Az informatikai biztonság alapjai

Pintér-Huszti Andrea

2023. szeptember 17.

Tartalom

Alapfogalmak

Alapfogalmak - Informatikai biztonság alapfogalmai

Példák a biztonság sérülésére

- $\mathscr{A}$ az alkalmazottak fizetési jegyzékét küldi el $\mathscr{B}$-nek. $\mathscr{E}$, aki nem jogosult ezen adatok hozzáférésére, figyeli az adatátvitelt és készít magának egy másolatot.
- $\mathscr{A}$ szeretne könyvtárához teljes jogosultságot adni az új felhasználóknak. Ehhez "üzenetet küld" a gépnek ($\mathscr{B}$-nek), hogy módosítsa a jogosultság kezelő állományt. $\mathscr{M}$ figyeli a kommunikációt és módosítja az üzenetet, jogosulatlanul hozzáadja saját adatait.
- $\mathscr{A}$ üzenetet küld brókerének ($\mathscr{B}$-nek), hogy vásároljon bizonyos értékpapírokat. Időközben, a megadott részvények veszítettek értékükből. $\mathscr{A}$ letagadja, hogy valaha is ilyen üzenetet küldött volna $\mathscr{B}$-nek.

Informatikai biztonság fogalma

Az informatikai biztonság az informatikai rendszer olyan, a védő számára kielégítő mértékű állapota, amely az informatikai rendszerben kezelt **adatok** *bizalmassága*, *sértetlensége* és *rendelkezésre állása*, illetve a **rendszerelemek** *sértetlensége* és *rendelkezésre állása* szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

- zárt védelem: olyan védelem, amely az összes releváns fenyegetést figyelembe veszi
- teljes körű: a védelmi intézkedések a rendszer összes elemére kiterjednek
- folytonosság: a védelem az időben változó körülmények és viszonyok ellenére is folyamatosan megvalósul
- kockázatokkal arányosság: egy kellően nagy intervallumban a védelem költségei arányosak a potenciális kárértékkel

- Információbiztonság (information security): az informatikai biztonságnál szélesebb, a szóban, írásban, az informatikai rendszerekben, vagy bármilyen más módon információk védelmére vonatkozik
  Információbiztonsági intézkedések:
  - Adatvédelem (data protection): a **személyes adatok jogszerű** kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége. (NAIH - Nemzeti Adatvédelmi és Információszabadság Hatóság)
  - Adatbiztonság (data security): Az informatikai biztonság részhalmaza, az **adatok** jogosulatlan megszerzése, módosítása és megsemmisítése elleni **műszaki és szervezési megoldások** rendszere. (NAIH)

Biztonsági célok - CIA hármas

NIST Special Publication 800-33:

Bizalmasság(Confidentiality) Titkos vagy személyes információkat (*privacy*) jogosulatlanok nem ismerhetik meg. A bizalmasságot az adatok tárolásánál, feldolgozásánál és továbbításánál is garantálni kell.

Sértetlenség(Integrity) Két fogalom:

- Adatintegritás (data integrity): Teljesülésekor az adat jogosulatlanul nem módosult tárolása, feldolgozása vagy küldése során.
- Rendszer sértetlensége (system integrity): A rendszer működése az elvártnak megfelelő, jogosulatlan módosításoktól mentes.

Rendelkezésre állás(Availability) Biztosítja, hogy a szolgáltatás az arra jogosultak számára a szükséges időben és időtartamra használható.

További biztonsági célok

Nyomonkövethetőség (Accountability) Az a tulajdonság, hogy egy entitás által végrehajtott tevékenység visszakövethető legyen az entitáshoz. A tevékenységek ellenőrzés céljára rögzítésre kerülnek azért, hogy visszakövethetőek legyenek, bizonyíték álljon rendelkezésre. Ez a tulajdonság lehetővé teszi a letagadhatatlanságot (non-repudiation), a behatolások (intrusion) detektálását, megelőzését.

