Támadási fák

Dr. Dobb's Journal December 1999

Biztonsági fenyegetések modellezése

Bruce Schneier cikke[1]

Bruce a Counterpane Internet Security cég műszaki vezetője, az Applied Cryptography (Alkalmazott titkosírás, második kiadás, John Wiley & Sons kiadó, 1995) szerzője és a Blowfish valamint a Twofish titkosító algoritmusok kidolgozója. A http://www.counterpane.com/ címen lehet kapcsolatba lépni Bruce-szal.

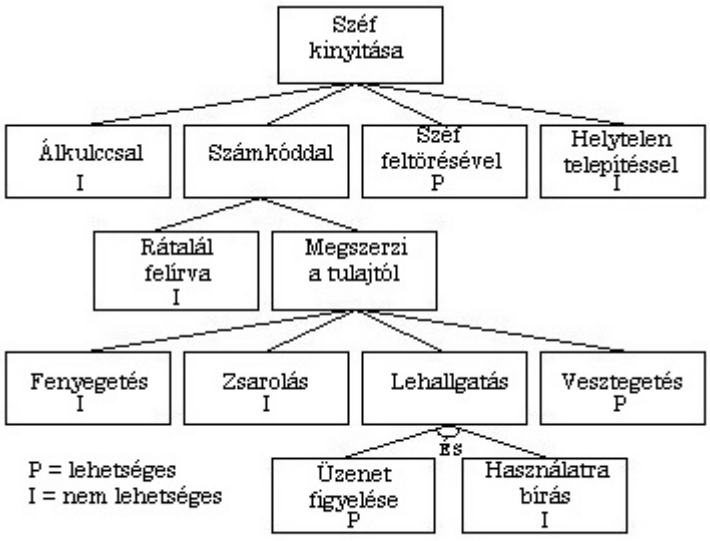
Nagyon kevés ember érti meg igazán a számítógép-biztonságot, ahogy ezt a számítógép-biztonsági cégek marketing anyagai is mutatják, melyek a „hacker-biztos program", „háromszoros-DES biztonság" és hasonlókat hangoztatják. Valójában a feltörhetetlen biztonság mindig feltörésre kerül, gyakran a fejlesztők által sohasem képzelt módon. Látszólag erős titkosítások is feltörésre kerülnek. A halandó ember képességein túlinak hitt támadások hétköznapiakká válnak. És ahogy az újságok az egyik biztonsági hibát a másik után jelentik, világossá válik, hogy a „biztonság" kifejezésnek nincs értelme, amíg nem tudjuk azt is, hogy „Kitől biztonságos?" vagy „Mennyi ideig biztonságos?"

Nyilvánvalóan egy számítógépes rendszerek elleni fenyegetettségeket modellező eljárásra van szükség. Amennyiben megismerjük az összes különböző támadási módot, melyen keresztül egy rendszer támadható, úgy megfelelő módon tudjuk megtervezni a védekezési lehetőségeket a támadások megakadályozására. Ha megismerjük, kik a támadók – nem beszélve a képességeikről, befolyásoltságukról és céljaikról – talán képesek leszünk a megfelelő védekezést alkalmazni a valós fenyegetések ellen.

A támadási fák

A támadási fák egy formális, tervszerű eljárást nyújtanak a biztonsági rendszerek leírására a különböző támadások alapján. A támadási fák alapvetően a rendszer elleni támadási lehetőségeket fastruktúrába szervezve írják le, ahol a fa gyökere a támadás célját, a levelek és a belőlük a gyökérhez vezető utak pedig a cél elérésének különböző módjait jelenítik meg.

Példának okáért az **1. ábra** egy egyszerű támadási fa egy széf ellen. A cél a széf kinyitása. A széf kinyitása érdekében a támadók álkulccsal nyitják ki a zárat, megfejtik a számkombinációt, kivágják a széf oldalát, vagy úgy állítják üzembe a széfet, hogy később könnyedén ki tudják nyitni. A számkombináció megtanulásához szükség van a felírt szám megtalálására vagy a széf tulajdonosától való megszerzésre. És így tovább. Mindegyik csúcs egy részcéllá válik, és a részcél utódai a részcél elérésének módjait jelentik. (Természetesen, ez csak egyetlen példa egy támadási fára, mely nem is teljes. Milyen egyéb támadásfajtákra tudsz gondolni, amivel elérheted a célt?)



