HADMÉRNÖK

IV. Évfolyam 2. szám - 2009. június

László Zsuzsanna
Budapesti Műszaki Főiskola
laszlozsuzsu@gmail.com

REJTJELBIZTONSÁG

Absztrakt

A rejtjelbiztonság (CRYPTOSEC = CRYPTOgraphic SECurity) biztonsági intézkedések és eszközök alkalmazása - beleértve a rejtjelző eszközök[1] fizikai biztonsági rendszabályainak alkalmazását is - abból a célból, hogy megvédjék a tárolás és az átvitel alatt az információt az illetéktelen felhasználás (megismerés) ellen. A rejtjelző eszközök és módszerek alkalmazásával megvalósított rendszabályainak összessége.

The cypher safety (CRYPTOSEC = CRYPTOgraphic SECurity) the application of safety measures and devices - including using the cypher clerk for the physical safety measures of devices - from the aim that the information should be protected under the storage and the transfer the unauthorized use (cognition). The totality of the measures of the cypher clerk accomplished with the application of devices and methods.

Kulcsszavak: *rejtjelbiztonság, rejtjelzés, kriptográfia, titkosítás ~ CRYPTOSEC CRYPTOgraphic SECurity, cypher safety, encoding, cryptography, encryption*

BEVEZETÉS

A második évezred utolsó évtizedében gyökeres változások következtek be a kommunikáció területén, melyek átformálták világunkat, gondolkodásmódunkat, új követelményeket támasztottak és komplex, bonyolult feladatok megoldására késztettek bennünket. Ebben az évtizedben - melyet sokan a digitalizáció arany korszakának hívnak - megszülettek azok az elméletek és alapelvek, nemzetközi szabványok és ajánlások, továbbá technológiák, melyek nyomán robbanásszerű fejlődésnek indulhatott a hírközlés, az informatika és az elektronikus média szinte valamennyi területe.

[1] Rejtjelző eszköz: nemcsak a rejtjelzést végző berendezés, kulcs, hanem a módszerekről, leírásokról szóló dokumentumok, működési utasítások, biztonsággal összefüggő szabályzatok (43/1994. (III. 29.) Kormányrendelet 1.§. 2, 3).

Az elmúlt időszakban a távközlés területén három irányzatot figyelhettünk meg. Ezek közül a legrégebbi és egyben a fejlődés fő motorja a digitalizálás. Ezzel szoros kapcsolatban áll a csomagkapcsolt átviteli technika és annak világméretben elterjedt formája az Internet. A harmadik alapvető fontosságú irányzat a hihetetlen gyorsasággal terjedő mobil távközlés. Megjelent az információs hadszíntér, vagy kibernetikus tér fogalma. Ma a figyelem fókuszában tehát az *információ* van. Vagyis annak megléte, vagy hiánya, tárgyhoz tartozása, időbenisége, megbízhatósága és pontossága. Kulcskérdéssé váltak azok a folyamatok, szervezeti és technikai rendszerek, amelyekben az információ gyűjtése, továbbítása, tárolása, feldolgozása és elosztása folyik.

Ezek a hatások kiemelten érintették a védelmi szférát, a hadseregeket és mindenekelőtt azok vezetési és irányítási rendszereit. A hadviselésben - ugyanúgy mint a polgári szektorban - célként (és döntő tényezőként) jelent meg az *információs fölény*, vagy információs uralom kivívása, mely az információ mindhárom dimenziójára (tárgyhoz tartozás, pontosság és időbeniség) komplexen kiterjedő támadó és védelmi jellegű információs műveletekkel érhető el.

A technika fejlődése, elterjedése megnövelte az információbiztonság szerepét, jelentőségét. A rendkívül gyors fejlődés miatt szinte követhetetlen a fenyegető tényezők felmérése, a megfelelő biztonsági intézkedések bevezetése. Korunk információs forradalma nem hozott egyértelmű fejlődést ezeken a területeken, inkább csak új problémákat vetett fel, melyek jelentősen megnehezítik a biztonság elérését. [1]

A fejlődés hatóerejévé a civil (üzleti) szféra vált. Jelentősen megnőtt a polgári eszközök felhasználása, a nemzetközi szabványok alkalmazása. A fejlődéssel való lépéstartás, ezzel együtt az információfölény biztosításának követelménye felveti az új eredmények azonnali felhasználási lehetőségének megteremtését. Folyamatosan növekszik az igénybe vett polgári szolgáltatások, hálózatok és rendszerek aránya. Eltolódás tapasztalható – ott, ahol azt a katonai követelmények lehetővé teszik - a saját rendszerek alkalmazása és fejlesztése irányából a polgári szolgáltatások igénybevételének irányába.

