Sigurnosno inženjerstvo

Matematički fakultet, Beograd

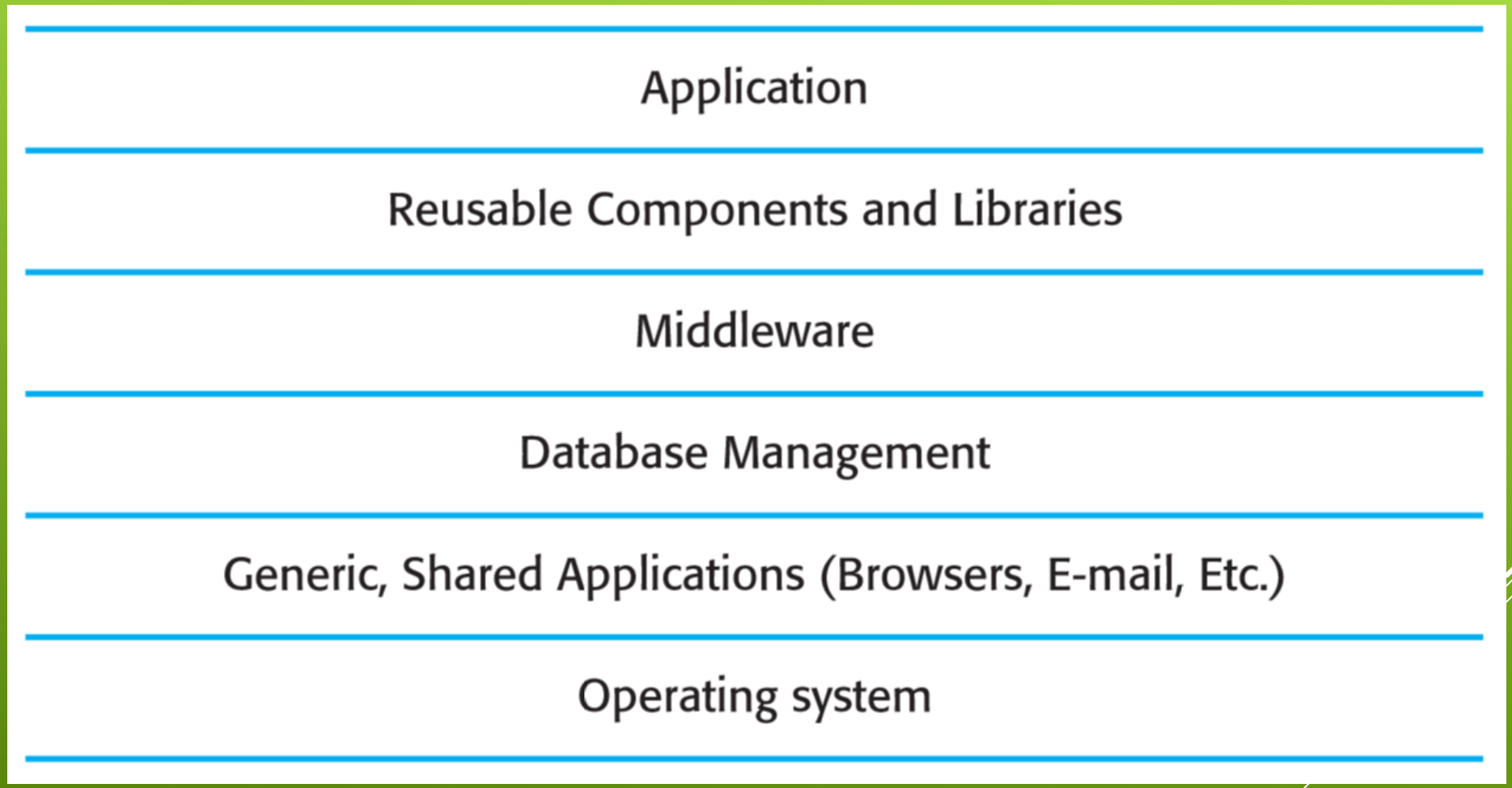
Seminarski rad iz predmeta Razvoj softvera 2

Filip Luković 1048/2013

ŠTA JE VAŽNO, A NAUČIĆEMO OVDE?

- **Shvatiti razliku između sigurnosti aplikacija i sigurnosti infrastrukture**
- **Naučiti kako procena rizika tokom životnog ciklusa i procena operativnog rizika utiču na dizajn sistema**
- **Biti svestan arhitektura i smernica za razvoj sigurnih aplikacija**
- **Razumeti pojam opstanka sistema i zašto je analiza opstanka bitna za složene softverske sisteme**

GDE SIGURNOST MOŽE BITI NARUŠENA?



