Dunakavics

A Dunaújvárosi Főiskola online folyóirata 2014. II. évfolyam VI. szám

Műszaki-, Informatikai és Társadalomtudományok

Budai Gábor
Tanulói és tanulási utak a rendszerváltástól napjainkig

Katona József– Ujbányi Tibor–Kővári Attila
Agy-számítógépek inter-fészek rendszerbe történő illesztése

Ujbányi Tibor–Katona József–Kővári Attila
IT biztonság egy gráf alapú modellje

Dunakavics

A Dunaújvárosi Főiskola online folyóirata 2014. II. évfolyam VI. szám

Műszaki-, Informatikai és Társadalomtudományok

Megjelelenik évente 12 alkalommal

Szerkesztőbizottság
András István, Kiss Natália, Rajcsányi-Molnár Mónika,
Talata István, Kukorelli Katalin

Szerkesztőség
Ladányi Gábor (Műszaki)
Nagy Bálint (Informatika és matematika)
Szakács István (Gazdaság és társadalom)
Klucsik Gábor (technikai szerkesztő)

Felelős szerkesztő Németh István
Tördelés Duma Attila
Szerkesztőség és a kiadó címe 2400 Dunaújváros, Táncsics M. u. 1/a.

Kiadja DUF Press, a Dunaújvárosi Főiskola kiadója
Felelős kiadó András István, rektor

A lap megjelenését támogatta TÁMOP-4.2.3-12/1/KONV-2012-0051
„Tudományos eredmények elismerése és disszeminációja
a Dunaújvárosi Főiskolán".
http://dunakavics.duf.hu

ISSN 2064-5007

Tartalom

BUDAI GÁBOR

Tanulói és tanulási utak a rendszerváltástól napjainkig 5

KATONA JÓZSEF–UJBÁNYI TIBOR–KŐVÁRI ATTILA

Agyszámítógép-interfészek rendszerbe történő illesztése 29

UJBÁNYI TIBOR–KATONA JÓZSEF–KŐVÁRI ATTILA

Az IT-biztonság egy gráf alapú modellje 39

Galéria
(Bodor Attila fotói) 48

UJBÁNYI TIBOR *–KATONA JÓZSEF **–KŐVÁRI ATTILA ***

Az IT-biztonság egy gráf alapú modellje

Összefoglalás: Egy esetleges információ, „kiszivárogtatás" esetén a kivizsgálás során a feltételezett elkövetők és a fellelt fontos nyomok közötti összes lehetséges kapcsolat reprezentálható és elemezhető, melyhez egy gráf alapú kiértékelési módszer nagy segítséget nyújt. A cikkben egy gráf alapú kiértékelési módszer kerül bemutatásra, amely segítségével a rendszer elsődleges támadási pontjait jelentő felhasználók/rendszerek azonosíthatóak.
Kulcsszavak: IT-biztonság, gráf, aktor.

Abstract: When information leaking out we can represent all of the possible contacts between the supposed perpetrators and important traces. The case can be analysed with a graph based evaluation method. In the article we present a graph based evaluation method that help to idetify users and systems which the primary attacking point of the systems.
Keywords: IT security, graph, actor.

Bevezető

Amikor informatikai biztonságról beszélünk, fontos tisztában lenni a kifejezés jelentésével. Informatikai biztonság alatt a számítógépes rendszerben kezelt adatok (és az azokat kezelő rendszer) védelmét értjük. Ezen a ponton meg kell említeni azt is, hogy az informatikai biztonság nem azonos az információbiztonsággal. Utóbbi ugyanis valamennyi kommunikációs rendszerben (írásban, szóban, elektronikus rendszerben) kezelt adatok védelmére vonatkozik, addig az informatikai biztonság fogalomkörét „csak" az informatikai rendszer védelme képezi [1].