Garancia, biztosíték (Assurance) A bizalom abban, hogy a négy másik biztonsági célt (bizalmasság, sértetlenség, rendelkezésre állás, nyomonkövethetőség) a biztonsági alrendszer megfelelően ellátja/eléri.

Fogalmak közötti kapcsolatok

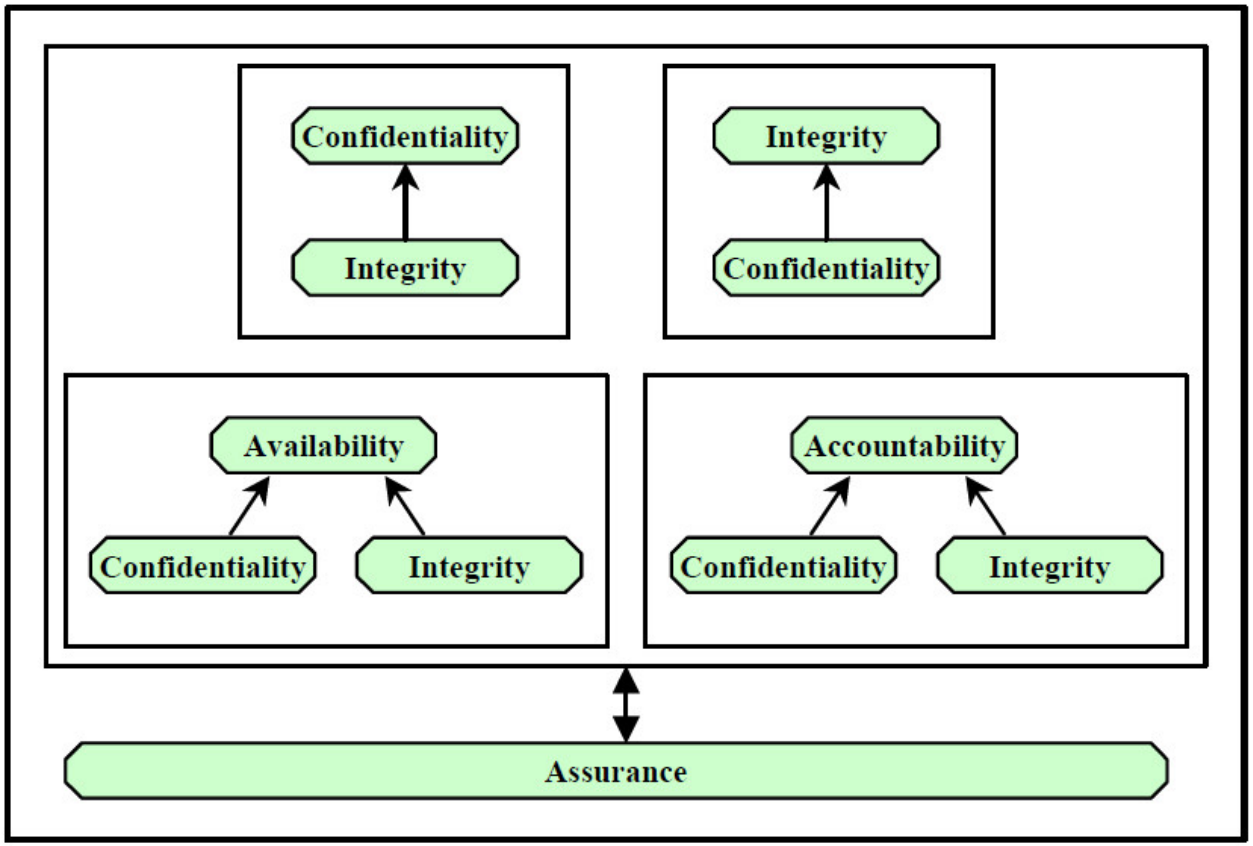


Figure 2-1 Security Objective Dependencies

ábra: NIST Special Publication 800-33

Fogalmak közötti kapcsolatok

- Bizalmasság függ a sértetlenségtől: Ha a rendszer sértetlensége sérült, akkor nem várható el, hogy a bizalmas adatok titokban maradtak.
- Sértetlenség függ a bizalmasságtól: Ha bizonyos információ (pl. jelszó) bizalmassága sérül, a sértetlenséget biztosító mechanizmusok kikerülhetőek.
- Rendelkezésre állás és nyomonkövethetőség függ a bizalmasságtól: Ha bizonyos információ (pl. jelszó) bizalmassága sérül, a rendelkezésre állást és nyomonkövethetőséget biztosító mechanizmusok kikerülhetőek.
- Rendelkezésre állás és nyomonkövethetőség függ a sértetlenségtől: Ha a rendszer sértetlensége sérült, akkor a rendelkezésre állást és nyomonkövethetőséget biztosító mechanizmusok szabályos működése is sérülhetett.

Hitelesség

Hitelesség (Authenticity) Valaminek a forrása az, amit megjelöltek, és a tartalma az eredeti.

- Felhasználó hitelesítése (Entity Authentication): Az a folyamat, amikor egy entitás meggyőződik egy másik entitás identitásáról.
- Üzenet hitelesítéső kód (Message Authentication Code): Egy rövid, fix hosszúságú érték, mely lehetővé teszi az üzenet *sértetlenségének* és *forrásának* ellenőrzését, de nem biztosítja a letagadhatatlanságot.

Sérülési szintek

Három szintet különböztetünk meg attól függően, hogy milyen fokú sérülés történik szervezeti, illetve személyi szinten.