SIGURNOST APLIKACIJE NASPRAM INFRASTRUKTURE

- **Sigurnost aplikacije** problem koji rešavaju softverski inženjeri tako da sistem koji razvijaju treba da odoli napadima

- **Sigurnost infrastrukture** je problem koji rešavaju menadžeri sistema. Potrebno je da podese sve komponente infrastrukture tako da odole napadima. Takođe oni moraju i popraviti sve bezbednosne rupe koje dolaze na videlo tokom rada sistema

UPRAVLJANJE BEZBEDNOŠĆU SISTEMA OBUHVATA

- **Upravljanje korisnicima i dozvolama**
  - **Dodavanje i uklanjanje korisnika iz sistema, rad sa dozvolama za odgovarajuće korisnike**
- **Instaliranje i konfigurisanje softvera**
  - **Instalacija i pravilno konfigurisanje sistema pomažu u smanjivanju ranjivosti sistema**
- **Praćenje, detektovanje i oporavak napada**
  - **Praćenje nedozvoljenih ulazaka u sistem, pravljenje strategije za sprečavanje napada, za oporavak i pravljenje rezernih kopija sistema ili podataka**

UPRAVLJANJE BEZBEDNSNIM RIZICIMA

- **Procena mogućih gubitaka koje mogu proizvesti napadi na sistem i balansiranje ovih gubitaka u odnosu na troškove razvijanja bezbednosnih mehanizama za suzbijanje istih**

- **Softverski inženjeri ne bi trebalo da odlučuju o ovome, već je to posao menadžmenta i politike firme**

- **Primer**

  Ugradnja čipova na kreditne kartice umesto magnetne trake je poboljšala sigurnost i otežala kopiranje

UPRAVLJANJE BEZBEDNSNIM RIZICIMA OBUHVATA

1. Preliminarnu procenu rizika

Ne donose se odluke o arhitekturi i sistemu, već o tome da li adekvatan nivo sigurnosti može biti postignut po razumnoj ceni

2. Procenu rizika tokom životnog ciklusa

Odvija se tokom razvoja sistema i određen je od strane tehničkog dizajna sistema i implementacionih odluka