* *Dunaújvárosi Főiskola, Informatika Intézet*
E-mail: ujbanyit@mail.duf.hu

** *Dunaújvárosi Főiskola, Informatika Intézet*
E-mail: katonaj@mail.duf.hu

*** *Dunaújvárosi Főiskola, Informatika Intézet*
E-mail: kovari@mail.duf.hu

[1] Muha Lajos (2008): Az informatikai biztonság egy lehetséges rendszertana (előadás szerk. változat) Robothadviselés 8. tudományos konferencia.

Ahhoz, hogy egy informatikai rendszerben védelemről és biztonságról beszélhessünk, ismernünk kell a rendszer komponenseit, hierarchikus felépítését, az egyes elemek és az alrendszerek, ill. a tágabb környezet közötti kapcsolatokat. [2] Az informatikai rendszerek ellen irányuló támadások alapvetően két nagy csoportra oszthatók: megkülönböztetünk külső és belső támadásokat. A külső támadások olyan szervezeten kívüli személyektől erednek, akik nem rendelkeznek hozzáférési jogosultsággal az informatikai rendszerhez. Az ilyen jellegű támadásokat a behatolók az interneten, hálózati kapcsolatokon keresztül hajtják végre. A belső támadások veszélye akkor áll fent, ha a támadó az informatikai rendszert illetően megfelelő hozzáférési jogosultsággal rendelkezik. Ezen felül a támadó számos olyan információ birtokában van, amelyek megkönnyítik a behatolást: ismeri a rendszer felépítését, fizikailag hozzáfér a számítógépekhez és a hálózati eszközökhöz. Tisztában van a belső házirenddel és ismeri az ott dolgozókat, ebből kifolyólag azt is tudja, hogy mely adatok azok, amelyek igazán fontosak a szervezet számára. Ismeri az adatok helyét, így könnyebben hozzáférhet a kritikus információkhoz és az esetleges sebezhetőségeket is könnyebben ki tudja használni. A belső támadások kapcsán azonban meg kell említeni, hogy nem minden támadás történik szándékosan: előfordulhat olyan eset is, amikor egy alkalmazott akaratlanul is behozhat vírust vagy más biztonsági veszélyt a rendszerbe.

Az egyik legelterjedtebb behatolási módszer az ún. megtévesztési technika (social engineering). Az eljárás lényege, hogy a támadó pszichológiai manipuláció útján befolyásolja az emberi viselkedést, amellyel a támadó ráveszi a gyanútlan felhasználókat arra, hogy védett adatokat adjanak ki a támadó számára. Ilyen adatok lehetnek például a személyes információk: felhasználónevek, jelszavak, bankszámlaszámok stb. Alapvetően három megtévesztési technika ismert: az adathalászat (phising), a telefonos adathalászat (vishing) és a hamis ürügy (pretext) technikája. [3]

Egy esetleges információ, „kiszivárogtatás" esetén a kivizsgálás során a feltételezett elkövetők és a fellelt fontos nyomok közötti összes lehetséges kapcsolat reprezentálható és elemezhető, melyhez egy gráf alapú kiértékelési módszer nagy segítséget nyújt.

[2] Peleskey Miklós Pál (2009): Hálózati csomópontok védelme hardver és szoftver eszközökkel, Debreceni Egyetem.

[3] Mitnick, K. D. (2006): A legendás Hacker 2. - A behatolás művészete.

Másrészt egy informatikai rendszer esetén előzetes elemzés végezhető arra vonatkozóan, hogy egy esetleges pszichológiai manipuláció (social engineering) alapú támadásnak elsődleges célpontja mely személyekre és információkra irányulhat.

