Sigurnost računalnih sustava

Ranjivosti

doc. dr. sc. Ante Đerek
doc. dr. sc. Stjepan Groš
izv. prof. dr. sc. Miljenko Mikuc
izv. prof. dr. sc. Marin Vuković

Podsjetimo se…

- Da bi se desio incident (narušila sigurnost) moraju postojati dva preduvjeta: **ranjivost** i prijenja
- **Ranjivost** (engl. vulnerability) je pogreška ili slabost u dizajnu sustava, implementaciji, upotrebi ili upravljanju koja se može iskoristiti za narušavanje sigurnosti sustava ili informacije.
- Ranjivosti su ključni element sigurnosti i zbog toga im posvećujemo značajnu pažnju na ovom predmetu

Kada i gdje nastaju ranjivosti?

- Ranjivost je moguće uvesti u bilo kojoj fazi životnog ciklusa sustava
  - Mi ćemo se baviti najviše programskim sustavima, ali mogu biti i drugi sustavi
  - Životni ciklus programskih sustava (engl. software development life cycle, SDLC)
- Životni ciklus programskih sustava sastoji se od sljedećih faza
  - (1) dizajn, (2) implementacija, (3) uvođenje u upotrebu, upravljanje, održavanje, (4) uklanjanje

Koraci u rukovanju ranjivostima

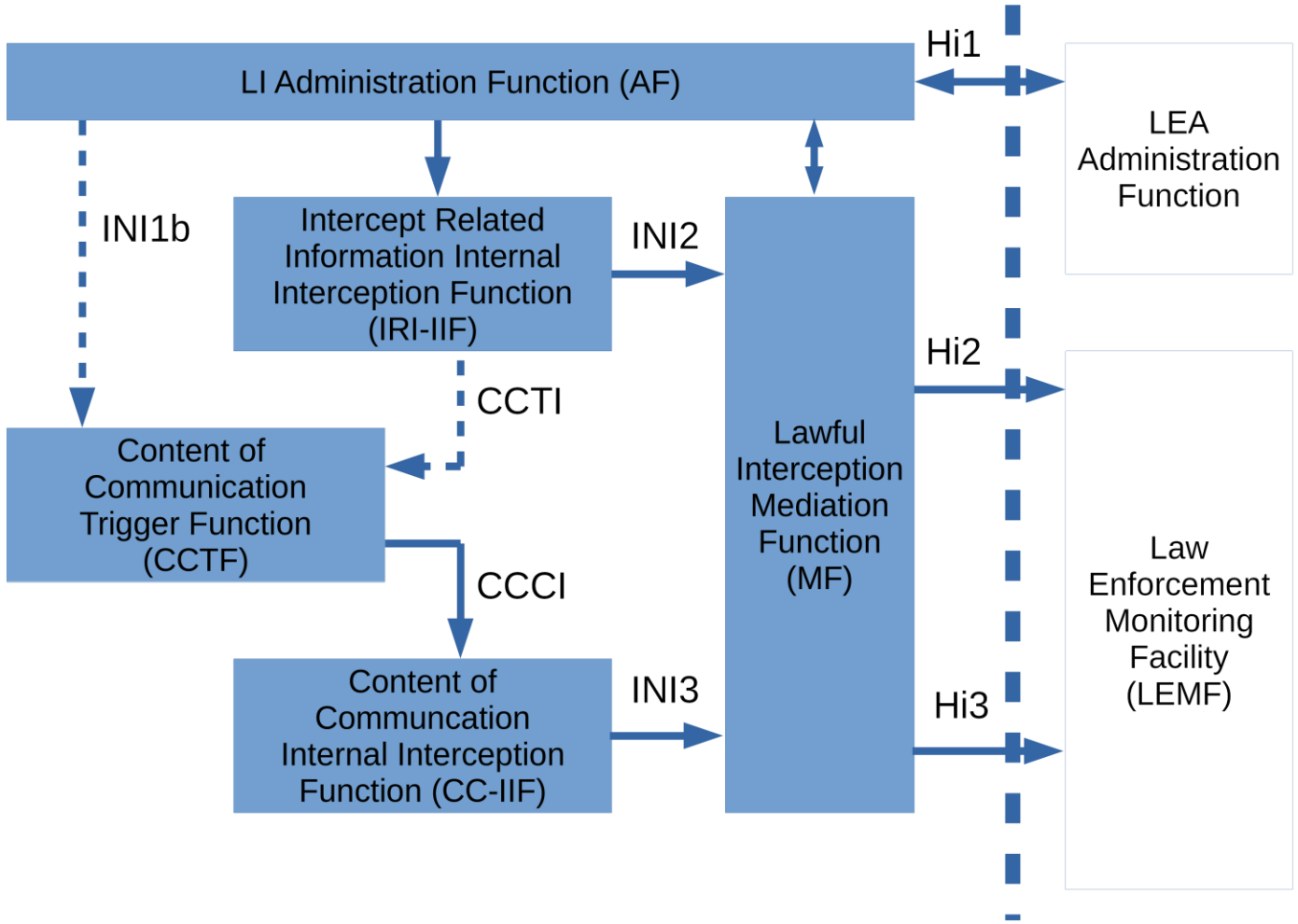
- U svakoj fazi životnog ciklusa koraci koje možemo provoditi kako bi izbjegli ranjivosti
  - Prvo nastojimo ne uvoditi ranjivosti
  - Zatim ih želimo što prije otkriti
  - Kada se otkriju treba ih ispraviti na odgovarajući način
  - Kada su otkrivene treba ih što prije ukloniti u produkcijskim sustavima
    - Ako je sustav već u produkciji