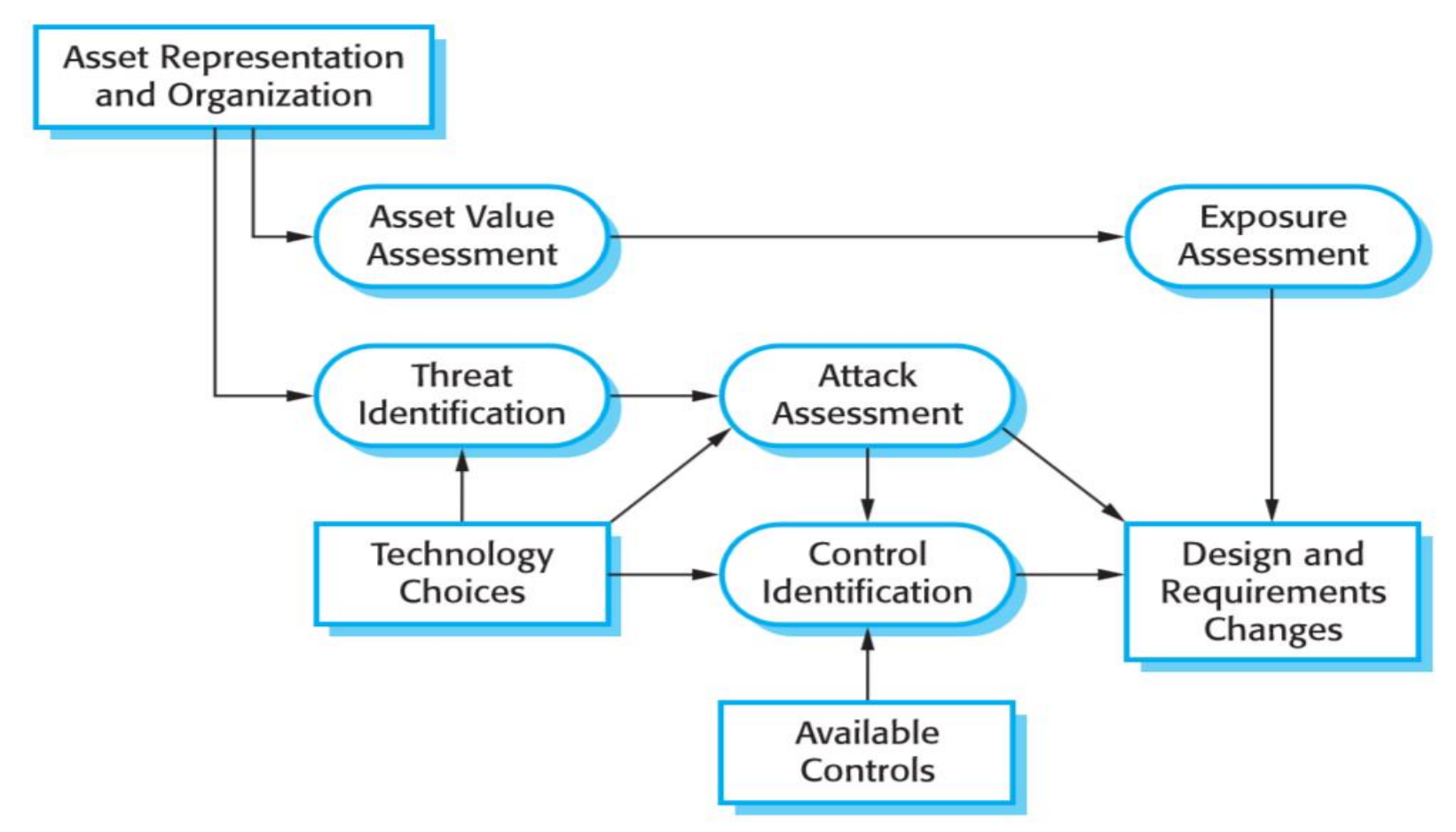
3. Operativna procena rizika

Nakon početka korišćenja sistema. Može da dođe do promene zahteva i načina korišćenja

SLUČAJEVI ZLOUPOTREBE

- **Važno je identifikovati slučajeve zloupotrebe sistema, tako što ćemo napraviti njihov skup**
- **Njihova analiza se koristi i kod preliminarne procene rizika, ali i kod procene rizika tokom životnog ciklusa**
- **Tipovi slučajeva zloupotrebe su kada**
  1. **Napadač dobije pristup nekim sredstvima**
  2. **Napadač učini deo sistema nedostupnim**
  3. **Napadač podmeće(menja) deo sistema**
  4. **Unose se lažne informacije u sistem**

SLUČAJEVI ZLOUPOTREBE



PROCENA RIZIKA TOKOM ŽIVOTNOG CIKLUSA

- **Kako bi trebalo da sigurnosne procedure budu implementirane**
- **Koji delovi sistema bi trebalo da budu zaštićeni**
- **Koje načine pristupa treba koristiti da se obezbedi ta zaštita**
- **Potrebno je znati nešto više detalja o tome šta treba zaštititi i o ranjivostima sistema**