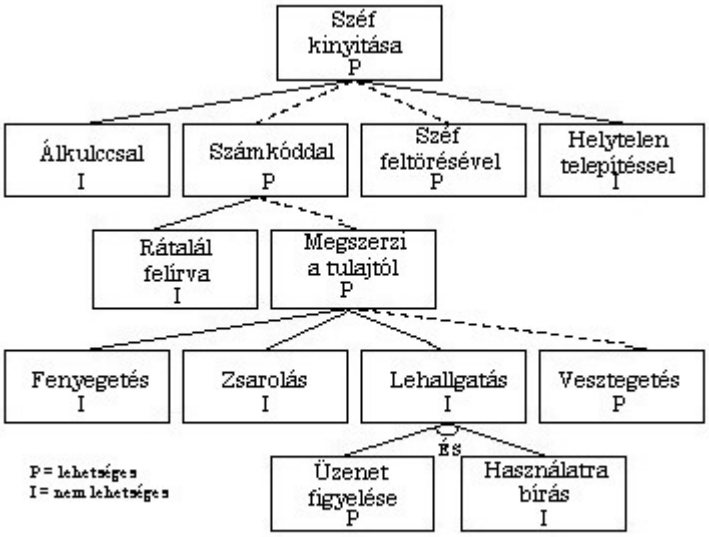
1. ábra: Támadási csúcs ok

Figyeljük meg, hogy vannak ÉS és VAGY csúcsok (az ábrákon minden VAGY, ami nem ÉS). A VAGY csúcsok alternatívák – például a négy út a széf kinyitásához. Az ÉS csúcsok különböző lépéseket jelölnek ugyanazon cél eléréséhez. Ahhoz, hogy lehallgassanak valakit a széfkombináció megadása köz-

[1] Original article: `http://www.schneier.com/paper-attacktrees-ddj-ft.html`. Translation: *zoli kincses*, special thanks: Anna Táborszki, Kálmán Perényi, Balázs Ugron & members of `elte.prog-mat` and `elte.diaklap` newsgroups :-).

ben, szükséges a kommunikáció lehallgatása ÉS a széf tulajdonosainak rávétele, hogy megadják ezt a széfkombinációt. A támadók nem érhetik el a célt, amíg mindkét részcél nem teljesül.

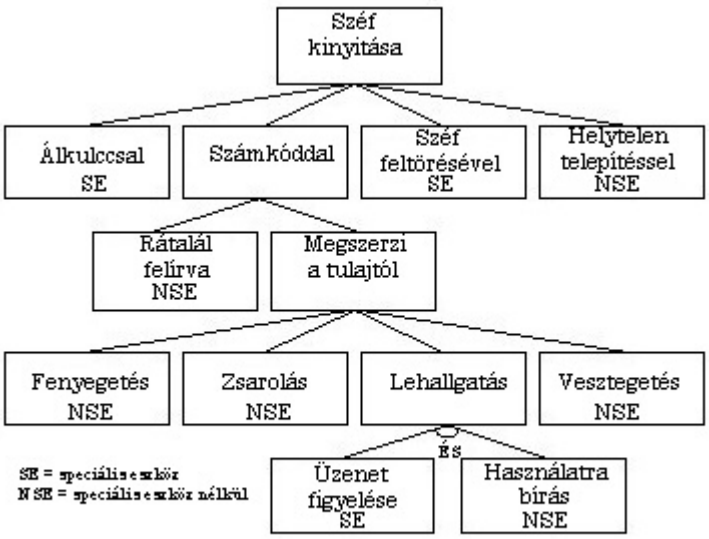
Ez az alap támadási fa. Amint kitöltötted, értékeket rendelhetsz – I (nem lehetséges) és P (lehetséges) az **1. ábrán** – a különböző csúcsokhoz, majd kiszámíthatod az egyes csúcsok értékét. (Újra kiemelem, ez egy szemléltető példa, az adatok nem irányadóak a széfem biztonságának megállapításához.) Az értékek hozzárendelése után – vélhetően ez a hozzárendelés a széf alapos vizsgálatának eredménye – kiszámítható a cél biztonsága. Egy VAGY csúcs értéke akkor lehetséges, ha *legalább egy* utóda lehetséges, és lehetetlen, ha az *összes* utóda lehetetlen. Egy ÉS csúcs értéke lehetséges, ha minden utóda lehetséges, és egyébként lehetetlen, ld. **2. ábrát**.