Ranjivosti u dizajnu sustava

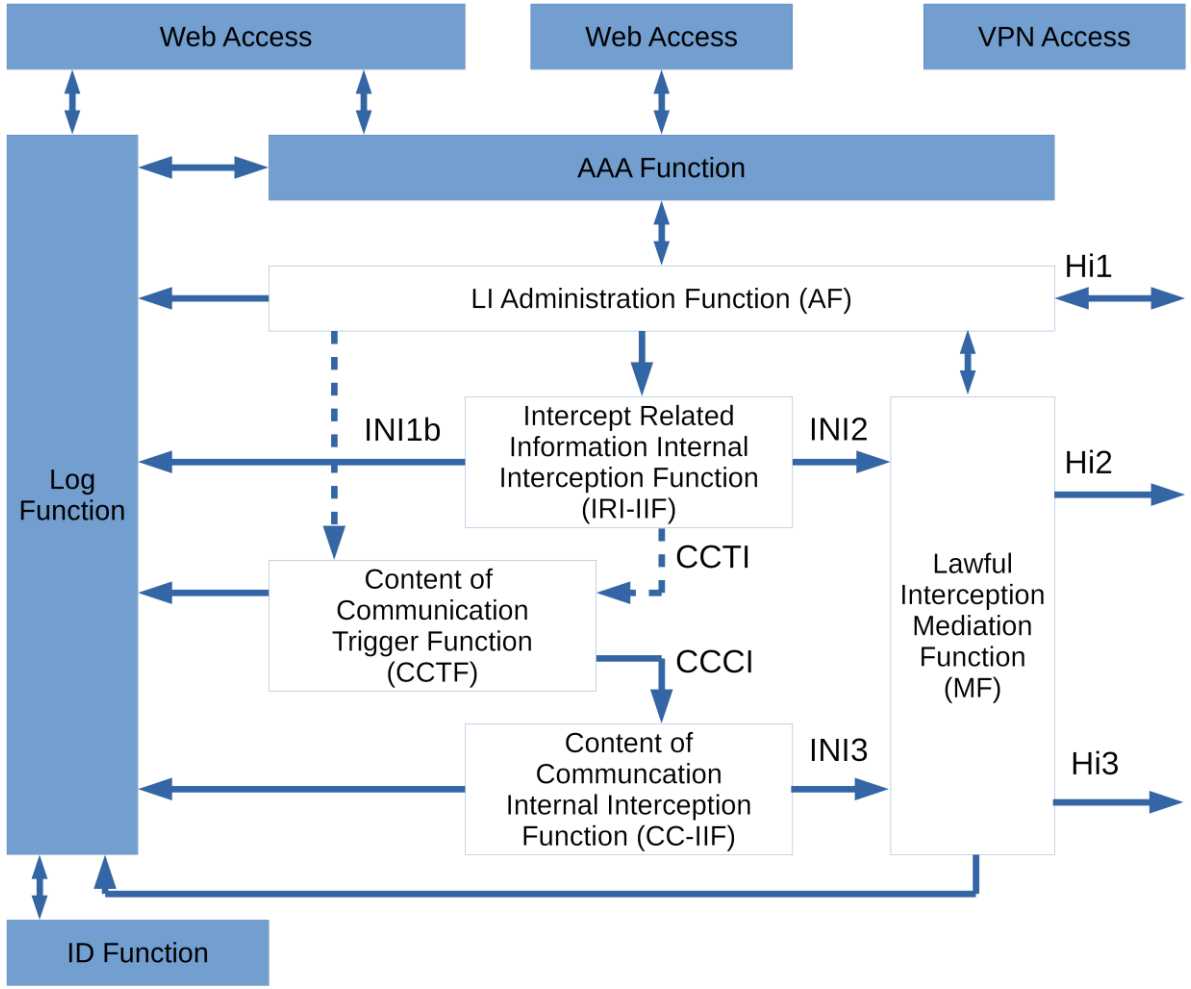
Ranjivosti

- Prva faza izgradnje bilo kojeg sustava je **dizajn**
  - Tijekom dizajna definiraju se ključne karakteristike sustava
  - Najčešće se specificira kroz **arhitekturu sustava** i **načela izgradnje sustava**
- Pogreške, odnosno slabosti, nastaju ako se ne predvidi ugrađivanje odgovarajućih sigurnosnih zaštitnih mehanizama
  - Nedostatna ili neodgovarajuća autentifikacija i autorizacija, bilježenje sistemskih i operativnih zapisa, …

Primjer arhitekture (1)



Primjer arhitekture (2)



Sprečavanje ranjivosti

- Za sprečavanje je potrebno od inicijalnog trenutka voditi računa o sigurnosti
- Temeljni mehanizam za ispravno dizajniranje sustava je **modeliranje prijetnji** (engl. Threat modeling)
  - Zadaća modeliranja prijetnji je utvrditi što prijeti sustavu i od čega se štitimo
  - Na temelju modela prijetnji definiramo sigurnosne zahtjeve
- Ispravljanje ranjivosti je sve teže kako se sve više odmiče u implementaciju i upotrebu sustava
  - U određenim situacijama više nije moguće ispraviti ranjivost te se moraju smišljati zaobilazne metode – a to često ne završi dobro

Otkrivanje ranjivosti

