HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Muha Lajos
muha.lajos@uni-nke.hu

FORMÁLIS BIZTONSÁGI MODELLEK I.
A DISZKRECIONÁLIS HOZZÁFÉRÉS-VÉDELEM

Absztrakt

A biztonságos informatikai rendszerek megteremtésére irányuló erőfeszítések folyamatosak. A nagy biztonságú informatikai rendszerek esetében alapvető követelmény a biztonság formális leírása és bizonyítása. Ezért már az informatikai biztonság kezdetétől számos formális modellt dolgoztak ki a biztonsági elvárások leírására és bizonyítására. Ez a cikksorozat ezeket a formális modelleket kívánja bemutatni, és felhasználhatóságuk szempontjából összehasonlítani. Jelen a cikk a hozzáférés-vezérlés elveit és alapvető eljárásait írja le.

Efforts to build secure computer systems are continuous. The formally description and verification of security is a fundamental requirement of the high-security information systems. Therefore, many formal models have been developed to describe and verification of security requirements. This article series aims to present them and their comparison, based on the usability. This article reviews basic principles and procedures of the access control.

Kulcsszavak: *informatikai biztonság, adatvédelem, bizalmasság, sértetlenség, formális modell, hozzáférés-ellenőrzés, biztonsági osztályok ~ information security, privacy, confidentiality, integrity, formal model, access control, security classes*

1. BEVEZETÉS

Az informatikai rendszerek biztonsága terén már az 1970-es évek elején felmerült az információvédelem formális meghatározásának, mint biztonságpolitikának, illetve e biztonságpolitika betartásának formális úton történő ellenőrzésének igénye. Ennek az igénynek a megvalósítására azóta számos mű (Bell-LaPadula modell [1], Biba modell [2], Clar-Wilson modell [3], stb.) született, amelyek az információvédelem kapcsán leírják [4]:

1. A biztonság formális meghatározását.
2. Az alanyok jogosultságainak meghatározását objektumokhoz és más alanyokhoz.
3. Az információ védelemmel kapcsolatos alapvető tulajdonságainak (bizalmasság, sértetlenség, elérhetőség, elszámoltathatóság) meghatározását,
4. Az adatokhoz való hozzáférés megoldási módjait.
5. Formális modellek felépítését az adatok védelme alábbi kérdéseinek vizsgálatához:
   - a bizalmasság biztosítása,
   - a sértetlenség biztosítása,
   - a jogosulatlan jogosultság áramlás (szivárgás),
   - a „biztonságos” adatáramlás biztosítása.
6. A formális modellek vizsgálatának eredményeit – az adatok megfelelő védelmét biztosító szabályok megfogalmazását.
7. A formális mechanizmusok (mátrixok, rácsok, gráfok) felhasználását az adatokhoz való hozzáférés megoldási módjainak, és azok áramlásának leírásához.

Ebben a cikkben a fentiek közül az adatok védelmére alkotott formális modellek ismertetése mellett azok összevetését, és a felhasználási lehetőségeiket szeretném bemutatni.

2. ALAPFOGALMAK

A cikk a következő fogalmakat használja:

- Biztonság,

  Információvédelem: Ebben a cikkben a NATO INFOSEC meghatározását veszem alapul: „a biztonsági rendszabályok alkalmazása a kommunikációs, információs és más elektronikus rendszerekben a feldolgozott, tárolt vagy továbbított információ bizalmasságának, sértetlenségének vagy rendelkezésre állásának véletlen vagy szándékos elvesztése ellen, és e rendszerek sértetlenségének vagy rendelkezésre állásának elvesztése ellen”. [5].
- Formális – informális – szemiformális [6]:
  - Informális leírás: valamilyen természetes nyelven készült leírás.
  - Szemiformális leírás: szabályelvű természetes nyelven készült leírás, pl. strukturált tervezési módszereknél használt adatfolyam, entitás-reláció, állapot-átmenet, stb.
  - Formális leírás: szintaktikusan és szemantikusan szabályozott specifikációs (formális) nyelven, tipikusan a matematikai logika nyelvén készült leírás.
  - Formális bizonyítás: Formális nyelven, levezetési szabályokkal és módszerekkel történő bizonyítás,
  - Formális biztonságpolitikai modell: formális nyelven leírt biztonsági politika modell;
- Alanyok (S-subjects): aktív entitások[1];
- Objektumok (O-objects): passzív entitások[2];

[1] felhasználók, akik az alkalmazásaikkal fenyegetést jelenthetnek.

