az OK gombra.
- Amennyiben szeretnénk a konzolt menteni, kattintsunk a Fájl menü Mentés parancsára.

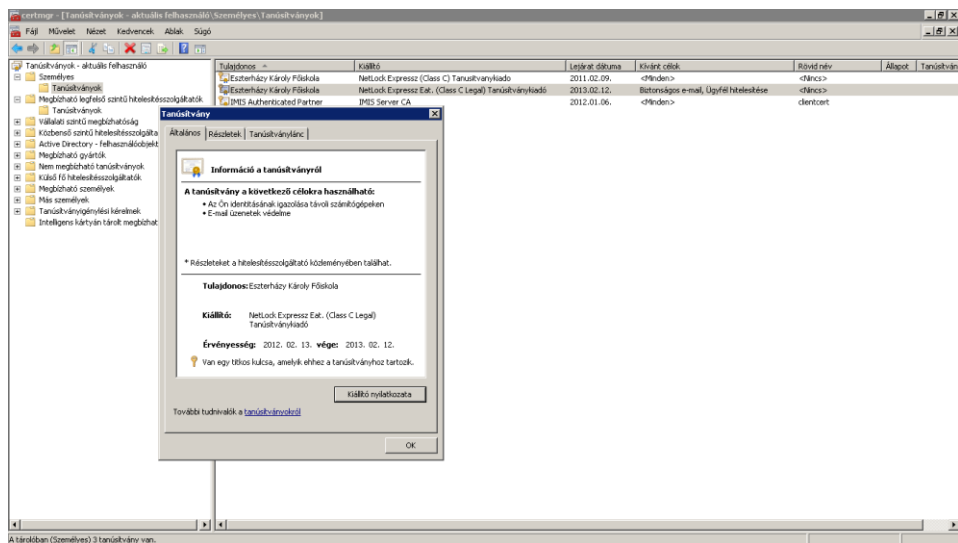
7.2.12. Tanúsítványkezelő modul használata

Az előzőekben leírt módon elérhető tehát a Tanúsítványkezelő modul. Nézzük a tanúsítványok típusait! Az egyik fontos csoport a Személyes tanúsítványok ág, ahol a felhasználóhoz, mint személyhez rendelt tanúsítványokat tudjuk kezelni. A listában természetesen csak akkor látunk adatokat, ha előzőleg beszereztünk, telepítettünk tanúsítványt. Ebben az esetben láthatjuk a tulajdonost, a kiállítót (CA-t), az érvényességi időt, illetve, hogy milyen célokra használható a tanúsítvány.

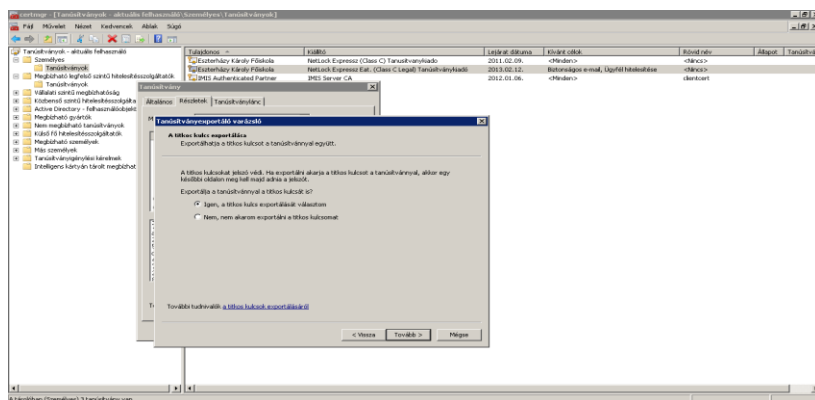


21. ábra: Személyes tanúsítványok

Duplán kattintva egy soron, meg tudjuk nézni részletesebben a tanúsítványhoz tartozó attribútumokat. A megjelenő ablakban – az Általános fülön – először egy bővebb leírás található a már eddig is ismert adatokról.

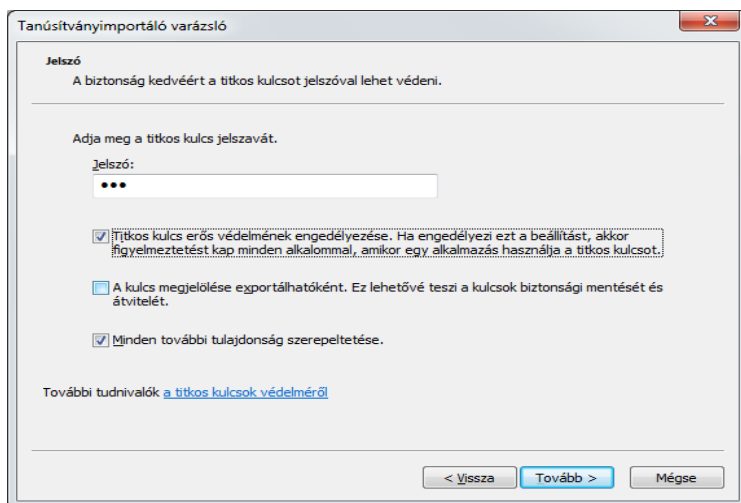


22. ábra: Tanúsítvány általános tulajdonságai



24. ábra: Titkos kulcs exportálása

A varázsló ezután egy .PFX típusú fájlt fog készíteni, amihez bekéri a jelszót, illetve a létrehozandó állomány helyét. Az így elkészült fájlt tudjuk átvinni másik eszközre, amelyen a Windows rendszer felismeri az állomány típusát, és duplán kattintva a .PFX állományon elvégezhető az importálási folyamat, szintén egy varázsló segítségével.

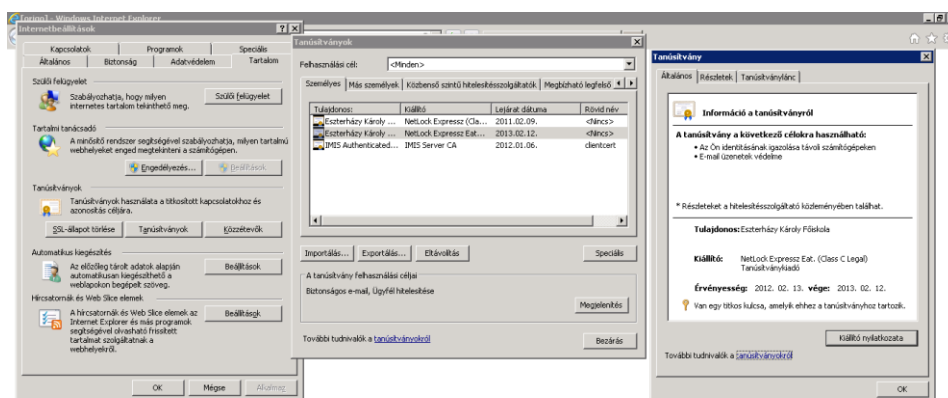


25. ábra: Tanúsítvány importálása

A folyamat közben természetesen meg kell adnunk a beállított jelszót, illetve egyéb tulajdonságokat is meghatározhatunk, ahogy az ábrán is látszik.

7.2.14. Tanúsítványok kezelése az Internet Explorerben

A Microsoft operációs rendszereiben lehetőség van arra is, hogy az Internet Explorer program keretein belül férjünk hozzá a tanúsítványokhoz. Ehhez az Eszközök menün belül válasszuk ki az Internetbeállítások menüpontot, majd a megjelenő ablakban a Tartalom fülön látjuk a Tanúsítványok gombot, kattintunk rá. Megjelenik egy párbeszédablak, amelyben természetesen ugyanazokat a tanúsítványokat látjuk, mint a Tanúsítványkezelőben, de kicsit más formában.



26. ábra: Tanúsítványok kezelése az Internet Explorerben

Ezen a felületen is lehet importálni, exportálni, eltávolítani a tanúsítványokat, illetve a Megjelenítés gombra kattintva megkapjuk ugyanazt a tulajdonság-lapot, mint amit a Tanúsítványkezelőben láttunk.

7.2.15. Tanúsítványok kezelése az Outlookban

A tanúsítványok felhasználásának egyik legnagyobb szerepe az elektronikus levelezésnél lesz, hiszen itt használhatjuk majd digitális aláírásként azokat. Nézzük meg, hogy hogyan állítható be a Microsoft levelező programjában, az Outlookban a digitális aláírás használata!

Az Outlook Eszközök menüjén keresztül érhető el az Adatvédelmi központ, ahol engedélyezhetjük, illetve beállíthatjuk a digitális aláírásunkat. Először megadhatjuk, hogy a program minden kimenő elektronikus levélhez automatikusan hozzáadja a digitális aláírást. Ezután a Beállítások... gombra kattintva kapunk egy ablakot, ahol egyéb opciók mellett kiválasztható az aláíró, illetve a

7.2.17. A digitális aláírás törvényi háttere

Magyarországon a törvény által definiált és alkalmazott fogalmak közül a legfontosabbak a digitális aláírások és az elektronikus dokumentum kategóriáit meghatározó bekezdések. A nyílt számítógépes hálózatokon kezdeményezett tranzakciók és – immár jelentős pénzmozgást is maguk után vonó – jogügyletek elsősorban ezek alapján lesznek a meglévő egyéb hagyományos jogi szabályozási rendszerbe beilleszthetők, következésképpen ennek alapján fűződnek majd hozzájuk a vonatkozó, hagyományos megfelelőiknél már működő jogi biztosítékok és konstrukciók.

A digitális aláírásokra vonatkozóan a törvény megkülönböztet (a digitális helyett elektronikus elnevezést használva, amely a technológia mellett a jogi fogalmat is magában foglalja) három típust:

- Egyszerű elektronikus aláírást, amelynek készítője egyedileg nem azonosítható, illetve segítségükkel nem megállapítható, hogy az aláírt dokumentum az aláírás óta változott-e?
- Fokozott biztonságú elektronikus aláírást, amely kizárólag az aláíró befolysága alatt álló aláíró eszközzel létrehozott, az aláíró személyazonosságának és az üzenet sértetlenségének megállapítását lehetővé tévő elektronikus adat.
- Minősített elektronikus aláírást, amely olyan fokozott biztonságú aláírás, melyet minősített hitelesítés-szolgáltató által kiadott tanúsítvány hitelesít.

A jogszabályból fakadó következmények közül a leglényegesebb, hogy minősített elektronikus aláírással ellátott bármely elektronikus okirat teljes bizonyító erejű magánokiratnak minősül akkor, ha a hitelesség ellenőrzéséhez szükséges tanúsítványt minősített hitelesítésszolgáltató bocsátotta ki.

Keressen magyar hitelesítésszolgáltatókat! Készítsen összefoglalót az aktuális árakról, lehetőségekről, vitassák meg hallgatótársaival az adatokat.

7.3. ÖSSZEFOGLALÁS, KÉRDÉSEK

7.3.1. Összefoglalás

A fejezet a hálózati kommunikáció hitelesítésére, titkosítására használt, az előző fejezetben megismert algoritmusok gyakorlati működését is magában

foglaló témakört mutat be. Így a hallgatók megismerkedtek a digitális (elektronikus) aláírás jelentőségével, használatával, törvényi szabályozásával.

Bemutattuk az eljárás működését, az alkalmazott digitális lenyomat-készítő algoritmusokat, a nyilvános kulcsú infrastruktúra szerkezetét. A fejezet második része a Microsoft rendszerein keresztül gyakorlatban is, bemutatta a tanúsítványok szerepét, kezelését.

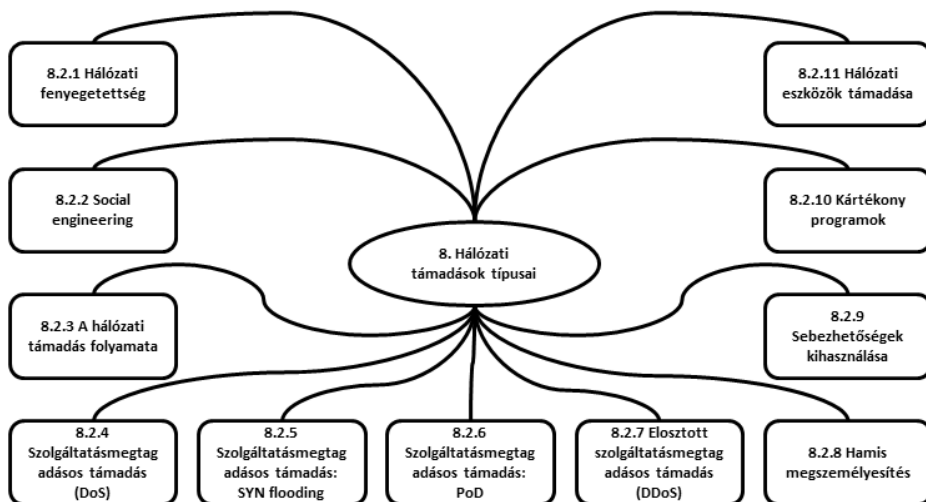
8 HÁLÓZATI TÁMADÁSOK TÍPUSAI

8.1 CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

A hálózati rendszerek, a hálózaton folyó kommunikáció védelme akkor biztosítható megfelelő szinten, ha tisztában vagyunk azokkal a veszélyekkel, fenyegetettségekkel is, amelyek ránk leselkedhetnek. Ennek a fejezetnek a célja, hogy azokat a veszélyforrásokat, támadási módszereket, fenyegetettségeket bemutassa, amelyek előfordulhatnak a számítógépes hálózatok használata közben.

Fontos tisztázni, hogy milyen módon vagyunk támadhatóak, így később saját rendszerünk gyengeségeit is könnyebben fel tudjuk mérni, illetve tudunk tenni a megelőzés érdekében. Maga a tananyag is ad felvilágosítást arra vonatkozóan, hogy hogyan lehet védekezni az adott támadási módszerrel szemben.

8.2. TANANYAG



8.2.1. Hálózati fenyegetettség

A hálózati támadások ismertetése előtt nézzük meg, milyen okok vezetnek oda, hogy egyáltalán ezek a támadások kivitelezhetőek legyenek, esélye legyen a komoly szaktudással rendelkező személyeknek arra, hogy a számítógépes

hálózaton keresztül illetéktelenül hozzáférjenek információkhoz, szolgáltatásokhoz, megmásítsanak adatokat, netán romboljanak.

A fenyegetettség egyik összetevőjét a hálózati infrastruktúra adja. Mit értünk ez alatt? Egy teljesen nyilvános, ismert architektúrát használunk, amelynek tervezésekor, létrehozásakor nem volt elsődleges szempont a biztonság. Hasonló módon a kezdeti (és ma is használt) protokollok sem biztonságosak, bár folyamatosan próbálják átalakítani, kiegészíteni biztonságot nyújtó funkciókkal ezeket a szabványokat is. A protokollok ráadásul globálisan használtak, ez a sok előny mellett azt is jelenti, hogy ugyanazzal a módszerrel gyakorlatilag a világ össze számítógépe elérhető, támadható. Biztonsági szempontból problémát okoz az a tény is, hogy a rengeteg felhasználó miatt olyan szolgáltatások, megoldások születnek, amelyek felhasználóbarátok, de emiatt egyszerűen használhatónak is kell lenniük.

A fenyegetettségek másik része az emberi tulajdonságokból adódik. Egyrészt néhány ember számára motiváló, hogy hozzáférjen olyan hálózati adatokhoz, szolgáltatásokhoz, amelyhez egyébként nem lenne joga. Sokan nevezik ezeket a személyeket hacker-nek, fontos azonban tisztázni, hogy eredetileg a hacker a jószándékú, a biztonsági réseket felderítő, azt jelentő és nem kiharcoló személyek megnevezése volt. Ma már a rossz szándékkal támadó személyeket is hacker-nek hívja a köznyelv.

A fenyegetettségek egyik legveszélyesebb típusát külön alfejezetben tárgyaljuk, mit gondol, mi lesz ez?

8.2.2. Social engineering

A fenyegetettségek nem mindig technológiai oldalról érkeznek, hiszen előfordulhat, hogy a támadni kívánt rendszer, program olyan védelemmel rendelkezik, amelynek feltörése még a legfelkészültebb támadó számára sem lehetséges. Sajnos ebben az esetben is kiszivároghatnak információk és elképzelhető, hogy a támadó bejut a rendszerbe.

Social engineering alatt olyan támadásokat értünk, amelyek az emberek hízsékenységét, naivitását használják ki. A magyar szakirodalomban is leginkább ezt az angol elnevezést használják. A fogalom egyébként Kevin David Mitnick (az egyik legismertebb számítógépes „betörő”) nevéhez fűződik, illetve ő volt az első, aki rendszeresen alkalmazta ezt a módszert.

A módszer a biztonsági rendszerek mindenkorl leggyengébb láncszemére, magára az emberi tényezőre összpontosít. Gyakorlatilag minden területen alkalmazható és nem kell nagyon komoly informatikai ismeretekkel rendelkezni ahhoz, hogy valaki alkalmazhassa ezt a technikát, csak tudnia kell bánni az em-

berekkel. A sikeres támadók többsége rendkívül jó emberi tulajdonságokkal rendelkezik, kedvesek, udvariasak, vagyis olyan jellemvonásokkal rendelkeznek, amelyek a gyors kapcsolatépítéshez és a bizalom kialakításához szükségesek. A megfelelő stratégiával és taktikával gyakorlatilag bármilyen információhoz képesek hozzájutni.

Sokan nem törődnek ezzel a fenyegetéssel, ez különösen igaz hazánkban is. Sok felhasználó úgy gondolja, hogy őt nem fogják megtámadni vagy becsapni, hiszen úgy sincs nála semmilyen fontos információ. Sokszor viszont éppen elég, ha saját hozzáférési adatait ki tudják belőle csalni, hiszen akkor a támadó már a rendszeren belül van, belülről (kikerülve így komoly védelmi rendszereket) könnyebben tud támadást intézni. A támadó nagyon jól ismeri ezt a hozzáállást és kérését olyan természetesen adja elő, hogy általában nem kelt gyanút, ennek következtében képes visszaélni az áldozat bizalmával.

Fontos tehát, hogy az informatikai rendszerek, megoldások mellett a felhasználók is fel legyenek készítve a támadások ellen.

8.2.3. A hálózati támadás folyamata

A hálózati támadás legtöbb esetben egy folyamatként fogható fel, kevés alkalommal kerül sor véletlenszerű, nem előre tervezett műveletre. Nézzük át röviden, milyen műveleteket hajt végre egy támadó, ebből is okulva, hogy hogyan védhetjük saját rendszerünket.

A támadó először egy felderítést végez. Amennyiben egy konkrét rendszert szeretne megtámadni valamilyen okból, akkor annak védelmi rendszerét fogja megvizsgálni. Előfordulhat, hogy nem konkrét rendszert akar támadni, ekkor olyan rendszereket, szolgáltatásokat keres, amelyek védelme nem tűnik tökéletesnek. Sajnos már vannak olyan programok, amelyek képesek automatikusan tesztelni az ilyen védelmi gyengeségeket. A támadó mindenesetre képes a hálózati forgalom scannelésére, megfigyelésére, és az így összegyűjtött adatok alapján (a megfelelő tudással, kitartással felvértezve) kiválasztani azt a technikát, módszert, amellyel megpróbál hozzáférést szerezni a hálózati erőforrásokhoz.

Ha sikerült áttörni a védelmi vonalat és valamilyen hozzáférést megszerezni, akkor gyakran élnek a támadók azzal a lehetőséggel, hogy a megszerzett jogosultságokat kiterjesztik, így újabb erőforrásokhoz, információkhoz juthatnak hozzá. Utolsó lépésként pedig (számukra) nagyon fontos módon egyrészt megpróbálják eltüntetni a tevékenységük nyomait (naplóállományokat átírnak, jogosultságokat megváltoztatnak, stb.), másrészt a későbbi behatolást elősegítő úgynevezett hátsó ajtókat (trójai programok telepítése, billentyűlenyomások rögzítése, stb.) nyitnak a védelmi rendszeren.

8.2.4. Szolgáltatásmegtagadásos támadás (DoS)

Az egyik elterjedt támadási mód a szolgáltatásmegtagadással járó támadás (Denial of Service vagy DoS), vagy más néven túlterheléses támadás.

A szolgáltatásmegtagadásos támadás általában egy meghatározott alkalmazás vagy operációs rendszer ismert gyengeségeit, esetleg valamilyen protokoll gyengeségét használja ki. Fő célja, hogy megakadályozza a feljogosított felhasználókat a rendszer vagy alkalmazás elérésében, így a számukra fontos információk, hálózati erőforrások használatában. A támadás következtében a kiszolgáló rendszer nagyon lelassul, gyakran elérhetetlenné válik, néha teljes egészében össze is omolhat.

A lényege, hogy lehetőség szerint megakadályozza a célgép elérését hálózaton keresztül, viszont a támadók nem jutnak illetéktelenül adatokhoz, nem szereznek hozzáférést a rendszerhez. Ebből a szempontból nem okoz nagy problémát, viszont nagy bosszúságot okozhat a felhasználóknak, akik esetleg nem a támadást látják az elérhetetlenségben, lassúságban, és másikkal, konkurens szolgáltatót fognak használni.

Nézzünk példát arra, hogyan lehet végrehajtani egy szolgáltatásmegtagadásos támadást!

8.2.5. Szolgáltatásmegtagadásos támadás: SYN flooding

A SYN flooding támadás a TCP három-utas kézfogásos üzenet visszaigazolás rendszerét használja ki. A hálózati kapcsolat kiépítése előtt az ügyfélgép kérésére a kiszolgáló egy portot rendel a kapcsolathoz, és ezt a portot ki kell hogy nyissa. Ezt a lépést nevezzük passzív portnyitásnak. Amennyiben a passzív port nyitva van, az ügyfél kezdeményezheti egy aktív port megnyitását, melynek során a három-utas kézfogás folyamata zajlik le.

- SYN: Az ügyfél egy SYN jelet küld a kiszolgálónak, sor kerül az aktív port megnyitásra. Az ügyfél a szegmens sorszámát egy véletlen értékre (X) állítja.
- SYN-ACK: A kiszolgáló válaszában egy SYN-ACK jelet küld vissza, illetve a nyugtázó szám értékét a kapott sorszám értéke plusz 1-re állítja (X+1), míg a csomag sorszámaaként egy másik véletlen számot választ ki (Y).
- ACK: Utolsó lépésben az ügyfél egy ACK jelet küld a kiszolgálónak, a sorozatszám a kapott nyugtázó érték lesz (X+1) és az ügyfél által küldött érték a kiszolgálótól kapott sorozatszám plusz 1 (Y+1).

Így mind az ügyfél, mind a kiszolgáló megkapja a kapcsolatfelvétel nyugtáját, megkezdődhet a kommunikáció.

A SYN flooding támadás során egy hamis IP címről küldi el a SYN üzenetet a támadó, amit a kiszolgáló a protokoll szabványának megfelelően fogad, majd a hamis IP címre visszaküldi a SYN-ACK üzenetet. Az eljárásnak megfelelően várja az ügyfél ACK nyugtáját, ezt viszont természetesen a hamis IP címről soha nem fogja megkapni. A kiszolgáló egy meghatározott várakozási idő (time-out) letelte után eldobja a kapcsolatot, azonban ha sok hamis SYN üzenetet kap a kiszolgáló, akkor a felesleges várakozási idők a szabályos kapcsolatok fogadását is drasztikusan lelassítják, esetleg teljesen lehetetlenné teszik.