Alacsony A sérülésnek csak *korlátozott* hatása van a szervezet, illetve a személy tulajdonára. A szervezet képes legfőbb feladatait végrehajtani, csak minimális kár keletkezik vagyontárgyaiban, bevétele csak minimális csökken, minimális személyi sérülés történik.

Közepes A sérülésnek *komoly* hatása van a szervezet, személy tevékenységére, tulajdonára. A sérülés jelentős kárt, bevétel csökkenést okoz, a szervezet még képes ellátni legfőbb feladatát, de hatásfoka jelentősen csökken.

Magas A sérülésnek *végzetes* hatása van a szervezet, személy tevékenységére, tulajdonára. Katasztrofális kár történik a vagyontárgyakban, tragikus költséget, személyi sérülést okoz, a szervezet nem képes ellátni feladait.

Példák - Bizalmasság

Alacsony Egyetemi kurzusokra regisztrált hallgatók névsora.

Közepes Hallgatók e-mail címe.

Magas Hallgatók érdemjegyeinek listája.

Példák - Sértetlenség

Alacsony Sok honlap lehetővé teszi, hogy ügyfelei leadhassák szavazatukat, véleményüket. Általában az így kapott eredmények csak irányt mutatóak. A rendszer implementálásánál nem alkalmaznak komoly védelmi mechanizmusokat.

Közepes Egy honlap lehetővé teszi, hogy a regisztrált felhasználók fórumon megvitassanak különböző témákat. Akár egy regisztrált felhasználó, akár egy külső támadó módosítja a bejegyzéseket. Ha a fórum szórakoztató jellegű, akkor pénzügyi kiesést (pl. reklám bevétel), adatvesztést jelenthet.

Magas Orvosi adatbázis bejegyzéseit egy arra nem jogosult alkalmazott (pl. ápoló)módosítja. A valótlan adatok akár tragikus, életveszélyes helyzetet is eredményezhetnek.

