

DunaKavics

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

Műszaki-, Informatikai és Társadalomtudományok

KATONA JÓZSEF–UJBÁNYI
TIBOR–KÖVÁRI ATTILA



A figyelem EEG-alapú vizsgálata-
jának alkalmazási lehetőségei
a tanulási folyamat várható
eredményességének jelzésére



UJBÁNYI TIBOR–KATONA
JÓZSEF– KÖVÁRI ATTILA
Felhasználói csoportok és
adatkapcsolatok vizsgálata az
IT-biztonság szempontjából



GYENGE ALEXANDRA
Híres hírhedt, a hírből hír lett,
avagy meddig hír a hír a DF-en



Dunakavics

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

Műszaki-, Informatikai és Társadalomtudományok

MEGJELENIK 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

KATONA JÓZSEF-UJBÁNYI TIBOR-KÖVÁRI ATTILA

*A figyelem EEG-alapú vizsgálatának alkalmazási lehetőségei
a tanulási folyamat várható eredményességének jelzésére*

5

UJBÁNYI TIBOR-KATONA JÓZSEF-KÖVÁRI ATTILA

*Felhasználói csoportok és adatkapcsolatok vizsgálata
az IT-biztonság szempontjából*

15

GYENGE ALEXANDRA

Híres hírhedt, a hírből hír lett, avagy meddig hír a hír a DF-en

25

Galéria

(a Dunaújvárosi Főiskola Fotókör – Pintér Zsolt – fotói)

46

Felhasználói csoportok és adatkapcsolatok vizsgálata az IT-biztonság szempontjából

Összefoglalás: Egy komplex, több felhasználós informatikai rendszerben az informatikai biztonság kiemelt jelentőségű. Az egyes rendszerek és az adatok védelme érdekében igen komoly biztonsági intézkedésekre és védelmi eszközökre van szükség. A maximális védelemi szintet azonban nem csak a külső támadások elleni védekezés, hanem az informatikai rendszer adatai és az azokhoz hozzáférő felhasználói csoportok eloszlása, és e csoportok kapcsolatai is meghatározzák. A cikk ezen felhasználói- és adatkapcsolatok összefüggéseit vizsgálja, és informatikai biztonság szempontjából optimális eloszlását határozza meg.

Kulcsszavak: IT-biztonság, kapcsolatok, entrópia.

Abstract: IT security has high priority in a complex, multi user IT system. Security systems and safety measure are needed to protect data and systems. The maximum protect level has determined by defense against external attacks and connections of users and user groups who access the system. In the article we examine these user connections, data links and define optimal dispersion of these based on IT security.

Keywords: IT security, connections, entropy.

* 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] Bodlaki Ákos–
Csernay Andor–
Mátyás Péter–Muha
Lajos–Papp Györ-
gy–Vadász Dezső
(1996): *Informatikai
rendszerek biztonsági
követelményei*. 12. sz.
ajánlás, 1.0 verzió.

Bevezető

Az IT-biztonság alapproblémája az adatok védelmének mikéntje. Maga a problémakör a leírható egy egyszerű modell segítségével. A modell középpontjában adatok állnak, amelyeket valamilyen módon védeni kell. Az adatok információt hordoznak, amely két oldalról közelíthető: az egyik oldalon a tulajdonosa védi, a másik oldalon pedig a támadó támadja. Mindkét fél a másiktól teljesen független módszerekkel próbálja elérni a célját [1].

Az informatikai rendszerek támadhatóságánál azok a felhasználók és alkalmazások játszanak kiemelt szerepet, amelyek minél több információhoz férnek hozzá az adott rendszerben. Ha egy felhasználói csoport vagy egy alkalmazás hozzáférést kap a kritikus adatok többségéhez, akkor elmondható, hogy biztonsági szempontból ezek a tényezők jelentik a legnagyobb veszélyt a rendszerre egy esetleges sikeres külső támadás esetén. Amennyiben egy felhasználónak, vagy a felhasználók egy csoportjának nagy adathalmazhoz van hozzáférése, akkor az adott felhasználó, felhasználói csoport védelme az adatok biztonságára kiemelt hatással van.