8.2.6. Szolgáltatásmegtagadásos támadás: PoD

Támadási lehetőséget biztosít a hálózati kapcsolatok tesztelésére létrehozott nagyon egyszerű megoldás, a ping használata is. A szabványban rögzített maximális 64 Kbyte méretnél nagyobb ICMP ping csomagok okozhatnak problémát.

A halálra pingeléses (Ping of Death – PoD) támadás lényege, hogy a támadó ilyen szabálytalan méretű ping csomagokat küld a megtámadott gépre. Az indokolatlanul nagy ping csomagot a rendszer nem minden esetben képes kezelni, így előfordulhat, hogy komoly problémát okoz a számítógépgép működésében.

Ismert hálózati környezetben célszerű úgy beállítani az eszközeinket, hogy azok a pingelésre válaszoljanak. Ismeretlen környezetben viszont ma már elfogadott, hogy számítógépeink pingelésre nem reagálnak, hiszen a szabvány szerint nem kötelező reagálni. Legegyszerűbben úgy védhetjük ki a támadást, ha a rendszer tűzfalát már így konfiguráljuk, melynek eredményeként az így beállított kiszolgálók sikeres támadása sokkal nehezebb.

8.2.7. Elosztott szolgáltatásmegtagadásos támadás (DDoS)

A szolgáltatásmegtagadásos támadás alapvetően egy egy elleni támadási mód, vagyis egyetlen ügyfél gépről próbálják megbénítani a kiszolgálót. Az informatikai eszközök és a számítógépes hálózatok fejlődése azonban lehetővé tette, hogy az egyetlen helyről érkező támadások ne okozzanak kivédhetetlen problémákat. Ezt felismerve jelent meg az elosztott szolgáltatásmegtagadásos támadás (Distributed Denial of Service – DDoS) módszere.

A támadás előzményeként a támadó (általában automatizáltan, valamilyen sérülékenységet kihasználva) rengeteg gépre „betör”, és ezeket a számítógépe-

ket „zombi”-vá alakítja, vagyis feltelepít egy rejtett támadóprogramot a fertőzött számítógépre.

A „zombi” gépek a számítógépes hálózaton keresztül távolról vezérelhetők a támadó gépéről (esetleg a támadás egy bizonyos időponthoz köthető). Amennyiben a támadó elég gépet fertőzött meg a támadóprogrammal, jelet ad a „zombiknak”, hogy kezdjék meg a támadást a kiszemelt célpont ellen. A jel hatására az összes „zombi” számítógép elindítja a támadást egyszerre, és bár külön-külön kis mennyiségű adattal dolgoznak, számosságuk okán (akár több-százezer támadó gép is előfordulhat) a sok kis adatcsomag hatalmas hálózati forgalmat, adatmennyiséget okoz, amelyre a megtámadott kiszolgáló nem tud érdemben reagálni.

8.2.8. Hamis megszemélyesítés

A támadások gyakran élnek a hamis megszemélyesítés módszerével, vagyis amikor a támadók elhitetik magukról, hogy ők jogosultak a szolgáltatások, erőforrások használatára.

Ennek a módszernek a legjellemzőbb módja a jogosult felhasználók jelszavának megszerzése. A jelszavak megszerzésére szintén több formában képesek a támadók, nagy veszélyt jelentve így a különböző rendszerekre.

Nézzünk néhány módszert, eljárást a jelszavak megszerzésére!

Shoulder surfing (kifigyelés): nemcsak az informatikában használt eljárás (bankautomatáknál is jellemző), lényege, hogy a támadó figyel a folyamatot, ahogy a felhasználó megadja a jelszavát. Ezt teheti egy zsúfolt helyen, de akár (filmbe illő módon) távcsővel a szemben lévő irodaházból. Fontos tehát, hogy amikor begépeljük a jelszavunkat, próbáljuk minél inkább takarásban tenni azt!

Keylogger (billentyűleütések rögzítése): ezek a programok képesek titokban rögzíteni a felhasználók minden billentyűleütését, így a jelszavakét is, sőt, már akár képernyőképek mentése is megoldható. Természetesen a keyloggereket telepíteni kell a számítógépre, vagyis már egy előzetes támadás után használhatóak. (Vagy céges környezetben, esetleg otthon, ha kíváncsiak vagyunk a gyermekünk tevékenységére, szintén használható ellenőrző funkcióként.) A keyloggerek ellen nagy biztonsággal védekezhetünk a vírusirtó alkalmazások telepítésével, működtetésével.

Sniffing (lehallgatás): a támadó a hálózati forgalom lehallgatásával, a csomagok elemzésével is hozzájuthat speciális esetekben a felhasználók jelszavához, így például jó tudni, hogy az FTP szolgáltatás használata esetén nem javasolt nagyobb jogosultsággal rendelkező felhasználói fiókkal belépni, mert a jelszót a protokoll titkosítatlanul továbbítja.

Brute force (nyers erő): a „legegyszerűbb” módszer a jelszavak megszerzésére, ha végigpróbáljuk az összes lehetséges karaktersorozatot! Természetesen ezt nem egyesével begépelve fogja megtenni a támadó, hanem speciális programmal, amely generálja a jelszavakat, majd automatikusan meg is próbál belépni azzal. Az egyetlen védelmi megoldás az lehet ez ellen a támadási forma ellen, ha a rendszer néhány rossz próbálkozás után zárolja a felhasználói fiókot, és ezután a helyes jelszó megadása után sem engedi bejelentkezést, csak a rendszergazda engedélye után.

8.2.9. Sebezhetőségek kihasználása

Sebezhetőségek alatt azokat az általában ismert hibákat, vagy rossz konfigurációkat értjük, amelyek a rendszer védelmét gyengítik.

Ezeket a problémákat a támadók képesek kihasználni, sokszor nem is célzottan támadnak, hanem olyan rendszereket keresnek, ahol ezek a sebezhetőségek fellelhetők. Ehhez szintén programokkal képesek automatikusan tesztelni, felderíteni, hogy adott rendszerek érzékenyek-e valamilyen sebezhetőségre nézve. Legegyszerűbb példa, hogy a számítógépen futó operációs rendszerre fölkerültek-e a frissítések?

A támadó gyakran használja a portscan funkciót, amellyel azt tudja tesztelni, hogy a felhasználó számítógépén melyik portok vannak nyitva, ezeken milyen szolgáltatásokat tud elérni, támadni.

A sebezhetőségek felderítése után úgynevezett exploit-okkal lehet támadni, amelyek olyan parancssorozatok, adathalmazok, amelyek képesek kihasználni a rendszer biztonsági rését, és jogosulatlan hozzáférést, nem várt működést okoznak.

A támadás ellen a rendszerek karbantartásával, frissítések telepítésével, helyes konfigurációs beállításokkal, tűzfalak használatával hatékonyan lehet védekezni.

8.2.10. Kártékony programok

Kártékony program alatt értünk minden olyan alkalmazást, amely akaratunk és tudtunk nélkül kerül a számítógépünkre, és valamilyen módon károsítani szeretne minket.

Mindenki által hallott fogalom a vírus kifejezés, bár nem biztos, hogy mindenki tisztában van azzal, hogy mik is a vírusok? A számítógépes vírusok apró, sokszor nagy szaktudással elkészített programok, amelyek álcázva kerülnek az áldozat számítógépére egy másik program részeként. Ma már jellemzően az interneten keresztül vagy elektronikus levél csatolt állományaként, vagy egy

weboldalról, akaratlanul letöltve. Sok fajtájuk létezik, de mindegyikre jellemző, hogy az adott gép megfertőzése után reprodukálják önmagukat, megpróbálnak terjedni, vagyis más számítógépeket, rendszereket is megtámadni. Legegyszerűbb példa, hogy a csatolt állományként bekerült vírus továbbküldi magát a címlistában szereplő felhasználóknak.

A kártékony programok közé tartoznak az úgynevezett trójai programok, amelyek úgy viselkednek, mintha valami hasznos funkciót látnának el (a felhasználó emiatt telepíti ezeket), miközben a háttérben előkészítik a támadó számára a behatolás lehetőségét, például megnyitnak egy portot.

A férgek a vírushoz hasonlatos ártó szándékú programok, viszont már nincs szükségük gazdaprogramra, önállóan képesek terjedni, kihasználva a számítógépes hálózatok adta lehetőségeket.

A kártékony programok elleni védekezést szolgálják a különböző antivírus programok, de fontos tudni, hogy teljes védelmet nem tudnak biztosítani, hiszen előbb mindig a vírusok, egyéb kártékony programok jelennek meg, csak ezután tudják kifejleszteni (ma már napok, sőt órák alatt) és a felhasználókhoz eljuttatni a megfelelő védelmi megoldásokat. Mindezekből következik, hogy nem elég telepíteni az antivírus szoftvert, azt rendszeresen frissíteni is kell!

8.2.11. Hálózati eszközök támadása

Gyakran egy-egy hálózati támadás nem a szerverek, felhasználók számítógépei ellen irányulnak, hanem az egyéb hálózati eszközöket veszik célba.

Az egyik ilyen támadási forma az ARP (Adress Resolution Protocol) mérgezés, melynek során hamis csomagokkal át lehet írni az egyes eszközök ARP tábláit (ez szolgál arra, hogy az Ethernet hálózatokon belül a MAC címekhez hozzárendeljük az IP címeket), így a helyes címzett helyett a csomagokat mi kapjuk meg, amit a lebukás elkerülése végett továbbküldhetünk az eredeti címzettnek is, viszont mi magunk is látjuk, olvashatjuk az üzenetet!

Veszélyes lehetőségeket rejt magában a routerek támadása is. Nagyobb hálózatok nagyobb funkcionalitással rendelkező eszközeinél is fontos, hogy ne hagyjunk lehetőséget a router menedzselési felületéhez való hozzáférést. Változtassuk meg az alapértelmezett azonosítókat, jelszavakat. Ugyanez az eljárás javasolt az otthonokban használt wifi-routerek esetén is!

A védekezés lehetőségét az eszközök már biztosítják, csak megfelelően konfigurálni kell azokat.

8.3. ÖSSZEFOGLALÁS, KÉRDÉSEK

8.3.1. Összefoglalás

A hallgatók megismerték azokat a hálózati fenyegetettségeket, támadási módszereket, amelyekkel akár a saját hálózatuk működtetése közben is szembe kell nézni. Az egyes módszerek, támadási eljárások ismertetése mellett arra is felhívtuk a figyelmet, hogy hogyan lehet kivédeni az adott módszert, milyen lépésekkel tehetjük biztonságosabbá hálózatunkat.

Tisztáztuk azokat a kifejezéseket, módszereket, amelyek megkönnyítik a védekezést, az arra való felkészülést.

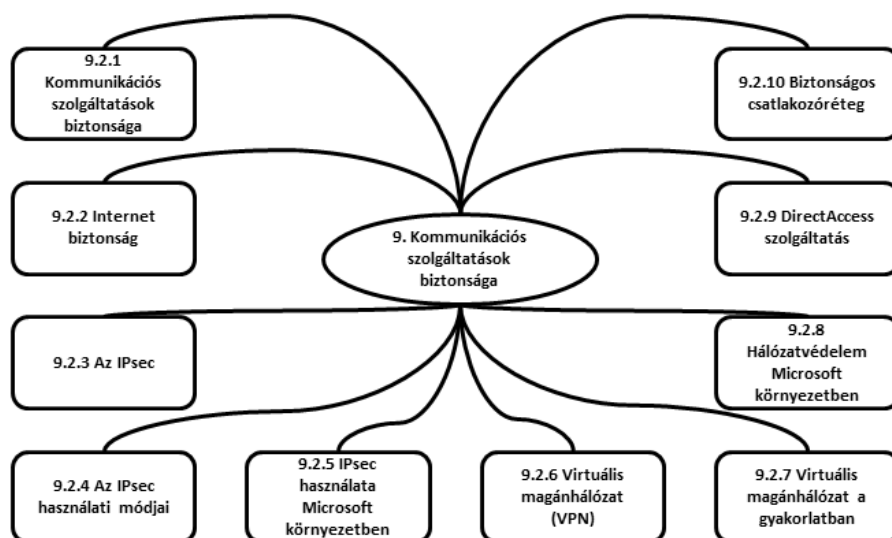
9 KOMMUNIKÁCIÓS SZOLGÁLTATÁSOK BIZTONSÁGA

9.1. CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

A fejezet célja, hogy megismertesse azokat a megoldásokat, módszereket, amelyeket azért hoztak létre, hogy biztonságos módon tudjanak a felhasználók kommunikálni egymással, illetve kiszolgáló alkalmazásokkal nyílt hálózatokon keresztül is.

Ezt a biztonságot a már tárgyalt kriptográfiai algoritmusok, eljárások biztosítják, de erre épülve létrejöttek különböző összetett szoftvertermékek, amelyek telepítése, konfigurálása, használata sokat javít a hálózatok biztonságán. Bemutatjuk a legelterjedtebb termékeket, az IPSec-et, a VPN megoldásokat, illetve a Microsoft legújabb fejlesztését. Az elmélet mellett a gyakorlati használatot is megismerik a hallgatók.

9.2. TANANYAG



9.2.1. Kommunikációs szolgáltatások biztonsága

A tananyag előző fejezeteiben áttekintettük elméletben azokat a kriptográfiai módszereket, algoritmusokat, titkosítási megoldásokat, amelyek képesek biztonságos kommunikációt biztosítani a felhasználók számára akár nyílt hálózatokon keresztül is.

Ebben a fejezetben azt vizsgáljuk meg, hogy milyen konkrét megoldások, protokollok, szolgáltatások jöttek létre, illetve használunk napjainkban a jellemzően internetalapú kommunikációnk során.

Fontos megjegyezni, hogy vannak már régóta használt megoldások, amelyeket biztonságosnak tekintünk, de ne felejtjük el, a technológia, az eszközök fejlődése azt is jelentheti, hogy a megszokott megoldások elavulttá, megbízhatatlanná válnak. Ezért célszerű figyelni és használni a legújabb megoldásokat, még akkor is, ha ezek bevezetése, használata megjelenésükkor esetleg nem teljesen elterjedt, illetve költséges.

9.2.2. Internetbiztonság

Az internetes kommunikáció a legelterjedtebb jelenleg, ezért nagyon fontosnak tekinthető, hogy az ezen a hálózaton folyó adatcsere is biztonságos legyen. A hálózat létrejöttékor ez nem volt lényeges szempont, később viszont komoly vitákat szült, hogyan alakítsanak ki egy olyan biztonsági rendszert, amely illeszkedik az addigi megoldásokhoz.

Az egyik vélemény szerint a leghatékonyabb titkosítást és sértetlenségi ellenőrzést a kommunikáló felek között, vagyis a végpontoknál lehet alkalmazni. Ezzel a megoldással az a baj, hogy gyakorlatilag az összes hálózati alkalmazást újra kell írni, hogy a biztonsági funkciókat kezelni tudják.

A másik nézet szerint a felhasználók nem törődnek a biztonsággal, nem is értenek a biztonsági technikákhoz, nem lesznek képesek kezelni megfelelő módon azt. Másrészt az alkalmazott szoftverek módosításához is rengeteg erőforrásra lenne szükség. Ezért azt javasolták, hogy a hálózati rétegbe kellene helyezni a hitelesítési, titkosítási folyamatokat, függetlenül a felhasználóktól.

Sokévnyi vita után végül az utóbbi elgondolás alapján dolgoztak ki egy eljárást, amelynek előnye még, hogy nem akadályozza meg azt a törekvést, hogy aki akar, az természetesen az alkalmazási szinten is beépíthet védelmi, biztonsági funkciókat.

Az így létrejövő szabványos megoldás IPsec néven került be az informatikai világba.

9.2.3. Az IPsec

Az IPsec (IP security- IP biztonság) tehát az internetes kommunikáció biztonságáért felelős keretrendszer, amely többféle szolgáltatásból és algoritmusból áll. A többféle szolgáltatás oka, hogy nem kötelező mindenkinek mindent használni, gyakorlatilag választható, hogy melyik funkciókat szeretnénk igénybe venni. A legfontosabbak egyébként a titkosítás, a sértetlenség biztosítása és a visszajátszásos támadások elleni védelem. A gyors működés is követelmény, ezért szimmetrikus kulcsú algoritmusokat használ a rendszer. A többféle algoritmus használata azt is lehetővé teszi, hogy változtatni lehessen rajta, vagyis a keretrendszer képes lesz a jövőben is együttműködni a fejlettebb titkosítási módszerekkel.

Az IPsec az összeköttetéseket SA-nak (security association – biztonsági kapcsolatnak) nevezik, ez egyirányú kapcsolatot jelent, amelyhez egy biztonsági azonosítót is hozzárendelnek. Amennyiben mindkét irányban biztonságos adatcserét szeretnénk, akkor két SA-ra lesz szükség. Az ilyen SA-ban továbbított csomagok tartalmazzák azokat a biztonsági azonosítókat, amelyeket a kulcsok és egyéb információk meghatározására használnak a csomag megérkezésekor.

Az IPsec-nek a csomagok szempontjából két fontos része lesz, az első új fejrészeket ír le, amelyek a csomagokban a biztonsági azonosítót, a sértetlenségért felelős adatokat és egyéb technikai információkat visznek át. A második rész az ISAKMP (Internet Security Association and Key Management Protocol – Internetes Biztonsági Kapcsolat- és Kulcskezelő Protokoll), amely a kulcsok kezelésével foglalkozik, rendkívül bonyolult, legfontosabb protokollja az IKE (Internet Key Exchange – Internetes Kulcscsere). Ez utóbbi első verziója sebezhető volt, ezért lecserélték, jelenleg a második verziója használatos.

9.2.4. Az IPsec használati módjai

Az IPsec használatára kétféle módon van lehetőség. Az egyik a szállítási mód (transport mode), amelyben az IPsec fejrészt közvetlenül az IP-fejrész mögé illesztik, ehhez természetesen szükséges az is, hogy az IP-fejrész protokollmezőjét megváltoztassák, amely jelöli, hogy még a TCP-fejrész előtt IPsec adatok jönnek. Az IPsec-fejrész hordozza a biztonsági információkat, így az SA azonosítót, a csomag sorszámát (ez SA-n belüli, nem TCP!), a sértetlenséget biztosító ellenőrzőösszeget.

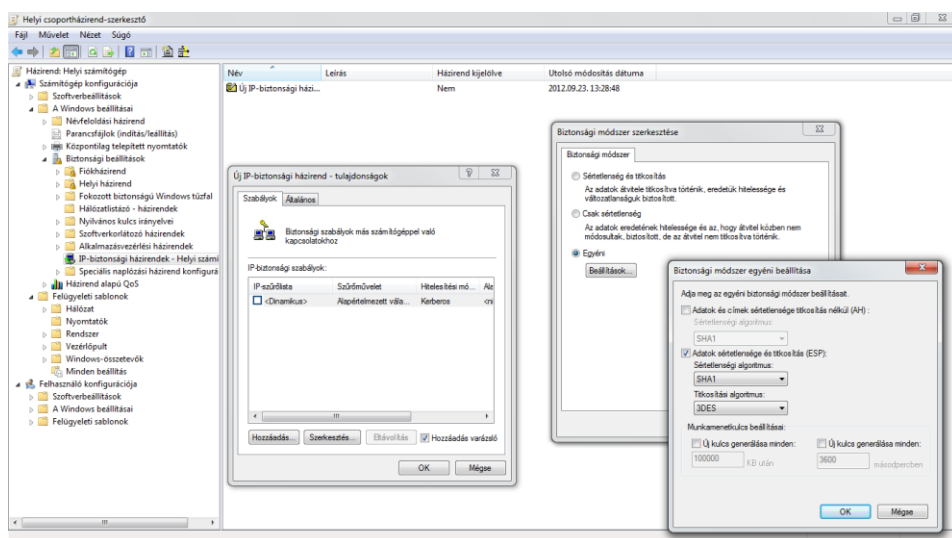
A második megoldásban, az alagútmódban (tunnel mode) a teljes IP-csomag bekerül egy új IP-csomagba, amely egy új IP-fejrészt is tartalmazni fog. Ez a mód akkor is használható, ha az alagút nem a két végpontot köti össze, hanem egyik oldalon csak például a helyi hálózat határán lévő tűzfalat. Ebben

az esetben a tűzfal képes az áthaladó csomagokat be- és kicsomagolni, a belső hálózatban a számítógépeknek, hálózati eszközöknek nem is kell tudni arról, hogy IPsec alapú kommunikáció történik egy ponttól.

Az alagútmód abban az esetben is jó szolgáltatást tesz, ha több TCP-összeköttetést egy folyamatként kezelünk, és azt titkosítjuk, így a forgalomanalízisre támaszkodó támadók ellen is védekezünk egyben.

9.2.5. IPsec használata Microsoft környezetben

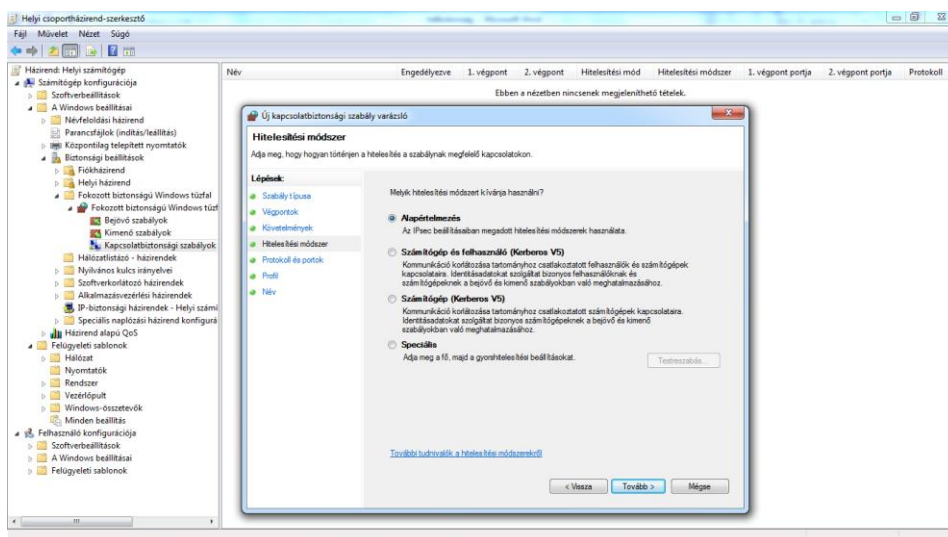
A Microsoft operációs rendszerei már régóta támogatják a szabványos IPsec eljárások használatát, az IPsec házirendeket csoportházirendeken keresztül állíthatjuk be, amelyek lehetővé teszik az IPsec opciók magas szintű beállítását.



29. ábra: IPsec házirend beállítása

A Helyi csoportházirend-szerkesztő megnyitása után a Számítógép konfigurációja/A Windows beállításai/ Biztonsági beállítások ágon belül található az IPsec-re vonatkozó tulajdonságokat meghatározó szabály helye. Kezdetben üres lesz a csomópont, létre kell hoznunk a házirendet, majd elvégezni a beállításokat. A kapcsolat biztonságát szabályozva részletesen beállíthatjuk a módszereket, hogy csak sértetlenséget, vagy azzal együtt titkosítást is szeretnénk-e használni. Az egyéni beállításokat választva akár mi magunk meghatározhatjuk a sértetlenség és a titkosítás algoritmusait.

