Biztonsági kockázatelemzés Markov-lánc segítségével

Dr. Leitold Ferenc
Dunaújvárosi Főiskola
fleitold@mail.duf.hu

A számítógép hálózatok biztonsága egyre nagyobb problémát jelent. A hálózati biztonság területén a manuálisan vagy célprogramok segítségével megvalósított támadások mellett az automatikusan terjedő kártevők is nagy veszélyt jelentenek. A támadók gyakran használják ki a kártevők hatását, esetenként szándékosan indítanak útjára kártevőket annak érdekében, hogy a fertőzött számítógépek távolról irányítható (botnet) hálózatát használják fel későbbi támadásokhoz. A kártevők alapvetően két fő tényezőre alapozzák terjedésüket: Kihasználhatják a felhasználó hiszékenységét, esetleg hozzá nem értését és ráveszik arra, hogy az általa biztonságosnak hitt objektumba rejtett kártékony kódot lefuttassa. Másrészről a kártevők építhetnek a számítógépen futó operációs rendszerek és alkalmazások biztonsági réseire és akár a felhasználó tudomása és engedélye nélkül automatikusan is vezérléshez juthatnak.

A számítógépes hálózatokon keresztül történő, a számítógépek és a felhasználók kommunikációját kihasználó támadások egyre nagyobb veszélyt jelentenek. Ide tartoznak a leggyakrabban az e-mail üzenetekben terjedő kártevők, a célzott támadások botnet hálózatok igénybevételével vagy anélkül, és ide sorolhatjuk a social engineering alapú, a személyes kommunikációra épülő támadásokat is. Ebben a cikkben a kommunikáción alapuló támadások, elsősorban a kapcsolatokra vonatkozó matematikai modellje kerül bemutatásra. A kommunikáció egyrészt a számítógépek közötti kapcsolatot jelenti, másrészt a számítógépek felhasználói közötti kommunikációt, illetve a számítógépek és a felhasználók közötti kapcsolatot is. A megtárgyalandó biztonsági modell alkalmas arra, hogy modellezze a támadási lehetőségeket. Segítségével azonosíthatók a támadó által elérhető pontok. A modell segítségével megállapíthatjuk, hogy a támadó által elérhető pontok közül melyek a legveszélyesebbek, azonosíthatjuk a kritikus kommunikációs csatornákat, protokollokat, így a modell lehetőséget ad arra, hogy megkeressük a biztonsági rendszerünk gyenge pontjait.

1. Bevezetés

A kommunikációs csatornák biztonsága két kérdéskört érint. A középkorban a futárral történő üzenetküldés legnagyobb kockázatát az út során történő információszerzés jelentette. Ezért az információt titkosították, rejtjelezték. Egy támadó két támadási módszer közül választhatott. Mint passzív támadó lehallgatja az üzenetet, megfejti és saját céljaira felhasználja, de NEM akadályozza az eredeti üzenet célba érkezését. Másrészt, mint aktív támadó megteheti azt is, hogy a lehallgatott információt módosítva küldi tovább, esetleg válaszol az eredeti üzenet küldőjének.

A középkorban még nem volt jelentős az a probléma, amit az jelenti, hogy a támadó ellenőrzése alá vonja az egyik végpontot (küldő vagy fogadó). Manapság azonban a csatorna lehallgatása mellett ez egy sokkal jelentősebb veszélyforrás jelent. A kommunikációs eszközök, az Internet gyors fejlődésével egy támadó valós időben felügyelheti a megtámadott eszközeit, illetve saját céljainak megfelelően befolyásolhatja működésüket.

