Az informatikai biztonság alapjai

Pintér-Huszti Andrea

2022. november 24.

Tartalom

Informatikai biztonság modellje, tervezési alapelvek

Alapfogalmak - Informatikai biztonság modellje

Alapfogalmak I.

biztonság alanya (asset) Az informatikai rendszer erőforrásai: hardver, hálózat és adathordozók, szoftver, adatok.

fenyegetés (threat) Olyan **lehetséges** művelet vagy esemény, amely sértheti az informatikai rendszer vagy az informatikai rendszer elemei védettségét, biztonságát.

sérülékenység (vulnerability) Az informatikai rendszer olyan gyengesége, amelyen keresztül valamely fenyegetés megvalósulhat. Kategóriák:

- rendszerelem módosulhat: nem megfelelően működik, rossz válaszokat ad, pl. a tárolt adatok jogosulatlanul megváltoznak
- rendszerelem szivárogtathat, pl. valaki jogosulatlan hozzáféréssel információkhoz jut
- rendszerelem nem elérhető vagy nagyon lassú, a rendszer vagy hálózat használata lehetetlen

Alapfogalmak II

támadás(attack) Fenyegetést előidéző cselekmény, mely valamilyen védett érték megszerzésére, vagy megsemmisítésre, károkozásra irányul.

Módja szerint:

1. aktív: Rendszerelemeket vagy azok működését módosítja
2. passzív: Rendszerinformációk megszerzése és felhasználása

Végrehajtója szerint:

1. belső: Jogosult a rendszerelem hozzáférésére, de arra nem jogosult módon használja fel.
2. külső: Egyáltalán nincs feljogosítva a rendszer használatára

A gyakorlatban a támadások nagy hányada belső támadás. A külső támadás célja sokszor a rendszerhez való hozzáférés, és azon belső támadás végrehajtása.

Alapfogalmak III.

kockázat (risk) A fenyegetettség mértéke, amely valamely fenyegető tényezőből ered. A kockázat egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.

Cél: a kockázat minimalizálása

Alapfogalmak IV.

védelmi intézkedés (countermeasure) Olyan eljárás, eszköz, technológia, mely csökkenti a rendszer sérülésének kockázatát.

Alkalmazás területe szerint:

1. Fizikai: kábelezés, védelmi eszközök, ajtók, tűzoltó készülékek, légkondicionálók stb.
2. Ügyviteli: szabályozások, eljárások, oktatás stb.
3. Technikai/algoritmikus: tűzfalak, autentikációs rendszerek, titkosítások stb.

Alapfogalmak IV.

védelmi intézkedés (countermeasure) Funkcionalitás szerint:

- Preventív intézkedések: Megelőzik a támadás bekövetkeztét (lehetnek fizikai, adminisztratív vagy technikai) pl. biztonsági frissítések, titkosítás
- Detektív intézkedések: Ha a preventív intézkedések meghiúsulnak vagy nem lehetségesek, akkor észleljük a támadást. pl. ellenőrző összeg, naplófájlok
- Korrektív intézkedések: Próbálják kijavítani a sérülést.(lehetnek technikai, adminisztratív) pl. backup/visszaállás

A védelmi intézkedések új sérülékenységeket eredményezhetnek.