- Provođenjem analize sustava
  - Analizu moraju obaviti osobe sa dovoljnom razinom znanja i iskustva
- Manifestacija ranjivosti u kasnijim fazama životnog ciklusa
  - Tijekom upotrebe sustava počnu se pojavljivati zahtjevi koje se ne može ispuniti
  - Incidenti čijom analizom se utvrdi da je do incidenta došlo zbog nedostataka u dizajnu sustava

Ranjivosti u implementaciji

Ranjivosti

- Ranjivosti su podskup programskih pogrešaka (bugs)
  - nije svaka programska pogreška istovremeno i ranjivost, ali svaka ranjivost je programska pogreška
- Posebna kategorija su **ranjivosti nultog dana** (engl. zero day vulnerability)
  - Otkrivene ranjivosti za koje ne zna nitko osim onoga tko ih je otkrio

Sprečavanje ranjivosti (1)

- Edukacija programera
  - Trebaju biti svjesni da je sigurnost bitna
  - Poštivanje uputa za pisanje sigurnog koda
    - Problem je što tih uputa ima previše, a rokovi su često kratki!
- Testiranje koda
  - S obzirom da su ranjivosti pogreške u kodu
- Revizija koda
  - Barem jedan drugi programer pregledava i komentira kod prije pohrane u repozitorij
  - Moguće postojanje zasebnog odjela ili grupe ljudi čija zadaća je praćenje sigurnosti