A biztonsággal korunk sokszor ismeretlen veszélyei miatt elkerülhetetlen foglalkozni, úgy a civil területeken, mint a védelmi érdekkörökben. A katonai szférában mindig is fontos volt az információ védelme, az utóbbi időben azonban pont ezen fenyegetettségek és a polgári befolyásoltság miatt felértékelődött ennek szerepe.

Az elmúlt években a politikai viszonyok is gyökeresen megváltoztak. A két világrendszer szembenállása megszűnt, a Varsói Szerződés felbomlott, majd közel egy évtized után Magyarország a NATO teljes jogú tagjává vált. A NATO csatlakozás hatásait és következményeit tekintve is jelentős változásokat hozott és még hoz ma is mind a Magyar Honvédség, mind országunk életében. A NATO-ba való belépésünk óta új követelményeknek kell megfelelni a biztonságpolitika területén is, hiszen nem csupán hazánk bizalmas információit kell féltenünk és óvnunk, hanem a Szövetségét is.

AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁG [2]

Az elektronikus információbiztonság (INFOSEC = INFOrmation SECurity) olyan intézkedések alkalmazását jelenti, - a nemzeti, két vagy többoldalú együttműködés alapján szervezett és üzemeltetett híradó, informatikai és egyéb elektronikus rendszerekben, és biztosító infrastruktúráikban - amelyek védelmet nyújtanak a megjelenített, tárolt, feldolgozott és továbbított minősített információk bizalmasságának, sértetlenségének és rendelkezésre állásának véletlen vagy szándékos csökkenése ellen. Az alkalmazott biztonsági rendszabályok összessége, beleértve a hozzátartozó fizikai, személyi, dokumentációs és eljárásbeli biztonságot is.

A *sértetlenség* (Integrity) a minősített információ azon tulajdonsága, amely teljes,

pontos, és ellentmondásmentes állapotát jellemzi. Biztosítja, hogy az információt nem lehet módosítani, megsemmisíteni jogosulatlan személy, vagy művelet által. A sértetlenséget a jogosulatlan, vagy nem megfelelő (téves) megsemmisítés, módosítás veszélyezteti.

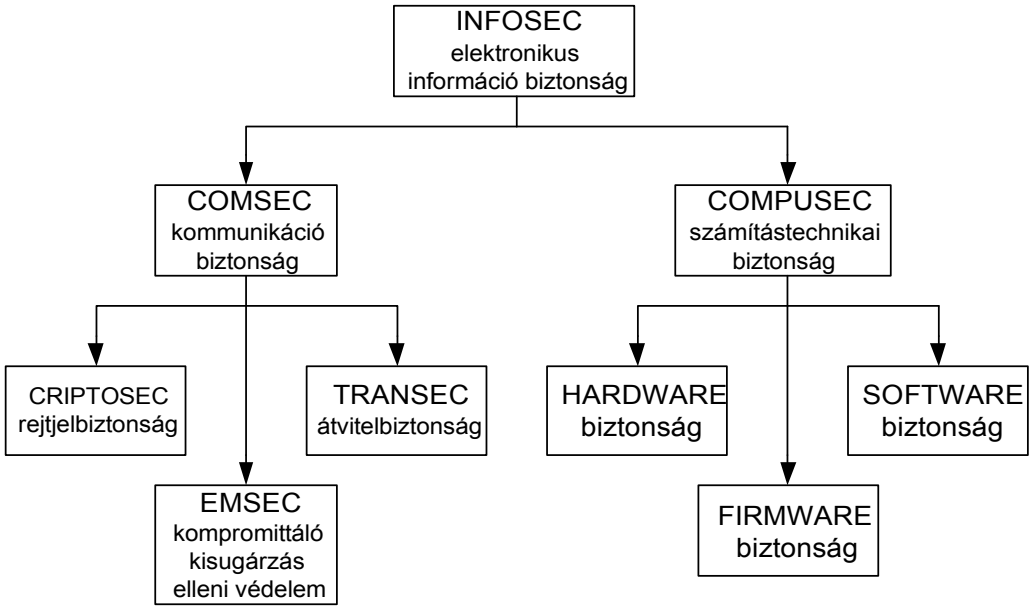
A *rendelkezésre állás* (Availability) a minősített információ azon tulajdonsága, amely a jogosult felhasználók számára történő, igényeiknek megfelelő hozzáférés és felhasználás lehetőségét jellemzi. Eljárások, eszközök alkalmazását jelenti, amelyek megakadályozzák a jogosultak hozzáférési lehetőségének csökkenését az érzékeny, vagy kritikus információkhoz szándékos külső vagy belső támadás, véletlen esemény, vagy más körülmények által. A rendelkezésre állás nemcsak a felhasználók tevékenységét segíti (pl. rendszergazda, biztonsági ellenőrzés). A „más körülmények által" kifejezés értelmezhető a megbízható szolgáltatások érdekében kialakított műszaki megoldásokra is, amely megnyilvánulhat a magas technikai színvonalú eszközök rendszeresítésében, vagy az eszközök, rendszerek megfelelő elemeinek redundanciájában és egyéb üzembiztonsági műszaki megoldásokban. A rendelkezésre állást többek között a szándékos vagy véletlen megsemmisítés, módosítás, valamint az (információ) szolgáltatás akadályoztatása veszélyezteti.