A Fokozott biztonságú Windows tűzfal az IPsec használatával, kulcscsere, hitelesítés, adatsértetlenségi ellenőrzés és opcionálisan adattitkosítás segítségével biztosítja a kapcsolat biztonságát. A tűzfalszabályokkal ellentétben, amelyek egyoldalúan működnek, a kapcsolatbiztonsági szabályokhoz mindkét kommunikáló számítógépnek a kapcsolatbiztonsági szabályokra vonatkozó házirenddel vagy egyéb kompatibilis IPsec szabályozással kell rendelkeznie. Természetesen előfordulhat, hogy így is létre kell hozni tűzfalszabályt, amely engedélyezi a kapcsolatbiztonsági szabály által védett hálózati forgalmat.



30. ábra: IPsec használata kapcsolatbiztonsági szabályban

9.2.6. Virtuális magánhálózat (VPN)

A virtuális magánhálózat (Virtual Private Network – VPN) egy olyan megoldás, amelyet úgy kell elképzelni, mint a meglévő számítógépes hálózatunk fölé épített másik hálózat. Azért nevezzük „magán”-nak, mert a VPN-en keresztülhaladó adatokat titkosítjuk, gyakorlatilag ezeket a kódolt adatokat becsomagoljuk az átküldött csomagokba, így azok nem láthatóak, olvashatóak az eredeti hálózaton. A virtuális elnevezés pedig talán nyilvánvaló: nem valódi magánhálózatról van szó, csak a nyilvánost használjuk úgy, mintha magán lenne. A titkosítás alapszolgáltatása a VPN-nek, de bizonyos körülmények (adatfolyamok elkülönítése, a hálózat logikai felépítésének egyszerűsítése) között titkosítás nélkül is használható.

A virtuális magánhálózatokat gyakran használják arra, hogy a vállalati erőforrásokhoz a dolgozók távolról hozzá tudjanak férni biztonságos módon. Így

akár otthonról, az interneten keresztül is kiépíthető egy biztonságos „alagút” a munkatárs és a vállalati környezetben működő VPN eszköz, úgynevezett koncentrátor között. A szolgáltatás tehát beépíthető hálózati eszközbe (például gyakran a router-be, illetve a tűzfalba), de megvalósítható szoftveres úton is.

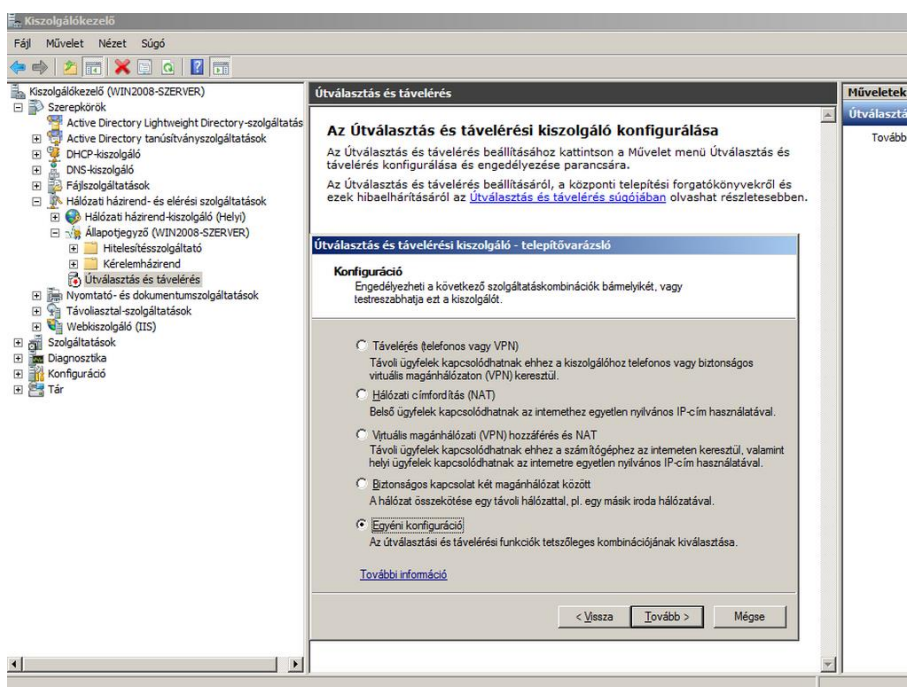
Az internetes kommunikáció során az IPsec használatával létrehozhatóak az alagutak, így minden ezen keresztül áthaladó csomag ugyanúgy néz ki, mint bármely másik adatcsomag. A csomagokban az egyetlen különbséget az jelenti (ahogy arról már volt szó), hogy az IP-fejrész után egy IPsec fejrész fog következni, de ez a különbség nem lesz hatással az üzenettovábbítás folyamatára, az útválasztók, tűzfalak működésére. Ennek a megoldásnak az egyik nagy előnye, hogy a felhasználók alkalmazásai számára is teljesen átlátszó marad az egész rendszer.

9.2.7. Virtuális magánhálózat a gyakorlatban

A Microsoft Server verziói képesek VPN kapcsolatok fogadására, kezelésére, nézzük meg, hogyan kell elvégezni a telepítést, konfigurálást. A szolgáltatás teljes kihasználásához szükséges az Active Directory használata is a kiszolgálón.

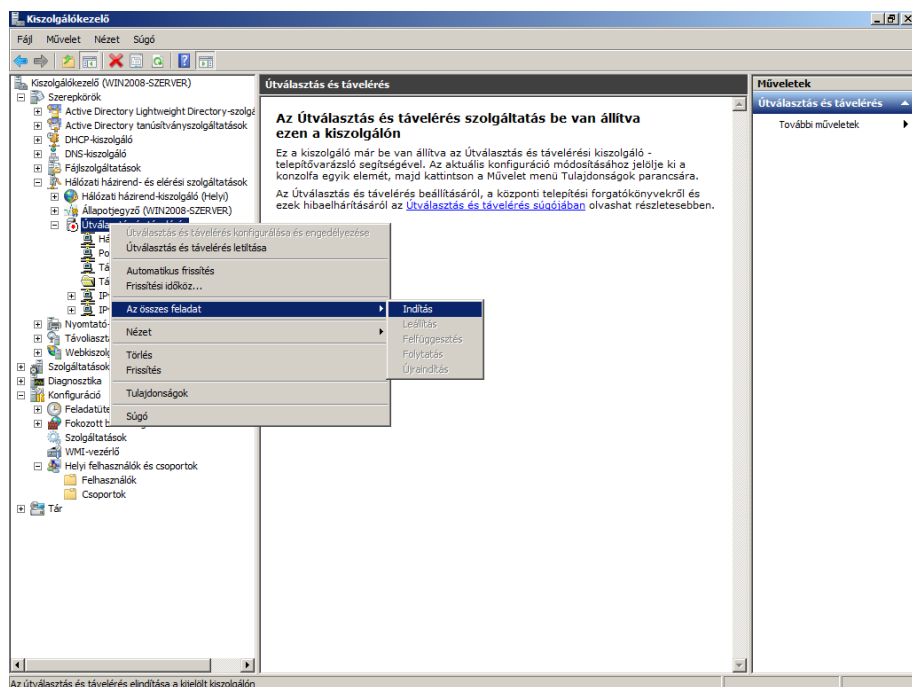
Telepítsük először a Hálózati házirend- és elérési szolgáltatások szerepkört a kiszolgálónkon. A folyamat során adjuk meg, hogy az Útválasztás és távelérés szerepkör is kerüljön engedélyezésre. A szerepkörök telepítése után kell elvégeznünk a megfelelő beállításokat.

A Kiszolgálókezelőben látni fogjuk a konzolfán az Útválasztás és távelérés ága, de még nem fut a szolgáltatás, ennek elindításához kattintsunk jobb egérgombbal a csomóponton, majd a megjelenő helyi menüben válasszuk az Útválasztás és távelérés konfigurálása és engedélyezése menüpontot! Újra egy varázsló indul el, amely segít elvégezni a megfelelő műveleteket. Az első ablakban válasszuk az Egyéni konfiguráció értéket.



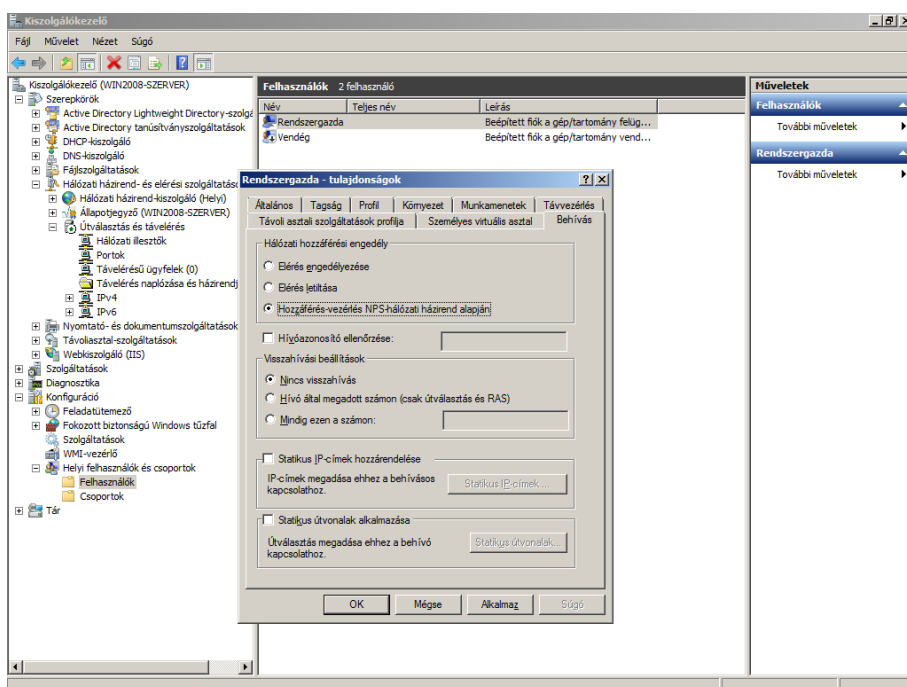
31. ábra: VPN telepítése Windows Server 2008 esetén

A következő ablakban választhatjuk ki ebben az esetben, hogy a virtuális magánhálózat kezelését szeretnénk a kiszolgálóra bízni. Ezzel gyakorlatilag be is fejeztük a telepítést, az operációs rendszer a szolgáltatást engedélyezi, az alapbeállításokat elvégzi, házirendeket létrehozza, de nem indítja el a szolgáltatást, ezt nekünk kell elvégeznünk.



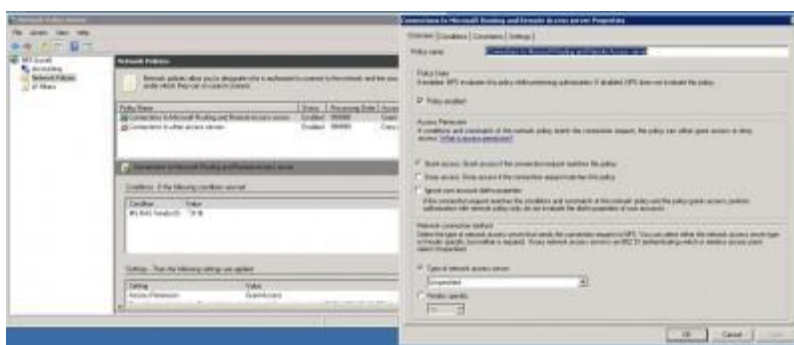
32. ábra: VPN szolgáltatás elindítása

A szolgáltatás elindítása után állítsuk be, hogy mely felhasználók létesíthetnek VPN kapcsolatot, ehhez az adott felhasználó tulajdonságlapját hívjuk elő, majd kattintsunk a Behívás fülre. Az engedélyezési folyamat nagyon egyszerű, válasszuk ki a Hozzáférés-vezérlés NPS-hálózati házirend alapján opciót.



33. ábra: Felhasználó VPN kapcsolatának engedélyezése

De mi az az NPS? Természetesen egy rövidítés, amely Network Policy Server elnevezést takarja a magyar nyelvű operációs rendszerekben. Itt tudjuk engedélyezni, hogy a távoli klienseink milyen szolgáltatásokhoz tudjanak kapcsolódni. A kép alapján engedélyezzük a hozzáférést.



34. ábra:

A VPN – mint a neve is mutatja – egy virtuális hálózathoz csatlakoztatja a számítógépünket. Mint minden hálózatban, itt is alapvető szükséglet egy IP cím, amint a virtuális hálózatba léptetett gépeink kommunikálni tudnak.

Most meg kell határoznunk, hogy milyen IP címtartományból kapjanak a klienseink címet. Két lehetőségünk van, az egyik a DHCP (ha rendelkezünk vele, pl.: a router-ünk is tud ilyet), a másik a kézzel beállított tartomány. Mindenki eldöntheti, hogy melyik a szimpatikusabb.

9.2.8. Hálózatvédelem Microsoft környezetben

A Microsoft kidolgozott modern operációs rendszereihez egy új megoldást, melyet Hálózatvédelemnek (Network Access Protection – NAP) neveztek el. A Hálózatvédelem egy olyan technológia, amely az ügyfél-állapotházirendek létrehozására, kényszerítésére és javítására szolgál, a Windows Vista, illetve későbbi verziók ügyfélként működnek, míg a Windows Server 2008 kiszolgálóként. A Hálózatvédelem alkalmazásával létrehozhatunk és automatikusan kényszeríthetünk az ügyfelekre állapotaházirendeket, amelyek tartalmazhatnak szoftverkövetelményeket, biztonsági frissítésekre vonatkozó követelményeket, a kötelezően szükséges számítógép-konfigurációra vonatkozó információkat és egyéb beállításokat. Az ügyfélszámítógépek, amelyek nem felelnek meg az állapotaházirendnek, korlátozott jogú hálózati hozzáférést kaphatnak addig, amíg a konfigurációjuk frissítése le nem zajlik annak érdekében, hogy megfeleljenek a házirendnek.

A NAP karantént vagy korlátozott hozzáférést képes kényszeríteni a következő hálózati kapcsolatok alapján:

- IPSec kapcsolatok
- Vezetékes kapcsolatok
- Vezeték nélküli (IEEE 802.11) kapcsolatok
- DHCP kapcsolatok
- Virtuális magán hálózatok
- HTTP-n alapuló kapcsolatok

A NAP alapján beszélhetünk az ügyfelek egészségi állapotáról (health status), illetve ezen állapot meglétét jóváhagyó úgynevezett egészségi állapotot jóváhagyó kiszolgálóról (Health Validation Server). A Hálózatbiztonság erre a kiszolgálóra támaszkodik annak érdekében, hogy meg tudja állapítani az ügyfél számítógépek egészségi állapotát.

Hogyan működik a NAP? Minden hálózati kapcsolat létrejötte előtt szükséges egy kérés az ügyféltől, aminek az NPS-en (Network Policy Server – Hálózati

háziprend-kiszolgáló) keresztül kell történnie (szerepkörként telepítendő a kiszolgálóra), és a következő módon kell működnie:

- Az ügyfél egy kérést küld a vezetékes vagy vezeték nélküli kapcsolatot használva.
- A kapcsolat fogadó fél (többféle eszköz, vagy szolgáltatás lehet, így DHCP, VPN, útválasztó, switch) ellenőrzi a hálózati háziprendet, hogy mi történjen a kéréssel.
- A háziprend-kiszolgáló (Network Policy Server) megadja a fogadó félnek a szükséges és helyes háziprendet.
- Az egészségi állapotot validáló kiszolgáló meghatározza az ügyfél egészségi állapotát, és ezt visszaküldi a fogadó félnek.
- Az ügyfél egészségi állapotától függően 2 döntés történhet:
 - Amennyiben az ügyfél nem tekinthető kellően egészségesnek, akkor csak korlátozott hálózati hozzáférést kap. A korlátozott hálózat karanténba helyezi az ügyfél rendszerét, amíg a teljes kapcsolódáshoz szükséges feltételek nem teljesülnek, az ilyen korlátozott hálózat csak a Windows Server Update szolgáltatásaihoz enged hozzáférést, illetve a naprakész állapot eléréséhez szükséges eszközökhöz. A NAP telepítésétől függően a nem megfelelő ügyfelek automatikusan frissíthetők, így a felhasználók gyorsan visszanyerhetik a teljes hálózati hozzáférést anélkül, hogy kézzel kellene frissíteni vagy újrakonfigurálni a számítógépeiket. Amint az ügyfél frissítése lezajlik, az egészségi állapota szintén újra ellenőrzésre kerül, így ha az új egészségi állapot megfelelő, akkor teljes hozzáférést kap a hálózathoz.
 - Ha az ügyfél állapota egészséges, akkor teljes hozzáférést kap a hálózat használatához.

9.2.9. DirectAccess szolgáltatás

A Microsoft a Windows Server 2008 R2 operációs rendszerében vezette be a DirectAccess szolgáltatását, amelynek segítségével a tartományhoz tartozó Windows 7 operációs rendszert futtató számítógépeknek lehetőségük van csatlakozni a belső hálózati erőforrásokhoz bármikor, bárhol, és ehhez nincs szükségük VPN kapcsolatra sem. A hálózati erőforrásokhoz úgy fér hozzá az internetre csatlakozott felhasználó, mintha közvetlenül a szervezet helyi hálózataán belül lenne, gyakorlatilag ugyanazokat a lehetőségeket veheti igénybe. További előnye a szolgáltatásnak, hogy az informatikai szakemberek számára a DirectAccess a külső mobil számítógépek, eszközök kezelését, menedzselését szintén lehetővé teszi. Minden alkalommal, amikor egy számítógép, amely tar-

tományi tag, csatlakozik az internethez, még mielőtt a felhasználó bejelentkezne, a DirectAccess szolgáltatás létrehoz egy olyan kétirányú kapcsolatot, amely lehetővé teszi az ügyfél eszköz számára, hogy teljesen friss legyen a hálózati házirendet illetően, és képes legyen szoftverfrissítéseket fogadni.

A DirectAccess biztonsági és teljesítménnyel kapcsolatos tulajdonságai közé tartozik a felhasználók hitelesítése, a titkosítás, és a hozzáférés-szabályozás. Megadható, hogy az egyes felhasználók melyik hálózati erőforrást vehetik igénybe, így természetesen akár teljes hozzáférés is adható, vagy esetleg csak néhány kiszolgálóra vagy hálózatra korlátozható a kapcsolódás. Könnyen szabályozható, hogy csak az olyan forgalom haladjon át a DirectAccess kiszolgálón, amelynek célja a vállalati hálózat, vagyis az internetes forgalmat eltereli, hogy az az ügyfél eszköz által használt átjárón keresztül haladjon.

A szolgáltatás az interneten keresztül folytatott kommunikáció titkosítására az IPsec-et használja, így alkalmazhatóak az IPsec titkosítási algoritmusai, mint a 3DES és az AES. Az ügyfelek létesítenek egy IPsec csatornát az IPv6 forgalom számára a DirectAccess kiszolgálóval, ez fog átjáróként szolgálni a vállalati környezetbe. Az ügyfelek természetesen akkor is képesek lesznek csatlakozni, ha tűzfal mögött vannak.

Apró hátrányként a DirectAccess használata megköveteli a legújabb operációs rendszerek, technológiák (így például az IPv6) használatát ügyfél oldalon is, ennek megfelelően a gyakorlatban egyelőre a VPN-nel együtt alkalmazzák.

9.2.10. Biztonságos csatlakozóréteg

Nagyon elterjedt megoldás a kommunikáció biztonságossá tételére az SSL nevű csomag használata, amely szinte minden platformon támogatott. Nem ebben a fejezetben fogunk róla bővebben beszélni, hanem a webbiztonságnál, mert bár az SSL nemcsak web-alapú kommunikációnál használható, jellemzően azért mai napig ott vesszük hasznát.

Az SSL-t a kifejlesztő cég, a Netscape átadta szabványosításra, így létrejött a TLS (Transport Layer Security – szállítási rétegbeli biztonság) protokoll, amely már nem kompatibilis a legújabb SSL verziókkal, viszont valamivel biztonságosabb megoldásnak tekinthető annál.

A TLS szintén ügyfél-kiszolgáló alapú alkalmazások számára teszi lehetővé a biztonságos kommunikációt, így biztosítva a lehallgathatóság és a hamisítás elleni védelmet. A kapcsolat létrehozásakor a kiszolgáló felé jelzi az ügyfél, hogy használni szeretne TLS-t. A kapcsolódás során az ügyfél és a kiszolgáló bizonyos paraméterek összehangolásával biztonságos kapcsolatot létesít egymással, ennek során az ügyfél egy listát biztosít a kiszolgáló számára az általa felhasz-

nálható titkosítási módszerekkel és hash függvényekkel. Ebből a listából a kiszolgáló a legerősebbeket fogja kiválasztani, majd elküldi a digitális aláírását, ami a nevéből, egy tanúsítványból és a kiszolgáló nyilvános kulcsából áll.

Az ügyfél ezután csatlakozhat, és elkészít egy munkafolyamat-azonosító kulcsot (session key). Ennek előállításához az ügyfél generál egy véletlen számot, amit titkosít a kiszolgáló nyilvános kulcsával együtt és ennek eredményét küldi a kiszolgáló számára, amit kizárólag az lesz képes visszafejteni a titkos kulcsa segítségével.

Ha a fenti műveletek közül valamely lépés nem sikeres, akkor a folyamat sikertelen lesz és a kapcsolat nem jön létre.

9.3. ÖSSZEFOGLALÁS, KÉRDÉSEK

9.3.1. Összefoglalás

A fejezetben azokat az összetett szoftvereket ismerték meg, amelyek a nyílt hálózatokon keresztül is képesek biztonságos kommunikációt biztosítani a részt vevők között.

Bemutattuk az IPSec működését, jelentőségét, használatát, hasonlóan a VPN általánosan használt eljárást is. Mindkét esetben a Microsoft rendszerein belül a telepítési, konfigurálási folyamatokat is. Ezen kívül szó volt olyan Microsoft termékekről, megoldásokról is, amelyek a legújabb operációs rendszerekben érhetőek el, nagyobb védelmet biztosítva a hálózati rendszereknek, így találkoztak a NAP és DirectAccess szolgáltatásokkal.

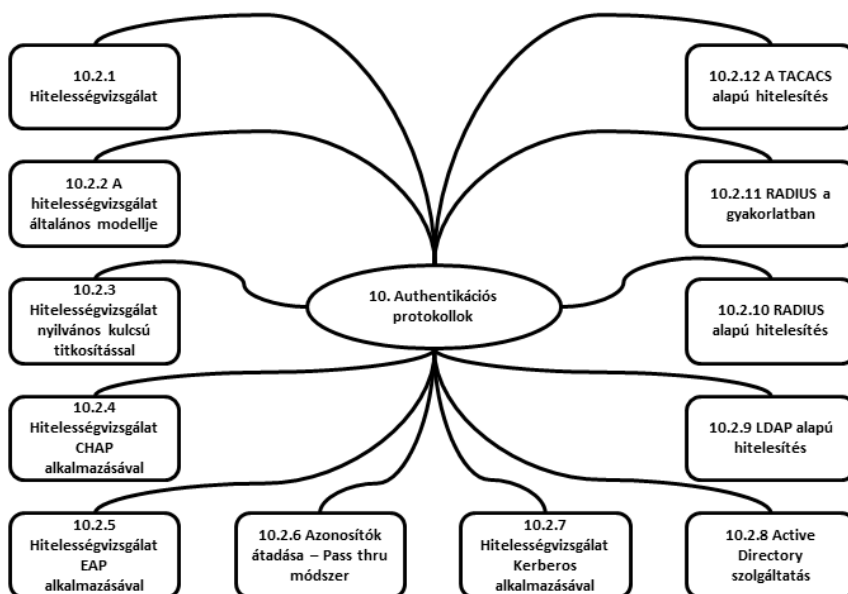
10 AUTENTIKÁCIÓS PROTOKOLLOK

10.1. CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

A fejezet célja a hitelességvizsgálat, az autentikáció megvalósítására szolgáló eljárások, módszerek megismertetése.