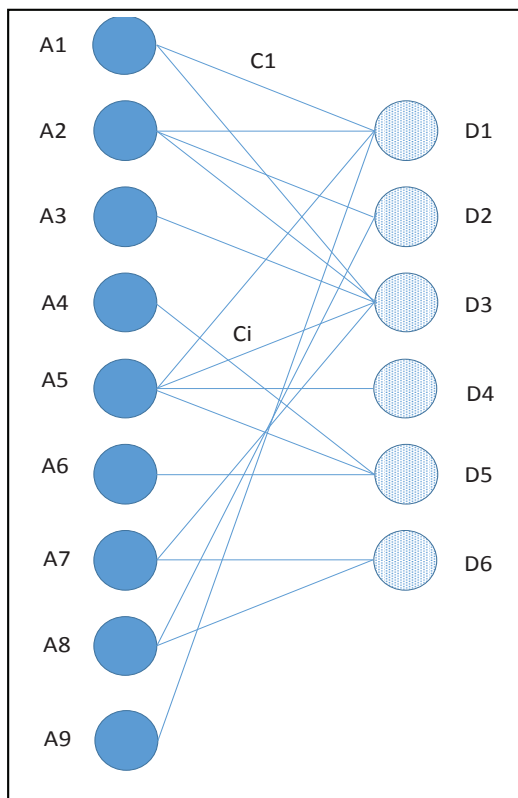
Az informatikai biztonság aspektusából az egyes együttműködő (vagyis kapcsolatban álló) felhasználók csoportjainak számát célszerű módon érdemes korlátozni. Erre azért van szükség, mivel ha egy felhasználó sok együttműködő (vagyis kapcsolatban álló) csoportnak tagja, akkor a kapcsolatok miatt az egyes csoportok által közösen elérhető adatok száma nagymértékben nő. Egy felhasználói csoport minél több más csoport által kezelt adathoz fér hozzá, akkor ennek a csoportnak egy külső támadás következtében történő megfertőzhetősége számos más csoportra áttérjedhet. Ezért egy támadás következtében az informatikai rendszer védelme érdekében e kulcsfontosságú felhasználói csoportok kiemelt jelentőséggel bírnak. Az előzőekben leírtak alapján tehát megállapítható, hogy az informatikai biztonság szempontjából valamilyen módon számszerűsíteni kell az egyes csoportok fontosságát, ezzel rámutatva az egyes csoportok számának, méretének és adathozzáférés kapcsolatainak az informatikai biztonságra gyakorolt hatására.

A felhasználói csoportokat és az adatokat, valamint a köztük lévő kapcsolatokat megadó rendszert úgy célszerű kialakítani, hogy lehetőség szerint ne legyenek benne a támadások szempontjából nagyobb jelentőséggel bíró, így valószínűsíthetően nagyobb mértékben veszélyeztetett pontok. Egy ilyen kialakítással biztosítható, hogy az átlagos biztonsági szint e rendszer vonatkozásában maximális legyen.

Adatkapcsolatok leírása páros gráf segítségével

Az [2] cikk alapján a felhasználók és az adatok kapcsolatai a páros gráfokkal ábrázolhatóak, ahogy az az 1. ábrán is látható.

1. ábra. A felhasználók és adatok kapcsolatait leíró páros gráf.



Az 1. ábra szerinti páros gráfban a felhasználókat és más – az információkhoz hozzáféréssel rendelkező, abba beavatkozó – rendszereket (webes vagy natív alkalmazások, stb.), valamint azok egyes csoportjait aktoroknak nevezzük és A-val jelöljük. Az adatelemeket (fájlokat) vagy összetett adatstruktúrát tartalmazó erőforrásokat (számítógépek, központi

[2] Ujbányi Tibor–Katona József–Kővári Attila (2014): IT-biztonság egy gráf alapú modellje. In: Kiss Natália–Nagy Bálint–Németh István Péter (Szerk.) *Tudományos terek*. Dunaújváros: DUF Press.

[2] Ujbányi Tibor–Katona József–Kővári Attila (2014): IT-biztonság egy gráf alapú modellje. In: Kiss Natália–Nagy Bálint–Németh István Péter (Szerk.) *Tudományos terek*. Dunaújváros: DUF Press.

szerverek, adattárházak, stb.) a továbbiakban adatstruktúrának nevezzük és D-vel jelöljük. Az aktorok és az adatstruktúrák között lévő hozzáférés-kapcsolatok (számítógép- vagy telefonhálózat, stb.) jelölik az információáramlás lehetséges módjait [2].