A *bizalmasság* (Confidentiality) a minősített információ azon tulajdonsága, amely a hozzáférés, megismerés megengedett lehetőségeit és módjait jellemzi. Az információkat nem lehet elfogni, azok nem fedhetők fel illetéktelen személyek, csoportok, vagy folyamatok számára, illetve a híradó és informatikai csatornákat - amelyek minősített információt szállítanak a rendszeren belül, a rendszer felé, vagy a rendszertől kifelé - nem lehet átirányítani. A bizalmasságot az illetéktelen hozzáférés, betekintés, megismerés veszélyezteti.

A *nyilvántarthatóság* (Accountability) a jogosult felhasználók, rendszerfelügyelők (és egyéb szereplők) minősített információkhoz való hozzáféréseinek (írás, olvasás, módosítás, törlés) és elvégzett műveleteinek (adás, vétel, rendszerrel kapcsolatos műveletek) egyéni elszámoltatási kötelezettségét jelenti.

A *hitelesség* (Authentication) a minősített információ azon tulajdonsága, amely forrásának eredetiségét, valódiságát jellemzi. Olyan biztonsági intézkedések kialakítását jelenti, amelyek segítségével megállapítható, hogy az átvitel során megérkezett küldemény azonos a feladott üzenettel, a feltüntetett forrás valóban megegyezik-e az információ valódi forrásával, vagy személy, alkalmazás azonosítását végzik, aki (amely) speciális kategóriájú információhoz igényel hozzáférést. A hitelességet többek között a jogosulatlan módosítás és a megszemélyesítés veszélyezteti. A hitelesítés feladatkör szorosan összefügg a bizalmassággal és a rendelkezésre állással, mivel az információkhoz és szolgáltatáshoz való hozzáférési kérést azonosítja és pozitív eredmény esetén engedélyezi az igényelt műveletet.

Az említett feladatok biztosítása komoly technikai megoldásokat és összetett szervezési feladatokat igényel, amely a következő szakterületek feladata:



1. ábra. Az elektronikus információbiztonság felosztása

A Magyar Honvédség – illetve tágabban vizsgálva a Magyar Köztársaság – pontosan ezzel a struktúrával jelenleg nem rendelkezik. A NATO azonban a minősített, elektronikus adatainak védelme érdekében a Szövetség a bemutatott tagozódás szerint kommunikál hazánkkal, tehát a kapcsolódó szakterületeknek előbb, vagy utóbb komolyabb, közvetlen együttműködésre lesz szüksége.

Két nagy területe a *kommunikációs* és *számítástechnikai* biztonság, amelyek között – az összetett eszközök és feladatok miatt – esetenként igen nehéz pontos határvonalat húzni.