A hitelességvizsgálat általános modellje mellett a hallgatók megismerik azokat az általánosan elterjedt protokollokat, amelyek napjaink hálózati rendszereiben működnek. Tisztázzuk felhasználási lehetőségeiket, alkalmazásuk esetleges formáit, veszélyeit, hiányosságait. Bemutatjuk a címtárak jelentőségét, használatát, illetve a fejezet második felében természetesen a gyakorlatban is, hogy hogyan kell telepíteni, konfigurálni egyes összetevőket a Microsoft rendszereiben.

10.2. TANANYAG



10.2.1. Hitelességvizsgálat

A hitelességvizsgálat, vagy elterjedt kifejezéssel az autentikáció olyan módszer, informatikai eljárás, amelynek során ellenőrizhető, hogy a kommunikációban részt vevő partner ténylegesen az a személy-e, akinek mondja magát, nem pedig egy jogosulatlan egyén. A számítógépes hálózatokon egy ilyen azonosítás, ellenőrzés nem mindig egyszerű feladat, a rosszakaratú, támadásra alkalmas környezetben is biztonságos megoldások alapvetően titkosításra épülő, összetett protokollok segítségével valósíthatók meg.

Fontos tisztázni, hogy a hitelességvizsgálat nem egyezik meg a jogosultságvizsgálattal. A hitelességvizsgálat ténylegesen csak azt ellenőrzi, hogy a másik kommunikáló fél valóban az, akinek mondja magát. A jogosultságok vizsgálata a másik fél hatáskörének eldöntésére vonatkozik. Így például ha egy fájlserveren Albert felhasználó szeretne törölni egy adott állományt, akkor a kiszolgáló két feltételt ellenőriz:

- Tényleg Albert kérte a műveletet (hitelességvizsgálat)?
- Albert letörölheti-e az adott állományt jogosultságvizsgálat)?

A kérést csak az egyértelmű igenlő válaszok után szabad végrehajtani, de fontos tisztázni, hogy az első kérdés a lényegesebb, hiszen a másodikra a kiszolgáló már egy helyi táblázatban megtalálja a megfelelő bejegyzést.

10.2.2. A hitelességvizsgálat általános modellje

Nézzük meg, milyen módon működnek a hitelességvizsgáló protokollok. Első lépésben Albert felhasználó elküld egy üzenetet közvetlenül Bélának, vagy egy kulcsszétosztó központnak (Key Distribution Center – KDC), amelyről feltételezzük, hogy megbízható módon működik. A kezdőlépés után több üzenetváltás is lezajlik a felek között. Ha a protokoll tökéletesen működik, akkor Albert biztos lehet benne, hogy Bélával kommunikál, és Béla is biztos lehet benne, hogy Alberttel beszél.

A protokollok többségében a kapcsolatfelvételt követően létrejön egy olyan titkos viszonykulcs (session key), amely a két fél kapcsolatára jellemző, és a kapcsolat közben a párbeszédes folyamat közben használják. A gyakorlatban az adatforgalmat jellemzően titkos kulcsú titkosítással kódolják, mert ez hatékonyabban használható, miközben a nyilvános kulcsú titkosítás a hitelességvizsgáló protokollban és a viszony kulcs létrehozásánál játszik szerepet.

A véletlenszerűen választott viszony kulcs azért jó megoldás, mert használatával le lehet csökkenteni a felhasználó saját, titkos vagy nyilvános kulcsával kódolt adatcsomagok mennyiségét, így lehet csökkenteni a támadó által meg-

szerezhető titkosított szöveget. Másik előnye ennek a megoldásnak, hogy minimalizálni lehet a kárt, ha egy kommunikációs folyamat összeomlik, és rossz kezekbe kerülnek csomagok, memóriablokkok.

10.2.3. Hitelességvizsgálat nyilvános kulcsú titkosítással

A kölcsönös hitelességvizsgálat biztonságosan megoldható nyilvános kulcsú titkosítással, nézzük meg ennek a folyamatnak a lépéseit!

- Első lépésben szerezzük meg a másik fél tanúsítványát, és győződjünk meg a tanúsítvány érvényességéről. Így hitelesen hozzájutottunk a másik fél – tanúsítványba foglalt – nyilvános kulcsához, biztosak lehetünk benne, hogy az ténylegesen az ő nyilvános kulcsa.
- Generáljunk egy friss véletlen számot, és a másik fél nyilvános kulcsával titkosítsuk. Az így előállított értéket küldjük el a másik félnek.
- A másik fél – akit biztonságosan azonosítani szeretnénk – először az üzenetünkben szereplő véletlen számot a saját tanúsítványához tartozó titkos kulcsával visszafejti (ezt a kódolást csak ő tudja elvégezni, hiszen az ő tanúsítványához tartozó titkos kulcs kizárólag az ő birtokában van). Ekkor még a másik fél nem tudhatja, hogy tényleg hiteles a kérés.
- A másik fél szintén megszerzi a mi nyilvános kulcsunkat, és ezzel titkosítja az általunk generált véletlen számot, egy saját maga által létrehozott véletlen értéket, és egy viszonykulcsot. A kódolás eredményét visszaküldi nekünk.
- Megkapjuk a választ és saját titkos kulcsunkkal visszafejti. Amennyiben visszakaptuk az általunk generált véletlen számot, akkor már biztosak lehetünk a másik fél valóságában. Miért biztos ez? Azért, mert ez az üzenet csak tőle jöhetett, más nem tudta visszafejteni az általunk küldött üzenetet, kitalálni a véletlen számunkat.
- Utolsó lépésként elfogadjuk a viszonykulcs használatát, amit úgy jelzünk, hogy a viszonykulccsal kódoljuk a másik fél által küldött véletlen számot, ezáltal saját hitelességünket is bizonyítjuk.

Vegyük észre, hogy a hitelestés során kihasználtuk a nyilvános kulcsú titkosítást, de az adatok már titkos kulccsal kerülnek kódolásra.

Az ilyen eljárásokat nevezzük kihívás-válasz alapú protokolloknak.

10.2.4. Hitelességvizsgálat CHAP alkalmazásával

A CHAP (Challenge Handshake Authentication Protocol – kihívás alapú azonosítási protokoll), a Windows 2000 előtti operációs rendszerekben használt felhasználó-azonosítási protokoll, a kihívás-válasz elv alapján működik. Csak munkaállomásra történő belépésnél (tehát tartománynál nem) alkalmazzák. A titkosításnál egyszer használatos kulcsot vesznek igénybe a jelszó titkosítására, kombinálva egy hash algoritmussal. Három kézfogásos protokollnak is nevezik, szemben az úgynevezett, ma már egyáltalán nem biztonságosnak tekinthető két kézfogásos PAP (Password Authentication Protocol) protokollal.

A protokoll menete:

A munkaállomás egy üzenetet küld a kiszolgáló felé, amelyben jelzi a bejelentkezési szándékát. A kiszolgáló válaszként visszaküldi a hash kulcsot, ezt nevezik a szakirodalomban kihívásnak. A munkaállomás a kapott kulccsal titkosítja a jelszót, és kombinálva a felhasználói azonosítóval együtt elküldi a kiszolgálónak, ez lesz a válasz. Utolsó lépésként a kiszolgáló ellenőrzi a beérkezett adatsort a saját táblázatában található azonosítóval, és kódolt jelszóval, ha azonosak, akkor engedélyezi a kapcsolatot, különben elutasítja. A lényeg, hogy a jelszó titkosítva kerül továbbításra a hálózaton.

A protokollnak létezik egy MS-CHAP (MD4) nevű változata, amelyet a Microsoft rendszereiben használnak. A módszer jellemzője, hogy minden adat titkosítva kerül átadásra.

10.2.5. Hitelességvizsgálat EAP alkalmazásával

A CHAP hitelességvizsgálatnál némileg rugalmasabb az EAP (Extensible Authentication Protocol – bővíthető autentikációs protokoll) eljárás, amely valójában nem is egy protokoll, hanem keretrendszer. Az eljárás lehetőséget ad egyedi hitelesítési metódusok alkalmazására is (a beépítettek mellett), így képes többféle módszert támogatni, miközben nem szükséges az ügyfelekkel előre megállapodni annak használatáról. Az EAP hitelesítési eljárása hasonlít a CHAP három utas kézfogásához, ám annál jóval több lehetőséget biztosít a felek számára. A hitelesítést kérő és a hitelesítést végző fél többféle üzenetet küldhet egymásnak.

Az EAP támogatja hitelesítő szerverek alkalmazását, így lehetővé teszi a hálózati eszközök számára, hogy a protokoll összes metódusának ismerete nélkül átengedjék a csomagokat.

Az EAP lock-step protokoll, ami azt jelenti, hogy a hitelesítést kérő addig nem küldhet új kérést a hitelesítő felé, amíg nem kapott attól választ. A kérő

mindaddig újraküldi a kérést, amíg nem érkezik válasz, vagy belső számlálója már megtöltja az újabb kérés elküldését. Ez utóbbi esetben megszakad a kapcsolat időtúllépés miatt. Az újraküldött és új kérések szétválasztása a hitelesítést kérő feladata, ezt megoldandó minden kérésnek egyedi azonosítója van. A hitelesítést végző félnek minden beérkező kérést meg kell válaszolnia, attól függetlenül, hogy az új kérés, vagy megismételt.

Az EAP eljárást az említett kedvező tulajdonságai teszik alkalmassá, hogy megbízhatatlan hálózaton is megfelelően működjön. A WPA és WPA2 vezeték nélküli szabványok hivatalosan is tartalmazznak néhányat az EAP metódusaiból.

10.2.6. Azonosítók átadása – Pass thru módszer

Ezt az azonosítási formát tartományok esetében alkalmazzák, abban az esetben, amikor például az egyik munkaállomásról a másik munkaállomásra szeretne valaki bejelentkezni. A protokoll kezdeti lépései azonosak az előző autentikációs módszerrel, vagyis addig, amíg a kiszolgáló megpróbálja összehasonlítani a saját adataival a beérkezett azonosító, titkosított jelszó párost. Viszont az nem található meg a saját adatbázisában, ezért összecsomagolja a kulcsot és a kapott adatokat, és elküldi az egészet a tartományvezérőnek. A tartományvezérő ezután ellenőrzi a kapott azonosítót, titkosított jelszót, amelyet képes visszafejteni, hiszen a kulcsot is megkapta. Az autentikációs döntés ez alapján történik meg, és kap róla üzenetet mindkét munkaállomás.

10.2.7. Hitelességvizsgálat Kerberos alkalmazásával

A Kerberos autentikációs módszert az MIT kutatói fejlesztették ki, a fő cél az volt, hogy a felhasználók biztonságosan hozzáférjenek a kiszolgálón található erőforrásokhoz. Maga az eljárás szabadon alkalmazható, de vállalati környezetben is használják számos helyen, így a Windows operációs rendszerek is képesek alkalmazni hitelesítéskor.

A Kerberos-féle autentikáció lényege, hogy a felhasználó az úgynevezett Kerberos kiszolgálónál azonosítja magát, ahonnan cserébe egy TGT-t (Ticket-Granting Ticket), azaz egy személyazonosság igazoló jegyet kap. Innentől kezdve a felhasználó ezzel az azonosítási jeggyel kaphat további jegyeket a többi számítógép szolgáltatásainak igénybeviteléhez.

A Kerberos eljárás során három komponenst használunk:

KDC (Key Distribution Center): a jegyek továbbításához szükséges titkosító kulcsok (session key, process key) generálását, karbantartását végzi.

AS (Authentication Service): a felhasználó kezdeti azonosítását végzi. Az azonosítás után kapja meg a felhasználó a TGT-t.

TGS (Ticket-Granting Service): a TGT birtokában innen igényelhet további jegyeket a felhasználó a különböző szolgáltatásokhoz (sőt elvben a saját számítógépéhez is.).

Titkosításhoz 3DES-t, azaz szimmetrikus kulcsot használnak. A titkosítás elvégzéséhez a kulcsot mindkét félnek ismernie kell, érdekes megoldásként a felhasználó jelszava a kulcs.

A protokoll működése röviden:

Felhasználó felveszi a kapcsolatot az AS-sel, titkosított módon. A kulcs (nevezük K1-nek) lesz a felhasználó jelszava.. Amennyiben a felhasználói jelszóval lehet dekódolni az átküldött adatokat, akkor az eljárás folytatódik. Következő lépésben az AS új kulcsot kér a KDC-től, ez lesz a K2. A felhasználó megkapja a TGT-t, benne a K2 kulcs értékével, a küldés során ezt az üzenetet K1-gyel titkosítják. A felhasználó a TGT birtokában a TGS-től tud igényelni további jegyeket (hozzátartozó kulcsokkal együtt) az egyes szolgáltatásokhoz.

10.2.8. Active Directory szolgáltatás

A Microsoft operációs rendszerei önállóan képesek kezelni a hitelesítési folyamatot, vagyis rendelkezhetnek saját adatbázissal, amelyek tárolják a felhasználók azonosító adatait, illetve azontúl egyéb információkat is. Nagyobb hálózatban (például vállalati környezetben) már elvárás az SSO (Single Sign-On – Egyszerűsített bejelentkezés) megvalósítása, vagyis amikor a különböző hálózati erőforrások használatához nem kell külön-külön bejelentkeznünk a kiszolgálókra, hanem egy egyszeri bejelentkezés során megkapjuk az összes jogosultságunkat.

A címtár-szolgáltatás Windows Server operációs rendszereken telepíthető, a Microsoft Active Directory névvel látta el ezt a terméket, de gyakran az AD rövidítéssel hivatkozunk rá. A címtárfán belül úgynevezett tartományok jönnek létre, az egyes tartományokon belül lehet létrehozni és konfigurálni a különböző hálózati objektumokat, így a felhasználókat és a számítógépeket is. A hálózaton belül ezek után kikényszeríthető, hogy a felhasználói számítógépekre is csak az AD keretein belül rögzített felhasználók tudjanak belépni, viszont ők ezzel az egyszeri belépéssel megkapják a tartományon belül a jogosultságokat, akár különböző hálózati erőforrásokhoz is.

Az AD szolgáltatás további előnye, hogy a távfelügyelet automatizálható, a már megismert helyi házirendek kiszélesíthetőek, a kiszolgálón található, előre beállított értékek terjesztésével a munkaállomások is egységesen és biztonságosan lesznek használhatóak. A központi nyilvántartás megkönnyíti a felhasználók és a rendszergazdák munkáját is.

A felhasználónak bejelentkezéskor az AD használatakor nem elég megadnia a nevét és jelszavát, hanem jeleznie kell azt is, hogy melyik tartományban található a fiókja. Az autentikációs folyamat során egyébként a Kerberos protokollt használja a Microsoft, de maga a címtár elérhető LDAP-on keresztül is, amelyről a következő alfejezetben lesz szó.

10.2.9. LDAP alapú hitelesítés

A directory (magyarul címtárfaként emlegetjük, vagy beszélhetünk „directory service”-ről, címtárszolgáltatásról) egy hierarchikus adatbázis, amely a relációs adatbázistól eltérően nem táblákba, sorokba, oszlopokba szervezve, hanem egy gráfhoz hasonló felépítésében ágakra bomló rendszerben tárolja az adatokat. Jellemzően olyan környezetben használjuk, ahol az alkalmazott lekérdezések száma jóval meghaladja a változtatások számát, illetve maga a lekérdezés egyszerű művelet, és általában minél kisebb válasszal jár. Az autentikáció biztosítása pontosan ilyen művelet, ezért jól használható a címtárfa a hitelesítés során.

Az LDAP (Lightweight Directory Access Protocol) egy protokoll, és nem egy konkrét termék. LDAP alapú kiszolgáló szabadon elérhető verziói is léteznek, a Microsoft termékei közül az Active Directory tekinthető címtárfa alapú megoldásnak.

Az LDAP használatához szükséges a TCP/IP alkalmazása, arra épülően lehet a protokoll segítségével lekérdezni, (esetlegesen keresni, megváltoztatni) a kiszolgálóként funkcionáló címtárakat, az abban tárolt adatokat (az azonosító adatokon túl akár egyéb tulajdonságokat, például e-mail címet, jogosultságokat). A hierarchián belül a következő rövidítések értelmezését célszerű megtanulni:

- DC (Domain Context): Tartományi környezet, a tartomány nevét írja le.
- OU (Organization Unit): Szervezeti egység, amennyiben az elérni kívánt objektum a tartományon belül valamely szervezeti egységben található, akkor DC jelölése mellett az OU-t is meg kell adni.
- CN (Common Name): Közös név, kötelező elem minden lekérdezésnél, az erőforrás objektumokra és típus nélküli tárolókra tudunk hivatkozni.

10.2.10. RADIUS alapú hitelesítés

A RADIUS (Remote Authentication Dial-In User Service) protokollt 1991-ben dolgozták ki, tehát egy aránylag „koros” hitelesítési megoldásnak tekinthető, ennek ellenére jelenleg is az egyik legnépszerűbb módja a bűjtött hálózati

kapcsolatok felhasználóinak hitelesítésére illetve a kapcsolatok kiépítésének engedélyezésére. A RADIUS szervereket eredetileg a különböző Internet Szolgáltatók (ISP) használták ügyfeleik jelszavas hitelesítésére, még a felhasználónak a szolgáltató hálózatába történő belépése előtt.

A nem Windows alapú rendszereken gyakran használják a távélérésű ügyfelek hitelesítésére, ebből adódó népszerűsége megkövetelte, hogy a Microsoft operációs rendszereiben is elérhető legyen. Legfőbb jellemezője napjainkban is a széleskörű alkalmazhatósága, így vezeték nélküli, 802.1x alapú, VPN, de akár betárcsázásos kapcsolatokban is használhatjuk a bejelentkezni kívánó ügyfelek hitelesítésére.

A RADIUS hitelesítési eljárásának első lépéseként a távoli felhasználó kérést küld a kiszolgáló felé. A felhasználónál a RADIUS ügyfél programja működik, míg a szerveren a kiszolgáló oldali megfelelő. A hitelesítési folyamat többféle protokollt képes támogatni, például az előzőleg már ismertetett CHAP felhasználható az elküldött hitelesítési információk titkosítására. Az ügyfél tehát összeállítja a kiszolgáló felé továbbítandó csomagot, ami tartalmazza a felhasználó nevét, jelszavát, a RADIUS ügyfél azonosítóját és esetlegesen egyéb attribútumokat. A jelszó titkosítását a CHAP végzi el, az MD5 eljárással.

Az így összeállított csomag eljut a kiszolgálóhoz, a RADIUS szerver fogadja az ügyfél kérését, feldolgozza azt. Ellenőrzést végez, hogy valóban az adott ügyféltől érkezett-e a csomag, így kizárja, hogy a kommunikáció során valaki módosítsa és továbbküldje a kiszolgáló felé. A biztonság tovább növelhető, ha az ügyfél rendelkezik digitális aláírással, mert a RADIUS szerver képes ellenőrizni azt is. Ezután következik az elküldött felhasználói név ellenőrzése, a nevet meg kell keresni a helyben tárolt felhasználói adatbázisban, vagy valamilyen központosított címtárban, ehhez használhat akár SQL-t, Kerberost, LDAP-ot, de összekapcsolható Active Directory-val is. A felhasználói név megtalálása után dekódolásra kerül a jelszó és megtörténik annak a helyességének az ellenőrzése is.

A RADIUS kiszolgáló az ügyfél kérésére három féle módon válaszolhat:

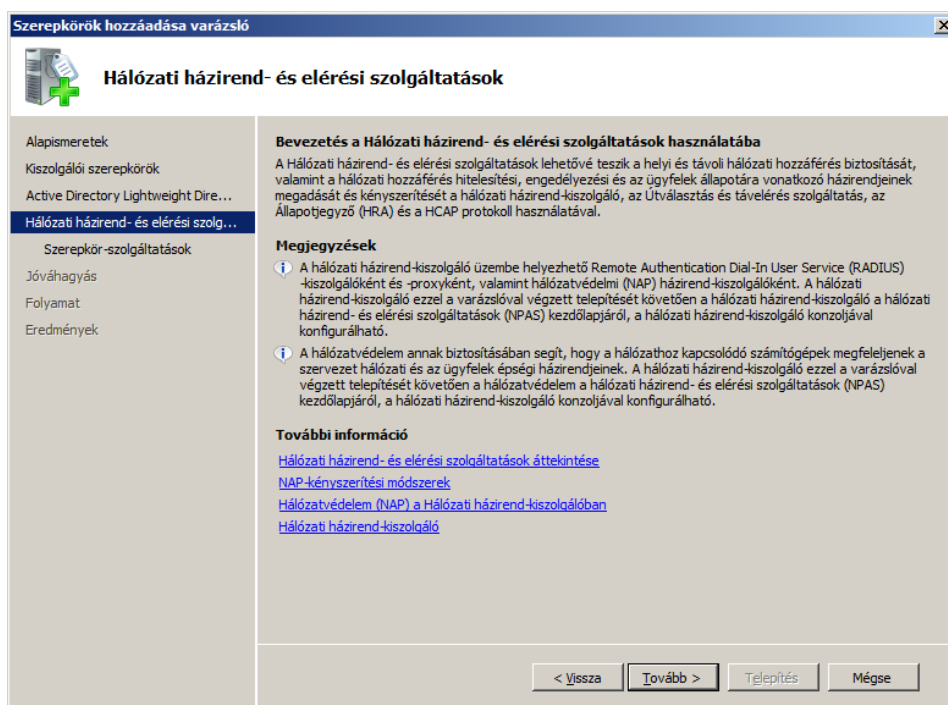
- Ha minden rendben van, összeállít a kiszolgáló egy csomagot, amelyben jelzi a bejelentkezés sikerességét, egy listát a RADIUS attribútumokról és minden szükséges adatot az adott szolgáltatások eléréséhez.
- Előfordulhat, hogy a hitelesítési folyamathoz nem elég a felhasználói név, jelszó páros, hanem további azonosítók megadására van szükség, ebben az esetben a kiszolgáló egy „kihívás” csomagot küld az ügyfélnek. Az ügyfélnek ezután a sikeres hitelesítéshez meg kell adnia a kért adatokat, amely lehet egy másodlagos jelszó, egy PIN-kód, vagy akár valamilyen token, például egy chipkártya.

- A kiszolgáló, amennyiben nem teljesül minden feltétel, akkor is összeállít egy csomagot, amelyben közli az ügyféllel a hitelesítési folyamat sikertelenségét, vagyis elutasítja a bejelentkezést.