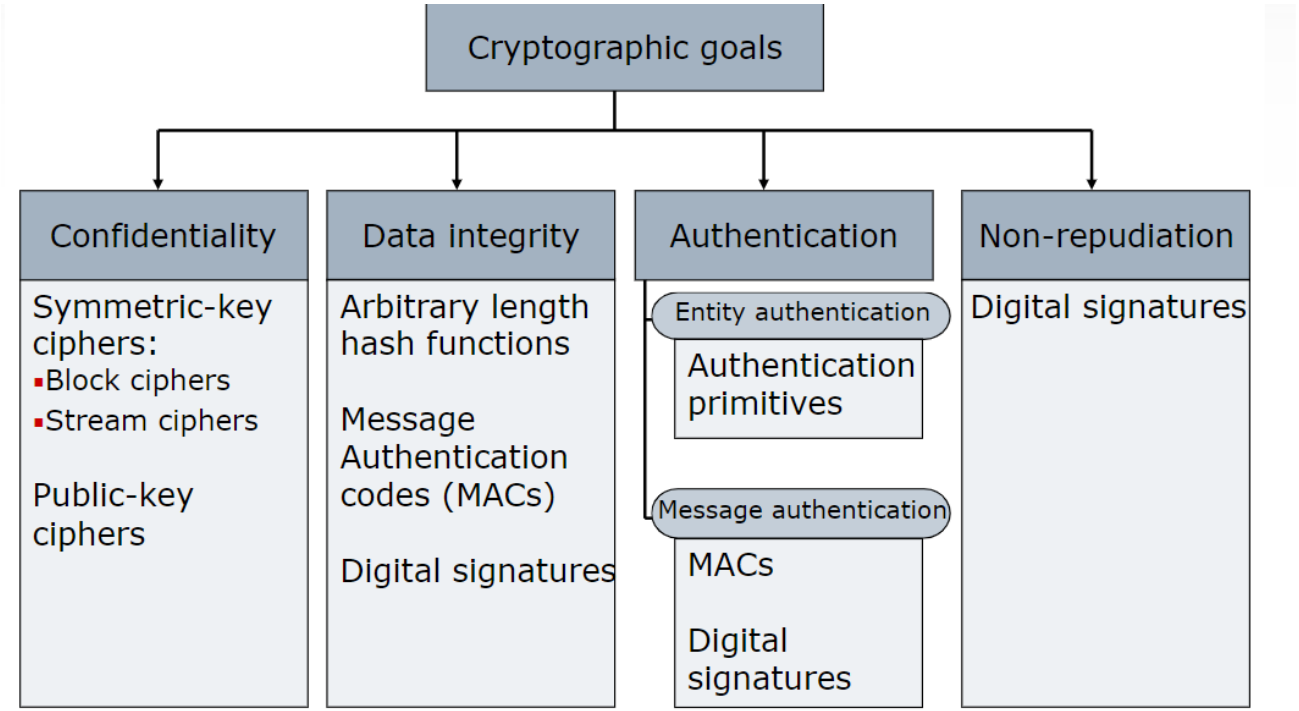
Példák - Rendelkezésre állás

Alacsony Webes telefonkönyv elérhetetlensége idegesítő lehet, de van más út egy telefonszám megszerzésére.

Közepes Egy alapítványi iskola honlapja információkat ad a támogatás módjáról. Ha a honlap nem elérhető, akkor a bevételük csökkenhet.

Magas Tekintsünk egy egészségügyi adatokhoz való hozzáférést vezérlő rendszert. Amennyiben ez a rendszer nem elérhető, akkor az orvosok nem jutnak hozzá az adatokhoz, mely akár a betegek életét is veszélyeztetheti.

Algoritmikus védelem - Kriptográfia



Alapfogalmak - Hálózati kommunikáció védelme

Hálózati kommunikáció védelme: OSI biztonsági architektúra

Hálózati kommunikáció védelme: OSI (Open Systems Interconnections) biztonsági struktúra (X.800 szabvány):

Biztonsági támadások Bármilyen tett, mely az információ biztonságát veszélyezteti.

Biztonsági mechanizmusok Eljárások, melyeket arra terveztek, hogy detektálja, megelőzze a támadást, vagy kijavítsa a támadás okozta kárt.

Biztonsági szolgáltatások Szolgáltatások, melyek védik az adatátviteli és feldolgozó rendszerek biztonságát. Egy biztonsági szolgáltatás egy vagy több biztonsági mechanizmust használ.

Hálózati kommunikáció - Biztonsági támadások

Két fő kategória:

Passzív támadások Az adatátvitel lehallgatása, monitorozása.
Cél: A továbbított adat megszerzése. Nehéz észrevenni, hiszen az átküldött adat nem módosul.