Számítástechnikai biztonság [3]

A számítástechnikai biztonság (COMPUSEC = COMputer SECurity) hardver-, firmver-, szoftvermegoldások alkalmazása, a számítástechnikai rendszer védelme és az információk vagy programok jogosulatlan megismerése, manipulálása, módosítása, törlése, a rendszerekbe történő beavatkozás vagy a szolgáltatás leállítás megakadályozásának megelőzése érdekében. Az információvédelmi rendszabályok alkalmazása a híradó, informatikai és egyéb rendszerekben a feldolgozott, tárolt vagy továbbított információk bizalmasságának, sértetlenségének vagy rendelkezésre állásának szándékos vagy véletlen megszűnése ellen.

FIRMVER biztonság

A FIRMVER feladata a processzorok, beégetett programok szintjén történő védelem megvalósítása, amelyet a tervezés, gyártás különböző fázisainál kell alkalmazni annak érdekében, hogy kialakított eszköz pontosan azt és akkor végezze, ahogy azt tervezték, illetve ezen kívül ne tartalmazzon más információt, esetleges műveleti képességet (időzítést, működés módosulást stb.).

HARDVER biztonság

A HARDVER biztonság a számítástechnikai rendszerekben olyan fizikai megoldások alkalmazása, amelyek biztosítják az INFOSEC célkitűzések elérését.

Széleskörű feladatai közé tartozik például a tesztelt, ellenőrzött hardver elemek biztosítását, a szükséges konfiguráció kialakításának és megváltoztatásának szabályozását, a javítási és karbantartási rendszer kézbentartását és az eszközök (hálózatok) hozzáférés védelem.

SZOFTVER biztonság

A SZOFTVER biztonság végrehajtó és felhasználói programok alkalmazásával a számítástechnikai eszközök (rendszerek) által kezelt információk, valamint azok forrásainak védelmét jelenti.

A SZOFTVER biztonság feladatai között szerepel a rendszer- és alkalmazói programok ellenőrzése, bevezetése, installálása, biztonsági másolatok készítése és tárolása, a vírusellenőrzés és ezzel kapcsolatos biztonsági rendszabályok, a különböző programok használati rendjének kialakítása és annak ellenőrzése.

A Magyar Honvédségnél nincs COMPUSEC szervezet. A számítástechnikai eszközök, rendszerek védelmét a különböző szintű informatikai szervezetek egyéb feladataik mellett végzik, hozzáférés védelem, programvédelem, adatvédelem témakörökre tagoltan.

Kommunikáció biztonság

A kommunikáció biztonság (COMSEC = COMmunication SECurity) olyan biztonsági intézkedések alkalmazása a kommunikációban, amelyek megakadályozzák az illetéktelen személyeket abban, hogy az üzenetek tartalmának birtokába jussanak, vagy a híradás vizsgálatával arra vonatkozó ismereteket szerezzenek, biztosítva a továbbított információ hitelességét. Lényeges, hogy nem csak magát az elektronikus információt kell védeni, hanem a feladó és a címzett adatait, az átadott információ hosszát, továbbítási útvonalát, egy pontra vonatkoztatva a kapott és küldött üzenetek számát, azok formáját stb., mert forgalom analízis segítségével szinte pillanatok alatt lényeges adatok derülhetnek ki harcálláspontokról, védett vezetési pontokról, a vezetés rendjéről és egyebekről. Így érthető, hogy a rejtjelzés mellett a másik két szakterület (amelyek a híradó rendszerek védelmével, illetve a végberendezésekkel foglalkoznak), szintén fontos szerepet töltenek be az információbiztonság érdekében.

Rejtjel-, átviteli, kisugárzás elleni és fizikai védelmi rendszabályok alkalmazására épülő védelem jogosulatlan személyek által-a kommunikációs eszközök megfigyelése alapján történő – értékes információhoz jutásának megakadályozása.

A különböző elektronikus végberendezések és átviteli utak és a kezelt, feldolgozott vagy továbbított adatok védelme.