[2] az adatok kezelését végző egységek (fájlok, könyvtárak, programok, stb.) – védelem alatt állnak.

- Hozzáférés-vezérlés (Access Control): "Az erőforrás jogosulatlan használatának megelőzése, beleértve erőforrás jogosulatlan módon való használatának a megelőzését" [7];
- Hozzáférési mód (Acces Method): az objektumokhoz való hozzáférés lehetősége, az adatáramlás iránya;
- Szabályok (Rules): a hozzáférés-vezérlés módjának meghatározása.
- Jogosultságok (Permissions): az objektumokon végrehajtandó tevékenységek végrehajtásának lehetősége (joga);
- Feljogosítás (Authorization): az alanyoknak az objektumok feletti jogosultságok megadása és felügyelete;
- Axiómák (Axioms): tulajdonságok, amelyeket a rendszernek teljesíteni kell, hogy az adott biztonsági modellben biztonságosnak fogadjuk el;
- Predikátumok (Predicates): annak meghatározására szolgálnak, hogy az alanynak van-e jogosultsága az objektumon, értéke lehet igaz (true) vagy hamis (false);
- Katonai biztonsági modell (Military Security Model): a minősített adatokat (szigoruan titkos, titkos, bizalmas, ...) tartalmazó (nem csak katonai!) rendszerekre vonatkozó modellek csoportja;
- Üzleti biztonsági modell (Business Security Model): a nem minősített adatokat (kiemelt jelentőségű, üzleti titok, nyílt) tartalmazó rendszerekre vonatkozó modellek csoportja.

3. A KLASSZIKUS HOZZÁFÉRÉS-VEZÉRLÉSEK ALAPJAI

A formális biztonsági modellek különböző hozzáférés-vezérléseken alapulnak. Ezeket a hozzáférés-védelem kialakítása során – formális biztonsági modellben való felhasználás nélkül is – alkalmazzák. Számtalan módosított, továbbfejlesztett változatuk létezik, itt csak a klasszikusnak nevezhető változataik kerülnek bemutatásra.

3.1. Az NTK szabály

A hozzáférés-vezérlések jelentős része a közismert *kell, hogy tudja*[3] elven alapul. A *kell, hogy tudja* elv azt jelenti, hogy egy adathoz (információhoz) csak az kaphat hozzáférési engedélyt, akinek adott információt a feladatköre miatt szükséges hozzáférnie (szükséges és elégséges jogosultság).

Az NTK szabály abból a feltételezésből indul ki, hogy minden objektum legalább egy adattárolóval (angolul container) kapcsolatban áll, *Container(O)* az *O* objektummal kapcsolatban álló adattárolók halmaza. *NTK(S)* az *S* alany által elérhető adattárolók halmaza. A biztonságpolitika a következő szabályokat valósítja meg:

Az *S* alany hozzáférhet az O objektumhoz, ha:

Container(O) $\subseteq$ *NTK(S)* (ha az *O* objektum minden tárolójához hozzáférhet az *S* alany).

A módosított NTK szabály

Az NTK szabály módosítása figyelembe veszi az adatáramlás irányát (írás, olvasás) is.

S alany olvasási joggal hozzáférhet O objektumhoz, ha:

Container(O) $\subseteq$ *NTK(S)* (ha az *O* objektum minden tárolójához hozzáférhet az *S* alany).

S alany írási joggal hozzáférhet O objektumhoz, ha:

Container(O) $\supseteq$ *NTK(S)* (ha az *S* alany csak az *O* objektum tárolóihoz férhet hozzá).