10.1.11. RADIUS a gyakorlatban

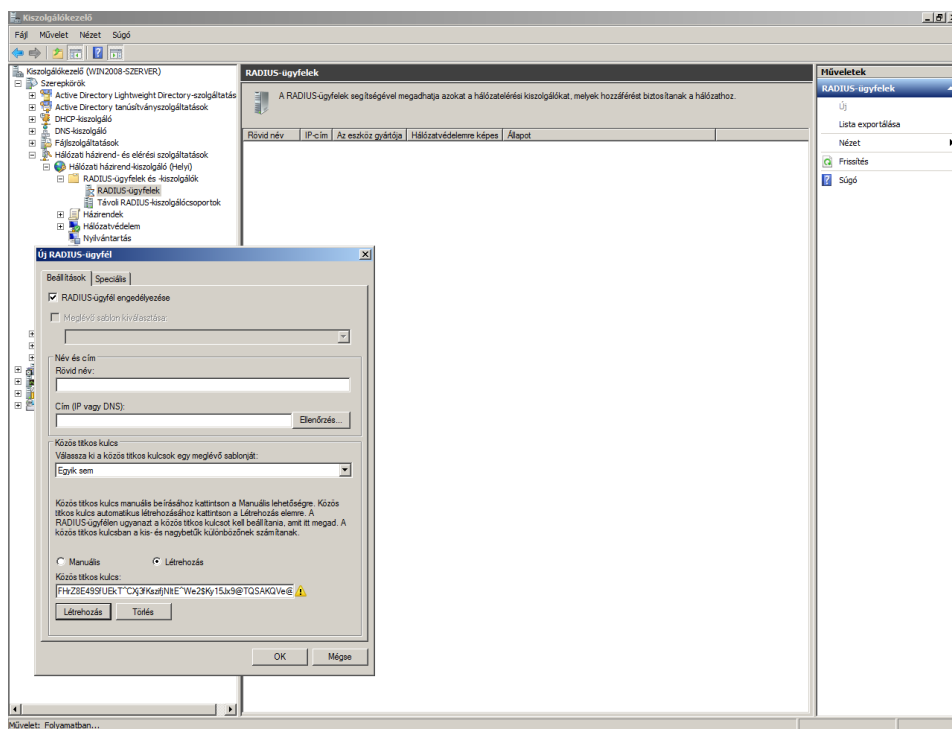
A RADIUS csomagok továbbítása a kiszolgáló és az ügyfél között nem a TCP, hanem az UDP használatával történik alapértelmezésben az 1812-es és 1813-as portcímeken. Az 1812-es portot az autentikációs, az 1813-as portot pedig a fiók üzenetek továbbítására használják. A portok értékét figyelembe kell venni a hálózatunk tervezésénél, a tűzfalakat és egyéb hálózati eszközöket ennek megfelelően kell konfigurálnunk.

A RADIUS kiszolgáló Windows operációs rendszerben a szerver kiadásokban található meg, szerepkörként kell telepítenünk, utána használható a hálózatunkon hitelesítési megoldásként. Indítsuk el a Szerepkörök hozzáadása varázslót, majd adjuk hozzá rendszerünkhöz a Hálózati házirend- és elérési szolgáltatások szerepkört.



35. ábra: RADIUS telepítése Windows Server 2008 esetén

A telepítés után azonnal igénybe is vehetjük a szolgáltatást, természetesen kiszolgálói oldalon néhány opciót meg kell adnunk! A Kiszolgálókezelőben, a Hálózati házirend- és elérési szolgáltatások ágon belül jelenik meg a Hálózati házirend-kiszolgáló funkció, amelyen belül tudjuk konfigurálni a RADIUS-ügyfeleket. Ezt a műveletet egy párbeszédablakban végezhetjük el:



36. ábra: RADIUS-ügyfél konfigurálása

Alapértelmezett opcióként engedélyezzük az ügyfelet, majd adhatunk egy rövid nevet, amellyel azonosíthatjuk a klienst. Meg kell adnunk a RADIUS-ügyfél IP-címét, vagy DNS nevét, illetve a használandó közös kulcsot, ezt természetesen majd a klienshez el kell juttatni. A kulcsot vagy manuálisan begépeljük, vagy egyszerűbb módon létrehozhatjuk a rendszerünkkel.

Az ablak Speciális fülén található a Szállító neve opció, amellyel megadhatjuk, hogy milyen gyártó általi RADIUS megoldást akarunk használni. Egy bő listából választhatunk, de ha nem vagyunk biztosak az ügyfél gyártójában, akkor nyugodtan válasszuk a (egyébként alapértelmezett) RADIUS Standard értéket.

A Windows server úgynevezett RADIUS-proxy-ként is üzemelhet, ekkor a beérkező csatlakozási kérélmeket továbbítja a beállított RADIUS-kiszolgálók

felé, amelyek képesek lesznek a kérelmek feldolgozására. A beállítás elvégzéséhez a Távoli RADIUS-kiszolgálócsoporthoz ágon belül kell megadnunk a szükséges tulajdonságokat, alapvetően a kiszolgáló címét, de beállíthatunk prioritásokat is, így a hálózaton belüli terheléelosztást is optimalizálhatjuk.

10.2.12. A TACACS alapú hitelesítés

A TACACS (Terminal Access Controller Access Control System) protokoll, mint az a nevéből is látszik, alapvetően terminálkiszolgálókra és hálózati útválasztókra való belépéseket tud kezelni.

Három típusa létezik:

- TACACS: Az eredeti protokoll, amelyet a Cisco vállalat vezetett be 1989-ben. A hitelesítés a következő módon történik: a felhasználó jelzi belépési szándékát a hálózati eszköz felé, amely ekkor bekéri a felhasználó nevét és a jelszavát. Ezután egyezteteti azokat egy TACACS kiszolgáló jelszó állományával. Amennyiben a felhasználói név és a jelszó érvényes a kiszolgáló engedélyezi a belépést, a felhasználó használhatja az eszközt.
- XTACACS (eXtended (kiterjesztett) TACACS): A TACACS protokoll továbbfejlesztése, amely 1990-ben került bevezetésre. Főbb újdonságai a rendszer naplóállományainak UNIX rendszernaplókba küldése, a beléptetett felhasználó shell-t kap az eszközön és ezután tud például telnetet, vagy egyéb kapcsolatot kezdeményezni, továbbá lehetőség nyílik több TACACS kiszolgáló használatára. Ez a verzió már multiprotokollos, tehát különböző típusú kapcsolatokra lehet vele engedélyt adni.
- TACACS+ (TACACS plusz): Ez a verzió lehetőséget biztosít arra, hogy egy különálló kiszolgáló végezze az autentikációt, az engedélyezést és a naplózást. A TACACS+ protokoll a felhasználóneveket és a jelszavakat MD5 kódolással küldi át a hálózaton. A TACACS+ képes továbbítani a különböző típusú jelszavakat, ezáltal lehetővé válik, hogy a felhasználók ugyanazzal a névvel és jelszóval többféle protokollt is igénybe vegyenek. A TACACS+ nyílt protokoll, bővíthető, így új jelszótípusokat is könnyen integrálhatnak bele, ami azt is jelenti, hogy bármilyen jelszó-adatbázissal alkalmazható, összekapcsolható.

10.2. ÖSSZEFOGLALÁS, KÉRDÉSEK

10.2.1. Összefoglalás

A fejezet a hitelességvizsgálat, az autentikáció általános modelljét, illetve ahhoz kapcsolódva a mai hálózati rendszerekben előforduló, használatban lévő

protokollokat, szolgáltatásokat mutatta be, melyek során a hallgatók megismerték azok működését, főbb tulajdonságait, alkalmazási lehetőségeit.

Az elméleti leírásokon túl a Microsoft rendszerein keresztül gyakorlatban is bemutatásra került, hogy hogyan lehet telepíteni, konfigurálni a szolgáltatásokat.

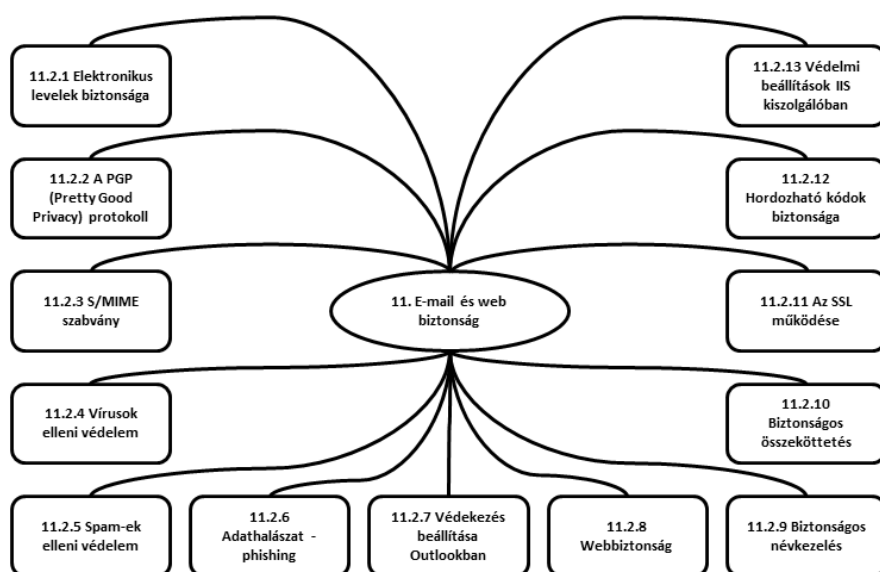
11 E-MAIL ÉS WEB BIZTONSÁG

11.1. CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

Bemutatjuk azokat a szabványokat, protokollokat, amelyek képesek biztonságot nyújtani a szolgáltatások használata esetén. Ismertetjük azokat a veszélyeket, módszereket, amelyek ellen védekeznünk kell, természetesen a védelmi megoldásokkal együtt.

A webbiztonsággal kapcsolatban elsősorban az SSL megoldást mutatjuk be, amely a legelterjedtebb biztonsági formula a weben.

11.2. TANANYAG



11.2.1. Elektronikus levelek biztonsága

Az elektronikus levelek küldése jelenleg is az egyik legnépszerűbb szolgáltatása a számítógépes hálózatoknak, rengetegen használják nap, mint nap, ami természetesen a támadók számára is kiváló vadászterület. Egy-egy elküldött elektronikus levél útja a címzettig akár több tucat közbeeső gépen keresztül is

mehet, mindegyik olvashatja, tárolhatja, módosíthatja ezeket az üzeneteket. Sokan ezt elfelejtik, vagy nem is tudnak róla.

Akik viszont ismerik ezt a tényt, közülük sokan szeretnének mégis olyan kommunikációt, amellyel biztosak lehetnek abban, hogy senki nem tudja elolvasni az üzenetet a címzetten kívül. Ennek a váagnak köszönhetően a biztonságos elektronikus levelek előállítása érdekében sokan használnak az előzőekben megismert titkosítási, hitelességvizsgálati megoldásokat, protokollokat.

A következőkben erre fogunk kitérni: milyen módon védhetjük meg üzeneteinket!

11.2.2. A PGP (Pretty Good Privacy) protokoll

A PGP (Pretty Good Privacy – elég jól biztosított személyiségi jog) protokollt Philip R. Zimmermann 1991-ben tervezte adattitkosítás és hitelesítés céljára. Leggyakrabban e-mailek aláírására, titkosítására használják, nagyon népszerű megoldás, mert ingyenesen használható és egyike a legstabilabban működő hálózatbiztonsági protokolloknak. Az eljárást kezdetben elektronikus üzenetek és hozzájuk csatolt állományok titkosítására, tömörítésére, hitelességvizsgálatra alkalmazták, de mára egyéb funkciókkal is kiegészítették, így például használható mappák, merevlemezek titkosítására, digitális aláírások kezelésére is. Napjainkban több operációs rendszerben beépítve megtalálható.

A PGP működése a kétféle titkosítási módszer egyesítésével létrehozott úgynevezett hibrid titkosításon alapul. A protokoll egyesíti a szimmetrikus titkosítás gyorsaságát és az aszimmetrikus titkosítás biztonságát. A PGP a kódolási eljárás során tömöríti a titkosítani kívánt üzenetet vagy adatot, ezután egy véletlen generálású kulccsal titkosítja. Ez a művelet még akár nagy mérettel rendelkező üzenet vagy adatsor esetében is gyorsnak tekinthető, hiszen szimmetrikus algoritmussal történik a kódolás. A következő lépésben a kulcs maga kerül titkosításra, ezt azonban már az aszimmetrikus titkosításból ismert nyilvános kulccsal végzi a protokoll. Így jön létre egy olyan adatcsomag, amelyre jellemző, hogy tartalmazza a titkosított üzenetet, adatot, illetve a visszafejtéshez szükséges kulcsot – titkosítva.

A PGP eljárás lépései:

- Tömörítés
- Szimmetrikus titkosítás egy véletlen generálású kulccsal
- A véletlen generálású kulcs titkosítása a címzett nyilvános kulcsával (aszimmetrikus titkosítás) – mivel a kulcs kis méretű, a titkosítás gyorsan megtörténik

- Küldés

A protokollt megvalósító programok minden operációs rendszeren elérhetőek, illeszthetőek akár a különböző elektronikus levelezést támogató ügyfél-programokhoz.

11.2.3. S/MIME szabvány

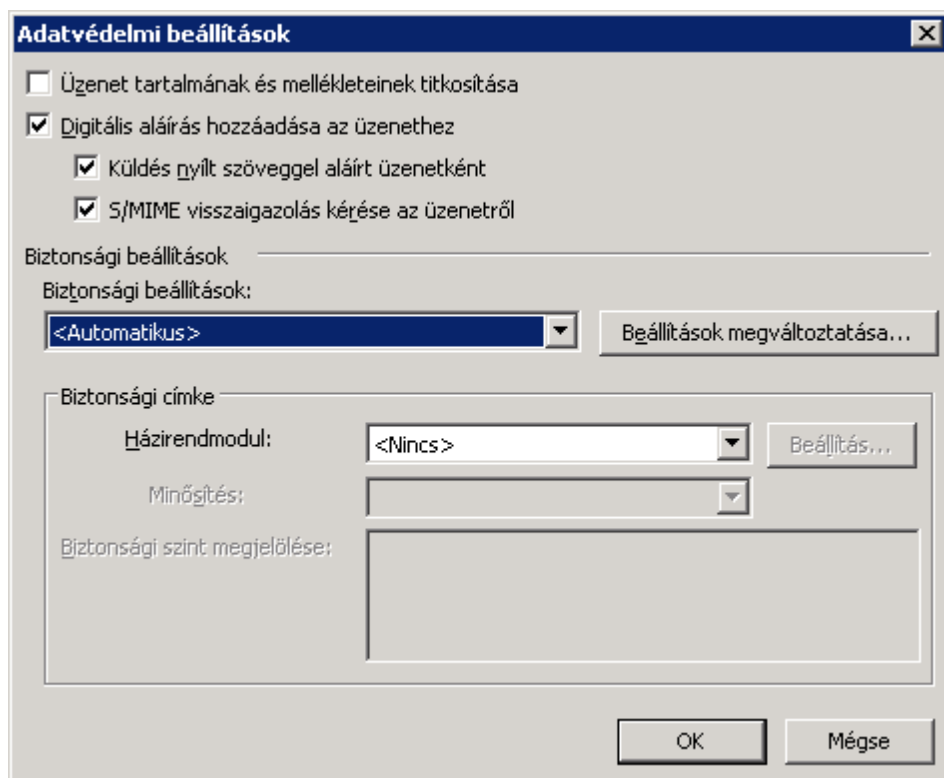
Az elektronikus levelekhez alkalmazható az S/MIME (Secure Multipurpose Internet Mail Extensions) szabvány is titkosításra. Az S/MIME célja, hogy egyszerűen lehessen üzeneteket elküldeni, oly módon, hogy biztonságban legyenek az illetéktelen személyek elől. A szabványt úgy tervezték, hogy bármilyen üzenetküldésre alkalmas formátumba egyszerűen beilleszthető legyen.

Az S/MIME a PGP-hez hasonlóan egy hibrid rendszer, amely egy „biztonságos borítékba” zárja a titkosított üzenetet, illetve az üzenet készítőjét hitelesítő tanúsítványt. Az üzenet titkosítása szimmetrikus algoritmussal készül, de a titkosítás során használt titkos kulcs kódolása már elektronikus aláírással van ellátva, vagyis aszimmetrikus titkosítás történik. Az elektronikus aláírás fogja megvédeni az üzenet és a boríték sérthetetlenségét. Az S/MIME más szabványok használatával készült, ez biztosítja széles körű használatot, alkalmazhatóságot.

Nézzük meg, hogyan lehet az Outlookban alkalmazni az S/MIME szolgáltatást!

Az S/MIME visszaigazolással olyan levelezési biztonsági szolgáltatáshoz jutunk, amellyel megerősítés kérhető arról, hogy az elektronikus üzenetünk módosítás nélkül megérkezett a címzetthez. Információt tartalmaz arról is, hogy ki és mikor nyitotta meg az üzenetet. Ezek az ellenőrző információk válaszüzenetként fognak megjelenni a Beérkezett üzenetek mappánkban. Az S/MIME visszaigazolás kérésében szerepelnie kell a digitális aláírásnak, ezért S/MIME visszaigazolás kéréséhez mindenképp digitális azonosítóval kell rendelkezünk.

Amennyiben az üzenetet S/MIME visszaigazolás kérésével szeretnénk küldeni, az Outlook Adatvédelmi beállítások ablakában el kell végezni a megfelelő beállításokat. Ezt megtehetjük üzenetenként is, vagy automatikusan az össze üzenetre vonatkozóan.



37. ábra: S/MIME visszaigazolás kérése

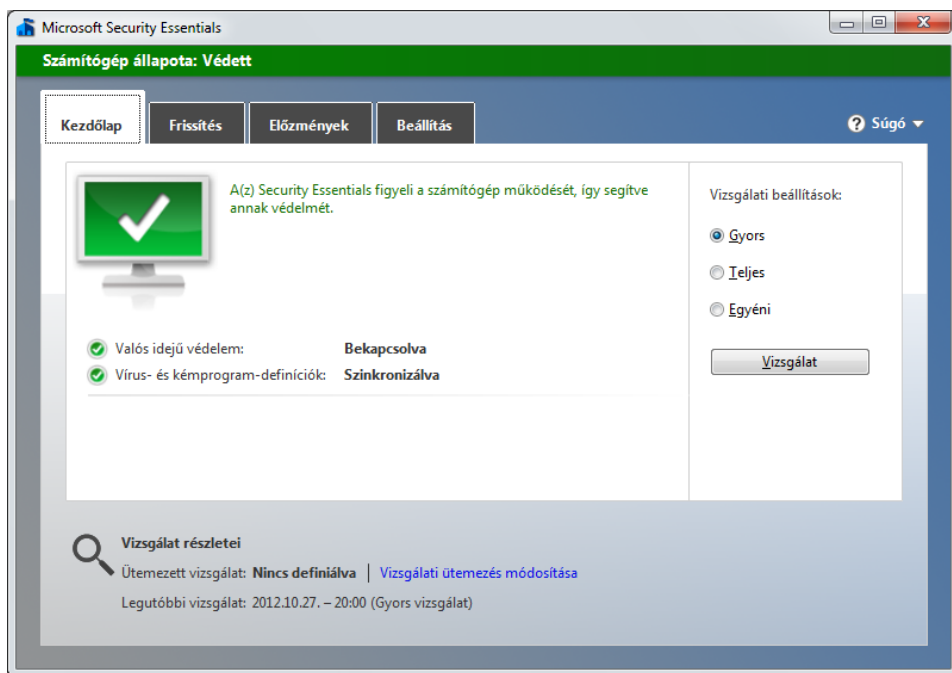
11.2.4. Vírusok elleni védelem

Jelenleg a vírusok jellemzően elektronikus levelek csatolmányaként terjednek, ez a leggyorsabb és leghatékonyabb módszer a terjesztésre.

A vírusok elleni védelem első vonalába célszerű egy antivírus alkalmazást telepíteni, megfelelően konfigurálni és használni. Ma már komplex, több területet (nemcsak az elektronikus levelezést védő) szoftverek állnak rendelkezésre, amelyek képesek hatékonyan ellenőrizni a beérkező üzeneteket.

A Microsoft az operációs rendszereihez ingyenesen elérhetővé és használhatóvá tett egy szolgáltatást, amely képes a vírusok és kémprogramok ellen hatékonyan védekezni. A Microsoft Security Essentials névre keresztelt termék letölthető⁹ és egyszerűen telepíthető operációs rendszerünkre. Használata nagyban hasonlít az egyéb antivírus alkalmazásokra, külön nem térünk ki rá.

⁹ <http://windows.microsoft.com/hu-HU/windows/security-essentials-download> 2012. május 16.



38. ábra: Microsoft Security Essentials kezelőablak

Fontos azonban tisztázni, hogy az elektronikus levelek szabványa szerint maga az üzenet mindig egy egyszerű szöveges állomány, ami önmagában nem képes futtatható kódot, így vírust sem hordozni.. Vagyis a vírusok csak az üzenethez csatolt állományokban lehetnek. Ez azt is jelenti, hogy a levelező kliensünkben nyugodtan megjeleníthetjük az üzenet tartalmát, csak a csatolt állományokkal vigyázzunk, csak megbízható forrásból származó fájlt töltsünk le, nyissunk meg, futtassunk, de azt is csak abban az esetben, ha előre megbeszéltük, esetleg az üzenetben szó van a mellékelt állományról. Miért? Mert ha a megbízhatónak vélt személy eszköze mégis megfertőződött, akkor a vírus onnan továbbküldi magát az ottani címlista alapján, de valószínűleg az üzenet szövegtartalma gyanús lesz!

Hasonlóképpen bizalmatlanul viszonyuljunk az üzenetben szereplő esetleges hiperhivatkozásokhoz, nem szabad felelőtlenül rákattintani, amíg nem győződünk meg arról, hogy biztonságos weboldalra jutunk, és nem egy vírusos állományt nyitunk meg.

Az ügyfél oldal mellett egyébként ma már gyakran alkalmaznak antivírus szoftvereket a levelezőszervereken is, ezzel is védve a felhasználókat.

11.2.5. Spamek elleni védelem

Mindenki, aki rendszeresen végez elektronikus levelezést, belefutott már spamekbe. A nagyon jól használható szolgáltatásnak sajnos van ilyen mellékága is, amelyet többféle céllal hoznak létre. A spa-ek az úgynevezett nem kívánt levelek, amelyeket szándékunk ellenére kapunk meg, legtöbbször valamilyen reklámüzenetként.

Hogyan működik? Automatikus programok megszereznek minél több e-mail címet (címlistákból, weboldalakról), majd gyakran fertőzött számítógépről küldik ki tömegesen az üzeneteket. Miért fertőzött gépekről? Mert a védekezés egyik módja, hogy úgynevezett fekete listákat (Real-time Black List – RBL) kezelnek központilag, ahová olyan címek kerülnek fel, amelyek aktív spam tevékenységet folytatnak.

A védekezés módja, hogy spamszűrő szoftvereket telepítünk, amit az antivírus programokhoz hasonlóan használhatunk az ügyfél gépeinken, illetve már magán a kiszolgálón is. A spamszűrők képesek a fekete listákkal összevetni a beérkező leveleket, és döntést hozni, hogy a levél spamnak minősüljön-e? A kiszolgálón futó szűrés hatására a spamnek minősített üzenetek el sem jutnak a felhasználóhoz. Ennek veszélye, hogyha esetleg téved a minősítés, akkor a hasznos levelet sem kapjuk meg. A helyi szűrők egy külön mappába teszik az általuk spamnek minősített leveleket, így nem okoznak bajt, de a felhasználó időnként ellenőrizheti, hogy ténylegesen nem kívánt üzenetek-e?

11.2.6. Adathalászat – phishing

Adathalászatnak nevezzük azt az eljárást, amikor egy csaló olyan weboldalt készít, üzemeltet, amely egy jól ismert cég, szervezet (például valamelyik bank) hivatalos oldalának tűnik, gyakorlatilag másolata annak, és megpróbál érzékeny személyes adatokat, például felhasználói azonosítót, jelszót, esetleg bankkártya adatokat illetéktelenül megszerezni.