PROCENA RIZIKA TOKOM ŽIVOTNOG CIKLUSA

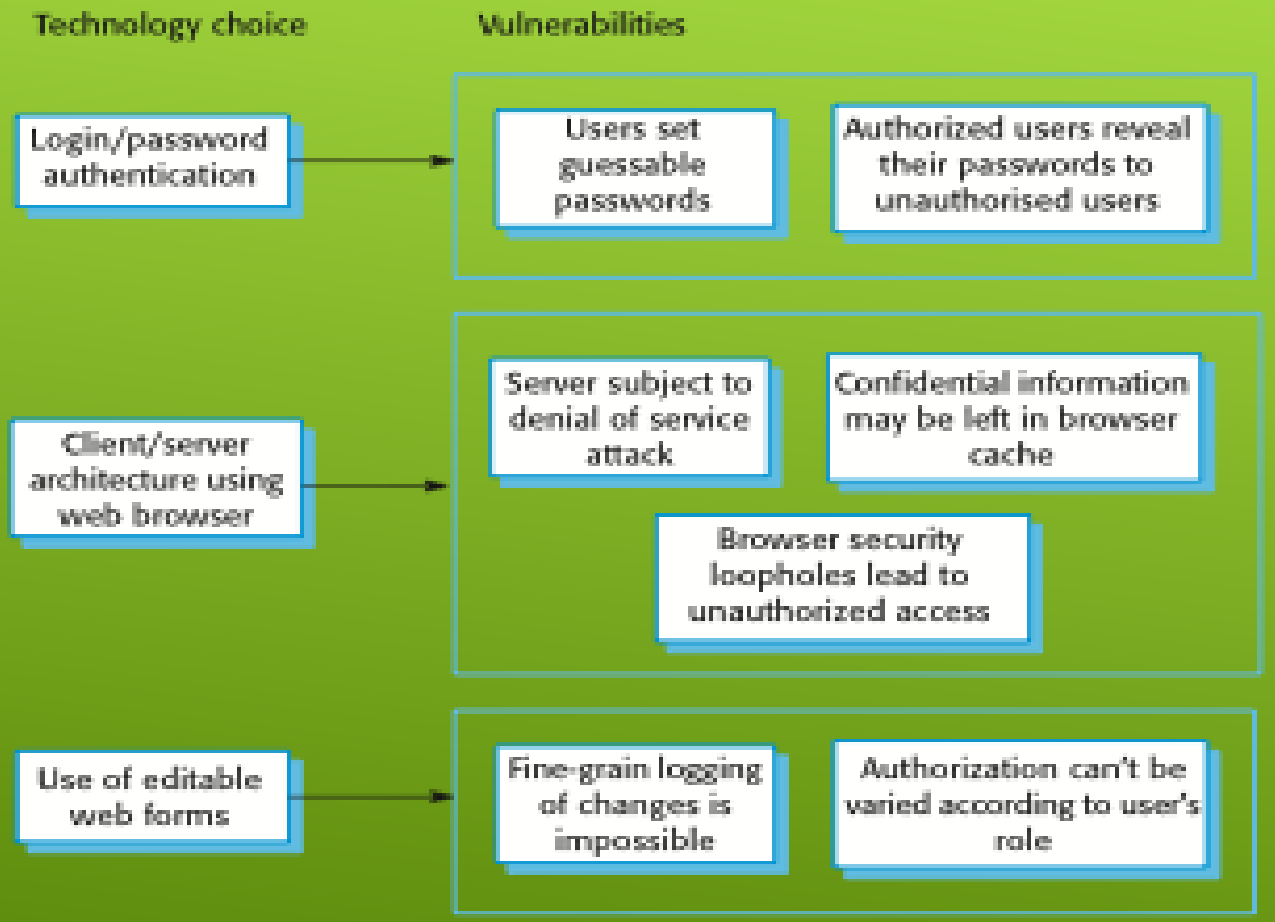
- **Primer 1**

  Može se doneti odluka da razdvojimo podatke o pacijentu i podatke o primljenim terapijama, koje pokazuju na pacijenta. Ukoliko je ključ ka pacijentovim podacima zaštićen, terapije su mnogo manje osetljivi podaci, jer se ne zna na kog pacijenta se odnose.

- **Primer 2**

  Tokom jedne sesije se podaci o korisniku kopiraju na hard disk, kako bi se omogućio rad ukoliko nestane internet konekcije. Ti podaci su osetljivi, jer laptop kao fizički uređaj može biti ukraden.

IZBOR TEHNOLOGIJA (SLABE TAČKE)



NEKI ZAHTEVI KOJI POSPEŠUJU SIGURNOST

- **Koristiti proveru šifri i pokretati je automatski svaki dan, a loše šifre prijaviti administratoru sistema**
- **Pristup sistemu je moguć jedino preko računara koji je odobren i registrovan od strane administratora sistema**
- **Klijentski računari imaju jedan instaliran pretraživač koji je odobren od strane administratora sistema**

OPERATIVNA PROCENA RIZIKA

- **Može doći do novih rizika zbog menjanja zahteva, infrastrukture sistema ili menjanja okruženja**
- **Takođe stari rizici koji su postojali tokom životnog ciklusa su aktivni**

BEZBEDNOSNI DIZAJN

- **Dizajn arhitekture**
  - Kako arhitektura utiče na bezbednost?
- **Dobra praksa**
  - Koje su smernice kojima se treba upravljati?
- **Upotrebni dizajn**
  - Sta treba da podržava sistem kako bi se izbegle ranjivosti

  Nakon puštanja u upotrebu?

DIZAJN ARHITEKTURE

- **Dva važne stavke na koje treba obratiti pažnju**
  - **Zaštita**

    Kako sistem treba da bude organizovan tako da kritični delovi budu zaštićeni?
  - **Raspodela**