[3] Need to know

Nézzünk egy példát:

A rendszerben található adattárolók: {céges adatok – *B*, pénzügyi adatok – *F*, személyes adatok – *P*, egészségügyi adatok - *M*},

Container(O) = {M, F}

$NTK(S_1)=\{F\}$, vagyis az S_1 alanynak csak a pénzügyi adatokhoz (*F*) van hozzáférése, ezért S_1 alany írhat *O* objektumba,

$NTK(S_2)=\{P\}$, vagyis az S_2 alanynak az egészségügyi és a pénzügyi adatokhoz (*M, F*) nincs hozzáférése, ezért S_2 alanynak nincs semmilyen hozzáférése az *O* objektumhoz,

$NTK(S_3)=\{C, F\}$, vagyis az S_3 alanynak a pénzügyi adatokon (*F*) kívül a céges adatokhoz (*B*) is hozzáférése van, de az egészségügyi nincs hozzáférése, ezért S_3 alanynak nincs semmilyen hozzáférése az *O* objektumhoz,

$NTK(S_4)=\{P, M\}$, vagyis az S_4 alanynak az egészségügyi adatokon (*M*) kívül a személyes adatokhoz (*P*) is hozzáférése van, de a pénzügyi adatokhoz (*F*) nincs hozzáférése, ezért S_4 alanynak nincs semmilyen hozzáférése az *O* objektumhoz,

$NTK(S_5)=\{F, M, P\}$, vagyis az S_5 alanynak hozzáférése van a pénzügyi és az egészségügyi adatokhoz (*M, F*) is, de ezenkívül a személyes adatokhoz (*P*) is, ezért S_5 alany olvashatja az *O* objektumot, de nem írhat bele.

3.2 Diszkrecionális hozzáférés-vezérlés

A diszkrecionális, vagyis szabad belátás szerint kialakított hozzáférés-vezérlés (röviden: DAC[4]), más néven mátrix modell, vagy jogosultságok táblázata az első hozzáférés-védelmi megoldás volt. A diszkrecionális hozzáférés-vezérlés az alapja az alanyok azonosítása. Az eljárást azért nevezik diszkrecionálisnak, mert legfontosabb jellemzője, hogy amennyiben egy alany rendelkezik egy objektumhoz valamilyen hozzáférési jogosultsággal, akkor ezt a jogosultságot szabad belátása szerint tovább adhatja más alanyoknak, vagyis ez a szabályozási mód az alanyoknak az objektumok feletti jogosultságok kiosztását jelenti. A DAC a gyakorlatban többnyire a közismert *hozzáférés-vezérlési lista* (röviden: ACL[5]) alkalmazásán alapul.

A DAC – bár szokás a formális modellek között emlegetni – valójában nem formális, hanem szemiformális modell, mivel leírása nem a matematikai logika nyelvén történik, hanem egy szabályelvű természetes nyelven készült entitás-reláció. A DAC megoldásának és alkalmazásának egyik első leírói G. Scott Graham és Peter J. Denning voltak a Protection – Principles and practice cikkükben [8]. A DAC alkalmazását az USA Védelemi Minisztérium kiadványa, a Narancs Könyv[6] [9] a C2 és a C1 biztonsági osztályokban írta elő kötelező tette. A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság 12. számú ajánlása [10] az alapbiztonsági osztályban, majd a Közigazgatási Informatikai Bizottság 25. számú ajánlása 1-2. kötete az IBIK [11] a 0., 1. és 2. biztonsági szinteken előírta az alkalmazását.

A védelmi rendszer elemei [8]:

- *objektumok* (pl.: fájl könyvtár, stb.) halmaza;
- *alanyok* (felhasználók, illetve az általuk futtatott folyamatok) halmaza;

[4] Discretionary Access Control

[5] Access Control List

[6] A borítójának színéről Narancs Könyv (Orange Book) néven közismerté vált Trusted Computer System Evaluation Criteria (TCSEC, magyarul Biztonságos Számítógépes Rendszerek Értékelési Kritériumai) az Amerikai Egyesült Államok Védelmi Minisztériumának 1983-ban kiadott nyilvános informatikai biztonsági követelménygyűjteménye, amelynek alkalmazása az USA-ban majd 20 évig kötelező volt a kormányzati, katonai rendszerek vonatkozásában.