Az ilyen jellegű támadások a rendszer „gyenge pontjának" tartott felhasználó hiszékenységét, sebezhetőségeit igyekszenek kihasználni. Az informatikai rendszerek támadása szempontjából elsődleges célpontok azok a felhasználók és alkalmazások, melyek minél több információhoz férnek hozzá az adott rendszerben. Az egyes információkhoz történő hozzáférések leírását, mint kapcsolatokat általában gráfok segítségével modellezik. [4, 5]

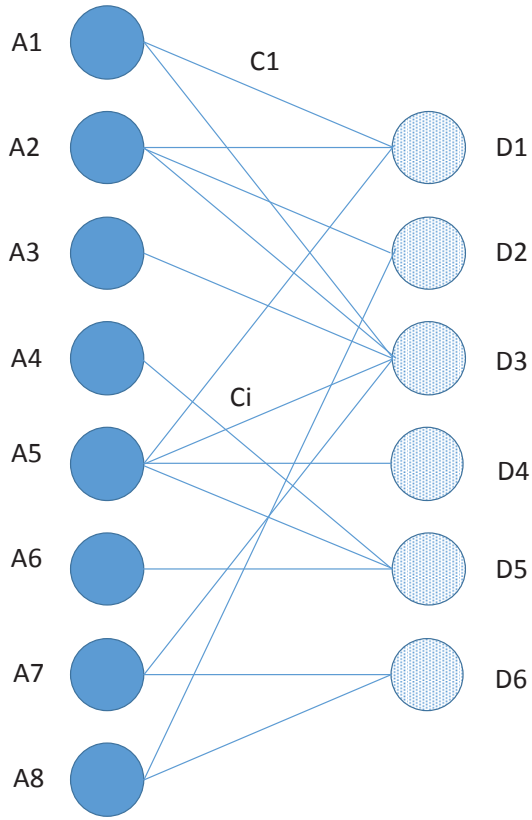
IT-biztonság gráf alapú elméleti modellje

A felállított elméleti modellben a felhasználókat és más az információkhoz hozzáféréssel rendelkező, abba beavatkozó rendszereket (webes vagy natív alkalmazások, stb.) és azok egyes csoportjait aktoroknak nevezzük. Az adatelemeket vagy összetett adatstruktúrát tartalmazó erőforrásokat (számítógépek, központi szerverek, adattárházak stb.) a továbbiakban adatstruktúrának nevezzük. Az aktorok és az adatstruktúrák között lévő hozzáférés kapcsolatok (számítógép- vagy telefonhálózat, stb.) jelölik az információáramlás lehetséges módjait. Az aktorok és az adatstruktúrák, mint egyes csomópontok és a közöttük lévő kapcsolatok, mint egyes élek segítségével a kapcsolati gráf ábrázolható. Egy ilyen módon megadott kapcsolati hálót ábrázoló gráfot mutat az *1. ábra*, melyben az egyes adatstruktúrák „D1"–„D6", az egyes aktorok „A1"–„A8" paraméterekkel vannak jelölve.

[4] Moser, L. E. (1987): Graph homomorphisms and the design of secure computer systems, Procee-dings of the Symposium on Security and Privacy, IEEE Computer Society. Pp. 88–96.

[5] Ou, X.–Boyer, W. F.–McQueen, M. A. (2006): A scalable approach to attack graph generation, Proceedings of the 13th ACM conference on Computer and communications security. Pp. 336–345.

1. ábra. Felhasználók és erőforrások kapcsolati hálóját leíró gráf.



Az *1. ábrá*n látható gráfban az egyes aktorok az egyes adatstruktúrákat a Ci-kapcsolaton keresztül megosztottan használják/férnek hozzá. IT-rendszerekben az egyes adatstruktúrahozzáférés-jogosultságok felhasználónként és felhasználói csoportonként definiálhatóak. Az egyes adatstruktúrák közös használata esetén lehetőség nyílik az egyes felhasználók közötti információátadásra, vagyis ez is egy információátviteli csatornaként jellemezhető.