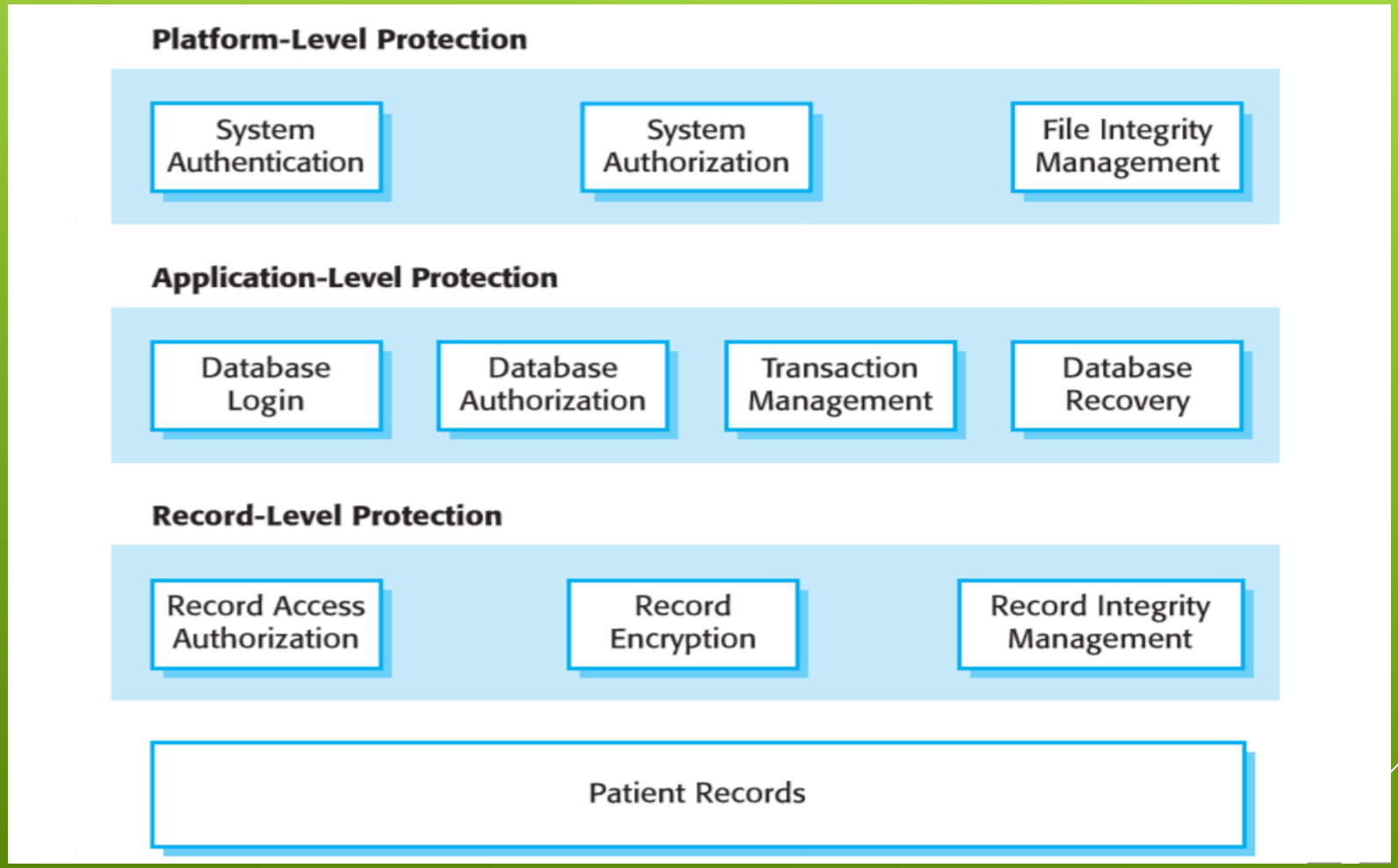
    Kako sistem treba da bude raspoređen tako da se minimizuje procenat uspešnih napada?

- **Nastaje konflikt**
  - **Zaštićene aplikacije su sporije i imaju lošije performanse**
  - **Teže je zaštititi delove koji su raspoređeni na različitim mestima**