Adatkapcsolatok leírása Venn-diagram segítségével

A páros gráf komplexitása könnyen ábrázolható Venn-diagramok segítségével. A gráf ezen tulajdonságának ábrázolhatósága azonban maga után von egy másik kérdést is, miszerint létezik-e valamilyen egyszerűbb ábrázolási forma a gráfok esetében, amely jól prezentálja a szerkezetet és rávilágít a legfontosabb információ csatornákra.

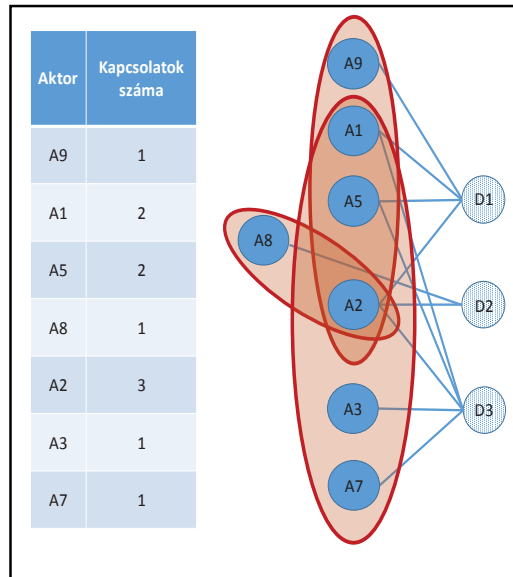
Az [2] szerint a Venn-diagram alapján megvizsgálható, hogy valamilyen biztonsági rés kihasználása esetén az egyes adathozzáférés szempontjából elkülönített csoportok között milyen esetekben jöhet létre ún. „kiszivárogo” információ. A Venn-diagram segítségével megállapítható, hogy a csoportok közötti információ-kiszivárogtatás az egyes csoportok közötti átfedések, mint csoportok közötti információ csatornák mentén valósulhat meg. Amennyiben az egyes aktori csoportokat leíró halmazok közötti információ csatornákat kívánjuk ábrázolni, úgy azt például a 2. ábrán látható Venn-diagram szerint tehetjük meg.

Adott számú aktor esetén, melyet jelöljünk Na-val, ha megvizsgáljuk az egyes lehetséges csoportok maximális számát, akkor az alábbi összefüggés írható fel:

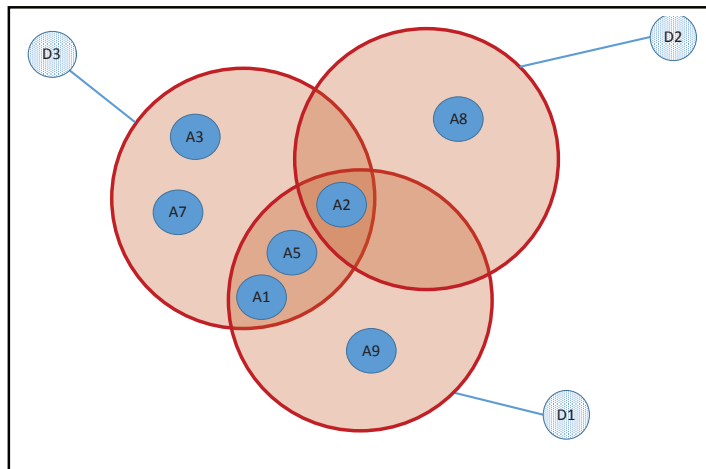
$$Cs_{\max} = 2Na - 1 \quad (1)$$

A létrehozható csoportok maximális száma már kevés számú aktor esetén is igen nagy. Ahhoz, hogy minimalizálni tudjuk a rendszer biztonsági kockázatát, meg kell határozni az egyes kapcsolatok jelentőségét. Az 2. ábrán megadott Venn diagram a 3. ábra szerinti halmaz ábrázolással is megadható, amelyben a halmazok metszetei jelentik az egyes csoportok közötti kapcsolatokat.

2. ábra. Adatkapcsolatok ábrázolása Venn-diagram segítségével.