A támadó első lépésben terjeszti a weboldala elérhetőségét, ehhez általában e-mailt vagy azonnali üzenetet küld a címzettnek, amiben valamilyen okkal (sokszor emberi tulajdonságokat kihasználva sok pénz ígéretével) ráveszi, hogy klikkeljen az üzenetben szereplő hiperhivatkozásra. Így az áldozat eljut az átalakított weblapra, ami külsőleg szinte teljesen megegyezik az eredetivel, és ha nem ismeri fel a csalást, akkor adatait begépezi a megadott űrlapokon, átadva azokat a támadónak.

Ez a támadás már összetettebb, de legjobb védekezés, ha figyelünk, és nem is kattintunk a gyanús levelekben található linkekre. Mitől gyanús egy levél? Ha a szövegben látható a magyartalanság, az automatikus gépi fordítás,

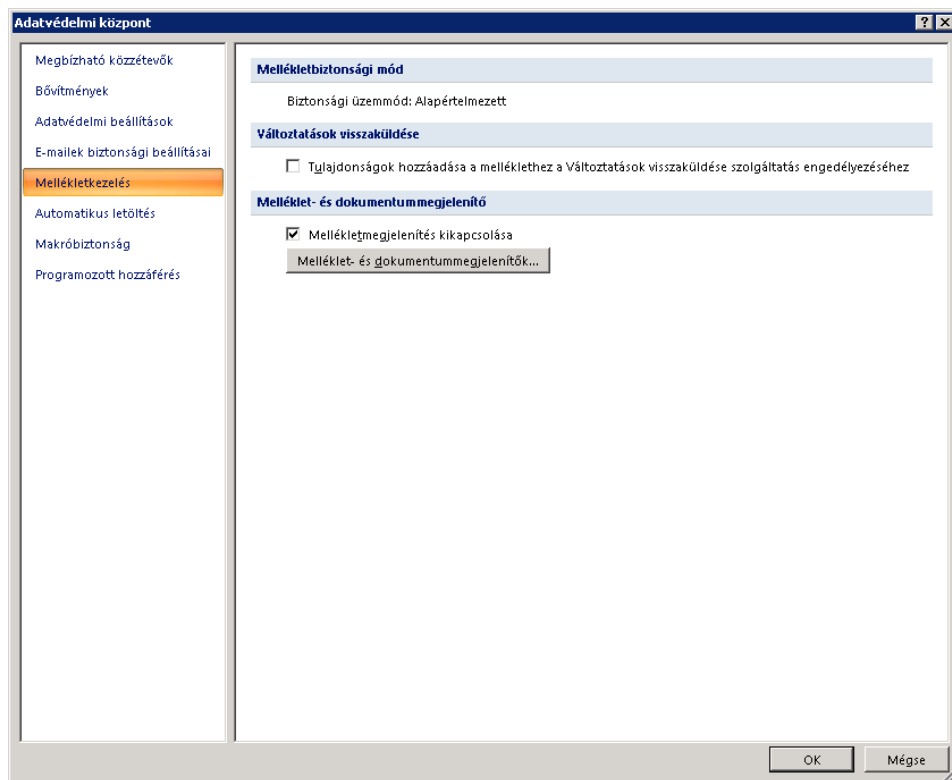
illetve miért pont ránk akarna egy ismeretlen afrikai hatalmas vagyonokat hagyni? Ne dőljünk be ezeknek a trükköknek, a bankok sem fognak tőlünk soha azonosító adatokat kérni, figyeljünk a weboldalak címére, hogy az a megszokott, hivatalos oldal legyen!

Az ilyen támadások elleni védelem alapjai egyébként megtalálhatók már a webböngésző programokban, a biztonsági csomagokból ismert phishing szűrő vészjelzést adhat a gyanús weboldalak meglátogatásakor. A leggyakrabban használt webböngészők esetén elmondható, hogy nagy hatékonysággal felveszik a harcot az adathalászok ellen. Érdeemes bekapcsolni a védelmet, a böngészők így ellenőrzik a meglátogatott oldalakat. A szűrést a megbízható oldalak fehér listája és az ismert adathalász oldalak fekete listája segíti, amely listák automatikusan frissülnek a számítógépünkön. Mivel állandóan újabb és újabb adathalász weboldalak jelennek meg, ezért ha a böngészőnk olyan oldalt töltene le, amely még nem szerepel a listán, akkor kapcsolatba lép egy olyan szerverrel, ahol frissített adatokat talál.

11.2.7. Védekezés beállítása Outlookban

Az előzőekben említett veszélyek ellen a Microsoft cég Outlook levelező kliensprogramja megpróbál megfelelő védelmet biztosítani, de újra hangsúlyoznánk, a programok nem tökéletesek, legnagyobb veszélyt még mindig az emberi tényező adja, hiszen hiába minősíti a szoftver spamnek a beérkező üzenetet, ha ennek ellenére a felhasználó rákattint a levélben található hipervivatkozásra.

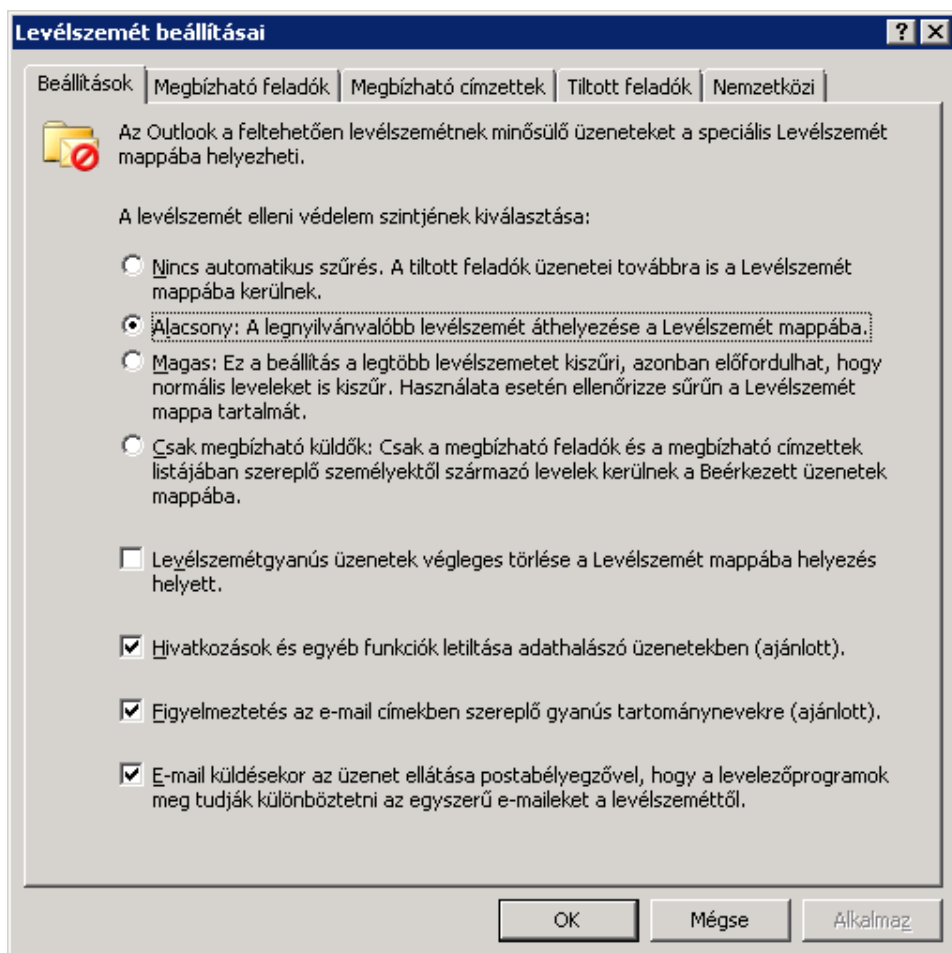
Az Outlook Adatvédelmi központja tartalmazza a biztonságra és mellékletkezelésre vonatkozó tulajdonságokat. A digitális aláírás beállítását már áttekin tettük, nézzük meg, hogy milyen lehetőségünk van a mellékletkezelés terén!



39. ábra: Mellékletkezelés Outlookban

Beállíthatjuk a mellékletek kezelésére szolgáló alkalmazásokat, illetve legbiztonságosabb megoldásként kikapcsolhatjuk a mellékletek kezelését.

A spamek szűrését az Outlook beépített módon tudja elvégezni, és a kéretlen leveleket a Levélszemét mappába helyezi át. A szolgáltatás beállítását a Műveletek menü, Levélszemét, Levélszemét beállításai menüponton keresztül tudjuk elvégezni.



40. ábra: Levélszemét beállítások Outlookban

Az ellenőrzés szintjének meghatározásával tudjuk szabályozni, hogy mennyire legyen szigorú a szoftver, majd megadhatunk egyéb opciókat, amelyek szintén a biztonságot szolgálják, így például letiltható a spamnek minősített levelekben a hiperhivatkozások közvetlen követése.

11.2.8. Webbiztonság

Az elektronikus levelezés mellett a másik leggyakrabban használt internetes szolgáltatás a web, ennek megfelelően fontos, hogy ebben a kommunikációs formában is képesek legyünk védeni az adatainkat, erőforrásainkat. A webes biztonság területét nagyjából három részre lehet osztani:

- A használt erőforrások és objektumok biztonságos megnevezése, azonosítása.
- Biztonságos, hitelesített összeköttetések létesítése a kiszolgáló és az ügyfelek között.
- Az ügyfélnek küldött futtatható kódok kezelése.

Ezeket a területeket kell tehát megfelelően védeni, amit megnehezít, hogy a webszerverek nagyon szem előtt vannak, hiszen mindenki könnyen elérheti a szolgáltatásaikat. Sokszor okozhat problémát, hogy az üzemeltetők (ez természetesen inkább kisebb szervezetekre igaz) nem veszik komolyan a rájuk leselkedő veszélyeket, esetleg nemtörődomségből, szakmai hiányosságok miatt nem konfigurálják be tökéletesen az alkalmazott szoftvereket. Szintén nem segít a védekezésben, ha gyors fejlesztésekre kerül sor, tesztelések, ellenőrzések nélkül.

A támadások hatására a támadó hozzáférhet a kiszolgálón található állományokhoz, átírhatja, lecserélheti azokat, jobb esetben csak ennyi történik, de előfordulhat, hogy a lecserélt oldalon keresztül felhasználói azonosítókhoz, adatokhoz jut hozzá.

A következő alfejezetekben a webes biztonság területeit járjuk körbe.

11.2.9. Biztonságos névkezelés

A webtartalmak megjelenítéséhez a böngészőnknek meg kell adni az URL-t, amely azonosítja az elérni kívánt erőforrást. Az URL tartalmazza a webkiszolgáló számítógép elérhetőségét, jellemzően a DNS címét. Itt érheti támadás az egész szolgáltatást, amelyet DNS megtévesztésnek nevezünk.

Amikor egy böngésző el szeretne érni egy weboldalt, akkor az általa megadott cím egy DNS kiszolgálóhoz kerül, amely visszaküldi az ügyfélnek a tartománynévhez rendelt IP címet. Ezt a címet fogja használni a webszerver megkereséséhez, innen töltődik le a megjelenítendő tartalom. A biztonsági rést az okozhatja, ha a támadó képes feltörni a DNS szervert, mert ebben az esetben megváltoztathatja a tartománynevéhez tartozó IP címet, így a kiszolgáló hamis címet fog visszaküldeni az ügyfélnek, természetesen akaratlanul megtévesztve, és esetleg kiszolgáltatta egy támadásnak.

Amennyiben sikerült a valódi webhely címe helyett a sajátunkat eljuttatni az áldozathoz, és egy eredetire hasonló weboldalt készítünk, megszerezhetjük azon keresztül az áldozat adatait, esetleg kártékony programokat tudunk a felhasználó gépére juttatni.

A megtévesztéses támadások elleni védelmet jelentheti a DNSsec (DNS security, DNS biztonság), amelyet 1994-ben kezdtek el kidolgozni, de sajnos ezt

a rendszert még nem használják teljeskörűen, így még vannak védtelen DNS kiszolgálók.

Az eljárás működése rendkívül egyszerű, nyilvános kulcsú kriptográfián alapul. Minden DNS környezet rendelkezik egy nyilvános és titkos kulcspárral, a kiszolgálók minden kiküldött információt aláírnak a származási körzet titkos kulcsával, így a kérelmező a nyilvános kulcs segítségével ellenőrizheti a szerver hitelességet.

A DNSsec három alapvető szolgáltatást nyújt:

- Bizonyítja az adatok származási helyét.
- Kiosztja a nyilvános kulcsokat.
- Hitelesíti a tranzakciókat és kéréseket.

Ha belegondolunk, az első szolgáltatás a legfontosabb, ennek segítségével tudjuk ellenőrizni, hogy a visszaadott adatokat tényleg a kiszolgáló küldte. A második szolgáltatás a nyilvános kulcsok biztonságos tárolását, és azok kikérését teszi lehetővé, míg a harmadik a támadások (visszajátszásos vagy megtévesztéses) elleni védelem miatt szükséges.

A DNS rekordok úgynevezett RRSet (Resource Record Set – erőforrás rekordkészlet) elnevezésű halmazokba kerülnek csoportosításra, amelyekre jellemző, hogy ugyanolyan névvel, osztállyal, és típussal rendelkező rekordok kerülnek majd egy halmazba. Egy RRSet több „A” rekordot is tartalmazhat, így például ha DNS névhez tartozó elsődleges és másodlagos IP címe is leképezhető. A biztonság érdekében minden RRSet egy hash értékkel is el van látva, (MD5 vagy SHA alkalmazásával). A lenyomatot a körzet egyéni kulcsával írják alá, így egy aláírt RRSet átvételekor az ügyfél ellenőrizheti, hogy azt tényleg a származási körzet egyéni kulcsával írták alá.

11.2.10. Biztonságos összeköttetés

Kezdetben a webszolgáltatás csak statikus tartalmak elérését tette lehetővé. Azonban a szolgáltatás egyre népszerűbbé válásával felmerült az igény arra, hogy olyan műveleteket is el lehessen végezni ezen a felületen keresztül, amelyek csak komoly biztonsági előírások mellett végezhetőek el (például banki tranzakciók). Az eredeti HTTP erre nem adott lehetőséget, annak készítésekor nem volt szempont a biztonság.

Az igény kielégítésére 1995-ben az akkori vezető böngésző készítője, a Netscape vállalat adott megoldást, amely biztonsági csomagot SSL (Secure Sockets Layer – biztonságos csatlakozóréteg) néven tették közzé. Az első változatokban később találtak biztonsági hibákat, jelenleg a 3.0-ás verzió az elter-

jedt. A szoftvert és protokolljait ma már széles körben használjuk, gyakorlatilag minden kiszolgáló és böngészőprogram képes alkalmazni.

Az SSL két fél között biztonságos összeköttetéseket hoz létre, és az alábbi lehetőségeket kínálja:

- Különböző paraméterek egyeztetése az ügyfél és a kiszolgáló között.
- Kölcsönösen hitelesíti az ügyfelet és a kiszolgálót.
- Titkos kommunikációt tud biztosítani.
- Az adatok sérthetetlenségét tudja biztosítani.

Az SSL gyakorlatilag egy új réteget jelent az internetes kommunikációban, helyét a szokásos protokollkészletben az alkalmazási (HTTP) és a szállítási (TCP) réteg közé tehetjük. Ez a réteg fogadja a böngészőből érkező kéréseket, és majd átadja azokat a TCP-nek a kiszolgálóhoz való továbbításra. Amennyiben létrejött a biztonságos összeköttetés, az SSL feladata lesz a tömörítés és a titkosítás elvégzése is. Ha a http az SSL felett használjuk, akkor HTTPS (Secure HTTP – biztonságos HTTP) protokollról beszélünk, még akkor is, ha maga a kommunikációs protokoll továbbra is a szabványos HTTP marad. A HTTPS másik portot (443) is használ a hagyományos (80) helyett. Az SSL-t jellemzően webböngészőkben használjuk, de fontos tisztázni, hogy egyéb alkalmazásokban is előfordulhat.

Az SSL-t szabványosítási célból a Netscape továbbadta, így 1999-ben megjelent az akkori SSL 3.0-ás verzió mellett a TLS (Transport Layer Security – szállítási rétegbeli biztonság) protokoll, amelynek jelenleg az 1.2-es verziója elterjedt.

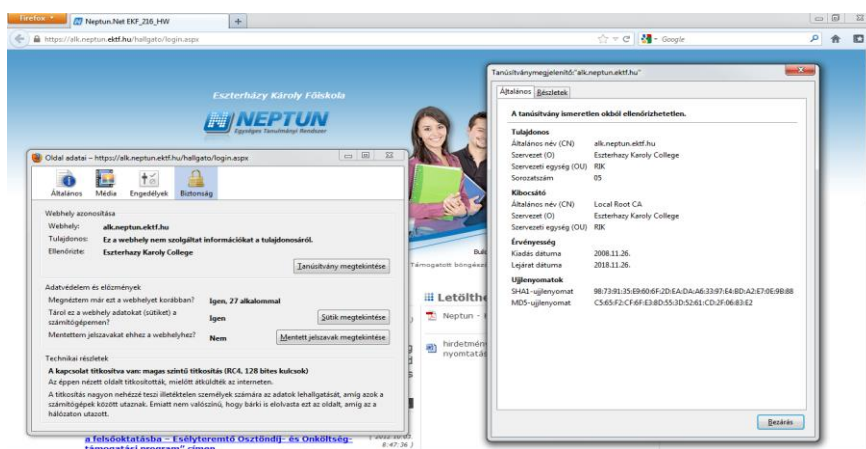
11.2.11. Az SSL működése

Az SSL réteg számos algoritmust és opciót támogat, amelyek közé tartozik a tömörítés megléte vagy hiánya, az alkalmazandó titkosítási algoritmusok.

Az SSL működése két alfolyamatra bontható. Az egyik a biztonságos kapcsolat kiépítését, a másik pedig annak használatát fogja jelenteni. Nézzük meg röviden a kapcsolat kiépítésének folyamatát!

- Első lépésben az ügyfél elküldi a kiszolgálónak az általa használt SSL verziószámát, az általa előnyben részesített tömörítési és titkosítási eljárásokat, illetve egy véletlen számot.
- A kiszolgáló visszaküldi az SSL verziót, kiválaszt egyet az ügyfél által felkínált algoritmusok közül használatra, majd elküldi saját véletlen számát. Ezen kívül a kiszolgáló elküld egy tanúsítványt, amely saját nyilvános kulcsát tartalmazza.
- A kiszolgáló végül küld egy „készen vagyok” jelzést az ügyfélnek.

- Az ügyfél véletlenszerűen kiválaszt egy 384 bit hosszú előzetes főkulcsot (premaster key), amelyet elküld a kiszolgálónak a kapott nyilvános kulccsal titkosítva.
- Ezek után mindkét fél ki tudja számolni a viszonykulcsot, amely az előzetes főkulcs és a két véletlen szám kombinációja, ezért az ügyfél küld egy kérést, hogy váltsanak kódolási típust, használják a viszonykulcsot. Az ügyfél ekkor végez a kiépítési alprotokollal, erről egy „kész” jelzéssel tájékoztatja a kiszolgálót.
- Utolsó lépésként a kiszolgáló nyugtázza a jelzést, kiépül a biztonságos összeköttetés.



41. ábra: SSL működés közben

11.2.12. Hordozható kódok biztonsága

A weboldalak ma már gyakran tartalmaznak apró programokat, köztük Java kisalkalmazásokat, ActiveX vezérlőket, és JavaScripteket. Ezeket hordozható kódoknak (mobile code) nevezzük, letöltésük és futtatásuk rengeteg előnnyel, hasznos funkcióval jár, viszont komoly biztonsági kockázatot is jelent egyben, ha rosszindulatú céllal készülnek.

- A Java kisalkalmazások biztonsága

Apró Java programokról beszélünk, amelyeket egy veremorientált JVM (Java Virtual Machine) nevű gépi kódra fordítanak le. Weboldalon is el lehet helyezni az appleteket, amelyek az oldallal együtt letöltődnek az ügyfél számítógépére, majd egy böngészőn belüli JVM értelmezőbe kerülnek. Mivel a kódot egy értelmező dolgozza fel, lehetőség van az utasítások ellenőrzésére. A rendszerhívásokat szintén értelmezik, amennyiben egy kisalkalmazás megbízható

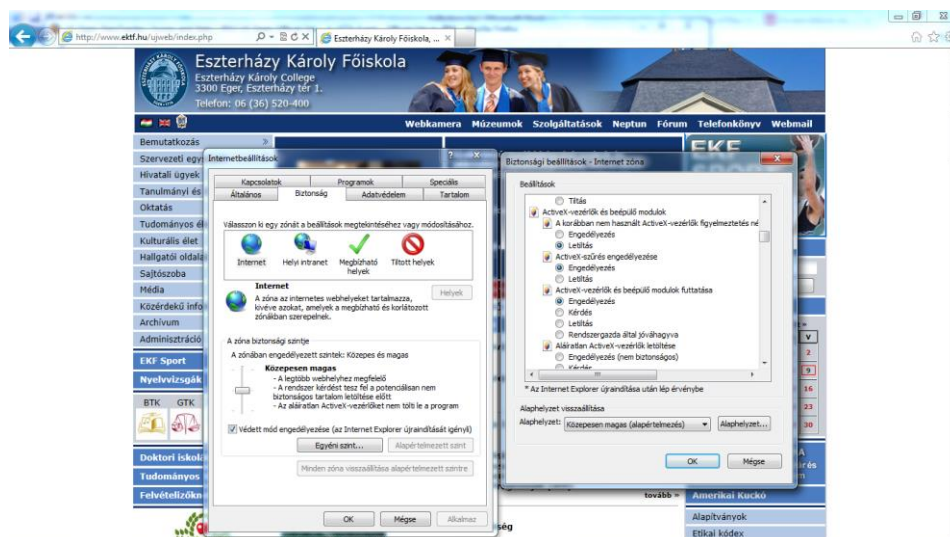
(például a merevlemezről futtatjuk), akkor rendszerhívásait minden további nélkül végrehajthatja, de ha nem megbízható (például az interneten keresztül kaptuk), akkor egy úgynevezett homokozóba (sandbox) lehet küldeni, így korlátok közé szorítjuk, és meg tudjuk gátolni abban, hogy hozzáférjen a rendszer fontosabb erőforrásaihoz. Abban az esetben, amikor egy kisalkalmazás egy helyi erőforráshoz próbál hozzáférni, akkor a hívást egy biztonsági felügyelőhöz irányítják jóváhagyásra. A felügyelő megvizsgálja a hívást a helyi biztonságpolitika fényében, majd ezután eldönti, hogy a művelet végrehajtható-e.

- ActiveX programok

Az ActiveX programok kis bináris programok, amelyeket weboldalakba lehet beágyazni. Amennyiben egy böngészőprogram egy ilyenrel találkozik, akkor ellenőrzi, hogy szabad-e futtatnia, és ha igen, akkor futtatja azt. Az ilyen ActiveX programoknak éppen annyi lehetőségük van, mint más felhasználói alkalmazásoknak, ennek következtében nagy károkat is képesek okozni az ügyfél gépen. Az egyetlen biztonsági művelet, a program futtathatóságának eldöntése, amely a kódok aláírásán alapszik (code signing). Minden ActiveX vezérlőt digitális aláírással látnak el, ami a kódból képzett lenyomat, amelyet annak készítője saját titkos kulcsával aláírt. Egy ActiveX vezérlő letöltésekor a böngésző először az aláírást ellenőrzi, a nyilvános kulccsal visszafejtve megtudja, nem változtattak-e valamit az átvitel során a kódon. Amennyiben az aláírás megfelelő, a böngésző megnézi saját táblázatában, hogy az ActiveX vezérlő készítője megbízható-e, vagy rákérdez a felhasználóra, ő megbízik-e a fejlesztőben. Ha a szerző megbízhatónak bizonyul, a programot futtatja a böngésző.