Modell

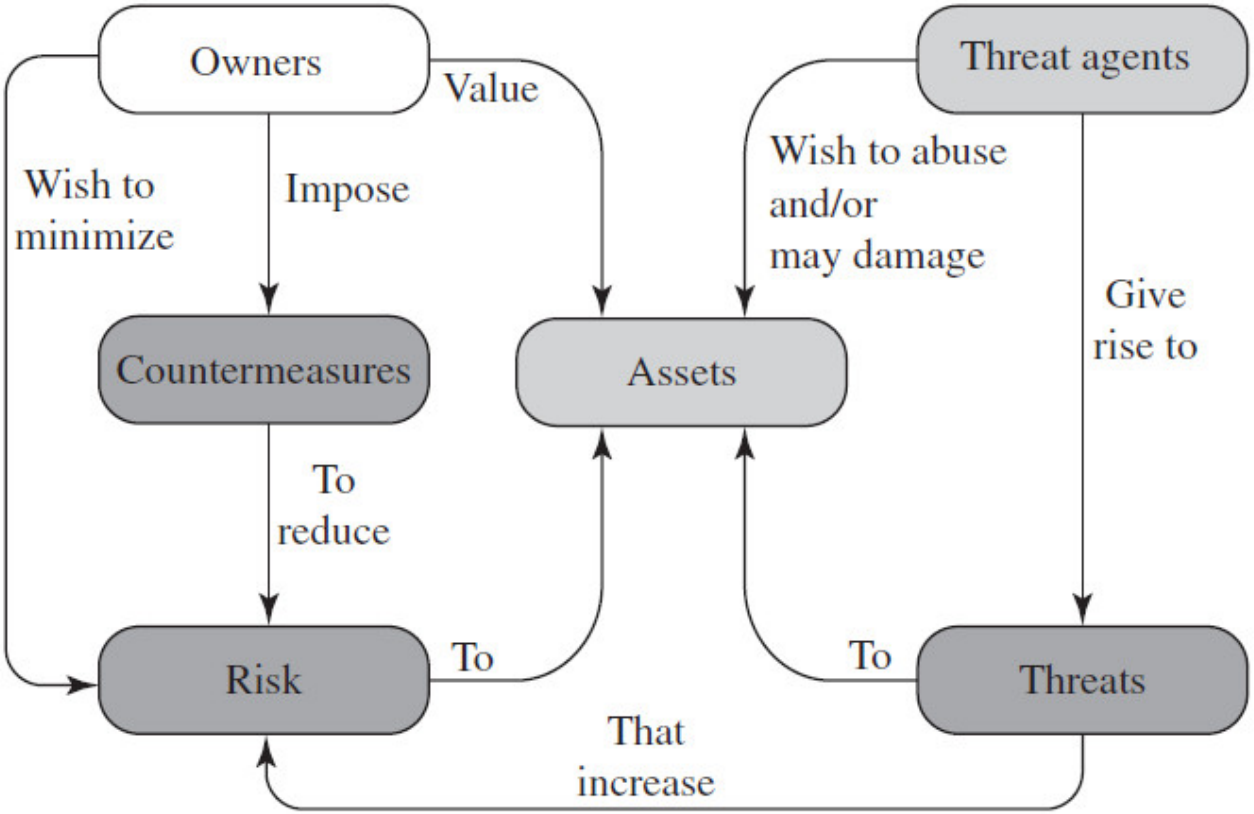

Figure 1.1 Security Concepts and Relationships

Alapfogalmak - Tervezési alapelvek

Tervezés folyamata

1. Mik azok a vagyontárgyak, erőforrások, amiket meg akarunk védeni?
   Teljes körűen kell felmérni a rendszerelemeket.
2. Milyen veszélyek fenyegetik az adott erőforrásokat?
   Kik/mik ellen védjük a rendszerelemeket, milyen lehetőségekkel, erőforrásokkal rendelkeznek.
3. Mekkorák a kockázatok? Milyen védelmi intézkedéseket vezessünk be?
4. Milyen hatásfokkal kezeli ezeket a kockázatokat a választott biztonsági megoldás?
   Sikeresség vizsgálata, kudarc gyakorisága.
5. A választott megoldás milyen új biztonsági réseket okoz?
   Működésbeli módosítások dominószerűen hullámzanak végig az adott rendszeren.
6. Megéri-e alkalmazni a megoldást?
   Pénz, idő, alkalmazás kényelmetlensége, csökkenő teljesítmény.