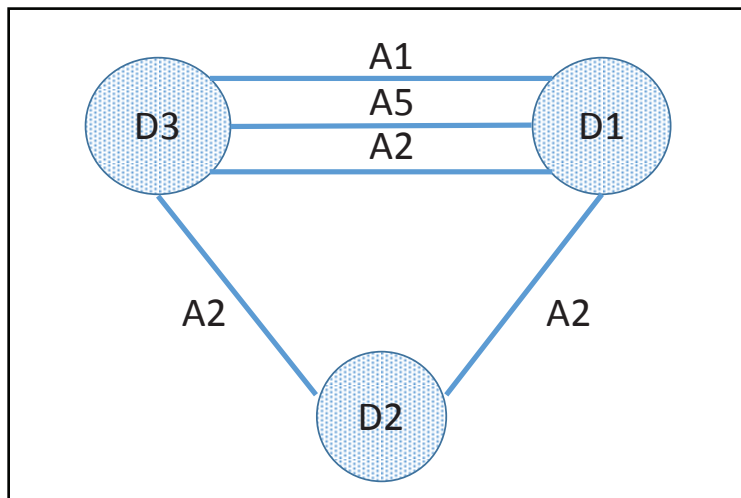


3. ábra. Adatkapcsolatok ábrázolása halmazok segítségével.



Az egyes halmazok közötti kapcsolatok az alábbiak szerint ábrázolható (4. ábra):

4. ábra. Kapcsolati háló.



Adatkapcsolatok leírása a kapcsolatok súlya alapján

A 4. ábrán látható kapcsolati háló az 1. ábra szerinti páros gráf adatstruktúra kapcsolatait bemutató egyszerűsített ábrázolási mód. A rendszer biztonságának optimalizálása érdekében ismernünk kell az egyes kapcsolatok jelentőségét. Egy kapcsolat jelentősége jellemzi azt, hogy hány aktor hány adatstruktúrához fér hozzá egy kapcsolaton keresztül. A kapcsolat jelentősége nő a kapcsolathoz hozzáférő aktorok számával, valamint a kapcsolaton keresztül elérhető adatstruktúrák számával is. Ennek alapján definiáljuk a kapcsolat jelentőségét (j) az adott csoportban lévő aktorok számának (N_a) és az általuk elérhető adatstruktúrák számának (N_d) szorzatával:

$$j_i = N_{a_i} \cdot N_{d_i} \quad (2)$$

Egy adott kapcsolat teljes rendszerre vonatkoztatott súlya (j_i) az alábbiak szerint definiálható:

$$p_i = \frac{j_i}{\sum_{i=1}^{Cs} j_i} \quad (3)$$

A 2. ábra szerinti példára vonatkozóan a kapcsolatok jelentősége és súlyai az 1. táblázat szerint alakulnak.

1. táblázat. A kapcsolatok súlyának meghatározása.

Cs (csoport azonosítószáma)	1	2	3
Na (aktorok száma)	4	2	5
Nd (elérhető adatstruktúrák száma)	3	3	3
j (kapcsolatok jelentősége)	12	6	15
p (kapcsolatok súlya)	0.36	0.18	0.46

Egy néhány aktorból és adatstruktúrából álló, ismert csoportokra tagozódás esetén a fenti táblázat szerint az egyes csoportok kapcsolati súlya könnyen meghatározható. Nagyvállalati környezetben nagyok sok felhasználó általuk elérhető adatstruktúra esetén ennek a felbontásnak a leképezése komplikált. Nagyszámú aktor és adatstruktúra esetén feltételezzük azt, hogy az egyes csoportokhoz tartozó kapcsolatok súlya véletlenszerűen, egyenletes eloszlás szerint alakulnak ki. Ahhoz, hogy statisztikailag elkerüljük a nagyszámú aktort és általuk elérhető nagymennyiségű adatstruktúrát, amely előnytelen, mivel egy csoporton belül bekövetkező kár így nagy számban elterjedhet, ezért a rendszerben az entrópia maximalizálására kell törekedni.

[2] Ujbányi Tibor– Katona József–Kővári Attila (2014): IT-biztonság egy gráf alapú modellje. In: Kiss Natália–Nagy Bálint–Németh István Péter (Szerk.) *Tudományos terek*. Dunaújváros: DUF Press.

[3] Biszak Előd (2013): Maximum Entropy Models. Budapest: Eötvös Loránd University, MSc thesis.