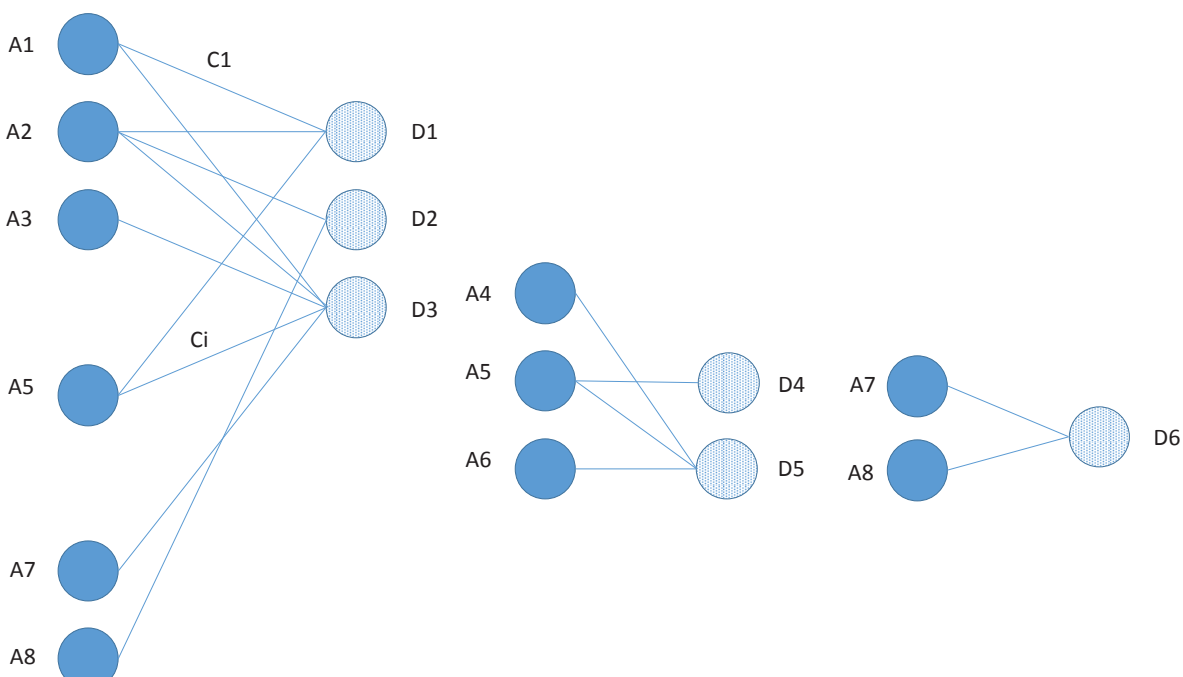
Az *1. ábra* szerinti gráfban az egyes aktorok mindegyikét egy adott szervezet felhasználóinak tekintjük, külső, szervezeten kívüli egyénekre, mint kívülállókra az adatok elérése szempontjából egyfajta potenciális veszélyforrásként tekinthetünk.

Az *1. ábrán* látható gráf csúcsainak halmazát fel tudjuk osztani egy A és B halmazra úgy, hogy az összes élre teljesül, hogy az egyik végpontja A-ban, a másik pedig B-ben van. Az ilyen típusú gráfokat páros gráfoknak nevezzük. Egy G páros gráf jelölése a következő:

$$G = (A,B) \qquad (1)$$

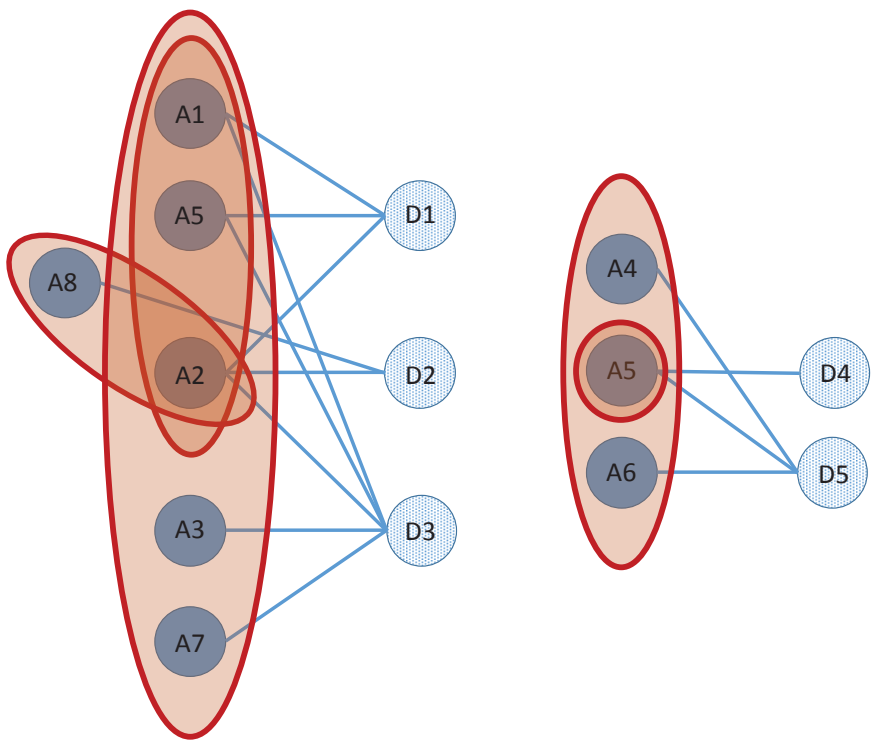
A gráf minden egyes éle implicit vagy explicit módon egy potenciális kommunikációs csatornaként vehető figyelembe. Mivel az adatokhoz vagy azok egy csoportjához több aktor is hozzáférhet, és a megadott gráf ezek összes lehetséges aktor-adatstruktúra kapcsolatait tartalmazza, ezért ezen aktorok által alkotott csoportok a teljes gráf egy részgráfját adják a *2. ábra* szerint.

2. ábra. Egyes felhasználói csoportok és azok adat hozzáférései alapján definiálható részgráfok.



Az így kapott részgráfok is párosak, mivel minden páros gráf minden részgráfja is páros. Az egyes páros részgráfok az adatkapcsolatok által magadott adathozzáférés alapján meghatározott aktori csoportok Venn-diagram segítségével is ábrázolhatóak. Ezen megadási mód esetén egyes aktorok és aktori csoportok kerülnek kihangsúlyozásra, amely struktúrája a *3. ábrán* látható.

3. ábra. Egyes aktori csoportok Venn-diagram szerinti ábrázolása.



A Venn-diagram topográfiája jól mutatja az egyes csomópontok egymáshoz képesti relatív kapcsolatait. A Venn-diagram alapján megvizsgálható, hogy valamilyen adatbiztonsági rés kihasználása esetén az egyes adathozzáférés szempontjából elkülönített csoportok között „kiszivárogó" információ milyen esetekben jöhet létre. Megállapítható, hogy a csoportok közötti információ-kiszivárogtatás a Venn-diagram alapján az egyes csoportok közötti átfedések mentén jöhet létre.

A valóságban az egyes felhasználók között számos kapcsolati szint is létrejöhet, amelyek az információ - továbbítás szempontjából kommunikációs csatornát képviselnek: barátok, család, egyéb szociális kapcsolatok által vagy akár más egymással közvetlen kapcsolatban álló felhasználók között. Ezeket az alternatív információs csatornákat, az itt átadott adatokat az adatforrásokhoz hasonló módon célszerű megadni. Az így előálló eltérő kapcsolatok által meghatározott összes lehetséges információs csatornák száma megfelelően elhelyezett, az információáramlás útjába iktatott közbenső csomópontok segítségével csökkenthetőek.