2. ábra: Lehetséges támadások

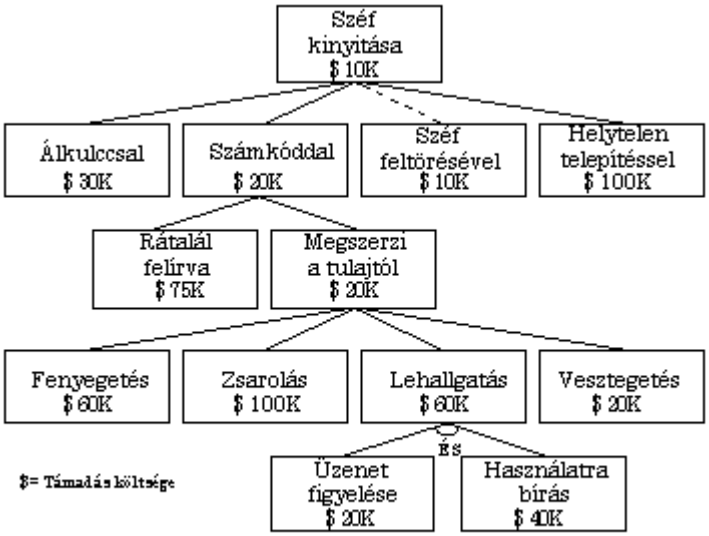
A **2. ábrán** a pontozott vonalak jelzik a lehetséges támadási módokat – a lehetséges csúcsok hierarchiáját egy levéltől a célig. Ebben a mintarendszerben két lehetséges támadás van: a széf feltörése vagy a széf tulajdonosának vesztegetése által a számkombináció megszerzése. Ennek tudatában már pontosan megállapítható, hogyan kell támadás ellen védeni a rendszert.

A csúcsokhoz a „lehetséges" és „nem lehetséges" értékek hozzárendelése csak egy lehetőség a fa használatakor. Tetszőleges logikai érték hozzárendelhető a levelekhez, majd ezek is hasonló módon terjednek felfele a fában: könnyű vagy nehéz, költséges vagy olcsó, aktív behatoló vagy passzív nem behatoló, legális vagy illegális, speciális felszereltség szükséges vagy nem szükséges. A **3. ábra** ugyanazt a fát mutatja be más logikai értékekkel.



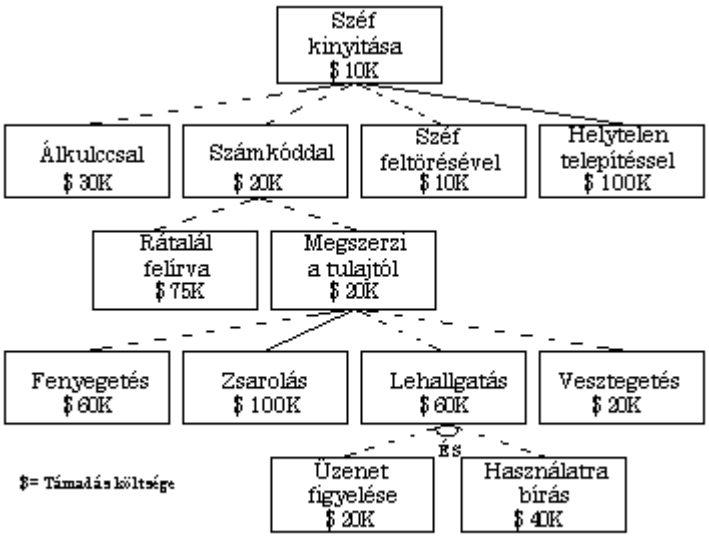
3. ábra: Speciális felszerelés szükséges