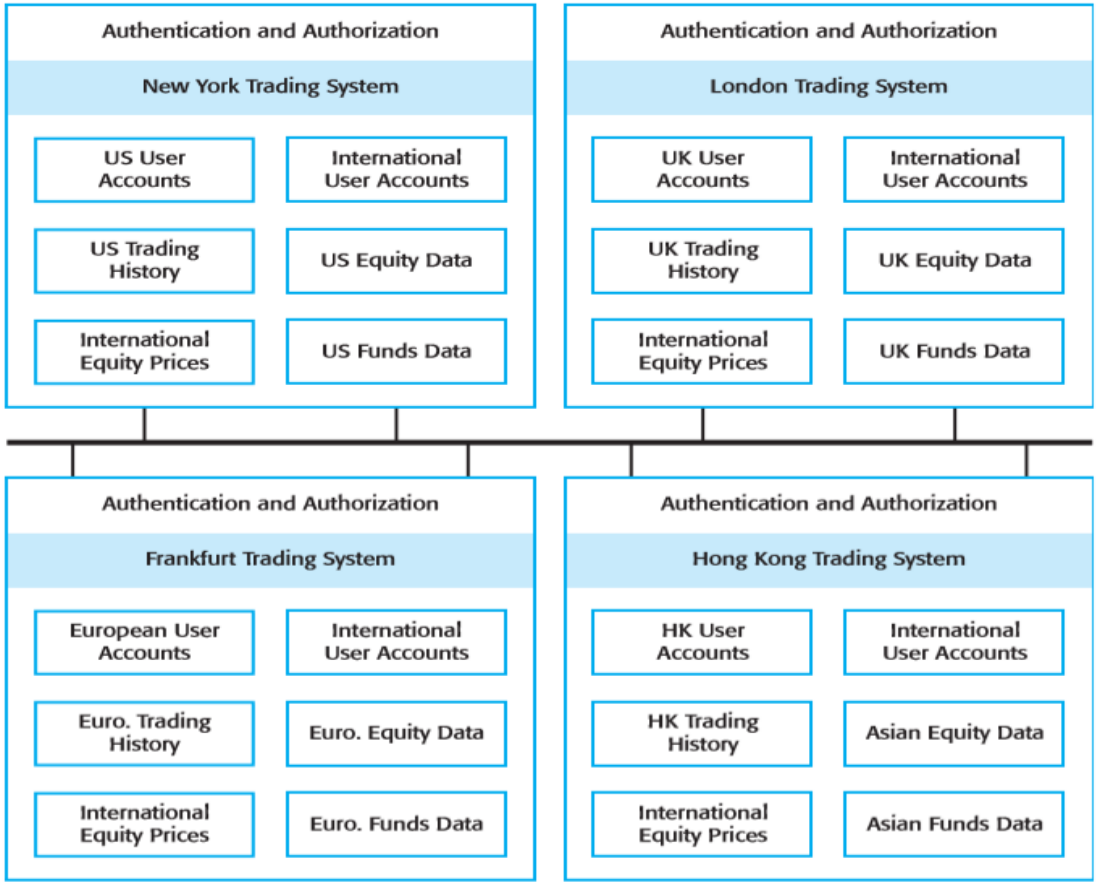
ZAŠTITA

- **Zaštita na nivou platforme**
  - Zavisno od platforme na kojoj se pokreće aplikacija
- **Zaštita na nivou aplikacije**
  - Mehanizam zaštite koji je integrisan u aplikaciju
- **Zaštita na nivou zapisa**
  - Zaštita pristupu pojedinačnim podacima

ZAŠTITA


Platform-Level Protection
System Authentication
System Authorization
File Integrity Management
Application-Level Protection
Database Login
Database Authorization
Transaction Management
Database Recovery
Record-Level Protection
Record Access Authorization
Record Encryption
Record Integrity Management
Patient Records

RASPODELA


Authentication and Authorization
New York Trading System
US User Accounts
International User Accounts
US Trading History
US Equity Data
International Equity Prices
US Funds Data
Authentication and Authorization
London Trading System
UK User Accounts
International User Accounts
UK Trading History
UK Equity Data
International Equity Prices
UK Funds Data
Authentication and Authorization
Frankfurt Trading System
European User Accounts
International User Accounts
Euro. Trading History
Euro. Equity Data
International Equity Prices
Euro. Funds Data
Authentication and Authorization
Hong Kong Trading System
HK User Accounts
International User Accounts
HK Trading History
Asian Equity Data
International Equity Prices
Asian Funds Data

DOBRE SMERNICE

- **Odluka o eksplicitnoj bezbednosnoj politici**
  - Definisati bezbednosnu politiku koja treba da se primenjuje na svim sistemima
- **Izbegavati jednu tačku neuspeha**
  - Potrebno je više od jednog neuspeha u bezbednosnim procedurama da se dobije sigurnosni propust
- **Pad sistema**
  - Čak i pri padu sistema, osetljivim informacijama se ne može pristupiti od strane neovlašćenih lica
- **Balansirati između sigurnosti i upotrebljivosti**
  - Izbegavati sigurnosne procedure koje otežavaju rad sistema. Nekada morate prihvatiti i slabiju sigurnost zbog performansi

DOBRE SMERNICE

- **Logovanje korisničkih akcija**
  - Održavanje evidencije radnji koje sprovode korisnici može pomoći pri analizi ko je šta uradio
- **Redudentnost i raznolikost smanjuju rizik**
  - Pravljenje više kopija podataka i korišćenje raznih infrastruktura smanjuju rizik od nauspeha
- **Validacija svih ulaznih podataka**
  - Proveravati da li su svi ulazni podaci unutar domena
- **Deljenje sistema**
  - Podeliti različite delove sistema u različite delove, tako da jedan korisnik ima samo pristup onome što mu treba i što sme da koristi