Tervezési alapelvek - Jogosultságok minimalizálása

- Ne adjunk több jogosultságot, csak annyit, amennyi feltétlen szükséges a feladat végrehajtásához.
- Preventív intézkedés, hiszen a jogosultságok korlátozásával csökkentjük a véletlen vagy direkt károkozást.
- Bármely informatikai rendszernél alkalmazható.
- Példák:
  1. A megosztott állományokhoz csak olvasási jogot adunk a felhasználóknak, ha csak erre van szükségük.
  2. A help desk kollégáknak nem adunk jogosultságot a felhasználói fiókok létrehozására, törlésére, ha csak a jelszó módosítását vezényelheti le.
  3. Szoftverfejlesztőknek nem adunk jogosultságot a szoftverek fejlesztői szerverekről az éles szerverekre történő átmásolására.

Tervezési alapelvek - Minimalizálás

- A jogosultságok minimalizálása alapelv testvére, csak a **rendszerkonfigurációra** vonatkozik.
- Olyan szoftvereket, alkalmazásokat, szolgáltatásokat ne futtassunk, melyek nem feltétlenül szükséges a biztonságos működéshez.
- Növeli a teljesítményt, tárhelyet takarít meg.
- Példa:
  Ha egy számítógép csak az elektronikus levelezés szolgáltatást biztosítja, akkor egyéb szolgáltatásokat lehetőleg ne installáljunk.

Tervezési alapelvek - Több szintű védelem

- Több szintű és többféle védelmet biztosítsunk
- Egy szintű vagy egyféle védelmet könnyebb támadni (bármilyen erősnek is hisszük), mint többet.
- Valamennyi védelmi mechanizmusnak szerepelni kell: preventív, detektív, korrektív
- Példa:
  Tűzfal használata az Internet és a LAN között és IP Security Architecture (IPSEC) segítségével titkosítják a bizalmas adatokat. Ha a tűzfalat feltörik, a támadóknak még mindig fel kell törniük a titkosítást.

Tervezési alapelvek - Open design

- Egy biztonsági mechanizmus elemeinek, működési módjának nyilvánosnak kell lenniük.
- Szakértők elemezhetik az algoritmusokat, így a felhasználók jobban bíznak bennük.
- 1883 Auguste Kerckhoffs alapeve: "az ellenség ismeri a rendszert", azaz azzal a feltétellel tervezzünk rendszereket, hogy az ellenség kezdettől fogva a teljes felépítését ismeri (Claude Shannon átfogalmazta)
- Példa:
  Csak a tikos kulcsokat tartsuk titokban, a titkosító algoritmusok nyilvánosak.

Tervezési alapelvek - Felosztás

- Parcellák, zónák, virtuális terek kialakítása
- Limitálja a kárt, ha egyik megsérül, más terek még védve vannak.
- Különböző zónákban futó alkalmazások egymástól elszigetelődnek.
- Példa:
  1. A webszerver szoftver kompromittálódása, nem befolyásolja a levelező szerver működését, ha külön szerverekre telepítjük, vagy virtuális szervereket hozunk létre.
  2. Solaris 10 operációs rendszer: *zónák*. A zóna egy virtuális operációs rendszer környezet, CPU idő, virtuális memória, hálózati sávszélesség, I/O teljesítmény stb. is szabályozható, virtuális szerverekként viselkednek.

Tervezési alapelvek - Az egyszerű megoldást válasszuk

- Az összetett, komplex rendszerek a legnagyobb ellenségünk.
- Nehéz tervezni, implementálni, tesztelni.
- Ha választani kell egy komplex, sokoldalú rendszer és egy egyszerű, mely kicsivel kevesebbet nyújt, válasszuk az egyszerűbbet.

Tervezési alapelvek - Pszichológiai elfogadhatóság

- Ha egy biztonsági mechanizmus gátolja az erőforrások könnyű hozzáférhetőségét, használatát, akkor a felhasználók kikapcsolhatják azt.
- A biztonsági mechanizmusnak a felhasználók számára transzparensnek kell lennie.
- A biztonsági algoritmusoknak követniük kell az emberi gondolkodást.