A kapcsolatok entrópiája Shannon-féle entrópiafüggvény és természetes alapú logaritmus alkalmazásával az alábbi módon írható fel [2]:

$$H = - \sum_{i=1}^{Cs} p_i \cdot \ln p_i \quad (4)$$

Tehát az entrópia maximalizálása azt jelenti, hogy a kapcsolatok súlyának eloszlása hozzávetőlegesen egyenletes, a csoportok kapcsolatainak száma közel állandó. Ez azt jelenti, hogy amennyiben egy csoportban nagyszámú aktor található, úgy az általuk elérhető adatstruktúrák számát minimalizálni kell. Ez az egyszerű modell csak a csoport méretét veszi figyelembe, nem tesz különbséget az egyes csoportok elvárt védelmi szintjei között.

Egy csoport külső támadások szempontjából meghatározható biztonsági szintjét a csoport felhasználóit és alkalmazásait érő támadások valószínűségével jellemezhető. A külső támadások sikerességét elsősorban a csoportra vonatkozó előírt biztonsági szabályok, szintek és azok betartása, betartatása, valamint az alkalmazott védelmi rendszer kialakítása és az alkalmazások sebezhetősége határozza meg. Egy adott csoport esetén a külső támadások gyakorisága (a_i) alapján meghatározható a csoportra jellemző biztonsági szint egy számszerűsíthető értéke. A biztonsági szint azonban nem csak a támadások számától, hanem azok veszélyességétől is függ (λ_i), ezért ezt a tényezőt célszerű egy súlyozási faktorral figyelembe venni.

Az előzők szerint a biztonság maximalizálásához a teljes rendszer entrópiáját kell maximalizálni. Ebben az esetben meg kell keresni azt a maximális entrópia melletti kapcsolati súly eloszlást, amely minimális kockázatot, maximális biztonsági szintet jelent. A külső támadások veszélyessége kevésbé befolyásolható, ezért az értékét konstansnak célszerű megválasztani (λ).

A maximum entrópia a Lagrange multiplikátor módszerével, a teljes rendszer átlagos támadási gyakorisága ($\bar{a}$) alapján az alábbiak szerinti diszkrét, nem egyenletes eloszlásra vonatkozólag [3]:

$$L = \max_{p_i} \left[- \sum_{i=1}^{Cs} p_i \cdot \ln p_i - \lambda \left(\sum_{i=1}^{Cs} p_i a_i - \bar{a} \right) - \mu \cdot \left(\sum_{i=1}^{Cs} p_i - 1 \right) \right] \quad (5)$$

Maximális entrópia esetén:

$$p_i = e^{-(\mu-1)} \cdot e^{-\lambda a_i} \quad i=1, 2, \dots, Cs \quad (6)$$

A (3) összefüggést felhasználva:

$$p_i = e^{-(u-1)} \cdot e^{-\lambda a_i} = \frac{1}{\sum_{i=1}^{Cs} j_i} \cdot j_i \quad (7)$$

$$p_i = \frac{1}{\sum_{i=1}^{Cs} e^{-\lambda a_i}} \cdot e^{-\lambda a_i} \quad (8)$$

Az eredmény felhasználható az entrópia maximalizálásán keresztül az egyes csoportok átlagos támadási gyakoriságának minimalizálására, mely biztonsági szempontból a megadott feltételek mellett a legelőnyösebb.

$$j_i = e^{-\lambda a_i} \quad (9)$$

Az (9) szerinti, a kapcsolatok jelentőségére felírható eredményből összességében levonható az a következtetés, hogy a nagyobb külső támadási gyakorisággal rendelkező csoportok esetén e csoport kapcsolatainak jelentőségét – melyet az aktorok és kapcsolatok száma határoz meg – a támadások gyakoriságának mértékével exponenciálisan csökkenteni kell.

Összefoglalás

Az informatikai biztonság szempontjából egy felhasználói csoportot tekintve a külső támadások száma és az adott csoport információs kapcsolatainak száma határozza meg a csoport biztonság szempontjából betöltött jelentőségét. A biztonság szempontjából úgy célszerű az egyes felhasználói csoportokat és azok információs kapcsolatait meghatározni, hogy a külső támadások szempontjából történő kitettségük minimális legyen.

Az előzőekben bemutatott modell alapján az informatikai rendszert leíró kapcsolati háló alapján, a kapcsolati súlyok felhasználásával entrópiafüggvény maximalizálásával meghatározható az adott csoportokra vonatkozó optimális felhasználói- és információskapcsolat-szám, mely az adott rendszer átlagos külső támadásokkal szembeni kitettségét minimalizálja.