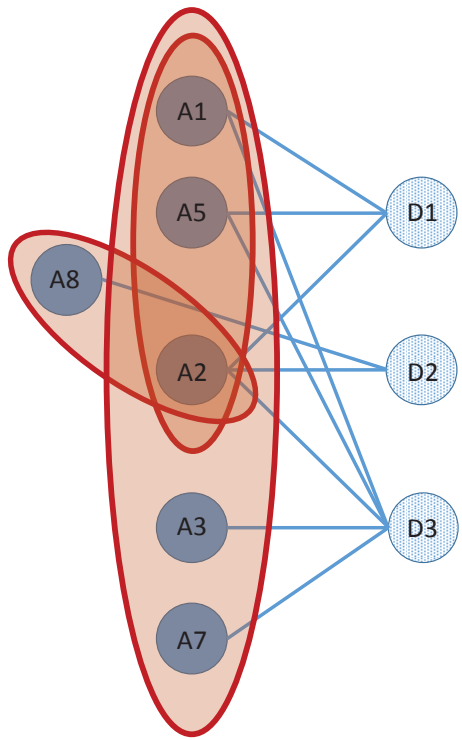
Az egyes felhasználók személyes, csak általuk elérhető adatokkal is rendelkeznek, mely kapcsolati hálót leíró gráf esetén a felhasználó és az egyes erőforrásokon elérhető adatok között egyetlen éllel jellemezhető a *4. ábrának* megfelelően.

4. ábra. Felhasználók személyes, csak általuk hozzáférhető adatait jelölő részgráf.

Ilyen típusú személyes adattal szinte minden felhasználó rendelkezik. Egy esetleges informatikai rendszer ellen irányuló, a rendszer biztonsági réseit vagy a pszichológiai manipulációt alkalmazó támadás ese-tén a támadás célpontja nem elsősorban a személyes, hanem az általánosan több elkülönített részterülettel/részleggel is kapcsolatos adatok elérése. Ennek megfelelően a támadás célpontja elsősorban azon felhasználók és rendszerek, melyek minél több részterület adataihoz rendelkeznek hozzáféréssel. Az aktorok és adatstruktúrák kapcsolati hálóját leíró gráfban ezen kulcsfontosságú csomópontok, azok kapcsolati száma alapján jól megfigyelhetőek, mint ahogy azt az *5. ábra* is mutatja.

5. ábra. Egyes kulcsfontosságú felhasználók és erőforrások azonosítása a kapcsolati szám alapján.

Aktor	Kapcsolatok száma
A1	2
A5	2
A8	1
A2	3
A3	1
A7	1



Az „A2”-vel jelölt aktor az, amely a legtöbb erőforráshoz, így adathoz hozzáfér, vagyis ennek a felhasználónak a manipulálása, vagy rendszer feltörése jelenti az információk elérése szempontjából a legnagyobb veszélyforrást. Az egyes aktorok az adatstruktúra kapcsolataik – így adatokhoz történő hozzáférésük – száma alapján jellemezhetőek. Az átlagostól eltérő, kiugró kapcsolati számmal rendelkező csomópontok jelzik az átlagosnál több adatstruktúrához hozzáférő, ebből adódóan jelentősebb támadási célpontot jelentő aktorok.

Összefoglalás

Az előzőkben bemutatott aktor-adatstruktúra kapcsolati hálón alapuló, a gráfban a kapcsolatok száma alapján feltárható legjelentősebb csomópontjait – ezen keresztül elsődleges támadási pontjait – jelentő felhasználók/rendszerek azonosíthatóak. Ez nagy segítséget jelent az informatikai rendszerek és a felhasználók védelemének megtervezése, a biztonsági szabályozások, rendszerek kialakítása, és a biztonság szempontjából legnagyobb veszélyforrást jelentő felhasználók oktatásánál. Az itt bemutatott egyszerű párosgráf-leíráson alapuló modell lehetőséget ad az adatkapcsolati számok vizsgálata alapján az egyes adathozzáférések aspektusából kulcsfontosságú aktorok azonosítására. Az informatikai rendszerek támadása kapcsán az elsődleges célpontokat ezen aktorok jelentik, mivel a legtöbb információhoz ők férnek hozzá. Ebből adódóan az adathalászat elleni védelem megtervezésekor és kialakításakor a megfelelő informatikai biztonsági rendszer kiválasztása és alkalmazása, valamint az informatikai biztonságot szabályozó házirendek, egyéb dokumentumok összeállításakor és bevezetésekor az egyes felhasználókra vonatkozóan a megfelelő oktatásra, a rendszerek esetében pedig azok konfigurálására kiemelt figyelmet kell fordítani.