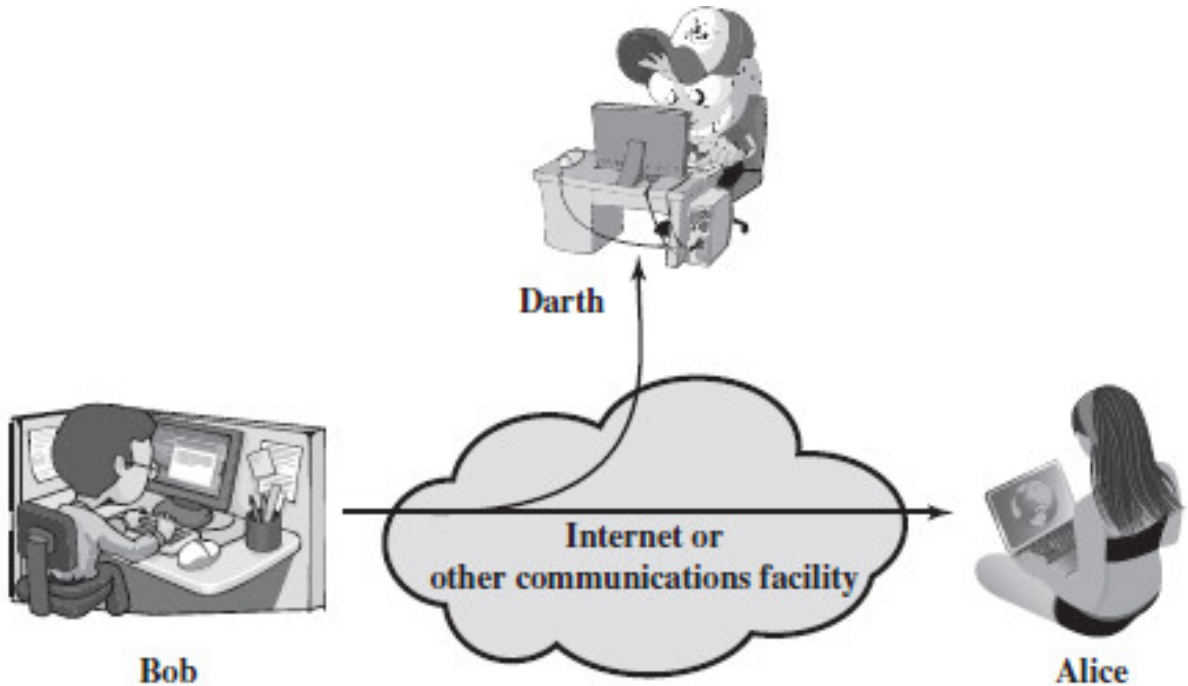
- Üzenet tartalmának megszerzése
- Forgalom elemzése

Aktív támadások Az adatfolyam módosítása, vagy egy hamis generálása. Nehéz teljes mértékben megelőzni.
Cél: A támadás detektálása és az okozott kár korrigálása.

- Megszemélyesítés
- Üzenet visszajátszása
- Adat módosítása
- Terheléses támadás (Denial of Service - DOS)

