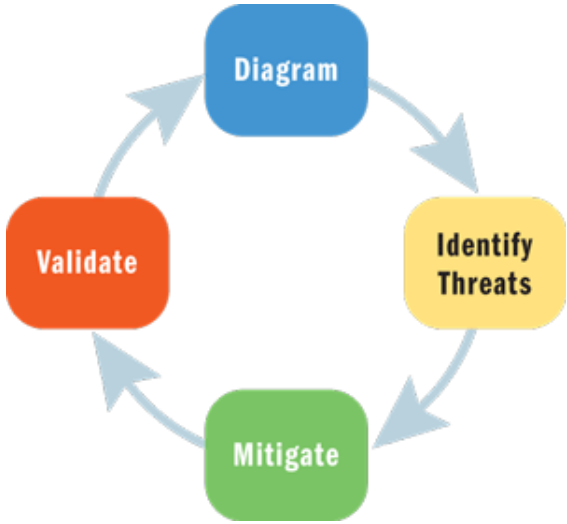
<RSA> Sigurnost informacijskih sistema </RSA>

<AES> predavanja </AES>

<CISSP> Modeliranje prijetnji</CISSP>



Summary

- Uvod
- Osnove modeliranja prijetnji
- Pristupi modeliranju prijetnji

Uvod

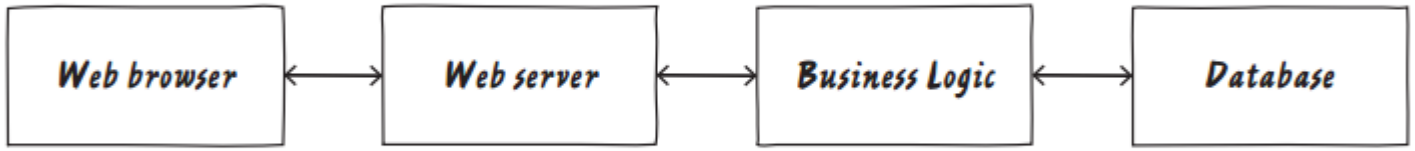
- Svako može naučiti kako se modelira prijetnja
  - Iz IT perspektive i više nego potreba danas
- Modeliranje prijetnji je proces primjena modela u cilju identifikovanja sigurnosnih problema
- Model osigurava apstrakciju bez viška tehničkih detalja
- Mnogo šira slika sistema bez da je isti i završen

Lekcija 1. Osnove modeliranja prijetnji

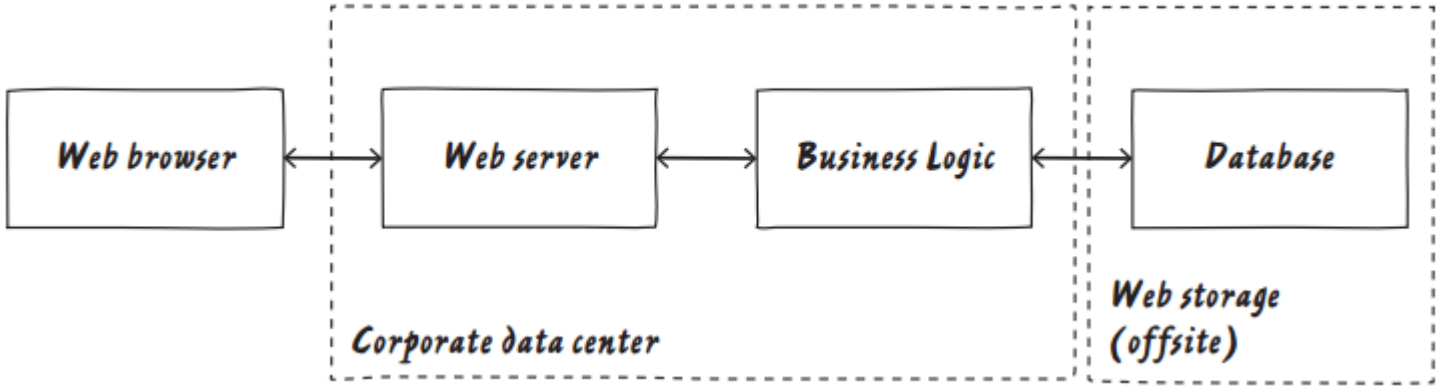
- Šta je to što pravimo?
- Gdje može biti problem?
- Šta možemo uraditi po pitanju problema?
- Validacija?