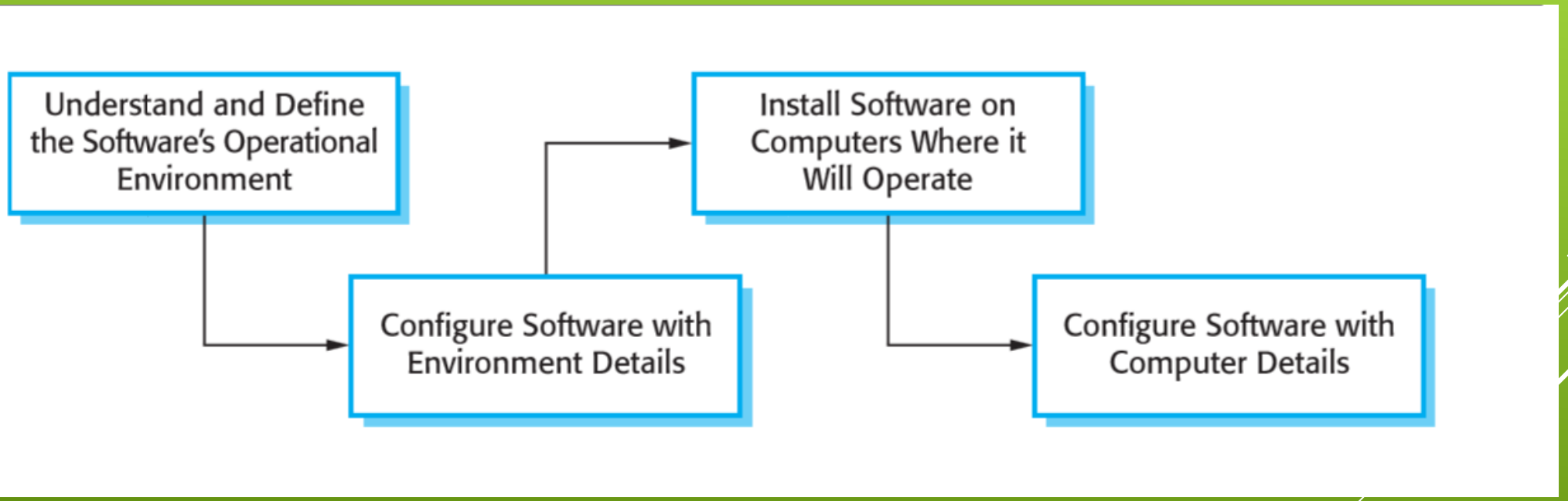
DOBRE SMERNICE

- **Upotrebni dizajn**
  - **Napraviti dizajn tako da se izbegnu problemi u primeni**
- **Dizajn za oporavak**
  - **Napraviti dizajn tako da se sistem lako oporavlja od napada**

UPOTREBNI DIZAJN

- **Podrazumeva konfigurisanje softvera za rad u svojoj radnoj sredini, instaliranje sistema i konfigurisanje u zavisnosti od platforme.**
- **Kao rezultat konfiguracionih grešaka mogu nastati ranjivosti sistema**
- **Ubacivanjem podrške puštanja u upotrebu u sistem smanjuje se verovatnoća od nastajanja ranjivosti**

PUŠTANJE U UPOTREBU



RANJIVOSTI PRI PUŠTANJU U UPOTREBU

- **Podrazumevana podešavanja**
  - **Podrazumevane postavke se mogu lako saznati, pa ih ne treba koristiti. Prvom prilikom treba promeniti podrazumevane postavke i tako smanjiti verovatnoću da napadač zna podatke**
- **Razvoj nije važniji od puštanja u upotrebu**
  - **Podešavanja i postavke koji su korišćeni za razvoj i debagovanje treba da budu isključeni nakon puštanja u upotrebu**

PODRŠKA PRI PUŠTANJU U UPOTREBU

- **Uključite podršku za pregled i analizu konfiguracije**
  - **Administrator sistema treba da vidi celu konfiguraciju, a samim tim i uoči greške**
- **Smanjiti podrazumevane privilegije i time smanjiti moguću štetu**
  - **Svesti privilegije administratora na minimum, ako neko dobije pristup admin nalogu nemaju direktan pristup funkcijama sistema**
- **Lokalizovati podešavanja**
  - **Sva podešavanja koja su vezana za jedan deo sistema treba raditi odjednom, da seneki deo ne bi zaboravio**
- **Obezbediti jednostavne načine za popravku ranjivosti**
  - **Kada se otkrije ranjivost potreban je lak način da se ona ukloni i suzbije**

OPSTANAK SISTEMA

- **Sposobnost sistema da obezbedi osnovne usluge dok je pod napadom ili nakon oštećenja dela sistema**
- **Analiza i dizajn opstanka sistema trebalo bi da budu deo procesa sigurnosnog inženjeringa**

OPSTANAK SISTEMA

- **Važnost opstanka sistema**
  - **<u>Naša ekonomija i životi se oslanjaju na računare i računarske sisteme</u>**
    - **Infrastruktura**
    - **Zdravstvo**
    - **Državna uprava**
  - **<u>Gubitci prilikom pada poslovnih sistema su brzi i veliki</u>**
    - **Aerodromski sistemi**
    - **Sistemi za plaćanje**
    - **Elektronske trgovine**