A honvédelmi miniszter 33/2002.(HK 13.) HM utasítása és a NATO elvek figyelembe vételével a kommunikációs biztonságot az alábbi területeken szükséges egységes egészként kezelni:

- átvitelbiztonság (híradóbiztonság);
- kompromittáló kisugárzás elleni védelem;
- rejtjelbiztonság;

Az átvitelbiztonság [2][4]

Az átviteli utak védelme (TRANSEC = TRANsport SECurity) biztonsági intézkedések alkalmazását jelenti az információátvitel védelme érdekében, az adatok elfogása, az átviteli folyamatba történő beavatkozás és a jogosulatlan felhasználás. Ez a terület nem tartalmazza a fizikai védelmet és a rejtjelanalízis elleni védelmet.

Az elektronikusan továbbított információk átviteli útjainak védelme azért szükséges, mert lehallgatással, forgalomanalizálással, megtévesztéssel többfajta módon is zavart lehet okozni a hálózatokban, illetve olyan adatokat lehet összegyűjteni, amely segítséget nyújt az információk, vagy az információs rendszerek elleni támadáshoz, a kriptográfiai analízishez. Ezért az elsődleges feladat az, hogy a fenyegető tényezőket minél nagyobb arányban feltárják még a rendszer működtetése előtt, és ezután következhet egy olyan rendszer kiépítése mely ezeknek a fenyegetettségeknek ellenáll.

A TRANSEC védelem nehezen felfedhető, bonyolult digitális üzemmódokkal valósítható meg, digitális átviteli hálózat vezetékes és mikrohullámú átviteli útjainak egyedi, vagy csoportos titkosítással történő védelmével és korszerű rádiós üzemmódokkal.

Az adatoknak a meghatározott védelmi szintnek megfelelően a teljes átviteli úton védettnek kell lenniük. Semmit sem ér az a védelem, amely néhány digitális kapcsolóelem között megbízható védelmet nyújt, de az összetett átviteli út egy vagy több szakasza nincs biztosítva, vagy valamelyik felügyelet nélküli kapcsolóelem kockázat nélkül elfoglalható. A TRANSEC megoldások mellett az átviteli utak alközponti csatlakozásai, illetve az alközponti hálózatok rengeteg olyan feladatot tartalmaznak (alépítmények, elosztódobozok, rendezők, épületek belső kábelezésének védelme stb.), amelyek a fizikai biztonság témakörébe tartoznak, így érthető, hogy ezeket a feladatokat és az elektronikus védelmi megoldásokat csak együtt szabad kezelni.

A korszerű átviteli üzemmódok (pl. frekvenciaugratás, szórt spektrum, speciális burkológörbék), alacsony kisugárzási energiájú módszerek és speciális antennák algoritmusos védelemmel és kiegészítő biztonsági szolgálatokkal (pl. időpecsét, hitelesítés, azonosítás) teszik biztonságosabbá az elektronikus átvitelt. A hálózati forgalom analizálása ellen a kommunikációs protokoll közlemények hiányában is továbbít jeleket (padding).

Az átvitelbiztonság a távközlési hálózatokban történő átvitel során alkalmazott információvédelmi rendszabályok összessége.

Fő célja megakadályozni a távközlési rendszerhez való külső hozzáférést, illetve a folyamatban lévő katonai tevékenység forgalomelemzéssel történő feltárását. Közvetlen, vagy közvetett zavar okozása; olyan adatok összegyűjtése, melyek segítséget nyújtanak a kriptográfiai analízishez.

A kompromittáló kisugárzási elleni védelem (EMSEC)

Az EMSEC (EMission SECurity) olyan biztonsági intézkedések, és eszközök alkalmazását jelenti, amelynek célja megóvni az áthaladó információ megjelenítését, és az elektromos berendezések kompromittáló kisugárzásának analizálását.

Az EMSEC feladatkört nem szabad elszakítani az általános fizikai biztonsági és az információbiztonság fizikai rendszabályaitól. Ezek az ún. TEMPEST eszközök (pl. számítógépek, monitorok, nyomtatók, faxok) - a biztonsági zónákra vonatkozó rendszabályok betartása mellett - elvileg bárhol alkalmazhatók, amely működési jellemzőnek azért megvan az ára is: az eszközök a normál kivitelhez képest 6-10-szer drágábbak.

A kisugárzott jelek felfogása és elemzése alapján történő felfedésének megakadályozására irányuló információvédelmi rendszabályok összessége.