Hasznos a csúcsokhoz a „költséges" és „nem költséges" hozzárendelés, de jobb lenne pontosan megadni, hogy mennyire költséges. Ugyancsak lehetséges folytonos értéket hozzárendelni a csúcsokhoz. A **4. ábrán** látható fában különböző értékek lettek hozzárendelve a levelekhez. A logikai értékekhez hasonlóan ezek az értékek is felfele terjednek a fában. A VAGY csúcsok értéke az utódok legkisebb értéke lesz, az ÉS csúcsoknak pedig az utódok értékének összege lesz az értéke. A **4. ábrán** a költségek kerültek terjedésre felfele a fában, és a legolcsóbb támadás került kiemelésre.



4. ábra: Támadás költsége

Figyeljük meg, hogy ez a fa felhasználható arra, hogy meghatározzuk, hol sebezhető a rendszer. Az **5. ábra** szemlélteti a 100.000$-nál olcsóbb támadásokat. Amennyiben csak azokkal a támadásokkal kell foglalkozni, melyek kevésbé költségesek (lehetséges, hogy a széf tartalma csak 100.000$ értékű), akkor csak ezekkel a támadásokkal kell foglalkozni.



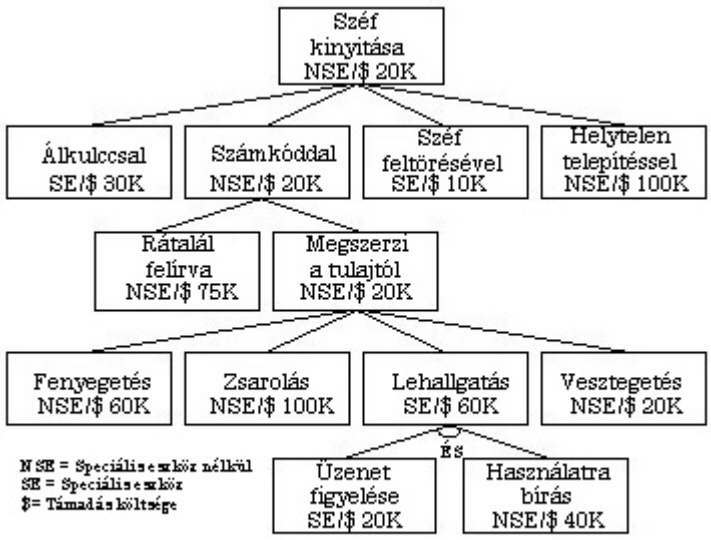
5. ábra: A 100.000$-nál olcsóbb támadások

Létezik még sok más csúcsokhoz rendelhető folytonos érték, beleértve a támadás sikerességének valószínűségét, annak valószínűségét, hogy a támadó megpróbál-e egy adott támadást stb.

A csúcsok és értékeik

Minden valódi támadási fában a csúcsoknak több különböző értéke lehet a több különböző típusnak megfelelően, mint logikai, és mint folytonos érték. A különböző értékek vegyíthetők, hogy még többet lehessen tanulni a rendszer sebezhetőségeiről. Például a **6. ábra** meghatározza a legolcsóbb támadást, melyhez nincs szükség speciális felszerelésre. Hasonló módon megtalálható a legolcsóbb alacsony kockázatú támadás, a legvalószínűbb passzív nem behatoló támadás, a legkisebb szakértelmet igénylő támadás, a legnagyobb valószínűséggel sikeres legolcsóbb támadás, a leginkább törvényes támadás stb. Minden alkalom-

mal, amikor a fában egy adott típusú támadást kell keresni, még többet lehet megtanulni a rendszer biztonságáról.



6. ábra: A speciális felszerelést nem igénylő legolcsóbb támadás

Ahhoz, hogy mindez működjön, szükséges a támadási fák és a támadókkal kapcsolatos ismeretek ötvözése. Különböző támadóknak különböző a szakértelme, a hozzáférése, a kockázattal kapcsolatos ellenérzése, pénze stb. Amennyiben a szervezett bűnözésről van szó, akkor a költséges támadásoktól kell tartani és olyan támadóktól, akik nem tartanak a börtöntől. Amennyiben terroristákról van szó, akkor az előzőkön felül olyan támadóktól kell tartani, akik készek meghalni a cél érdekében. Amennyiben a rendszer biztonságát felmérő unatkozó egyetemi hallgatókról van szó, akkor nem kell tartani a törvénytelen támadásoktól, mint a vesztegetés és a zsarolás. A támadó tulajdonságai meghatározzák, hogy a támadási fa mely részeitől kell tartani.