A számítógép hálózatok biztonsága egyre nagyobb problémát jelent. A hálózati biztonság területén a manuálisan vagy célprogramok segítségével megvalósított támadások mellett az automatikusan terjedő kártevők is nagy veszélyt jelentenek. A támadók gyakran használják ki a kártevők hatását, esetenként szándékosan indítanak útjára kártevőket annak érdekében, hogy a fertőzött számítógépek távolról irányítható (botnet) hálózatát használják fel későbbi támadásokhoz. A kártevők alapvetően két fő tényezőre alapozzák terjedésüket: Kihasználhatják a felhasználó hiszékenységét, esetleg hozzá nem értését és ráveszik arra, hogy az általa biztonságosnak hitt objektumba rejtett kártékony kódot lefuttassa. Másrészről a kártevők építhetnek a számítógépen futó operációs rendszerek és alkalmazások biztonsági réseire és akár a felhasználó tudomása és engedélye nélkül automatikusan is vezérléshez juthatnak.

További problémát jelent a személyek közötti kapcsolat. A Social Engineering módszereit felhasználva egy támadó ráveheti egy általa el nem érhető számítógép felhasználóját, hogy hajtson végre néhány műveletet a számítógépén. Akár például, hogy látogasson meg egy weboldalt, ahol persze korábban egy olyan kódot helyezett el, amivel aztán átveheti a vezérlést a számítógép felett.

2. A modell elemei

Az ebben a cikkben megtárgyalandó biztonsági modell segítségével a számítógépeket, a rajtuk futó folyamatokkal, a számítógépeket felhasználó személyeket (legyen az egy laikus felhasználó vagy akár egy hozzáértő támadó), valamint a köztük lévő kapcsolatokat szeretnénk modellezni. A számítógépeken alkalmazások, folyamatok futnak. Minden egyes olyan folyamatot, amely képes arra, hogy online vagy offline módon más folyamatokkal kommunikációt létesítsen entitásnak definiáljuk.

Az entitások között kommunikációs csatornákat feltételezünk, melyek alkalmasak arra, hogy a kommunikációs csatorna működését leíró szabályoknak megfelelően biztosítsa az üzenetek küldését. Online módon történő kommunikációt jelent, ha az adott entitás az őt tartalmazó számítógép segítségével valamely kommunikációs csatornán keresztül kommunikációt folytat egy másik számítógép valamely entitásával. Ez tipikusan az Interneten keresztül valósulhat meg. Egy ilyen kommunikációs csatornán üzenetek folyama zajlik, mely üzenetek szabályait a kommunikációs csatornához rendelt protokoll írja le.

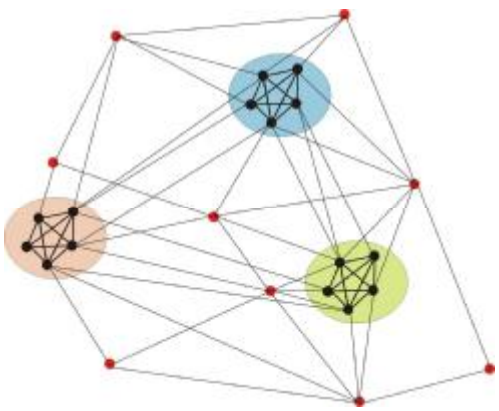
Offline módon történő kommunikáció esetén egy entitás az őt tartalmazó számítógép háttértárán elhelyezett adatfájlt tölti be és értelmezi. Ebben az esetben a másik folyamat, amellyel a kommunikáció zajlik, az a folyamat, amely az adott adatfájlt létrehozta. Ez a folyamat akár egy másik számítógépen is lehet és vagy valamilyen adathordozón vagy pedig valamely online kommunikációs csatornán juttatta el az adatfájlt a másik számítógépre. Ebben az esetben a kommunikációs csatorna szabályait az adatfájl formátumleírása jelenti.

A számítógépen futó folyamatok mellett az entitások körébe beleértjük magukat a számítógépet felhasználó személyeket is, ők is képesek arra, hogy más entitásokkal kommunikáljanak. A folyamatokkal való kommunikáció tipikusan a felhasználói bevitellel illetve az alkalmazások, folyamatok üzeneteivel valósulhat meg, de az is elképzelhető, hogy más felhasználóval alakítsanak ki kapcsolatot, vele kommunikáljanak (például: személyesen vagy telefonon).