Támadások - Üzenet tartalmának megszerzése

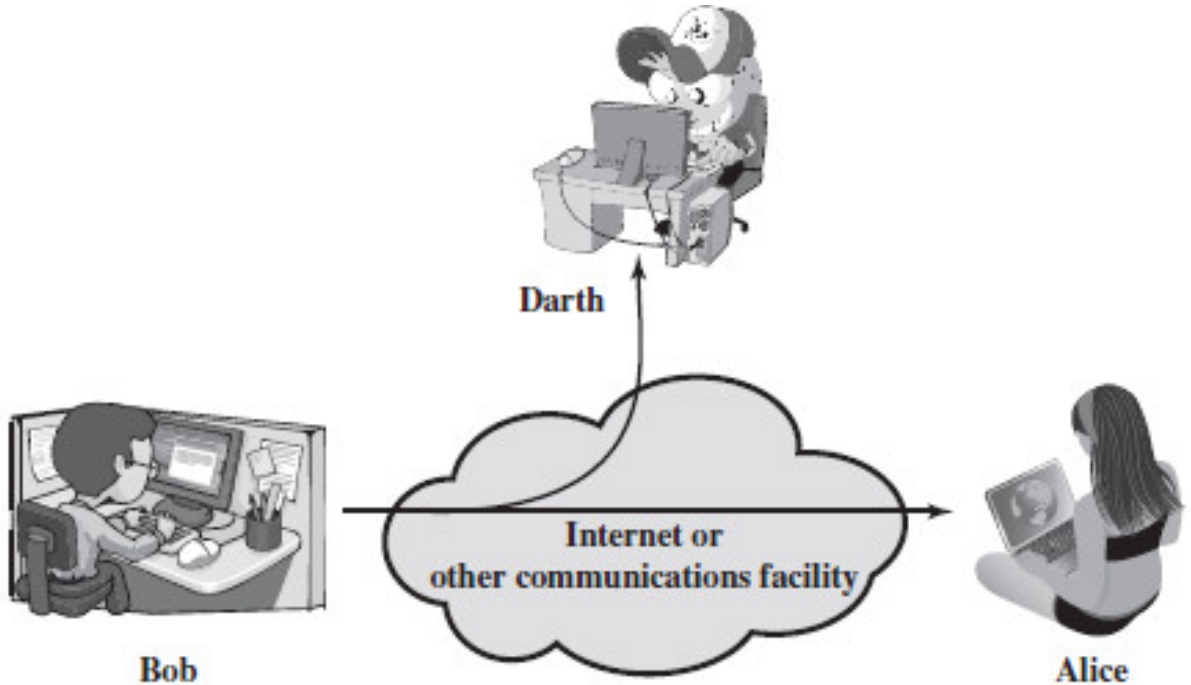
A támadó lehallgatja a csatornát és szeretné tudni az elküldött üzenet (pl. e-mail, átküldött állomány, telefonbeszélgetés) tartalmát.



(a) Passive attacks

Támadások - Forgalom elemzése

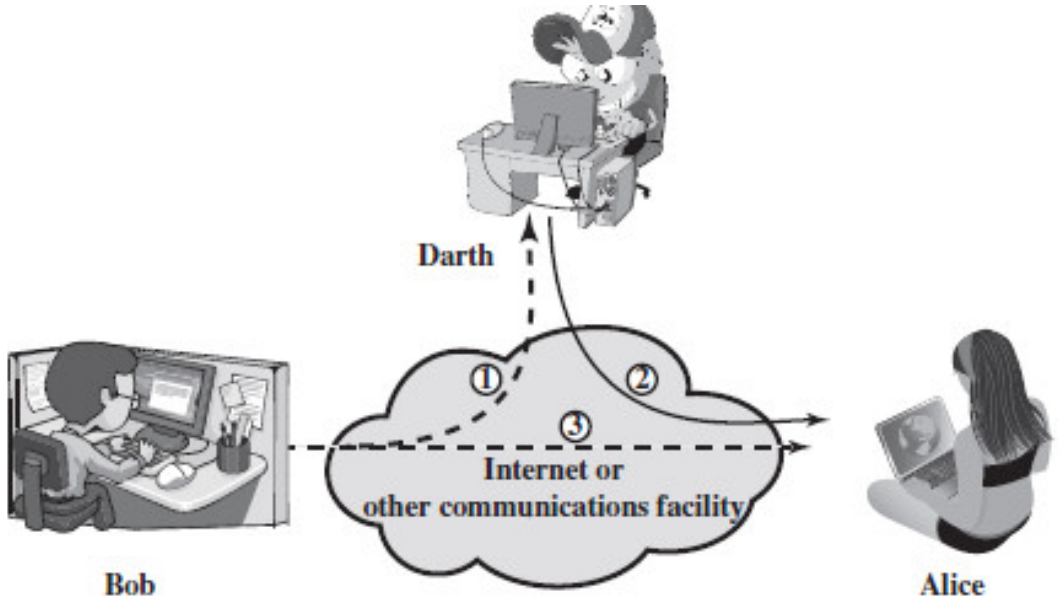
Tegyük fel, hogy a támadó a lehallgatott üzenetekből nem tudta megszerezni az információt. A támadó megfigyeli ezen üzenetek formátumát, meghatározhatja a kommunikáló felek helyét, kilétét, az üzenetek hosszát, gyakoriságát. Ezen információk alapján kitalálhatja egy üzenet tartalmát.