- JavaScript

A JavaScriptre vonatkozóan nincs semmilyen biztonsági szabvány, eljárás. Az alapvető probléma ebben az esetben is az, hogy egy idegen kód futtatása a számítógépünkön nem biztonságos, viszont a hordozható kódok látványos grafikát, és gyors interakciót tesznek lehetővé, sok webfejlesztő ezt fontosabbnak tartja, mint a biztonságot. A böngészők beállításai között megadható, hogy engedélyezzük-e a JavaScriptek futtatását, vagy sem.

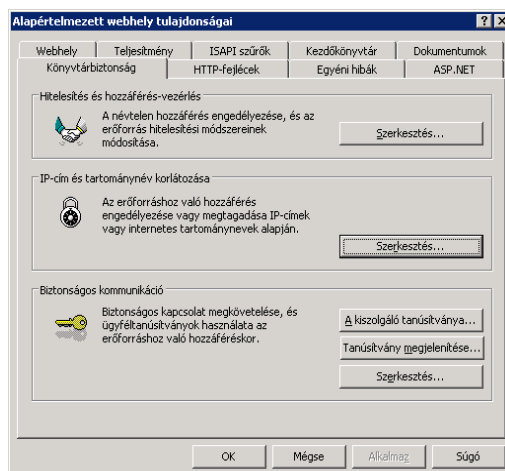


42. ábra: Biztonsági beállítások Internet Explorerben

11.2.13. Védelmi beállítások IIS kiszolgálóban

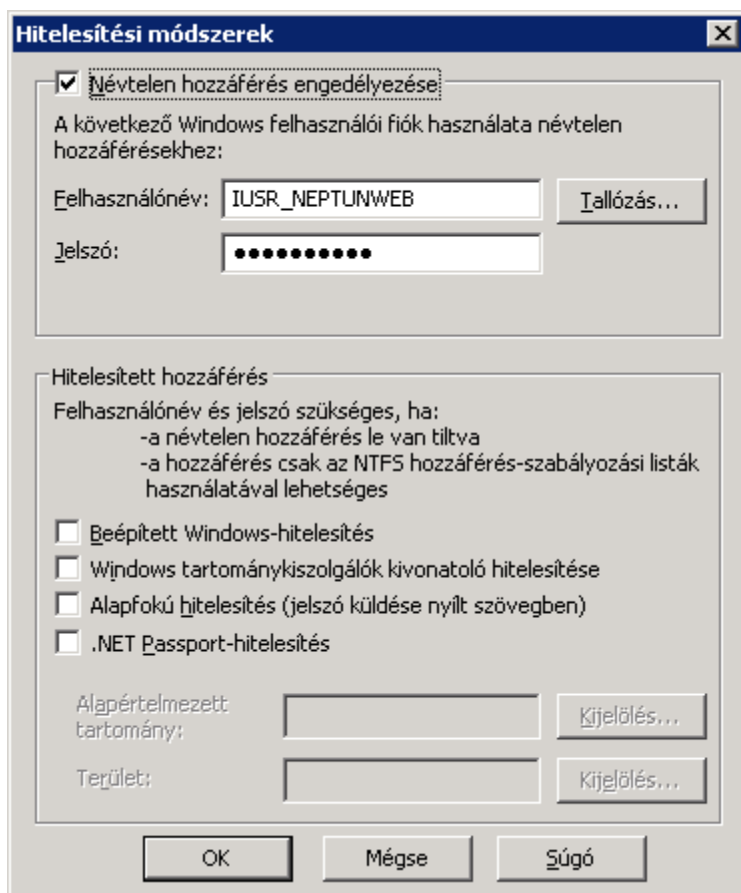
A Microsoft által készített webkiszolgáló program alkalmas biztonsági megoldásokat alkalmazni, így az SSL eljárás használatára, képes biztonságos összeköttetést létrehozni az ügyfelekkel.

Indítsuk el az IIS kezelőprogramját! A Webhelyek tulajdonságlapján, a Könyvtárbiztonság fülön végezhetjük el a biztonsági beállítások nagy részét.



43. ábra: Biztonsági beállítások az IIS-ben

Megadhatóak hitelesítési és hozzáférés-vezérlési adatok, amelyekkel szabályozhatjuk, hogy a kapcsolat során névtelenül lehet böngészni, vagy valamilyen módon azonosítani kell magát a felhasználónak.



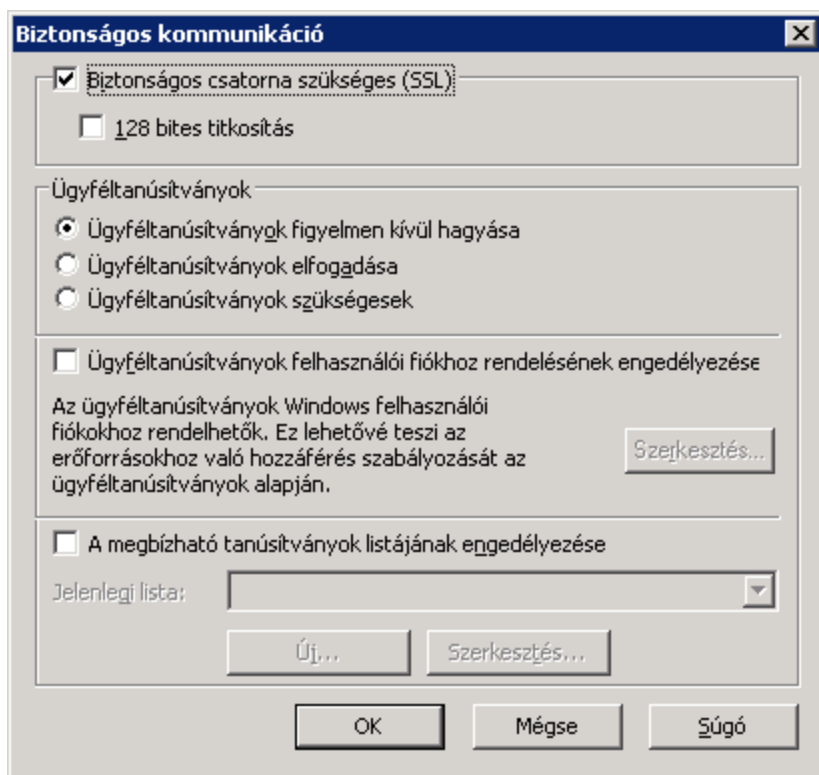
44. ábra: Hitelesítés beállítása az IIS-ben

Korlátozható a kiszolgáló elérhetősége, megadhatjuk, hogy milyen IP-címtartományokból, vagy milyen tartományokból fogad csak kérést a szerverünk. Így könnyedén beállítható például, hogy csak a belső hálózathoz legyen elérhető a szolgáltatás.

Az utolsó részben adhatjuk meg a biztonságos kommunikációra vonatkozó opciókat. Egy varázsló segít a tanúsítvány kezelésében, ami szükséges lesz az SSL alkalmazásához. A tanúsítvány beszerezhető valamilyen hivatalos CA-tól, ebben az esetben nagy a valószínűsége, hogy a böngészők automatikusan elfogadják azt, mert beépítve tartalmazznak elfogadott CA-khoz tartozó nyilvános

kulcsokat. Készíthetünk saját tanúsítványt is, ebben az esetben az ügyfelek böngészői nem tudják eldönteni, hogy tényleg érvényes-e a tanúsítvány, ezért a felhasználó engedélye után fogják csak kiépíteni a kapcsolatot.

A Szerkesztés... gombra kattintva kapjuk az alábbi panelt:



45. ábra: Biztonságos kommunikáció beállításai

Beállíthatjuk, hogy a weboldal csak SSL-en keresztül érhető el, ekkor sima HTTP kéréseket nem is fog elfogadni a kiszolgáló. Amennyiben kétirányú hitelesítést szeretnénk alkalmazni, akkor azt az ügyféltanúsítványok kezelésénél tudjuk beállítani, sőt, akár Windows felhasználói fiókokhoz is rendelhetjük azokat.

11.3. ÖSSZEFOGLALÁS, KÉRDÉSEK

11.3.1. Összefoglalás

A fejezet a két leggyakrabban használt internetszolgáltatás, az elektronikus levelezés és a webszolgáltatás biztonsági problémáit, veszélyeit, és az azokra adott válaszokat járja körbe.

A hallgatók megismerték az elektronikus levelezés veszélyeit, a védekezés módszereit, az ezt megkönnyítő protokollokat, szabványokat. Bemutattuk a különböző kártékony programokat, felhívtuk a figyelmet az ezek elleni védekezés fontosságára, lehetőségeire.

Megismerték az SSL használatának alapjait, működésének tulajdonságait, illetve Microsoft környezetben a telepítés, konfigurálás lépéseit is.

12 VEZETÉK NÉLKÜLI HÁLÓZATOK BIZTONSÁGA

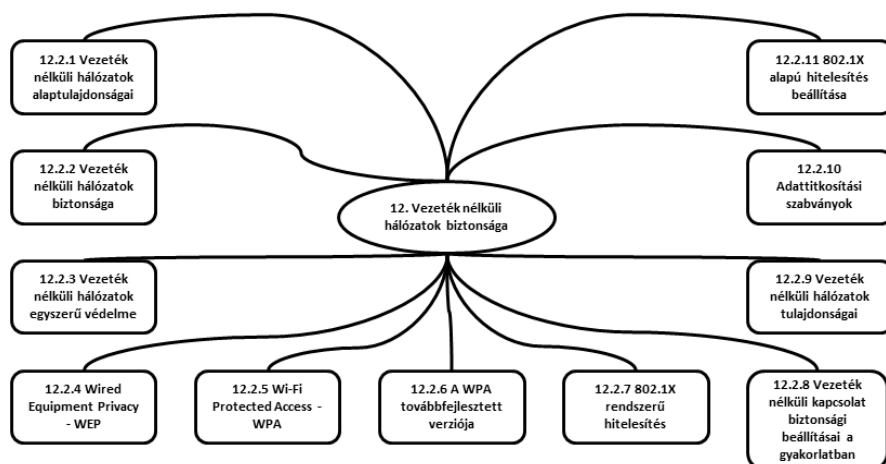
12.1. CÉLKITŰZÉSEK ÉS KOMPETENCIÁK

A mobil technológiák rengeteg előnyük mellett rendelkeznek egy nagy hátránnyal is, a biztonságos kommunikáció megoldása több problémát okoz, mint a vezetékes hálózatok használata esetén.

A fejezet célja, hogy a vezeték nélküli hálózatokban használt biztonsági megoldásokat, protokollokat megismertesse a hallgatókkal, így képesek lesznek a későbbiekben alkalmazni ezeket a megoldásokat, saját környezetükben is biztonságos módon tudják üzemeltetni a vezeték nélküli hálózatokat.

Az elméleti leírások mellett bemutatjuk a Microsoft rendszerein keresztül a telepítési, konfigurálási lépéseket is.

12.2. TANANYAG



12.2.1. Vezeték nélküli hálózatok alaptulajdonságai

A számítógépes hálózatok használatához a kezdetektől fogva szükség volt valamilyen kábeles, vezetékes megoldásra, amellyel az egyes eszközöket össze lehetett kötni. Mivel jellemzően helyhez kötött, nagyobb méretű eszközökről

volt szó, ezért nem okozott különösebb gondot, hogy néha bizony bonyolult vezetékhálózatot kellett kiépíteni, használni a számítógépek között.

Napjainkra viszont elvárás, hogy a kisméretű, mozgatható mobil eszközeinkkel is teljes mértékben és minél egyszerűbben tudjuk használni a számítógépes hálózatokat, azok szolgáltatásait. Ráadásul ez egyre fontosabb szempont lesz, hiszen az asztali számítógépek szerepét kezdik átvenni a laptopok, táblagépek, okostelefonok.

A mobil eszközök nagy segítséget jelentenek felhasználók számára, akik így nincsenek helyhez kötve, gyakorlatilag bárhol használhatóak, illetve kisebb energiafogyasztással jár a használatuk. A hálózati kapcsolatot pedig jellemzően már nem vezetéken keresztül létesítik (sok eszközben erre már nincs is csatlakozási pont), hanem valamilyen vezeték nélküli megoldással, amelyek jellemzően mikrohullámú adatátvitelt jelentenek.

A nyilvánvaló előnyök mellett a technológia legnagyobb problémája éppen a biztonság, a vezetékes megoldásoknál szükséges fizikai kapcsolat nélkül is hozzá lehet férni a forgalmazott adatokhoz, ellenőrizhetetlen módon. Egy cég informatikai rendszere lehet a legjobban beállított, legerősebben konfigurált tűzfal mögött, ettől még a vezeték nélküli hálózati kommunikáció akár egy parolóban álló gépkocsiban könnyűszerrel lehallgatható.

12.2.2. Vezeték nélküli hálózatok biztonsága

A legelterjedtebb vezeték nélküli megoldás az IEEE 802.11-es szabványában meghatározott adatátviteli forma (melynek közkeletű elnevezése a wifi szócska), melynek már több változata is hivatalossá vált az elmúlt években, így beszélhetünk 'a', 'b', 'g' és a legújabb 'n' szabványról. A technikai jellemzők mellett az egyes szabványokban egyre komolyabb biztonsági megoldásokat is bevezettek, de sajnos ma sem jelenthető ki, hogy az ilyen módon forgalmazott adataink teljes biztonságban lennének.

A titkosítás nélküli hálózatokban a hatókörön belül minden eszköz (amelyről akár nem is tudunk) képes az üzeneteket fogadni, elolvasni. A biztonsági megoldások arra törekednek, hogy titkosított kapcsolatot létesítsenek az illetékes eszközök, vagyis csak azok tudjanak egyáltalán kapcsolódni a hálózathoz, illetve a hálózati csomagokat titkosítva küldik egymásnak.

12.2.3. Vezeték nélküli hálózatok egyszerű védelme

A vezeték nélküli hálózatok több olyan egyszerű védelmi megoldást is kínálnak, amelyek beállíthatóak a hozzáférési pontokon, és amelyek alapvetően nem az adatok titkosítását végzik, hanem az illetéktelen hozzáférést, vagyis

magát a kapcsolódást próbálják blokkolni. Ezek a megoldások azonban nem nyújtanak teljes biztonságot.

Az első ilyen védelmi opció, hogy nem tesszük nyilvánossá a hálózat SSID (Service Set Identifier) értékét, ezt a hozzáférési pont konfigurációjában beállíthatjuk rejtettnek. Ebben az esetben az eszköz nem szórja az SSID értéket, vagyis a hatótávolságon belül lévő egyéb eszközök nem tudnak róla, hogy kapcsolódhatnak. A kapcsolat létrehozása ekkor nem automatikus folyamat, hanem a felhasználónak kell beállítania a paramétereket, így ismernie kell az SSID értékét is.

A másik egyszerű megoldás, hogy a hozzáférési pont konfigurációja tartalmaz olyan megszorításokat, hogy csak az ott beállított MAC (Media Access Control) címekkel rendelkező eszközök kapcsolódhatnak. Sajnos ez a megoldás nem teremt nagy biztonságot, mert bár a MAC címek minden fizikai eszközbe elvileg „be vannak égetve”, egyéb tényezők miatt szoftveresen átállíthatóak ezek az értékek, így a hálózati forgalom figyelése után aránylag könnyen kideríthető (és beállítható a saját számítógépre) egy olyan MAC cím, amelyet a hozzáférési pont elfogad.

Az egyszerű védelem után nézzük meg, milyen titkosítási módszereket támogatnak a vezeték nélküli hálózatok szabványai!

12.2.4. Wired Equipment Privacy – WEP

A 802.11-es szabvány első módszerként a Wired Equipment Privacy (vezetékeskel egyenértékű biztonság) – vagy röviden: WEP – nevű, adatkapcsolati szinten működő protokollt írja elő biztonsági megoldásként. A WEP-et arra tervezték, hogy – ahogy az elnevezésében is szerepel – ugyanolyan biztonságot lehessen elérni, mint a vezetékes hálózatok esetén. (Érdekesség, hogy alapvetően a vezetékes hálózatok semmilyen biztonságot nem nyújtanak, így aránylag egyszerűen elérhető ugyanaz a szint...)

A WEP funkciót engedélyezni kell a kommunikációban részt vevő eszközök mindegyikén, akkor tudnak egymással adatokat cserélni titkosított formában. A módszer lényege, hogy minden állomásnak lesz egy titkos kulcsa, amelyet a bázisállomás is ismer. Sajnálatos módon arról a szabvány nem rendelkezik, hogy a kulcsok hogyan kerüljenek kiosztásra, így lehetséges, hogy a gyártó osztja ki előre, de akár az is, hogy az eszköz választ magának és azt küldi el egymásnak a nyilvános kulccsal titkosítva. Maga a titkosítás Ronald Rivest RC4 eljárására épül, amely nyilvános.

A legnagyobb problémát az okozza, hogy a kommunikáció közben a kulcsok hosszú ideig nem változnak, így megfelelő mennyiségű hálózati forgalom

(ez akár pár perc alatt is összegyűlhet) mellett a titkos kulcs a csomagokból visszafejthető.

Összefoglalva kijelenthető, hogy a WEP abszolút nem biztonságos, lehetőleg ne használjuk!

12.2.5. Wi-Fi Protected Access – WPA

Miután kiderült, hogy a WEP nem nyújt megfelelő biztonságot, elkezdtek kidolgozni más megoldást, amely megnyugtatja a felhasználókat, így jött létre a Wi-Fi Protected Access (Wi-Fi védett hozzáférés) – röviden: WPA – titkosítási szabvány.

A szabvány a WEP-hez hasonlóan az RC4-es eljárást használja 128 bites kulccsal, viszont lényeges különbséget jelent a TKIP (Temporal Key Integrity Protocol, ideiglenes biztonságos kulcs protokoll) bevezetése. A TKIP folyamatosan cserélgeti a kapcsolat során használt kulcsot, amiből következik, hogy a támadó hiába fejtené meg a kulcsot, akár rövid időn belül, semmire sem megy vele, főleg, ha egy kulcsot a rendszer rövidebb ideig használ, mint annak a feltöréséhez szükséges idő. Nagy előnye az eljárásnak, hogy kompatibilis az összes korábbi wifi-t használó eszközzel, nem szükséges azokat lecserélni a protokollváltás miatt, hátránya viszont, hogy ugyanazt az RC4 titkosítási algoritmust használja, mint a gyengének bizonyult WEP protokoll, így még mindig nem nyújt tökéletes védelmet. Az igazi biztonságot a WPA is csak akkor nyújtja, ha kellően hosszú és összetett jelszót használunk.

12.2.6. A WPA továbbfejlesztett verziója

Szinte a WPA megjelenésével egy időben elkészült annak továbbfejlesztett változata is, amely a WPA2 elnevezést kapta. A legtöbb vezeték nélküli kommunikációt támogató eszköz együtt tartalmazza mind a WPA, mind a WPA2 protokoll kezelését. A WPA2 minden, 2006. március 13. után készült vezeték nélküli eszközben kötelezően támogatott, csak így kaphatja meg a WiFi jelölést.

Miben más a WPA2? A legfőbb különbség a WPA-hoz képest az addig használt RC4 algoritmus helyett az AES (Advanced Encryption Standard) titkosítási eljárás használata a kódolás során. Plusz funkcióként a WPA2 használja a négylépéses azonosítási protokollt, így képes nagyobb biztonságot nyújtani a kapcsolódáskor történő támadások ellen.

A WPA2 eljárás hátránya, hogy nem kompatibilis a régebbi (802.11 a, b szabvány szerint működő) eszközökkel, illetve jónéhány olcsóbb g-s eszköz sem támogatja, így azok beszerzésekor érdemes ellenőrizni, hogy képes-e használni a protokollt?

12.2.7. 802.1X rendszerű hitelesítés

Vállalati környezetben a nagyobb biztonság érdekében gyakran használják az IEEE 802.1x szabvány (amely a vezeték nélküli hálózatokban az eszközök között zajló kommunikációt írja le) szerinti megoldást. Két hálózati eszköz összekapcsolásának és az erőforrások elérésének elengedhetetlen feltétele a részt vevő felek hitelesítése.

A 802.1X rendszerű hitelesítés ilyen folyamatot végez az ügyfélgép és egy, a hozzáférési ponttal kapcsolatban lévő kiszolgáló között, vagyis a vezeték nélküli hálózatok 802.1X alapú hitelesítésének három fő összetevője van:

- A hitelesítő (a hozzáférési pont).
- A kérelmező (az ügyfél).
- a hitelesítő kiszolgáló.

A 802.1X szerinti hitelesítési folyamat egyszerűsített sémája a következő lépésekben foglalható össze:

- Az ügyfél küld egy „hozzáférést kérek” üzenetet a hozzáférési pontnak, minek hatására a hozzáférési pont felkéri az ügyfelet, hogy azonosítsa magát.
- Az ügyfél a felkérésre egy azonosító csomaggal válaszol, amelyet a hitelesítő kiszolgálónak továbbküld a hozzáférési pont.
- A hitelesítő kiszolgáló elvégzi az azonosítást, pozitív esetben „elfogadom” csomagot küld vissza a hozzáférési pontnak.
- A hozzáférési pont a sikeres azonosítás után beállítja az ügyfél portját engedélyezettre, innentől kezdve engedélyezi az adatforgalom folytatását.

A hitelesítés során felhasználói azonosító adatokat – például felhasználói jelszót – használunk, de ezen adatok átvitele nem a vezeték nélküli hálózaton történik. A vezeték nélküli ügyfélgép egy hitelesítési kérelmet kezdeményez a hozzáférési ponton, amely például egy EAP-kompatibilis (Extensible Authentication Protocol) RADIUS kiszolgálón hitelesíti az ügyfélgépet. A RADIUS kiszolgáló többféle módon hitelesítheti a felhasználót (jelszóval, tanúsítvánnyal) vagy a számítógépet (annak MAC-címével). A vezeték nélküli ügyfél elvileg addig nem csatlakozhat a hálózatra, amíg ez az ellenőrzés sikeresen le nem zajlott. Nem minden hitelesítési módszer használ RADIUS kiszolgálót, megoldható WPA használatával is, amelyet be kell írunk a hozzáférési pontba és a hálózatot használni kívánó összes eszközbe.

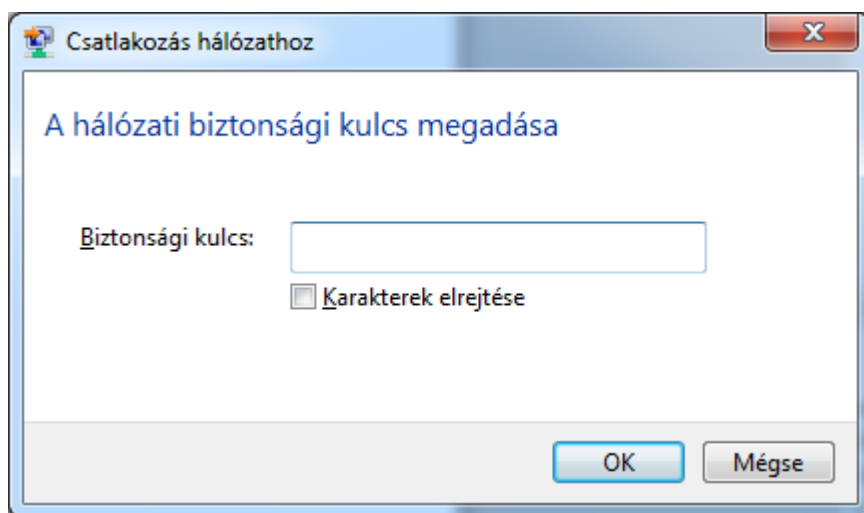
Többnyire a 802.1X alapú hitelesítés támogatja a dinamikus, munkamene-tenként és felhasználónként változó kulcsokat, így erősítve a kulcs biztonságát.