Alapfogalmak - Fenyegetések, támadások

Erőforrások és vagyontárgyak fenyegetései

Hardver Rendelkezésre állására irányuló fenyegetések a leggyakoribbak. Véletlen vagy szándékos fizikai rongálás, lopás. Pendrive-ok, tabletek, DVD-k stb. eltulajdonítása során az adatok bizalmassága is sérül. Fizikai és adminisztratív intézkedések adhatnak védelmet.

Szoftver Rendelkezésre állásra irányuló fenyegetés: alkalmazás törlése, módosítással haszontalanná válhat. Technikai védelem: Backup

Sértetlenségre irányuló fenyegetés: szoftver módosítása, vírusok.

Szoftverkalózkodás: másolatok készítése jogosulatlanul (nehéz a probléma megoldása)

Erőforrások és vagyontárgyak fenyegetései

Adat Védeni kell, mert *értékes, egyedi*. Mind továbbítás, tárolás, feldolgozás során sérülhet.
Bizalmasságra irányuló fenyegetés: pl. személyes adatok, tervek, gazdálkodási adatok jogosulatlan olvasása, megszerzése adatbázisokból
Sértetlenségre irányuló fenyegetés: adatok módosítása
Rendelkezésre állásra irányuló fenyegetés: adat törlése véletlenül vagy szándékosan

Támadási fák - Támadások, fenyegetések megadása

A támadási fa a rendszer sérülékenységeit kiaknázó lehetséges támadásokat, fenyegetéseket tartalmazza.

- A fa *gyökere* a támadás célja.
- A *levélelemek* a támadások különböző módjait adják meg.
- A gyökérből kiinduló utak nem levélelem csúcsai a cél eléréséhez szükséges részcélok.