Az egy számítógépen belül elhelyezkedő entitásokat, mint az entitások egy halmazát összetartozónak definiáljuk. Feltételezzük, hogy ha egy támadó sikeresen megtámadott egy entitást, akkor képes arra, hogy felügyelje, illetve befolyásolja az adott számítógéphez tartozó többi entitást is.

3. Gráf reprezentáció

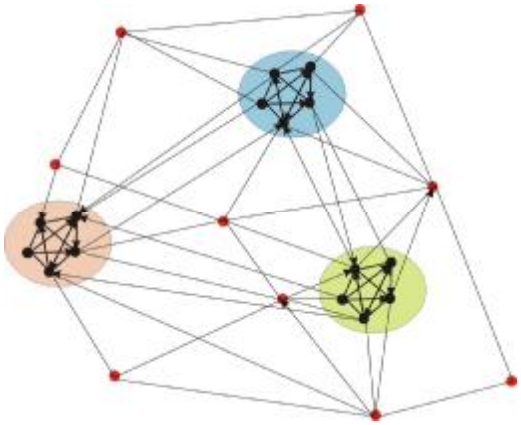
A biztonsági modell elemeit egy gráfként reprezentálhatjuk, ahol a csomópontokat az egyes entitások jelentik, melyek a számítógépeken futó folyamatokat, illetve magukat a számítógép felhasználó személyeket jelképezik. A csomópontok közötti élek jelképezik az entitások közötti kommunikációs csatornát. Két folyamat közötti kommunikáció valamilyen adatátvitelt jelent online vagy offline módon. Természetesen személyek között is lehet kapcsolat, hiszen bármely személy bármely más személlyel kapcsolatba kerülhet (például telefonon felhívja). A folyamatok és személyek közötti kapcsolat esetén lényeges megkülönböztetnünk a kommunikáció két irányát. Míg a számítógépek felhasználói a megfelelő beviteli mezők segítségével alakíthatják az egyes folyamatok működését, addig a folyamatok is küldhetnek üzenetet a felhasználónak.



1. ábra: Egy egyszerű gráfmodell

A piros pontok a felhasználókat a fekete pontok a számítógépeken belüli folyamatokat jelképezik. A színes ellipszisek az egy számítógépen belül, az összetartozó folyamatokat mutatják.

A kommunikációs csatorna irányainak a megkülönböztetésével a modell irányított gráffal történő reprezentálásához juthatunk. Ez sokkal élethűbben mutatja be a valós körülményeket, hiszen a protokollok esetén általában nem tekinthetjük egyformának a két irányt. Különösen igaz ez a szerver-kliens alapú kommunikáció esetén.



2. ábra: Irányított gráfmodell

Modellünk így azt mutatja, hogy mely entitások állnak egymással kapcsolatban. Az egyes irányított élekhez azonban súlyozást is rendelhetünk, attól függően, hogy az adott kommunikációs csatorna megfelelő iránya mennyire alkalmas arra, hogy egy támadó megtámadjon egy másik entitást. Abban az esetben, ha ez az érték 0, akkor erre nincs lehetőség, és minél nagyobb, annál könnyebben kihasználható a csatorna.

4. Mátrix reprezentáció

A gráfmodell alapján elkészíthetjük modellünk mátrixreprezentációját is. Itt minden sornak és minden oszlopnak megfeleltetünk egy-egy entitást. A mátrixban lévő számok pedig a két csomópont közötti kommunikációs csatorna megfelelő irányához, mint a gráfbeli irányított élhez rendelt értéket jelentik.

Mindezek alapján, ha a mátrixban az értékeket úgy választjuk meg, hogy minden sorban az ott szereplő értékek összege pontosan 1 legyen, akkor a valószínűségszámítás bolyongási feladatainál ismert Markov-lánchoz juthatunk. Tekintsük ugyanis az entitások azon állapotvektorát, amely minden egyes entitáshoz tartalmazza azt az értéket, hogy az adott entitás mennyire támadható. Feltételezhetjük, hogy maga a támadó, mint személy is szerepel az entitások között, és kezdetben őt tekintjük egyedül veszélyesnek. Így a kezdeti állapotvektorban a támadónak megfelelő érték 1, a többi érték pedig 0.