Primjeri resursa za sigurno kodiranje

- SEI CERT Coding Standards
  - https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards
  - Za programske jezike Java, C++, C te platformu Android
- Microsoft Secure coding guidelines
  - https://docs.microsoft.com/en-us/dotnet/standard/security/secure-coding-guidelines
  - Razvoj sigurne programske podrške na platformi .Net
- Common Weakness Enumeration
  - https://cwe.mitre.org
  - Popis tipova slabosti u programskim i sklopovskim sustavima

Sprečavanje ranjivosti (2)

- Statička analiza koda
  - Korištenje alata koji analiziraju izvorni kod
- Dinamička analiza koda
  - Kod, ili njegovi dijelovi, se izvršavaju te se tijekom izvršavanja predaju različiti neispravni ulazi u potrazi za pogreškom
  - Neizrazito testiranje (engl. Fuzzy testing) vrlo popularno – specifičnost je u načinu generiranja ispitnih uzoraka
- Formalne metode
- Dobar popis alata na Wikipediji
  - https://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis

Liste najčešćih ranjivosti

- Postoji nekoliko lista najčešćih ranjivosti, dvije su najpoznatije OWASP Top 10 i CWE Top 25
- OWASP Top 10
  - The Open Web Application Security Project (OWASP) organizacija nudi mnoštvo informacija o sigurnosti
  - OWASP naglasak stavlja na Web aplikacije te su ranjivosti specifične za Web aplikacije
  - Zadnja verzija iz 2017 godine
- CWE Top 25
  - Common Weaknesses Enumeration – aktivnost organizacije MITRE da se katalogiziraju i kategoriziraju slabosti u programskoj podršci

Ranjivosti u upotrebi

Ranjivosti

- Tijekom upotrebe ranjivosti mogu nastati zbog
  - pogrešaka proizvođača
  - neispravnog korištenja sustava
- Pogreške proizvođača tek u ovoj fazi postaju vidljive
- Neispravno korištenje
  - Primjerice, nije uključena autentifikacija iako postoji mogućnost i zbog toga bilo tko može pristupiti zaštićenom resursu
  - Prilikom postavljanja lozinki nije uključen sustav koji sprečava korištenje trivijalnih lozinke ih je moguće pogađati

Sprečavanje ranjivosti

- Temeljni način otkrivanja pogrešaka je pregledavanje sustava
  - Ručno pregledavanje i testiranje koje provode osobe s dovoljno znanja i vještine
  - Pregledavanje korištenjem alata
- Sprečavanje pogrešaka i slabosti u upotrebi
  - Jako teško izvedivo bez ljudi koji jako dobro poznaju sustav koji koriste
  - Korištenje alata koji provjeravaju konfiguracije te upozoravaju na potencijalne manjkavosti
    - Potencijalno isti alati kao iz za otkrivanje pogrešaka

Otkrivanje ranjivosti

- Ručno i automatizirano otkrivanje ranjivosti nisu međusobno isključivi
  - Svaki ima prednosti, ali i mane u odnosu na drugog
- Ručno otkrivanje ranjivosti (pentest)
  - Može otkriti i nove, do sada nepoznate, ranjivosti
  - Potencijalno mala količina lažno pozitivnih i lažno negativnih nalaza
  - Ne skalira i jako ovisi o znanju i vještinama osobe koja provodi analizu
- Automatizirano otkrivanje ranjivosti (vuln. scanning)
  - Potencijalno puno lažno pozitivnih i lažno negativnih
  - Može otkriti samo ono što je algoritamski „pronalazivo” i isprogramirano

Implementacijske ranjivosti u upotrebi (1)

- Kada se ranjivost otkrije potencijalno su ranjive sve implementacije u upotrebi
  - Obzirom da se radi o implementaciji korisnik ne može ništa napraviti!
- Dominantan način ispravljanja je korištenjem zakrpa (engl. patch)
  - Proizvođač programske podrške ispravi ranjivost u kodu i podiže minornu verziju
  - Datoteke koje su promijenjene u odnosu na prethodnu (minornu) verziju se skupljaju u zakrpu (patch)
  - Sustavom nadogradnje (potencijalno automatske) zakrpa se distribuira svim korisnicima

Implementacijske ranjivosti u upotrebi (2)

- Proizvođači programske podrške također izdaju upozorenja
  - Primjeri
    - https://support.microsoft.com/en-us/topic/microsoft-security-advisory-insecure-library-loading-could-allow-remote-code-execution-486ea436-2d47-27e5-6cb9-26ab7230c704
    - https://access.redhat.com/errata/RHSA-2021:0922
- Ako zakrpa nije odmah dostupna proizvođači daju privremene mjere zaštite (engl. workaround)
  - Posebno ako se radi o kritičnim ranjivostima
  - Primjerice, savjetuju da se neki (ranjivi) modul isključi, blokira pristup s mreže ako se radi ranjivosti dohvatljivoj s mreže, itd.