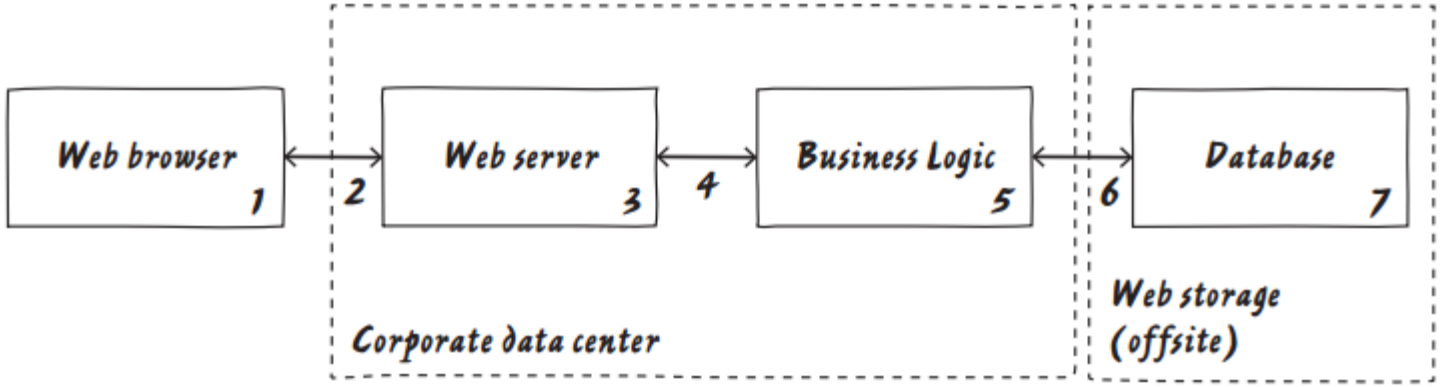
Šta je to što pravimo?

- Dijagrami su najbolji način komunikacije tokom razvoja bilo koje sistema
- Uzmimo za primjer web aplikacija koja se sastoji iz više komponenti
- Prvi korak je identifikacija granica povjerenja „trust boundries“
  - Granica je prostor gdje drugi ljudi ili procesu kontrolišu različite stvari



...šta je to što pravimo?





Gdje može biti problem?

- Primjeri:
  - Kako da znamo da browser koristi prava osoba?
  - Šta ako se modifikuju podaci u bazi?
  - Da li je transfer između zona siguran?
- Ove i slične prijetnje se mogu identifikovati pute STRIDE:
  - Spoofing
  - Tampering
  - Repudiation
  - Denial of Service
  - Information Disclousure
  - Elevation of Privilege
- Nikada nemojte ignorisati prijetnju ma koliko ona bila „mala“

Šta možemo uraditi po pitanju problema?

- Postoje četiri tipa akcija koje možemo uraditi:
  - Ublažavanje prijetnje (Mitigating)
  - Uklanjanje prijetnje (Eliminating)
  - Prebacivanje prijetnje (Transferring)
  - Prihvatanje rizika (Accepting)

Spoofing

THREAT TARGET	MITIGATION STRATEGY	MITIGATION TECHNIQUE
Spoofing a person	Identification and authentication (usernames and something you know/have/are)	Usernames, real names, or other identifiers: ❖ Passwords ❖ Tokens ❖ Biometrics Enrollment/maintenance/expiry
Spoofing a "file" on disk	Leverage the OS	❖ Full paths ❖ Checking ACLs ❖ Ensuring that pipes are created properly
	Cryptographic authenticators	Digital signatures or authenticators
Spoofing a network address	Cryptographic	❖ DNSSEC ❖ HTTPS/SSL ❖ IPsec
Spoofing a program in memory	Leverage the OS	Many modern operating systems have some form of application identifier that the OS will enforce.