12.2.8. Vezeték nélküli kapcsolat biztonsági beállításai a gyakorlatban

Az elméleti leírások után nézzük meg, hogy tehetjük biztonságosabbá vezeték nélküli kapcsolatainkat a biztonsági funkciók használatával a gyakorlatban, Windows operációs rendszerünkben!

Természetesen a vezeték nélküli kapcsolat létrehozása előtt a hozzáférési ponton is el kell végezni a megfelelő biztonsági beállításokat (ennek mikéntjére most nem térünk ki), és ezek ismeretében leszünk képesek a saját eszközünkön is elvégezni a konfigurálási folyamatot.

Amennyiben első esetben akarunk létrehozni egy vezeték nélküli kapcsolatot, akkor alapbeállítások mellett az operációs rendszerünk érzékelni fogja az SSID értékét és felkínálja a csatlakozás lehetőségét. A kapcsolódás kérésekor az operációs rendszer megpróbálja létrehozni a kapcsolatot, ha titkosított a kapcsolat, akkor automatikusan rákérdez a biztonsági kulcsra, amelyet a hozzáférési pont kér tőlünk.



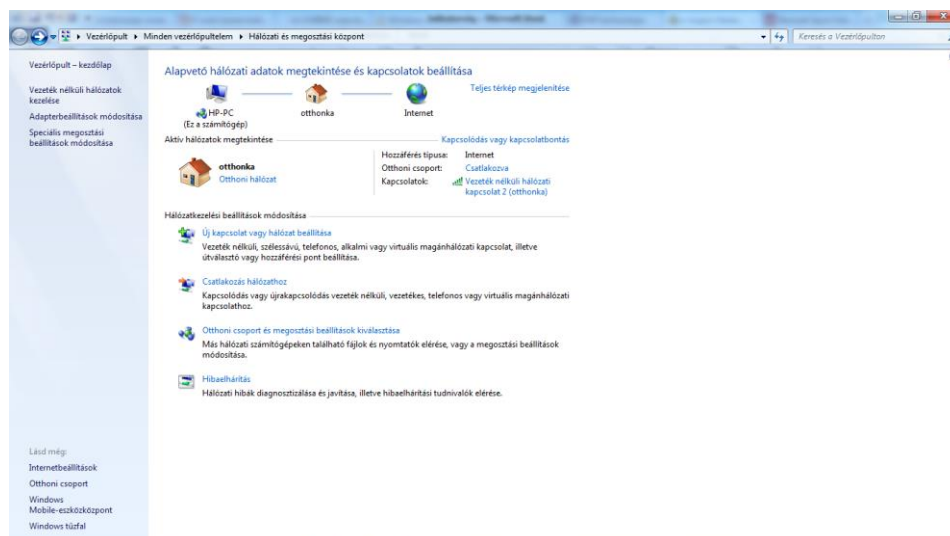
46. ábra: Biztonsági kulcs megadása

Ennek sikeres megadása után megtörténik a kapcsolódás, használhatjuk a vezeték nélküli kapcsolatot, ráadásul az operációs rendszerünk megjegyzi a

kulcsot, így többször nem is kell beírunk azt, ha ugyanehhez a hozzáférési ponthoz szeretnénk kapcsolódni.

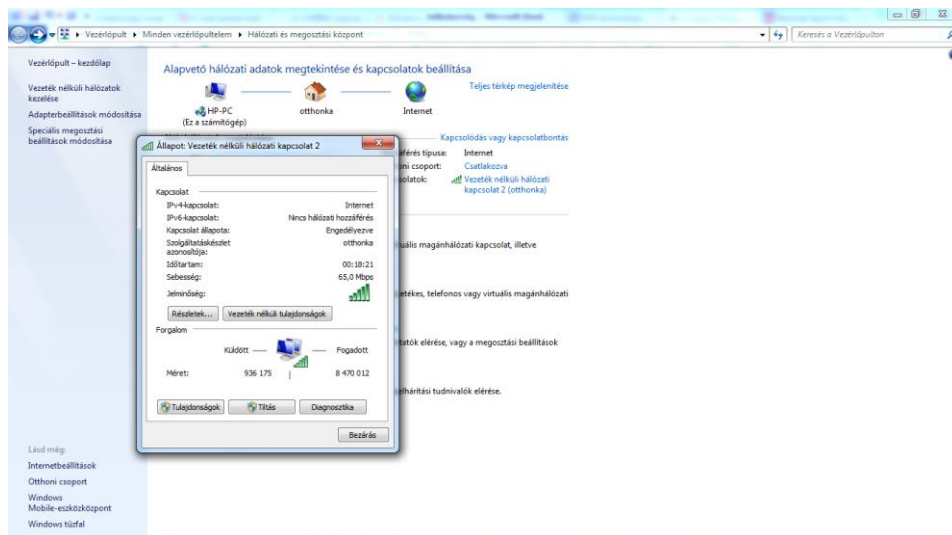
12.2.9. Vezeték nélküli hálózatok tulajdonságai

A vezeték nélküli hálózati kapcsolatok tulajdonságait a Windows Hálózati és megosztási központ alkalmazásában tudjuk részletesen konfigurálni.



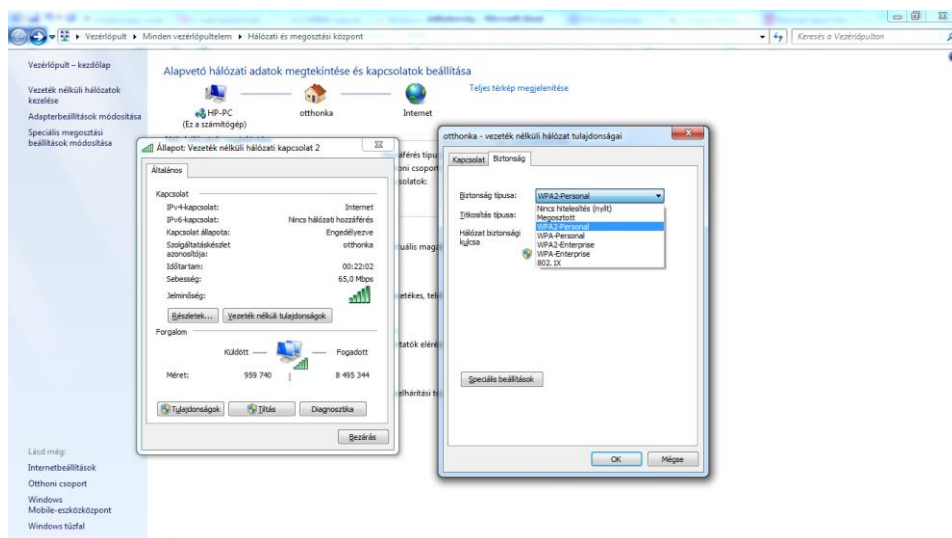
47. ábra: Hálózati és megosztási központ

A Vezeték nélküli kapcsolat linkre kattintva megkapjuk az adott kapcsolathoz tartozó tulajdonságlapot, ahol láthatjuk, hogy éppen milyen opciók mellett érjük el a hálózatot.



48. ábra: Vezeték nélküli hálózati kapcsolat tulajdonságai

A Részletek gombra kattintva megnézhetők a hálózati adatok, csakúgy, mint vezetékes hálózati kapcsolat esetén. Mi viszont most kattintsunk a Vezeték nélküli tulajdonságok gombra, amely hatására megjelenik egy újabb ablak, itt tudjuk a specifikus tulajdonságokat megnézni, beállítani.



49. ábra: Vezeték nélküli hálózat biztonsági beállításai

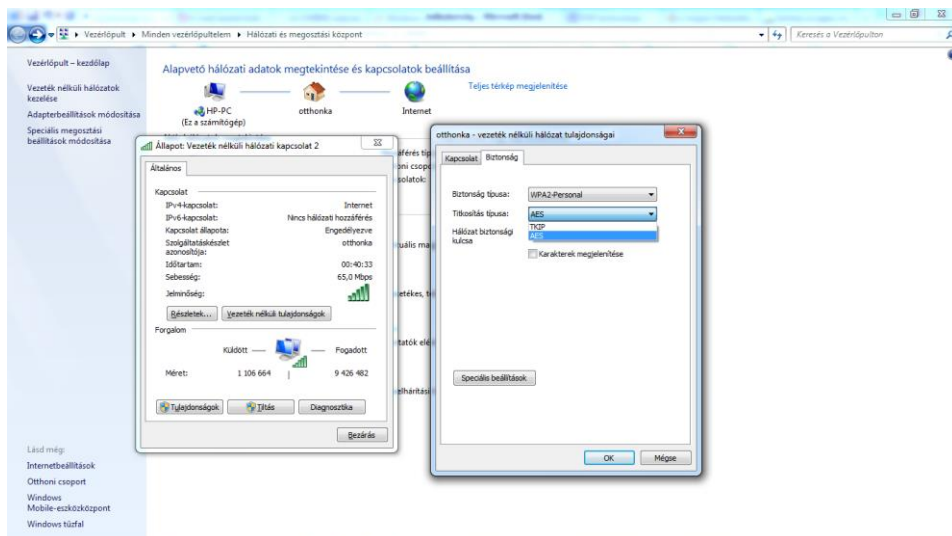
A Kapcsolat fülön az SSID-re vonatkozó opciók adhatóak meg. A Biztonság fülön találhatóak azok a tulajdonságok, amelyek a kapcsolat biztonsági beállításait tartalmazzák. A típusnál adhatjuk meg, hogy melyik szabvány szerint szeretnénk használni a kapcsolatot, ahogy erről már volt szó, természetesen ez függ a hozzáférési pont beállításaitól is. Ha az előző alfejezetben leírt módon kapcsolódtunk, akkor a szoftverek automatikusan egyeztettek, és nem szükséges ezt az opciót kiválasztanunk.

Amiről még nem volt szó a WPA ismertetésekor, hogy a gyakorlatban létezik mind a WPA, mind a WPA2 típushoz egy Personal és egy Enterprise változat is. A kettő között a különbség annyi, hogy az Enterprise változatot vállalati környezetre tervezték, így használatához valamilyen hitelesítő kiszolgáló is szükséges, például egy RADIUS szerver. A Personal változatok inkább az otthoni használat követelményeinek felelnek meg, tényleg csak a két kommunikáló fél között kell megosztani a kulcsot.

12.2.10. Adattitkosítási szabványok

A vezeték nélküli kapcsolatok biztonsági beállításánál tudjuk megadni az adattitkosítás módját is. Szintén egységesen be kell állítanunk minden eszközben a megfelelő értéket, csak akkor tudnak egymással kommunikálni.

WPA, illetve WPA2 esetén általában két adattitkosítási típus közül választhatunk:



50. ábra: Adattitkosítás típusának megadása

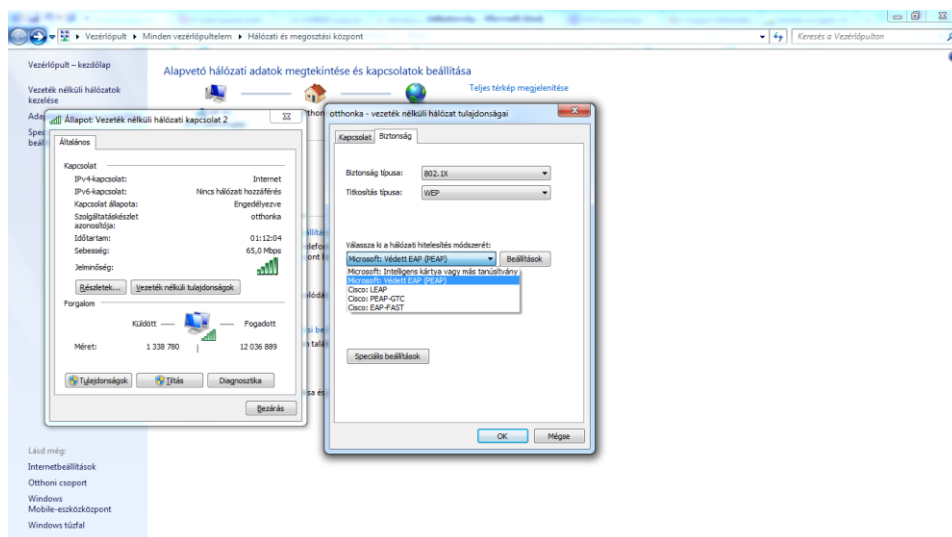
A TKIP (Temporal Key Integrity Protocol) csomagonkénti kulcskeverést, üzenetépség-ellenőrzést és kulcsváltó mechanizmust alkalmaz.

Az AES (Advanced Encryption Standard) a vezeték nélküli összeköttetések titkosítására szolgáló újabb módszer, amelyet az IEEE 802.11i szabvány ír le részletesen. Az AES eljárás erősebb titkosítást biztosít, mint a TKIP, akkor választjuk az AES adattitkosítást, ha erősebb adatvédelemre van szükségünk.

12.2.11. 802.1X alapú hitelesítés beállítása

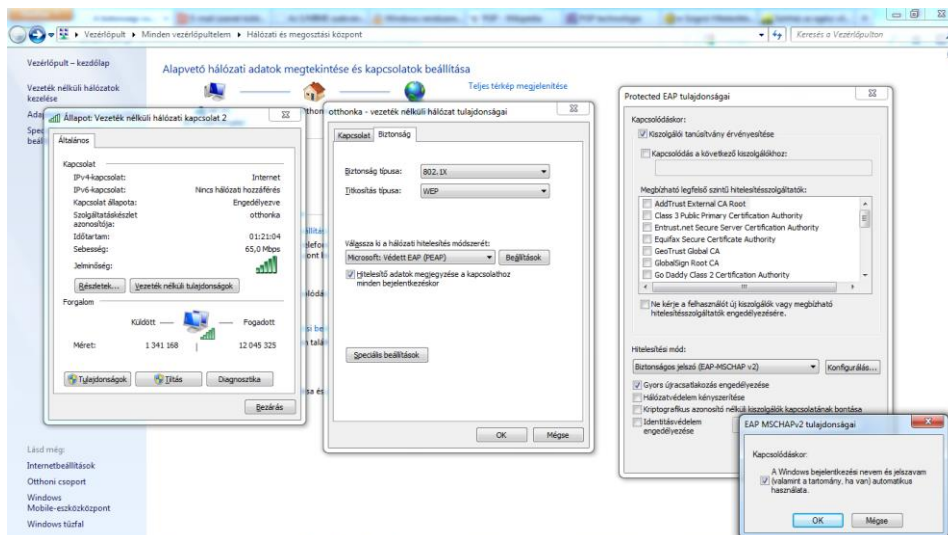
Elméletben már volt szó a 802.1X alapú hitelesítésről, nézzük meg, hogyan állítható be a Microsoft operációs rendszereiben!

A vezeték nélküli hálózat biztonsági típusainál tudjuk megadni ezt a módot is. A titkosítás típusa WEP lesz alapértelmezetten.



51. ábra: 802.1X alapú hitelesítés beállítása

Ezután még kiválaszthatjuk a hálózati hitelesítés módszerét, annak megfelelően, hogy milyen módszert választottunk a hitelesítő kiszolgálón. Bármelyik módszert is választjuk, további beállításokat tehetünk arra vonatkozóan, hogy hogyan történjen a hitelesítés, például megadható a használni kívánt tanúsítvány elérési helye, vagy beállíthatók az azonosításra szolgáló adatok.



52. ábra: Hitelesítési módszer részletes konfigurálása

Nézzünk egy rövid leírást a különböző hitelesítési módokról:

A PEAP (Protected Extensible Authentication Protocol) eljárás egy új EAP alapú IEEE 802.1X szerinti hitelesítési típus, amely kihasználja a kiszolgáló oldali EAP-Transport Layer Security (EAP-TLS) megoldás adta lehetőségeket. Különböző hitelesítési módszereket támogat, köztük a felhasználói azonosítókat, jelszavakat, az egyszer használatos jelszavakat és a GTC (Generic Token Card) azonosítókártyákat is.

A Cisco LEAP (Cisco Light EAP) eljárás a felhasználó által megadott bejelentkezési jelszó alapján a 802.1X szabvány szerint hitelesíti a kiszolgálókat és az ügyfeleket. Amikor egy vezeték nélküli hozzáférési pont egy olyan RADIUS kiszolgálóval kommunikál, amely a Cisco LEAP-et támogatja, akkor a protokoll gondoskodik a hozzáférés szabályozásáról. Kölcsönös hitelesítést végez az ügyféleszköz és a vezeték nélküli hálózat között, és egyedi felhasználói titkosító kulcsokkal védi az átvitt adatokat, amelyet dinamikusan képes változtatni.

Az EAP-FAST a PEAP mechanizmushoz hasonlóan alagutat használ az adatforgalom védelmére, de különbség, hogy az EAP-FAST nem tanúsítvánnyal hitelesít. Amennyiben az ügyfélnek nincs előre megadott PAC (Protected Access Credential) kulcsa, EAP-FAST üzenetcserét kérhet a kulcs eljuttatásához, amelynek során dinamikusan kap egy kulcsot a kiszolgálótól.

A protokoll két módszerrel képes eljuttatni a PAC-t: vagy kézileg egy sávon kívüli biztonságos mechanizmussal, vagy automatikusan. Lényegében a kézi

átadási művelet bármilyen típusú lehet, az a fontos, hogy a hálózati rendszergazda megfelelően biztonságosnak tartsa. Az automatikus kulcsküldés titkosított alagutat létesít, hogy így védje az ügyfél hitelesítési adatait és a neki küldendő PAC kulcsot. Ez a megoldás nem minden esetben éri el a kézi módszer biztonságát, de mindenképpen biztonságosabbnak tekinthető, mint a LEAP hitelesítési módszere.

Összegezve, az EAP-FAST eljárás két részre osztható: az eljuttatásra és a hitelesítésre. Az eljuttatási fázisban kapja meg az ügyfélgép az első PAC-t. Ezt ügyfelenként és felhasználónként csak egyszer kell elvégezni.

12.3. ÖSSZEFOGLALÁS, KÉRDÉSEK

12.3.1. Összefoglalás

A fejezet a vezeték nélküli hálózati megoldások biztonsági problémáit írja le. A hallgatók megismerkedtek a biztonságot nyújtó különböző megoldásokkal, protokollokkal, tisztáztuk azt is, hogy melyiket milyen környezetben célszerű használni.

Az elméleti leírásokon túl gyakorlatban is bemutattuk Microsoft operációs rendszer esetén a beállítási lehetőségeket, az alkalmazható adattitkosítási szabványokat, hitelesítési eljárásokat.

13 ÖSSZEFOGLALÁS

13.1. TARTALMI ÖSSZEFOGLALÁS

Mindennapi életünk olyan szerves részévé vált az informatika, a számítógépes hálózatok, az internet, hogy gyakran meg is feledkezünk arról a technológiai háttérrel, amire szükség van a szolgáltatások használatához. Ráadásul egy átlagos felhasználó nincs is tisztában azzal, hogy rengeteg veszély fenyegeti a hálózaton töltött idő, az elektronikus kommunikáció során.

A tananyag a számítógépes hálózatok biztonsági kérdéseit és az azokra adott válaszokat, megoldásokat veszi végig. Bemutatja a hálózati kommunikáció sérülékenységet, a lehetséges támadási formákat, illetve azokat az eljárásokat, módszereket, amelyekkel mint informatikai szakemberek megakadályozhatjuk a különböző támadásokat.

A biztonsági alapismeretek mellett foglalkoztunk a hálózati operációs rendszerek által nyújtott lehetőségekkel mint pl. a hozzáférési jogosultságok, állományok titkosítása. Bemutattuk a kriptográfiát mint tudományágat, de az elméleten túl megnéztük azokat az eljárásokat, algoritmusokat, protokollokat, amelyeket napjainkban is használnak az informatikai rendszerek titkosításra, hitelesítésre, a biztonságos kommunikáció megvalósítására. Külön fejezetek foglalkoztak a „népszerű”, gyakran használt szolgáltatásokkal, technológiákkal, így az elektronikus levelezés, a webhasználat, a vezeték nélküli kapcsolatok biztonságáról is sokat megtudhattak a tananyagból.

Az egyes megoldások megismeréséhez, megértéséhez a Microsoft operációs rendszerek és rendszerszintű alkalmazásokat mutattuk be, de természetesen hasonló módon egyéb platformokon is használhatóak az itt leírt technológiák.

13.2. ZÁRÁS

A tananyag talán legfontosabb mondanivalója, hogy nincs tökéletes megoldás az elektronikus kommunikáció védelmére. Ezt sose felejtjük el! Viszont próbáljunk megtenni mindent annak érdekében, hogy az általunk használt alkalmazások, rendszerek minél inkább biztonságosabbak legyenek. Ehhez ismerünk kell a lehetőségeket, vagyis azokat a védelmi megoldásokat, amelyek adott időpontban a legnagyobb biztonságot tudják nyújtani. Az informatika gyorsan változó, fejlődő tudományág, nem egyszerű minden történést, fejleszt-

tést aprólékosan nyomon követni, de amennyiben egy rendszer felügyeletét ránk bízta, akkor legyünk tisztában a legújabb fenyegetettségekkel, támadási formákkal és természetesen tegyünk meg mindent annak érdekében, hogy ki tudjuk védeni azokat.

13. KIEGÉSZÍTÉSEK

13.2. IRODALOMJEGYZÉK

Hivatkozások

Könyv

- BERTA István Zsolt Dr.: *Nagy e-szignó könyv: Amit az elektronikus aláírásról tudni akartál, csak féltél megkérdezni.* Budapest, Könyvműhely, 2011
- GÁL Tamás, SZABÓ Levente, SZERÉNYI László: *Rendszerfelügyelet rendszergazdáknak,* Budapest, Szak Kiadó, 2007
- ILLÉS Márton – BÁNFI Tamás: *Tűzfalak evolúciója.* Budapest, BalaBit White Papers, 2003.
- LENGYELNÉ MOLNÁR Tünde: *Digitális jogok kezelése.* Eger, Eszterházy Károly Főiskola, 2011.
- TANENBAUM, S. Andrew: *Számítógép-hálózatok.* Budapest, Panem kft., 2004.
- VIRRASZTÓ Tamás: *Titkosítás és adatrejtés: Biztonságos kommunikáció és algoritmikus adatvédelem.* Budapest, NetAcademia Kft., 2004.

Elektronikus dokumentumok / források

- A kriptográfia története.* [elektronikus dokumentum] [2012. május 16.] <URL: http://hu.wikipedia.org/wiki/A_kriptogr%C3%A1fia_t%C3%B6rt%C3%A9nete>
- A számítógép védelme.* [elektronikus dokumentum] [2012. május 16.] <URL: <http://windows.microsoft.com/hu-HU/windows/security-essentials-download>>
- Informatikai Tárcaközi Bizottság: *Informatikai biztonsági módszertani kézikönyv.* 1994. [elektronikus dokumentum] [2012. június 28.] <URL: http://www.itb.hu/ajanlasok/a8/html/a8_m3_1.htm>