Način iskorištavanja ranjivosti

- Metoda, kod ili nekakav drugi artefakt koji iskorištava ranjivost (engl. exploit)
- Baza javno dostupnih exploita
  - https://www.exploit-db.com/
- Postojanje javno objavljenog exploita čini ranjivost značajno opasnijom
  - Napisati exploit nije jednostavno
- Pojam *shellcoda*
  - Kratki kod koji iskorištava ranjivost i potom pokreće nešto drugo

Baza ranjivosti CVE

- Common Vulnerability Enumeration (CVE) je često korišten način označavanja i katalogiziranja ranjivosti
  - Jedinstveni identifikator neovisan o proizvođaču programske podrške
  - Sustav definirala organizacija MITRE (dosta uključena u sigurnost!)
  - Oznake su oblika *CVE-yyyy-nnnnnn*
  - Baza javno dostupna na Internetu https://cve.mitre.org/cve/
  - Često se koristi i alternativna lokacija s nekim dodatnim informacijama https://nvd.nist.gov/

Primjer CVE zapisa

CVE-ID	
CVE-2021-27078	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-26412, CVE-2021-26854, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27078 • URL:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27078	
Assigning CNA	
Microsoft Corporation	
Date Record Created	
20210210	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20210210)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	
This is a record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.	
SEARCH CVE USING KEYWORDS: Submit You can also search by reference using the CVE Reference Maps.	
For More Information: CVE Request Web Form (select "Other" from dropdown)	

Rangiranje ranjivosti

- U velikim sustavima broj ranjivosti može biti značajan
  - Ispravljanje ranjivosti može biti vrlo zahtjevno
- Potrebno je imati procjenu koliko je pojedina ranjivost značajna
  - Ta informacija uz kontekst (potencijalna šteta, mjesto gdje je ranjivost) omogućava procjenu koliko je svaka ranjivost „ozbiljna” – procjena rizika(!)
- Proizvođači u svojim upozorenjima koriste različite skale za ocjenu
  - Teška usporedba ranjivosti različitih proizvođača

Metoda izračuna ozbiljnosti ranjivosti

- Common Vulnerability Scoring System (CVSS)
  - Trenutno u verziji 3.1
  - Česta upotreba sa bazom ranjivosti CVE
  - https://www.first.org/cvss/v3-1/
- Raspon mjere je od 0 do 10 u koracima 0.1

Ozbiljnost	Raspon
Nikakva	0.0
Mala	0.1 – 3.9
Srednja	4.0 – 6.9
Visoka	7.0 – 8.9
Kritična	9.0 – 10.0

Izračunavanje CVSS-a (1)

- U izračunu CVSS-a uzimaju se u obzir tri komponente
  - Bazna komponenta, vremenska komponenta, okruženje
- Bazna komponenta
  - Inherentne karakteristike ranjivosti, neovisne o vremenu i okruženju
    - Način pristupa (preko mreže, susjedni čvor, lokalno, fizički), kompleksnost napada (niska, visoka), potrebne privilegije (nikakve, niske, visoke), interakcija korisnika (nije potrebna, potrebna), utjecaj na CIA (nikakav, niski, visoki)

Izračunavanje CVSS-a (2)

- Vremenska komponenta
  - Parametri koji se s vremenom mijenjaju
    - Zrelost koda za iskorištavanje ranjivosti (nepotvrđeno, PoC, funkcionalan, visoka), razina sprečavanja ranjivosti (službena ispravka, privremena ispravka, zaobilazna zaštita, nedostupno), pouzdanost izvještaja (nepoznato, razumno, potvrđeno)
- Okruženje
  - Parametri ovisni o okruženju
    - Uzimaju se u obzir specifičnosti okoline, primjerice, koliko okolina otežava ili olakšava pristup ranjivosti, kolika je osjetljivost okoline na kompromitiranje CIA svojstava
- Kalkulator
  - https://www.first.org/cvss/calculator/3.0