A támadási fákkal a „mi van, ha?" játék is megvalósítható a lehetséges védekezésekkel. Például a **6. ábrán** a cél elérése 20.000$-ba kerül. Ez azért van, mert a legolcsóbb speciális felszerelést nem igénylő támadás a kombinációt ismerő személy megvesztegetése. Mi van, ha olyan védelem kerül alkalmazásra, mint az illető személy jobb megfizetése, hogy nehezebben lehessen lefizetni? Amennyiben feltételezhető, hogy 80.000$ az illető vesztegetési ára (fontos, hogy ez csak példa, a valóságban elvárás kikutatni a védelmi intézkedés hatását az adott csúcs értékére), akkor a támadás költsége 60.000$-ra nő (valószínűleg a gengszter bérlésére, aki a fenyegetést elvégzi).

Egy PGP-s példa

A **7. ábrán** a népszerű PGP e-mail biztonsági program támadási fája található. Mivel a PGP egy összetett program, a támadási fája is összetett, és egyszerűbb szövegesen leírni, mint grafikusan. A PGP többféle biztonsági tulajdonsággal rendelkezik, így ez csak egy a sok PGP támadási fa közül. Ez a bizonyos támadási fa az „egy PGP-s levél elolvasása" céllal rendelkezik. Más célok lehetnek még: „más aláírását hamisítani egy üzenetre", „kicserélni az aláírást egy üzeneten", „észlelhetetlenül módosítani egy PGP-vel aláírt vagy titkosított üzenetet" stb.

Cél: PGP-vel titkosított levél elolvasása. (VAGY)
1. Üzenet dekódolása. (VAGY)
  1.1. Aszimmetrikus titkosítás feltörése. (VAGY)
    1.1.1. Aszimmetrikus titkosítás feltörése nyers erővel. (VAGY)
    1.1.2. Aszimmetrikus titkosítás feltörése matematikai módszerekkel. (VAGY)
      1.1.2.1. RSA feltörése. (VAGY)
      1.1.2.2. RSA modulus felbontása / ElGamal diszkrét logaritmus kiszámítása
    1.1.3. Aszimmetrikus titkosítás kriptoanalízise.
      1.1.3.1. RSA / ElGamal általános kriptoanalízise. (VAGY)
      1.1.3.2. RSA / ElGamal gyengeségeinek kihasználása. (VAGY)
      1.1.3.3. RSA / ElGamal elleni órajel-támadások.
  1.2. Szimmetrikus kulcsú titkosítás feltörése.
    1.2.1. Szimmetrikus kulcsú titkosítás feltörése nyers erővel. (VAGY)
    1.2.2. Szimmetrikus kulcsú titkosítás kriptoanalízise.
2. Az üzenet titkosításához használt szimmetrikus kulcs egyéb eszközökkel történő meghatározása.
  2.1. A feladó rászedése, hogy azzal a privát kulcsával titkosítson, melynek a nyilvános kulcsa ismert (VAGY)
    2.1.1. A feladó meggyőzése arról, hogy egy hamis kulcs (ismert egyéni kulccsal) a tervezett fogadó kulcsa.
    2.1.2. A feladó meggyőzése arról, hogy egynél több kulcsot használva titkosítsa üzenetét – az egyik kulcs a fogadó tényleges kulcsa legyen, a másik pedig olyan, amelynek privát kulcsa ismert.