– *szabályok* az alanyoknak az objektumokhoz való hozzáférésének vezérléséhez

Az egyes objektumokhoz való hozzáférési jogot a alanyok számára az objektum tulajdonosa[7] (owner) állítja be. A hozzáférés-vezérlési listában implicit vagy explicit módon szerepel az objektum, az alany és az engedélyezett, illetve tiltott művelet. Kivétel nélkül minden hozzáférési kísérlet ellenőrzésre kerül.

Az alapvető hozzáférési műveletek:

– olvasás (read),
– írás (write),
– végrehajtás (execute).

A DAC megvalósítására tipikus példája a „klasszikus" UNIX operációs rendszer hozzáférés-védelmi megoldása. Ez egy egyszerű, de kevésbé rugalmas hozzáférés-védelmi rendszer, ahol csak az alapvető hozzáférési műveletek, az olvasás, az írás és a végrehajtás alkalmazhatóak.

Az alanyokat (felhasználókat) egyedi azonosítóval rendelkeznek és egy elsődleges, azonos védelmi szintű alanyok csoportjának tagja. Az alanyokat és az objektumokat egy (csoportszám, tagszám) párossal azonosítják, ahol az objektumok felveszik az őket létrehozó alany kódjait. Az objektum és ahhoz hozzáférni kívánó alany kódpárosa alapján az alany az alábbi három csoport valamelyikébe sorolható, és minden objektumnál e három csoportra vonatkozó jogosultságok szerepelnek:

- tulajdonos, ahol a csoportszám és a tagszám azonos,
- csoport, a csoportszám megegyezik,
- világ (mindenki a tulajdonoson, a tulajdonos csoportjának tagjain kívül), egyik kódszám sem egyezik meg.

A megvalósításhoz minden objektumhoz hozzárendelésre kerül egy 12 bites szó, amelyből 9 bit a hozzáférés-védelem leírása, ahol a hárombites csoportokban az olvasás, írás és a végrehajtási jogok szerepelnek. Például

rwx rw- ---

Az első három bit a tulajdonos olvasási, írási és végrehajtási jogát jelöli. A következő három bit a tulajdonos csoportja tagjainak olvasási és írási jogát jelöli. A tulajdonoson, a tulajdonos csoportjának tagjain kívüli felhasználóknak nincs semmilyen hozzáférési joga.

A hozzáférési mátrix a S_i alany által az O_j objektumon elvégezhető lehetséges $A(S_i, O_j)$ hozzáférési műveleteket jeleniti meg.

		OBJEKTUMOK						
		Alanyok			Fájlok		Eszközök	
		S_1	S_2	S_3	F_1	F_2	D_1	D_2
ALANYOK	S_1		block wakeup		Read write		seek	
	S_2			Stop		update		Seek
	S_3				Delete	execute		

1. ábra. Egy hozzáférési mátrix részlete [8]

[7] Az objektum tulajdonosa annak létrehozója, vagy akire átruházták ezt a tulajdonságot.

Az un. kiterjesztett hozzáférési mátrixban[8] megjelenik a tulajdonosi jog (owner) és a hozzáférés-vezérlést kezelő jog (control), valamint a *jogmásolás* lehetősége. A tulajdonosi jog az adott objektumon lehetővé teszi más alanyok hozzáférési jogainak kezelését. Tulajdonosa minden objektumnak csak egy lehet. A hozzáférés-vezérlést kezelő jog csak alanyok között értelmezett és lehetővé teszi más alanyok hozzáférési jogainak kezelését. Ahhoz, hogy egy adott objektumon valamely alany meglévő hozzáférési jogait átadhatóak legyen egy másik alanynak, bevezetésre került a jogmásolási, mint vezérlési lehetőség. A jogmásolás lehetőségét *-gal jelölik. A kiterjesztett hozzáférési mátrixban kívül rendszerenként eltérő hozzáférési műveleteket (módosítás, törlés, jogosultságkezelés, stb.) is megvalósítanak.