Napomena o mjerenjima u sigurnosti

- Mjerenje u znanosti i inženjerstvu je ključno
  - Vjerojatno ste to već uočili tijekom svog školovanja
- CVSS može ostaviti dojam da je mjerenje u sigurnosti riješen problem
- Međutim, **mjerenje u sigurnost je daleko od riješenog problema**
  - Postoje različite ad-hoc metode ali teško ili gotovo nemoguće ih je evaluirati i validirati; a rade se i mnoge druge greške

Traženje ranjivosti

- Postoje ljudi koji se (polu)profesionalno bave traženjem ranjivosti u raznim sustavima
  - Dosta često se specijaliziraju za pojedini sustav i za te potrebe grade odgovarajuće alate
  - Neki svoja otkrića objavljuju na stručnim konferencijama (npr. BlackHat) **nakon** što etički prijave ranjivost proizvođaču
- Osviještene tvrtke pozivaju istraživače da im ispitaju ranjivost (tzv. Bug bounty programi)
  - Za otkrivanje i prijavu ranjivosti istraživače se financijski nagrađuje
  - Google Vulnerability Reward Program, Microsoft Bug Bounty Program, Facebook Bug Bounty

Etičko traženje i prijavljivanje ranjivosti

- Traženje i prijava ranjivosti je potencijalno vrlo opasno
  - Može se doći u sukob sa zakonom
    - Protuzakonito je neovlašteno pristupati sustavima – u svim državama
  - Proizvođač programske podrške ili vlasnik sustava mogu uzvratiti tužbom
- U slučaju otkrivanja neke ranjivosti ne smije se odmah javno objaviti njeno postojanje
  - To omogućava napadačima i „script kiddyjima” napade na sustave
- Potrebno je prvo obavijestiti dobavljača programske podrške
  - Proizvođaču se omogućava ispravak pogreške i ažuriranje ranjivih sustava

Tržište ranjivosti

- Ranjivosti nultog dana su na velikoj cijeni
  - Omogućavaju provaljivanje na zaštićene sustave!
- Istraživač koji ih otkrije ima sljedeće mogućnosti
  - Prodaja na crnom tržištu
    - To rade tzv. Blackhats
    - Mogu se postići vrlo veliki iznosi po ranjivosti, ali je upitna legalnost
    - Cijene nisu javne, ali je tvrtka Zerodium objavila svoj cjenik pa se može steći osjećaj o kojim iznosima se radi
  - Prodaja sigurnosnim tvrkama
    - Ovo rade Whitehats i Grayhats
    - Ranjivost se može prodati tvrtkama koje na temelju toga poboljšavaju svoje proizvode
    - Obavještava se i proizvođača programske podrške

Ranjivosti u upravljanju i uklanjanju

Pogreška ili slabost u upravljanju

- Ovo su pogreške koje nastaju zbog upravljačkih (engl. management) ili administrativnih (engl. administrative) propusta
  - Procedura za otvaranje korisničkih računa nije dobro propisana te se daju ovlasti koje su više nego što je potrebno za obavljanje neke zadaće
  - Nije definirano tko je zadužen za nadzor sistemskih i operativnih zapisa Web poslužitelja pa ih nitko ne provjerava
- Ove ranjivosti sprečavaju se definiranjem odgovarajućih politika i procedura
  - Otkrivanje ovih ranjivosti obavlja se pregledom procedura od strane stručnjaka

Ranjivosti u uklanjanju

- Kada se sustavi uklanjaju treba paziti na podatke koji se na njima nalaze
- Primjeri ranjivosti
  - Skeneri/printeri imaju diskove na kojima se nalaze podaci
  - Prodaja polovnih računala i diskova
    - Što ako svoj laptop/računalo prodate nekome nepoznatom?
    - Što ako ga odnesete u servis ili posudite nekome
      - ovo nije ranjivost uklanjanja već upotrebe

Hvala!