A kisugárzás elleni védelem többek között megvalósítható az elektromágneses kisugárzás TEMPEST technológia segítségével történő megakadályozásával, vagy korlátozásával. TEMPEST az árulkodó kisugárzások vizsgálatára és értékelésére, illetve az ellenük való védelmet biztosító rendszabályokra vonatkozó kifejezés.

Rejtjelbiztonság [1] [5]

A rejtjelbiztonság (CRYPTOSEC = CRYPTOgraphic SECurity) biztonsági intézkedések és eszközök alkalmazása - beleértve a rejtjelző eszközök[2] fizikai biztonsági rendszabályainak alkalmazását is - abból a célból, hogy megvédjék a tárolás és az átvitel alatt az információt az illetéktelen felhasználás (megismerés) ellen. A rejtjelző eszközök és módszerek alkalmazásával megvalósított rendszabályainak összessége.

A CRYPTOSEC az INFOSEC tevékenység alapja, amely a Magyar Honvédségben a jelenlegi rejtjeltevékenységnek felel meg. A honvédség e tevékenysége törvényi szabályozás alapján egységesen felépített és irányított, egyetemes felelősséget viselő tevékenység, amely független attól, hogy melyik katonai szervezet információját, milyen végberendezéssel, eljárással védi számítástechnikai, rádió, vagy éppen vezetékes távbeszélő rendszerben.

A hálózat biztonsága fordított arányban áll kiterjedésével. Védett hálózatot korlátozott számú felhasználóval, speciális célokra célszerű létrehozni. A nagykiterjedésű minősített információk védelmére szolgáló hálózatokban a védelmet végpontok közötti rejtjelző eszközök alkalmazásával lehet hatékonyan és biztonságosan megoldani.

Minősített információk - adott fizikai környezeten belüli - elektronikus továbbítása rejtjelzés nélkül csak elkülönített, hozzáférés elleni védelemmel, vagy az illetéktelen hozzáférést (annak szándékát) jelző, láthatóvá tévő belső hálózatokon történhet. Az ilyen hálózatokat, főleg stacioner környezetben, számítástechnikai helyi hálózatok kialakítására célszerű létrehozni. Ha a hálózat valamely ponton kikerül a felügyelt zónából, vagy az objektum területéről, a kilépő részt rejtjelzéssel kell védeni.

A rejtjeltevékenységre vonatkozó nemzeti szabályokat együttesen kell alkalmazni a NATO rejtjeltevékenységre előírt minimum biztonsági követelményekkel, azzal a kitétellel, hogy eltérő szabályozás esetén, a szigorúbb szabályt kell alapul venni.

A rejtjelzés fogalma

Rejtjelezés minden olyan tevékenység, eljárás, amelynek során valamely adatot abból a célból alakítanak át, hogy annak eredeti állapota a megismerésére illetéktelenek számára rejtve maradjon. A rejtjelzés részét képezi a rejtjelzett adat eredetivé való visszaállítása is.[3] A szakirodalom a rejtjelzést az algoritmusok (kriptográfiai módszerek), a kulcsrendszerek és a védelmi rendszer területekre osztja fel.

A rejtjelző (kriptográfiai) algoritmusok

Az alapvető felosztás kulcs nélküli, kulccsal működő rejtjelző algoritmusokat és egyéb – a rejtjelzés kiterjesztett feladataihoz tartozó – algoritmusokat különböztet meg.

Kulcs nélküli rejtjelző algoritmus esetén a rejtjelzés és visszafejtés a kommunikációban résztvevők által egyeztetett protokoll alapján történik. A folyamatban a

[2] Rejtjelző eszköz: nemcsak a rejtjelzést végző berendezés, kulcs, hanem a módszerekről, leírásokról szóló dokumentumok, működési utasítások, biztonsággal összefüggő szabályzatok (43/1994. (III. 29.) Kormány-rendelet 1.§. 2, 3).
[3] 43/1994 (III. 14.) Kr. 1. §.

nyílt szöveg és az algoritmus vesz részt. A módszer hátránya, hogy az algoritmus kompromittálódása esetén nincs más lehetőség, mint új megoldás rendszerbe állítása.

A kulccsal történő rejtjelzés esetén a nyílt szöveg rejtjelzésére az algoritmusra és egy kulcsként működő sorozatra van szükség. Az algoritmus és a kulcs függetlenek, egymásra vonatkozó információk belőlük nem nyerhetők.