Bankszámla feltörése - Internet bank felhasználó hitelesítés alkalmazás

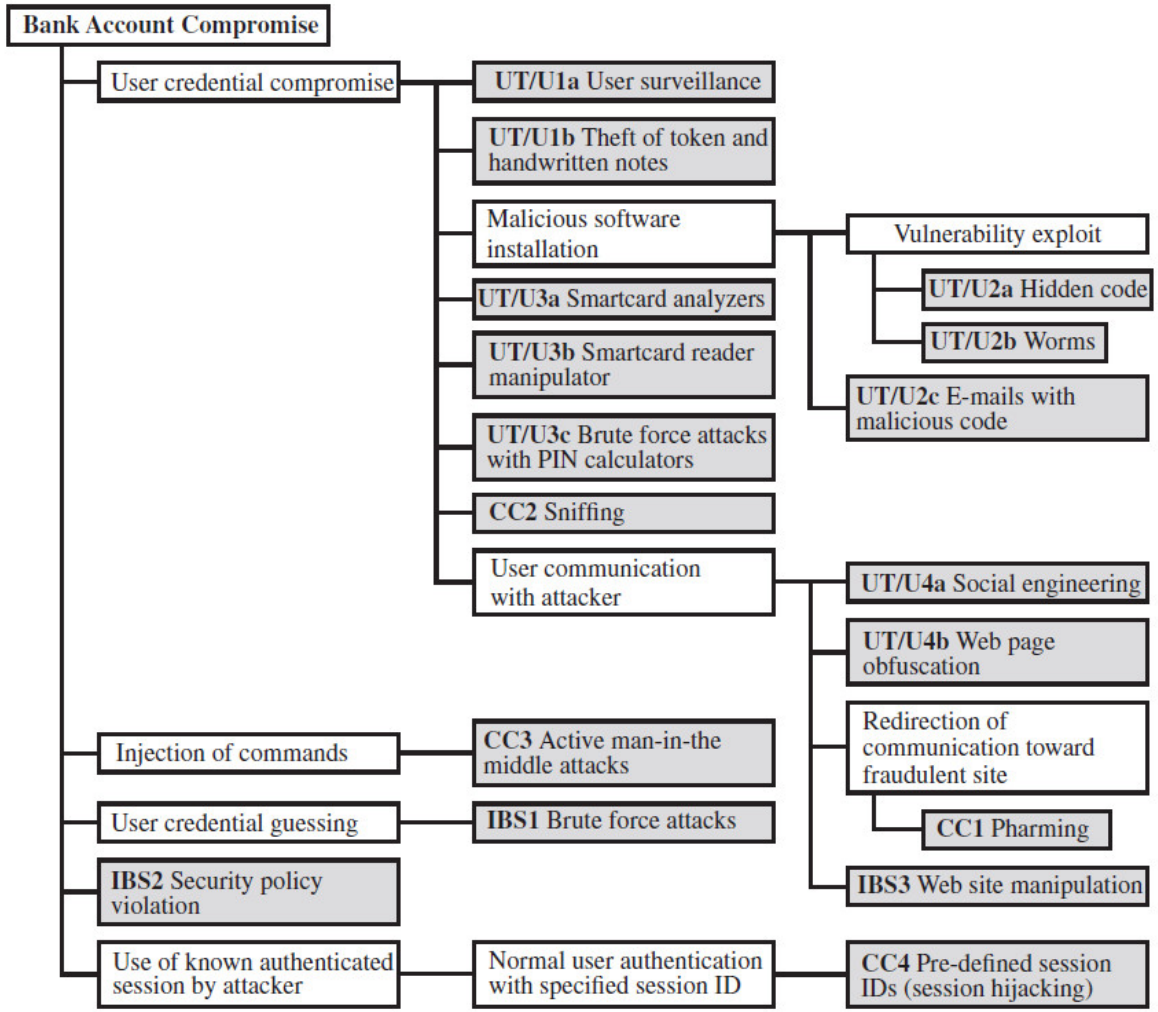

Figure 1.4 **An Attack Tree for Internet Banking Authentication**

Bankszámla feltörése - Internet bank felhasználó hitelesítés alkalmazás

- Felhasználói terminál, felhasználó (UT/U): Ezek a támadások a felhasználói eszközöket célozzák meg, pl. token, smartcard, jelszó generátorok vagy felhasználói tevékenységek.
  pl. *féreg (worm)*: Olyan program, amely a számítógép hálózaton keresztül terjed és károkozó hatását önmaga reprodukálásával, továbbításával éri el.
- Kommunikációs csatorna (CC): Kommunikáció során felmerülő támadások.
  pl. *hálózati forgalom lehallgatása (sniffing)*: csatorna figyelésével bizalmas adatok megszerzése
- Internet bank szerver (IBS): Off-line támadások az Interent bank alkalmzást hosztoló szerverrel szemben.

Bankszámla feltörése - Internet bank felhasználó hitelesítés alkalmazás

- Utasítások befecskendezése (Injection of commands): A támadó megfigyeli az UT és IBS közötti kommunikációt. A támadások lényege egy legális résztvevő megszemélyesítése.
- Felhasználó személyazonossági adatainak kitalálása: Nyers erő támadás, teljes kimerítő kipróbálások a felhasználó hitelesítési sémával szemben véletlen felhasználói nevek és jelszavak küldésével. A támadás módja *osztott* zombi számítógépeken automatizált felhasználói név és jelszó generálása.
  Zombi számítógép: az Internetre kapcsolódó számítógép, melyeket a támadó irányítása alá vesz és erőforrásait saját célra használja.

Bankszámla feltörése - Internet bank felhasználó hitelesítés alkalmazás

- *Adathalászat - Pharming*: A támadó valamilyen rosszindulató szoftver vagy kémszoftver segítségével az eredeti lapról egy másik, hamisított weblapra téríti el a felhasználót.
- *Munkamenet-eltérítés (Session hijacking)* Érvényes, már belépett felhasználó sessionId-jét (vagy session key-jét) próbálja meg megszerezni, hogy jogosulatlanul információhoz vagy szolgáltatáshoz jusson a támadó.
- *Pszichológiai manipuláció (Social engineering)*: Az emberi természetet igyekeznek kihasználni, személyes információk megszerzése céljából.