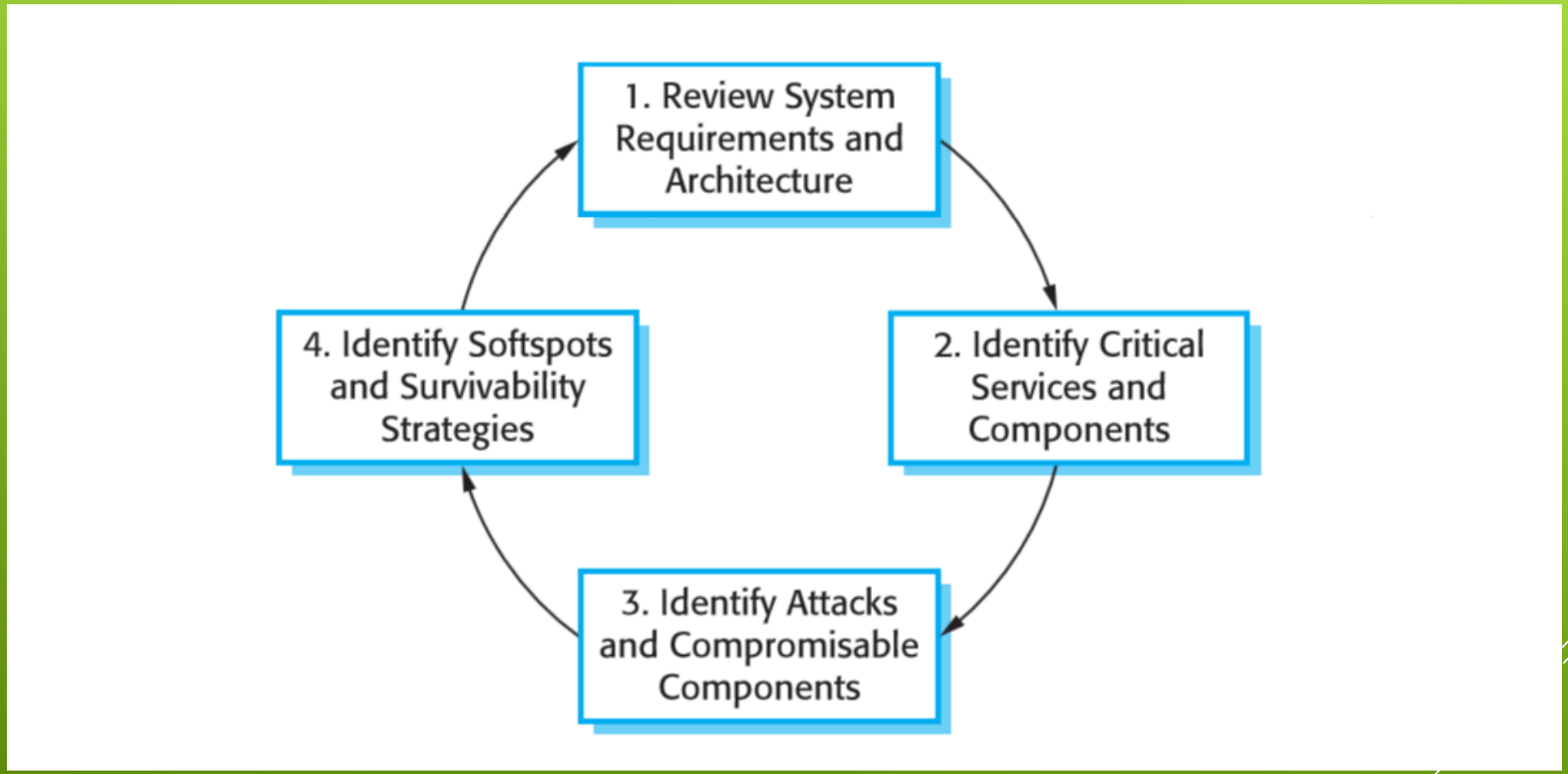
DOSTUPNOST USLUGA

- **Koje usluge sitema su najkritičnije za biznis?**
- **Kako ti servisi mogu biti kompromitovani?**
- **Koji je minimalni kvalitet servisa koji mora biti podržan?**
- **Kako ovi servisi mogu biti zaštićeni?**
- **Koliko vremena je potrebno za oporavak u slučaju da servis postane nedostupan?**

STRATEGIJE OPSTANKA

- **Otpornost**
  - Treba izgraditi sistem tako da bude u mogućnosti da se odupre napadima
- **Prepoznavanje**
  - Sistem treba da sadrži detekciju napada i procenu štete koja može nastati
- **Oporavak**
  - Izgradnja dela sistema za pružanje usluga dok je sistem pod napadom

STRATEGIJE OPSTANKA



KLJUČNE AKTIVNOSTI KOD OPSTANKA

- **Razumevanje sistema**
  - Pregledati ciljeve, zahteve i arhitekturu sistema
- **Identifikacija kritičnih resursa**
  - Identifikovati usluge koje moraju uvek biti aktivne
- **Simulacija napada**
  - Osmisliti kritični scenario i testirati ga, da se vidi kako sistem tada funkcioniše
- **Analiza preživljavanja**
  - Identifikovati strategije koje se mogu primeniti

JEDAN OD NAJVEĆIH NAPADA

- **Tokom hladnog rata, CIA je pronašla način da onesposobi sibirske gasovode. Oni su umesto bombi ili raketa iskoristili upad u kompjuterski sistem i izazvali toliko veliki haos da se vatra videla i iz svemira.**

KRAJ

Pitanja? Komentari?