(a) Passive attacks

Támadások - Megszemélyesítés

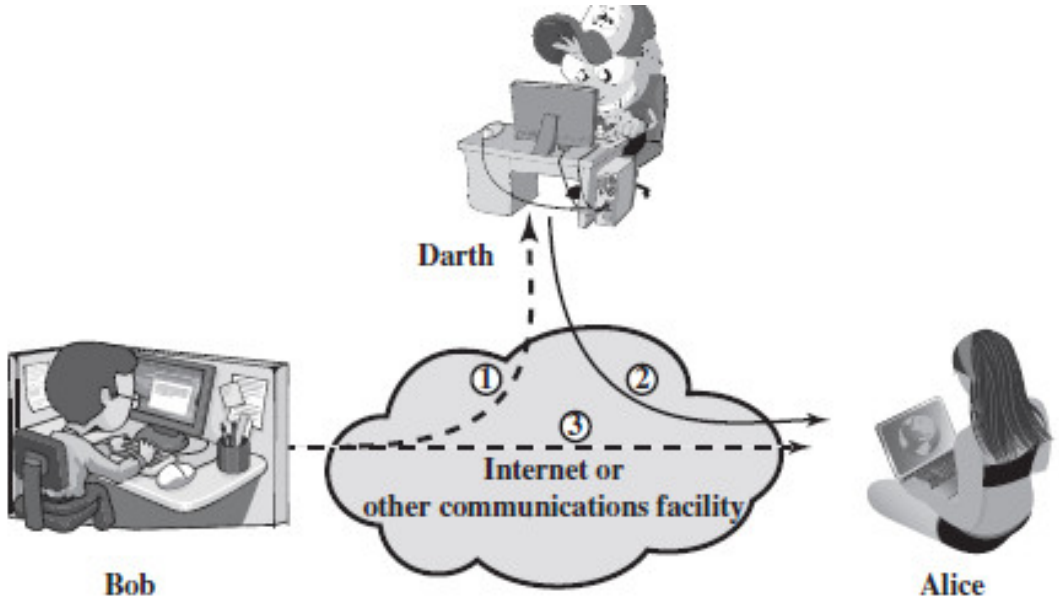
A támadó eljátsza a legális fél szerepét. (2) Általában ehhez a támadáshoz szükséges valamely másik aktív támadás (pl. üzenet visszajátszása).