2.1.3. Üzenet titkosítása a háttérben egy másik nyilvános kulccsal, a feladó tudta nélkül.
2.2. A fogadóval aláíratni a titkosított szimmetrikus kulcsot. (VAGY)
2.3. A feladó számítógép-memóriájának megfigyelése. (VAGY)
2.4. A fogadó számítógép-memóriájának megfigyelése. (VAGY)
2.5. A kulcs meghatározása pseudo véletlenszám-generátorból. (VAGY)
2.5.1. A `randseed.bin` állapotának meghatározása az üzenet kódolásakor. (VAGY)
2.5.2. Szoftver (vírus) beültetése, amely kiszámíthatóan módosítja a `randseed.bin` állapotát. (VAGY)
2.5.3. Szoftver beültetése, amely közvetlenül befolyásolja a szimmetrikus kulcs-választást.
2.6. Vírus telepítése, amely felfedi a szimmetrikus kulcsot.
3. Rászedni a címzettet, hogy segítsen az üzenetet dekódolásában. (VAGY)
3.1. Választott titkos szöveg alapú támadás a szimmetrikus kulcs ellen. (VAGY)
3.2. Választott titkos szöveg alapú támadás a nyilvános kulcs ellen. (VAGY)
3.3. Az eredeti üzenet elküldése a fogadónak. (VAGY)
3.4. A fogadó kimenő leveleinek figyelése. (VAGY)
3.5. Az eredeti üzenet `Reply-to:` illetve `From:` mezőjének hamisítása. (VAGY)
3.6. Üzenet elolvasása, miután a fogadó kikódolta azt.
3.6.1. Üzenet lemásolása a fogadó merevlemezéről vagy virtuális memóriájából. (VAGY)
3.6.2. Üzenet lemásolása mentés adatokból. (VAGY)
3.6.3. A hálózati forgalom figyelése. (VAGY)
3.6.4. Elektromágneses szimatoló technikák használata az üzenet elolvasásához, ahogy az megjelenik a képernyőn. (VAGY)
3.6.5. Üzenet visszanyerése nyomtatásból.
4. A fogadó privát kulcsának megszerzése.
4.1. RSA modulus felbontása / ElGamal diszkrét logaritmus kiszámítása. (VAGY)
4.2. Privát kulcs megszerzése a fogadó kulcskarikájáról. (VAGY)
4.2.1.Kódolt privát kulcskarika megszerzése. (ÉS)
4.2.1.1. Lemásolás a felhasználó winchesteréről. (VAGY)
4.2.1.2. Lemásolás a lemezes mentésekről. (VAGY)
4.2.1.3. A hálózati forgalom figyelése. (VAGY)
4.2.1.4. Vírus/féreg telepítése, hogy felfedje a kódolt privát kulcs másolatát.
4.2.2. Privát kulcs kikódolása.
4.2.2.1. IDEA kódolás feltörése. (VAGY)
4.2.2.1.1. IDEA feltörése nyers erővel. (VAGY)
4.2.2.1.2. IDEA kriptoanalízise.
4.2.2.2. Jelszó megtanulása
4.2.2.2.1. Billentyűzet figyelése, amikor a felhasználó begépeli a jelszót. (VAGY)
4.2.2.2.2. Felhasználó meggyőzése, hogy felfedje a jelszót. (VAGY)
4.2.2.2.3. Billentyűzet-figyelő szoftver használata a jelszó rögzítéséhez, amikor azt a felhasználó begépeli. (VAGY)
4.2.2.2.4. Jelszó kitalálása.
4.3. A fogadó számítógép-memóriájának figyelése. (VAGY)
4.4. Vírus beültetése a privát kulcs felfedéséért.
4.5. Megbízhatatlan közös/privát kulcspár generálása a fogadónak.

7. ábra: Támadási fa a PGP-ellen

Azonnal nyilvánvalóvá válik a támadási fa alapján, hogy az RSA vagy az IDEA titkosítási algoritmusok feltörése nem a legcélravezetőbb támadás. Több megoldás is létezik valaki PGP-vel titkosított levelének az elolvasására a kriptográfia feltörése nélkül. Elkapható a képernyőkép, amikor dekódolja és elolvassa az üzenetet (trójai program használatával, mint a Back Orifice, egy TEMPEST[2] lehallgatóval, vagy egy rejtett kamerával), megszerezhető a privát kulcs, miután megadták a jelszót hozzá (újra Back Orifice vagy egy számítógépes vírus segítségével), kinyerhető a jelszót (biztosnak vehető, hogy sokkal kisebb az entrópiája, mint az azt generáló 128 bites IDEA kulcsnak). A dolgok rendszerében az algoritmus és a kulcshossz választása a legkevésbé befolyásolja a PGP általános biztonságát. A PGP-nek nem elég biztonságosnak lennie, de olyan környezetben is kell használni, amely kihasználja ezt a biztonságot anélkül, hogy bármilyen új biztonsági hiányosságot eredményezne.