Tampering

THREAT TARGET	MITIGATION STRATEGY	MITIGATION TECHNIQUE
Tampering with a file	Operating system	ACLs
	Cryptographic	❖ Digital Signatures ❖ Keyed MAC
Racing to create a file (tampering with the file system)	Using a directory that's protected from arbitrary user tampering	ACLs Using private directory structures (Randomizing your file names just makes it annoying to execute the attack.)
Tampering with a network packet	Cryptographic	❖ HTTPS/SSL ❖ IPsec
	Anti-pattern	Network isolation (See note on network isolation anti-pattern.)

Repudation

THREAT TARGET	MITIGATION STRATEGY	MITIGATION TECHNIQUE
No logs means you can't prove anything.	Log	Be sure to log all the security-relevant information.
Logs come under attack	Protect your logs.	❖ Send over the network. ❖ ACL
Logs as a channel for attack	Tightly specified logs	Documenting log design early in the development process

Information Disclousure

THREAT TARGET	MITIGATION STRATEGY	MITIGATION TECHNIQUE
Network monitoring	Encryption	❖ HTTPS/SSL ❖ IPsec
Directory or filename (for example `layoff-letters/adamshostack.docx`)	Leverage the OS.	ACLs
File contents	Leverage the OS.	ACLS
	Cryptography	File encryption such as PGP, disk encryption (FileVault, BitLocker)
API information disclosure	Design	Careful design control Consider pass by reference or value.

Denial of Service

THREAT TARGET	MITIGATION STRATEGY	MITIGATION TECHNIQUE
Network flooding	Look for exhaustible resources.	❖ Elastic resources ❖ Work to ensure attacker resource consumption is as high as or higher than yours.
		Network ACLS
Program resources	Careful design	Elastic resource management, proof of work
	Avoid multipliers.	Look for places where attackers can multiply CPU consumption on your end with minimal effort on their end: Do something to require work or enable distinguishing attackers, such as client does crypto first or login before large work factors (of course, that can't mean that logins are unencrypted).
System resources	Leverage the OS.	Use OS settings.

Elevation of Privilege

THREAT TARGET	MITIGATION STRATEGY	MITIGATION TECHNIQUE
Data/code confusion	Use tools and architectures that separate data and code.	❖ Prepared statements or stored procedures in SQL ❖ Clear separators with canonical forms ❖ Late validation that data is what the next function expects
Control flow/ memory corruption attacks	Use a type-safe language.	Writing code in a type-safe language protects against entire classes of attack.
	Leverage the OS for memory protection.	Most modern operating systems have memory-protection facilities.

Validacija

- Zadnji korak je validacija dijagrama
- Uključiti sve aktere u sistemu i odgovoriti na pitanja.
  - Da li je model kompletan?
  - Da li je mode precizan?
  - Da li su pokrivene sve sigurnosne odluke
- Ako je odgovor DA na sva pitanja može se krenuti na slijedeći korak
- Ako je odgovor NE ide se na ažuriranje dijagrama