(b) Active attacks

Támadások - Üzenet visszajátszása

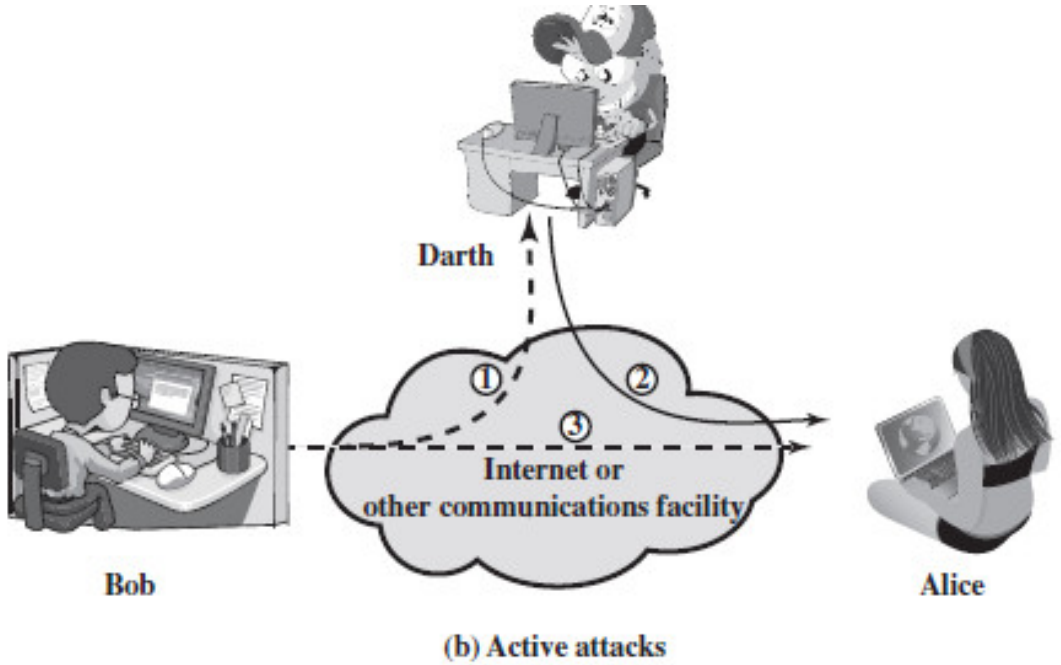
A támadó lehallgatja az üzenetet, majd újra elküldi (1, 2, 3).



(b) Active attacks

Támadások - Adat módosítása

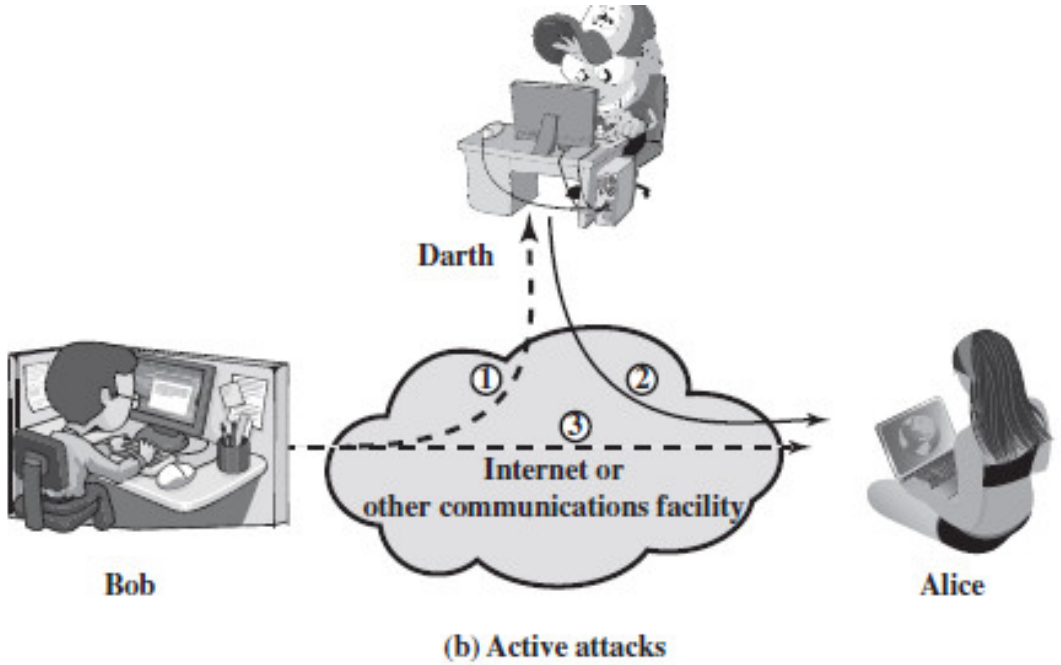
A támadó az üzenetek valamely részét, vagy a sorrendjét megváltoztatja (1, 2).



(b) Active attacks

Támadások - Túlterheléses támadás

A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat (3).



(b) Active attacks

Relationship

	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	x	x			x			
Data origin authentication	x	x						
Access control			x					
Confidentiality	x						x	
Traffic flow confidentiality	x					x	x	
Data integrity	x	x		x				
Nonrepudiation		x		x				x
Availability				x	x			