		OBJEKTUMOK						
		Alanyok			Fájlok		Eszközök	
		S_1	S_2	S_3	F_1	F_2	D_1	D_2
ALANYOK	S_1	control	owner block wakeup	owner control	read * write *		seek	Owner
	S_2		control	stop	Owner	update	owner	seek *
	S_3			Control	Delete	owner execute		

2. ábra. Egy kiterjesztett hozzáférési mátrix részlete [8]

A DAC használatához fel kell tételeznünk, hogy:

1. a felhasználók védik a saját információikat
2. a felhasználók megoszthatják jogosultságaikat a többi felhasználóval
3. a felhasználók meghatározhatják a másokhoz rendelt hozzáférési típusát.
4. a felhasználók felelősek a biztonságpolitikáért.

A diszkrecionális hozzáférés-vezérlést használja sok PC-s és hálózati operációs rendszer, így a MS Windows NT és a MS Windows 2000 operációs rendszer, számos hagyományos UNIX és LINUX operációs rendszer hozzáférés-védelme is a diszkrecionális hozzáférés-vezérlésen alapul. A nem nagy biztonságú adatbázis-kezelők is többnyire a diszkrecionális hozzáférés-vezérlést használják.

A DAC nagy hibája, hogy nem tudja garantálni az adatok bizalmasságát! Ha valakinek olvasási joga van egy objektumhoz, akkor ő már másolhatja is ezeket az adatokat a *copy/paste* segítségével. Sőt – mint azt többek között William Stallings és Lawrie Brown a Computer Security: Principles and Practice című könyvükben [12] bemutatják – egy alany az O_1 objektumon meglévő olvasási jogát kihasználva, egy un. trójai program segítségével az O_1 objektumban lévő információt képes elolvás után az O_2 objektumba kiírni, és ehhez olvasási jogot adni egy olyan alany részére is, akinek ez kifejezetten tilos volt.

A fenti szituáció elkerülésére hozták létre *a kötelező hozzáférés-vezérlési modelleket* (röviden MAC[9]). E modellek közös tulajdonsága, hogy nem az objektumokkal végezhető műveletekre, hanem az azokban tárolt információ áramlására fektetik a hangsúlyt.

[8] Extended access matrix

[9] Mandatory Access Control

IRODALOM

[1] D. Elliot BELL, Leonard J. LAPADULA: *Secure Computer Systems: Mathematical Foundations and Model*, Mitre Corporation, 1975.

[2] Kenneth J. BIBA: *Integrity Considerations for Secure Computer Systems,* Mitre TR-3153, Mitre Corporation, Bedford, Massachusetts, 1977.

[3] David D. CLARK and David R. WILSON: *A comparison of Commercial and Military Computer Security Policies*, in Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (SP'87), pp. 184–193, Oakland, CA, USA, 1987.

[4] Krzysztof LIDERMAN: *Podstawowe Twierdzenie Bezpieczeństwa*, Biuletyn Instytutu Automatyki i Robotyki WAT, pp. 85-102, Warszawa, 2011.

[5] *Security within the North Atlantic Treaty Organisation (NATO)* – C-M(2002)49, NATO, 2002.

[6] BODLAKI Ákos, MUHA Lajos: *Az informatikai biztonság tanúsítási és minősítési eljárásrendjének terve*, tanulmány a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság részére, Budapest, 1997.

[7] *ISO 7498-2:1989: Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture*, International Organization for Standardization, 1989.

[8] G. Scott GRAHAM, Peter J. DENNING: *Protection – Principles and practice*, Joint Computer Conference 40, pp. 417-429, AFIPS Press, Montvale, N.J., USA, 1972.

[9] *Trusted Computer System Evaluation Criteria* – CSC-STD-001-83, Department of Defense, Washington D.C., 1983.

[10] BODLAKI Ákos, CSERNAY Andor, MÁTYÁS Péter, MUHA Lajos, PAPP György, VADÁSZ Dezső: *Informatikai rendszerek biztonsági követelményei*, Miniszterelnöki Hivatal, 1996.

[11] Déri Zoltán, Lobogós Katalin, Muha Lajos, Sneé Péter, Váncsa Julianna: *Informatikai Biztonság Irányítási Követelmények (IBIK)*, Miniszterelnöki Hivatal, Budapest, 2008.

[12] William STALLINGS, Lawrie BROWN: *Computer Security: Principles and Practice*, Prentice Hall Press Upper Saddle River, NJ, USA, 2007.