Támadási fa létrehozása

Hogyan lehet létrehozni egy ilyen támadási fát? Először azonosítani kell a lehetséges támadási célokat. Minden egyes cél egy külön fát határoz meg, bár egyes al-fákon vagy csúcsokon osztozhatnak. Ezek után ki kell gondolni minél több támadást mindegyik cél eléréséhez. Ezeket a fához kell adni. Addig kell ismételni ezt az eljárást a fában lefelé haladva, amíg készen nem lesz. Oda kell adni a fát valaki másnak, és hagyni kell, hogy gondolkozzon az eljárásról és hozzáadjon bármilyen csúcsot, ami eszébe jut. Ezt kell ismételni, amíg szükséges, vélhetően hónapokon át. Természetesen mindig ott a lehetőség, hogy kifelejtődik valami a fából, de idővel egyre jobb lesz. Mint minden biztonsági elemzés, a támadási fák létrehozása is egyfajta elkötelezettséget kíván, és gyakorlat kell hozzá.

Amint elkészült a támadási fa, és minden csúcs értéke kivizsgálása került (ezek az értékek változni fognak az idővel, ahogy a támadások egyre könnyebbé válnak, és ahogy egyre pontosabb információ nyerhető az értékekről), biztonsági döntésekhez használhatók a támadási fák. Megnézhetők a cél-csúcs értékek, hogy látható legyen, a rendszer célja ki van-e téve támadás veszélyének. Kideríthető, hogy a rendszer veszélyben van-e egy bizonyos támadással szemben, mint például a jelszó kitalálás. Használható a táma-

[2] Itt: elektromágneses kisugárzást és lehallgatást jelent. Bővebben: `http://www.eskimo.com/~joelm/tempest.html` (a ford.)

dási fa, hogy sorba vehetők legyenek a rendszer biztonsági feltételezései; például a PGP biztonsága feltételezheti, hogy senki sem tudja a fejlesztőket megvesztegetni. Kideríthető a rendszer egy módosításának vagy egy új sebezhetőség felfedezésének a hatása: az új információk alapján újraszámolható a csúcsok értéke, és látható, milyen hatással vannak a célra. Összehasonlíthatók és rangsorolhatók a támadások – melyik a legolcsóbb, melyik lehet leginkább sikeres, és hasonlók.

A legmeglepőbb eredmény, ami az ilyen elemzésekből kiderül, hogy az emberek által sebezhetőnek hitt területek többnyire nem azok. Például a PGP esetében az emberek általában a kulcshosszak miatt aggódnak. Vajon 1024 vagy 2048 bites kulcsokat használjanak? A támadási fát nézve az RSA kulcshossz nem igazán lényeges. Annyi más támadási lehetőség van – billentyűzet-lehallgató telepítése, a program módosítása az áldozat gépén – melyek sokkal könnyebbek, mint az RSA nyilvános kulcsának megtörése. A kulcs növelése 1024 bitről 2048 bitre olyan, mintha ahelyett, hogy egy kisebb palánkkal vennék körbe a célt, egy hatalmas karót szúrnának a földbe azt remélve, hogy az ellenség majd pont beleszalad. A támadási fák az egész rendszer felett adnak áttekintést.

A támadási fákat értékessé tevő tényezők egyike az, hogy újrafelhasználható módon kezelik az ismereteket. Amint egyszer elkészült a PGP támadási fa, sok olyan helyzetben használható, mely a PGP-t használja. A PGP elleni támadási fa egy nagyobb támadási fa részévé vált. Például a **8. ábra** egy olyan támadási fát mutat be, melynek az a célja, hogy elolvassanak egy adott levelet, amelyet az egyik Windows98-as gépről a másikra küldtek. A fa cél-csúcsait nézve látható, hogy a teljes PGP támadási fa és széfkinyitási támadási fa beemelhető ebbe a fába.