Szimmetrikus algoritmus alkalmazásakor a rejtjelzett szöveg előállítása és visszaállítása során azonos jelsorozatra, kulcsra van szükség (ezt jelzi a „szimmetrikus" kifejezés). Az „azonos jelsorozat" feltételezi valamilyen biztonságos továbbítási megoldás (elektronikus továbbítás, szállítás) meglétét, mivel az üzenet címzettjének az eredeti üzenet visszaállításához szüksége van a kulcsra.

Aszimmetrikus rejtjelző algoritmus esetén a rejtjelzés és a nyílt szöveg visszaállítása eltérő kulcs alapján történik. Minden felhasználó két kulccsal rendelkezik, de a nyilvános vagy a titkos kulcs bármelyikének ismeretében a másik kulcs nem kikövetkeztethető. A módszer lényege, hogy a rejtjelzett szöveg bármelyik kulccsal előállítható, de ugyanaz a kulcs a nyílt szöveget nem képes visszaállítani, csak a párja. A nyilvános kulcs így nyílt csatornákon továbbítható, akár nyilvánosságra is hozható.

A rendszer fontos része a kulcsok elosztása és hitelesítése, amelyeket erre a célra kialakított megfelelő garanciák alapján hitelesített szolgáltatók végeznek. Ez azért lényeges, mivel a kommunikáció szereplői nem szükségszerű, hogy ismerjék egymást, így a szolgáltatótól átvett kulcs azonosíthatja őket az ismeretlen partner előtt. Hamis kulcs esetén egy harmadik fél beékelődhet a kommunikáló felek közé, és közöttük közvetítve megszerezheti, sőt módosíthatja is a közleményeket.

Az aszimmetrikus rejtjelzés lassúságának enyhítése érdekében a két rejtjelző módszert együttesen alkalmazzák (vegyes vagy hibrid rejtjelzés). Ilyenkor a rejtjelzett kommunikáció szimmetrikus rendben történik, az ehhez szükséges kulcsok továbbítására a rendszer aszimmetrikus eljárást alkalmaz.

Egyéb algoritmusok

Az egyirányú függvények alkalmazásának napjainkban egyre terjedő feladatai vannak, mert a módszer jól használható azonosításra. Ennek során az algoritmus egy jelsorozatot kódol, majd a kódolt sorozatot összehasonlítja egy tárolt, ugyanilyen módszerrel kódolt jelsorozattal, amelynek eredményeképpen megvalósulhat egy engedélyezési vagy elutasítási eljárás. A bemenő jelsorozat lehet a számítógép felhasználójának bejelentkezési jelszava, a beléptető rendszer kódja vagy egy személy valamilyen érzékelő által letapogatott és digitális jelsorozattá alakított biometrikus jellemzői (tenyér- vagy újlenyomat, retina- vagy hangminta). A folyamat lényege, hogy a tárolt (etalonként használt) adatok rejtjelzettek, a tár feltörése esetén is csak egy értelmezhetetlen adathalmazhoz lehet hozzáférni. A távoli helyről történő bejelentkezés hasonló védelme biztosítja, hogy az átviteli út jelszót nem továbbít nyíltan, így az elfogott, kódolt jelszóval a támadó nem sokat ér.[4]

A hash függvény a nyílt szöveg meghatározott elemeiből egy mintát (lenyomatot) állít elő, ami csak arra az egy nyílt szövegre jellemző. A lenyomatot a rejtjelzett közleményhez csatolva kell elküldeni. A vevő visszafejtés után a kapott nyílt szöveggel ugyanazon függvény szerint megismétli az eljárást, és meggyőződik arról, hogy a továbbított adaton nem történt-e változtatás (hitelesítési funkció).

A rejtjelzett közleményhez csatolt hash függvény értékének a szöveg rejtjelzésétől eltérő módon történő rejtjelzése digitális aláírásként működve azonosítja a feladót. Ugyanez a módszer kiegészítve az idő bedolgozásával (időpecsét) védi a közlemény vevőjét a

[4] Ez nem véd a rögzített jelszó későbbi illetéktelen felhasználása ellen, amit további védelmi elem beépítésével lehet megakadályozni.

visszajátszásos támadás ellen. Létfontosságú, hogy az alkalmazott algoritmus ne legyen megkerülhető, vagy ne tartalmazzon rejtett kapukat, amelyeken keresztül a kulcs ismerete nélkül is ki lehet nyerni a továbbított nyílt adatokat.