Ekkor a kezdeti állapotvektor és az állapotátmenetet jelentő mátrix segítségével megkaphatjuk, hogy a támadó mely más entitásokat vonhat az ellenőrzése alá, illetve azt is, hogy ez milyen erőfeszítést jelent, mennyire könnyű ezt véghezvinnie.

Az állapotátmeneti mátrixban szereplő a_{ij} érték tehát 0, ha nincs lehetőség arra, hogy az i. entitás felügyeletével rendelkező támadó megszerezze a j. entitás felügyeletét, egyébként $a_{ij} > 0$. Az a_{ij} érték a kommunikációs csatornára, a protokollra, illetve az i. és j. entitásra jellemző érték. Értékét több tényező befolyásolja:

- A kommunikációs csatorna, illetve kommunikáció szabályait leíró protokoll megbízhatósága, támadhatósága.
- A folyamatot jelentő j. entitás megbízhatósága, biztonsági rései, az azokra vonatkozó javítások. Nem mindegy például, hogy a Microsoft Outlook Express sok évvel ezelőtti 5-ös verzióját, vagy például a jóval biztonságosabb The Bat levelezőt használjuk.
- Amennyiben a j. entitás személy, úgy az ő hiszékenysége is befolyásolja az a_{ij} értéket.

- Befolyásoló tényező lehet maga az idő, hiszen egy biztonsági rés ismertté válásával a támadhatósági lehetőség is növekszik.

5. Biztonsági megfontolások

Az ismertetett biztonsági modell segítségével a támadó lehetőségei könnyen vizsgálhatóak. Nem csupán az informatikai jellegű támadások, hanem a social engineering adta módszerek is vizsgálhatók. Vegyük észre hogy ha egy támadó a támadást egy belső személy segítségével szeretné véghez vinni, akkor az ő meggyőzésére számos módszer közül választhat:

- Megteheti, hogy például telefonon felhívja és egy megbízható személynek kiadva magát ráveszi a gyanútlan belső személy, hogy látogasson el egy weboldalra.
- Az átverő üzenetet akár emailben is elküldheti.
- Igénybe veheti egy kártevő segítségét, amely akár hasonló eszközzel próbál hatni a belső munkatársra.
- Személyesen is megpróbálhatja rávenni, hogy a támadó által megadott cselekvéssort hajtsa végre a számítógépén.

A modell segítségével jól vizsgálhatók azok a problémák, amelyek azon alapulnak, hogy egyes kommunikációs csatornákhoz tartozó protokollok más szabály szerinti formátumú adatfolyamot szállítanak valamely entitáshoz. Például egy JPEG képet az SMTP vagy a HTTP protokoll szállíthat a célszámítógép valamely képkezelő alkalmazása számára.

6. Irodalomjegyzék

[1] R., Szabó : “TCP/IP Networks and IP Telephony” in dr. G., Gordos ed. *Telecommunications Networks and Informatics Services,* , Scientific Association for Infocommunications Hungary, pp.394-402 http://www.hte.hu/ob/eng/hte_ob_eng.pdf

[2] *ITU-T Y 2011/(10/2004) Next Generation Networks – Frameworks and functional architecture models* ITU-T / ATIS Workshop “Next Generation Technology and Standardization“ Las Vegas, 19-20 March 2006. http://www.itu.int/ITU-T/ngn/introduction.html

[3] *Microsoft Security Bulletin* MS04-028, http://www.microsoft.com/technet/security/bulletin/MS04-028.mspx, 2006.

[4] Microsoft Security Advisory (912840)
http://www.microsoft.com/technet/security/advisory/912840.mspx, 2006

[5] Microsoft Security Bulletin MS02-072
http://www.microsoft.com/technet/security/Bulletin/MS02-072.mspx, 2002