Cél: Egyik Windows98-as gépről a másikra küldött egyedi üzenet elolvasása
1. A küldő meggyőzése az üzenet felfedésére. (VAGY)
  1.1. Felhasználó megvesztegetése.
  1.2. Felhasználó megzsarolása.
  1.3. Felhasználó megfenyegetése.
  1.4. Felhasználó megtévesztése.
2. Az üzenet elolvasása bevitelkor (VAGY)
  2.1. A képernyő elektromágneses kisugárzásának figyelése (védelem: kisugárzás ellen árnyékolt számítógép használata)
  2.2. A képernyő vizuális figyelése
3. Az üzenet elolvasása a küldő számítógépén történő tároláskor.
    (védelem: SFS biztonságos fájlrendszer használata a merevlemez titkosítására) (ÉS)
  3.1. Hozzáférés a merevlemezhez. (védelem: fizikai zár minden ajtón és ablakon)
  3.2. Egy SFS-sel védett fájl elolvasása.
4. A levél elolvasása, amikor a küldőtől a címzett felé tart. (védelem: PGP alkalmazása) (ÉS)
  4.1. Az üzenet elkapása átvitel közben. (védelem: átviteli-réteget titkosító program alkalmazása)
  4.2. PGP-vel titkosított üzenet elolvasása.
5. A fogadó meggyőzése a levél felfedésére. (VAGY)
  5.1. Felhasználó megvesztegetése.
  5.2. Felhasználó megzsarolása.
  5.3. Felhasználó megfenyegetése.
  5.4. Felhasználó megtévesztése.
6. A levél elolvasása miközben olvassák (VAGY)
  6.1. A képernyő elektromágneses kisugárzásának figyelése (védelem: TEMPEST számítógép használata)
  6.2. A képernyő vizuális figyelése
7. Az üzenet elolvasása a fogadó számítógépén történő tároláskor. (VAGY)
  7.1. Hozzáférés a dekódolás után a merevlemezen tárolt üzenethez.
    (védelem: SFS biztonságos fájlrendszer használata a merevlemez titkosítására) (ÉS)
    7.1.1. Hozzáférés a merevlemezhez. (védelem: fizikai zár minden ajtón és ablakon)
    7.1.2. Egy SFS-sel védett fájl elolvasása.
  7.2. A mentésben dekódoltan tárolt üzenet megszerzése.
8. Az üzenet papírmásolatának megszerzése. (védelem: a papírmásolatok széfben tárolása) (ÉS)
  8.1. Fizikai hozzáférés a széfhez.
  8.2. Széf kinyitása.

8. ábra: Egy általános számítógépes rendszer elleni támadás

Ez a skálázhatóság azt jelenti, hogy nem kell mindenben szakértőnek lenni. Ha PGP-t kell használni egy rendszerben, nem kell tudni a PGP támadási fa részleteit; amit tudni kell, az a cél lehetséges értékei. Ha az ember egy számítógépes biztonsági szakember, nem kell tudnia, milyen bonyolult egy bizonyos széf feltörése; csak a cél-csúcs értékeit kell tudnia. Amint felépít egy könyvtárat bizonyos számítógépes programok, ajtó- és ablakzárak, hálózatbiztonsági protokollok, vagy egyéb elleni támadási fákból, újra használhatja őket, amikor csak szüksége van rá. Egy ilyen rendszer nagyon hasznos a támadási szakértelem kategorizálásáról gondoskodó nemzeti biztonsági ügynökség számára.

Következtetés

A támadási fák egy formális módszertant nyújtanak a biztonsági rendszerek és alrendszerek elemzéséhez. Egyfajta biztonsággal kapcsolatos hozzáállást kínálnak, a biztonsági szakértelem megszerzésének és újrafelhasználásának egy módját, valamint a biztonsággal kapcsolatos változásokra történő válaszadás lehetőségét. A biztonság nem egy termék – egy eljárás. A támadási fák az alapot szolgáltatják az eljárások megértéséhez.