Nem hagyható figyelmen kívül a fejlődés sem, mert a számítástechnikai kapacitások gyakran havonta döntenek meg újabb csúcsokat, támogatva a kriptoanalízis hatékonyságát. Ugyanígy nem lehet kizárni, hogy valamelyik kutatóműhely nem talál olyan megoldást, amely más vagy korszerűsített módszerével meggyorsítja a megfejtést.

A rejtjelző kulcsok

A szimmetrikus és az aszimmetrikus rendszer egyaránt azon alapul, hogy a kommunikációban részt vevők rendelkeznek a kódoláshoz és dekódoláshoz szükséges kulcsokkal. A kulcsok azonos algoritmus esetén is egymástól függetlenek, előállításuk körülményeiből, illetve az egyes kulcsokból nem lehet következtetni más kulcsokra.

A rejtjelzés lényege, hogy olyan kulcsok alapján történjen, amelyeket nem lehet semmilyen adatból, állapotból vagy jelenségből kikövetkeztetni. A kellő hosszúságú, biztonságos véletlen szám generálásra alapozott kulcselőállítás és -sokszorosítás hierarchikus, központilag szabályozott folyamat. A sok helyen alkalmazott álvéletlen sorozatok (pseudo random) – annak ellenére, hogy hosszú periódusidejük miatt véletlen sorozatoknak tűnnek – megfelelő módszerekkel kiszűrhetők, így rejtjelzésre nem alkalmazhatók. A valódi véletlen sorozatok olyan fizikai eseményektől származó sorozatok (pl. fehér zaj, termikus zaj), amelynek esetében a sorozat egy korábbi eleméből nem lehet következtetni egy későbbi elemre.

A kulcsok időszakos váltása szükségessé teszi a lejárt kulcsok azonnali megsemmisítését, mert az esetlegesen kompromittált lejárt kulcs lehetővé teszi az elfogott rejtjelzett üzenetek utólagos megfejtését.

A rejtjelzés védelmi rendszere

A rejtjelzés eddigi két szegmense mutatta, hogy az alkalmazott eszközök, módszerek hatásossága azon múlik, hogy mennyire kizárt az illetéktelen megismerés veszélye. Az átviteli megoldások korszerű módszerekkel becsaphatók, az algoritmusokon rejtett bejáratok (back door) lehetnek, illetve a kezeléssel, üzemben tartással kapcsolatos írott, vagy egyéb formájú anyagok (vagy egy részük) számtalan módszerrel beszerezhetők. A vélhető támadást ezen okok miatt nem mindig kriptográfiai irányból kell feltételezni, illetve gyakran nincs is szükség elsődleges vagy teljes információkra (pl. elég, ha a kulcsképzés hiányossága miatt a feltörési idő töredékére csökken, vagy kompromittáló kisugárzás miatt a nyílt információ és a továbbított rejtjelzett anyag összehasonlítható). Emiatt a rejtjelzési folyamatot, mint rendszert védve ki kell alakítani azt a belső biztonsági gyűrűt, ami a kriptográfiai állóképesség szintjére emel minden védelmi elemet. A megerősítés jelentheti a fizikai vagy személyi védelmi elemek további szigorítását, de ugyanilyen eszköz a rejtjelző besorolású anyagok dokumentumainak elkülönítése.[5]

[5] 43/1994. (III. 29.) Kormányrendelet 17. § 1–2.

Felhasznált irodalom:

[1] Ködmön József: Kriptográfia; Computer Books Kiadó Kft.; Budapest,1999

[2] Kuti-Kollár-Lajos: Biztonság és titokvédelem a NATO szabályai szerint; Honvéd kiadó, Budapest, 1999

[3] Dr. Váncsa Juliana-Magyar Ferenc: Az informatikai rendszerek védelméről; Új Honvédségi Szemle, 2000/5.

[4] Magyar Ferenc: Globalizáció és információ biztonság; Hadtudomány X. évfolyam, 3. szám

[5] Kassai Károly: Az elektronikus információk védelmének területei; Hadtudomány