Lekcija 2. Pristupi modeliranju prijetnji

- Šta je tvoj model prijetnji?
- Branstorming pristup
- Strukturni pristup

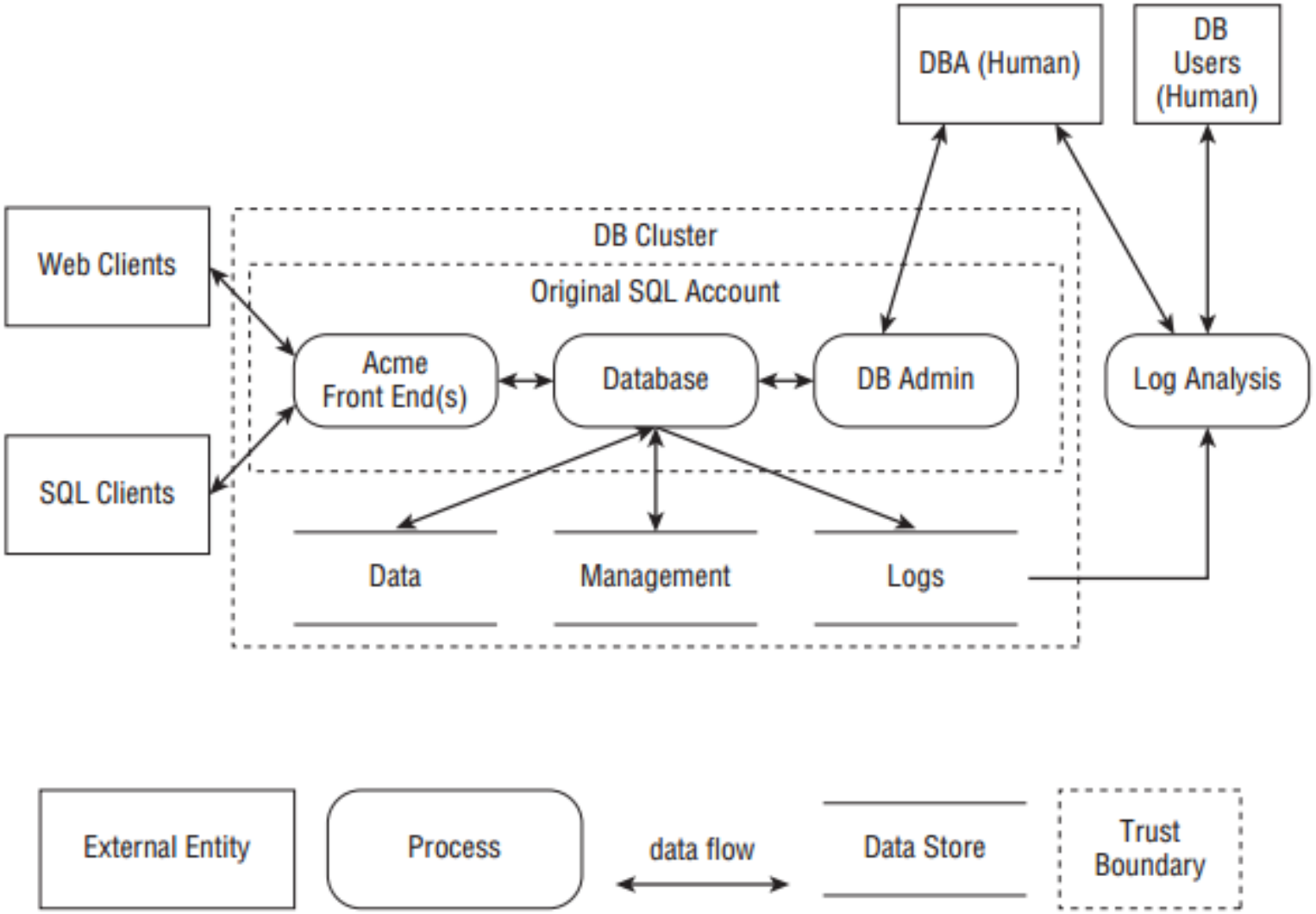
Šta je tvoj model prijetnji?

- Generalni primjeri mogu izgledao ovako:
  - Lopov koji želi ukrasti novac
  - Uposlenici kompanije koji imaju pristup osjetljivim dokumentima
- IT primjeri
  - Nesigurna mreža
  - Napadač koji želi da ukrade browser sesiju (cookie)
  - Napadač koji želi da čita i mijenja podatke
    - Bez tragova
- Neophodno je da imamo jasan odgovor na ovo pitanje
- U suprotnom može doći do nekonzistetnosti i gubitka resursa

Branstorming pristup

- Tradicionalni pristup prikupljanju ideja
- Postoje tri faze:
  - Generisanje ideja
    - Ograničiti ili totalno isključiti kritikovanje u ovoj fazi
  - Analiziranje
  - Odabir ideja
- Varijante
  - Analiza scenarija
  - Filmski pristup razvoja scenarija

Strukturni pristup



Pitanja