SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 14:

Organizacione, fizičke i pravne metode zaštite, društveni aspekti

URLs:

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige:

  www.conwex.info/draganp/books.html
- Teme za seminarske radove:

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Napomena

- Ovo je skraćena verzija prezentacije / predavanja na temu **“Organizacione, fizičke i pravne metode zaštite, društveni aspekti”**

Organizacione, fizičke i pravne metode zaštite, društveni aspekti

- Sadržaj poglavlja i predavanja:
  - 14.1 Organizacione metode zaštite
  - 14.2 Fizičke metode zaštite
  - 14.3 Pravni aspekti sigurnosti
  - 14.4 Društveni aspekti sigurnosti

Quote

"Those who desire to give up freedom in order to gain security will not have, nor do they deserve, either one."

– Benjamin Franklin

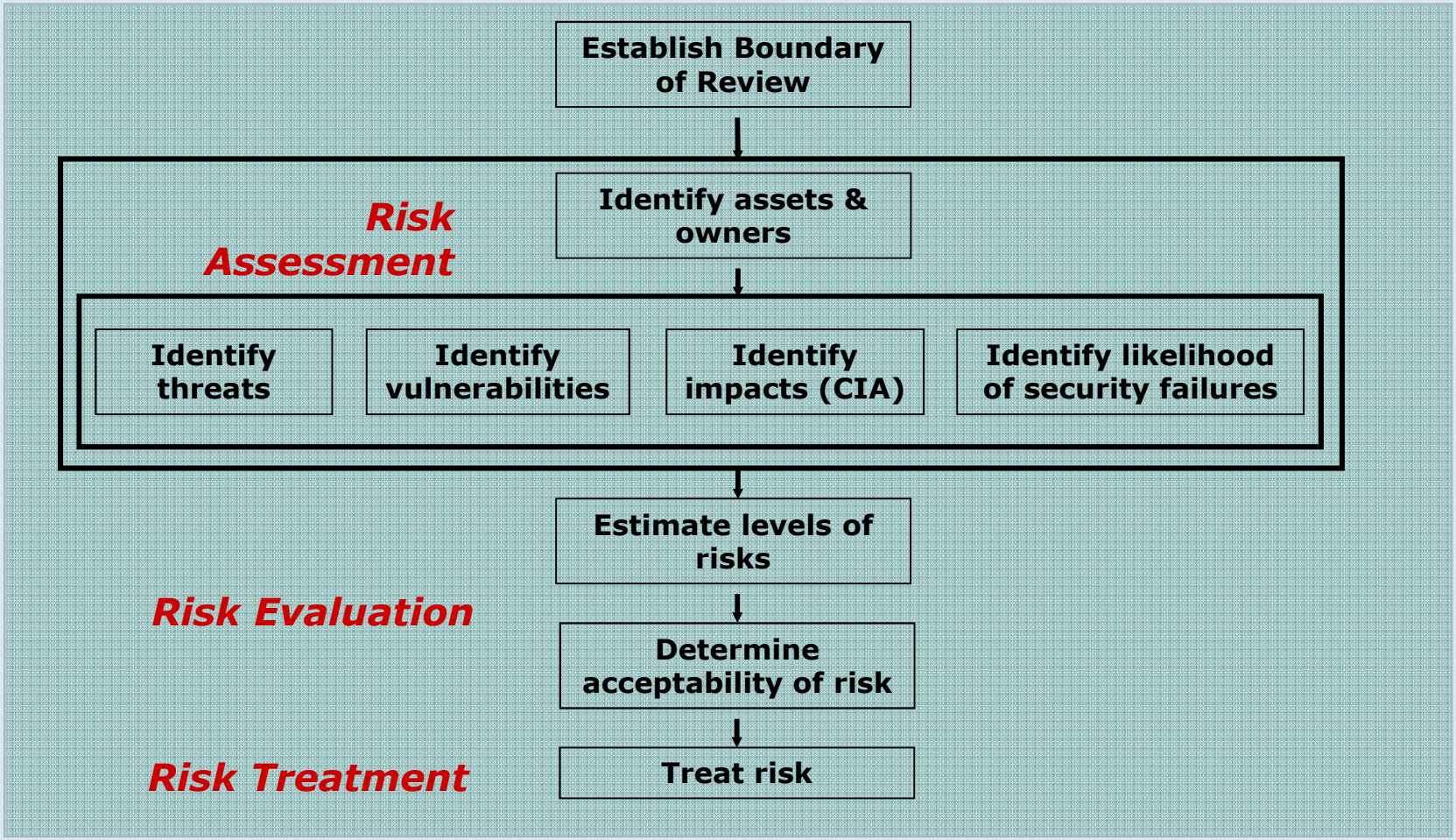
Potrebna predznanja

- Programiranje
- Za primenu:
  - Računarske mreže i protokoli
  - Operativni sistemi
  - Sistemsko programiranje
  - Strukture i modeli podataka, baze podataka

Upravljanje rizikom

- Upravljanje rizikom (engl. *risk management*)
- Projektovanje zaštite zahteva analizu rizika
- Rizik je mera opasnosti
  - mogućnost da nastane oštećenje ili gubitak neke informacije, hardvera, intelektualne svojine, prestiža ili ugleda.
  - definiše se eksplicitno
    - "rizik narušavanja integriteta baze podataka klijenata"
    - "rizik odbijanja usluga *on-line* portala banke"
    - "rizik gubitka podataka neophodnih za poslovanje preduzeća"

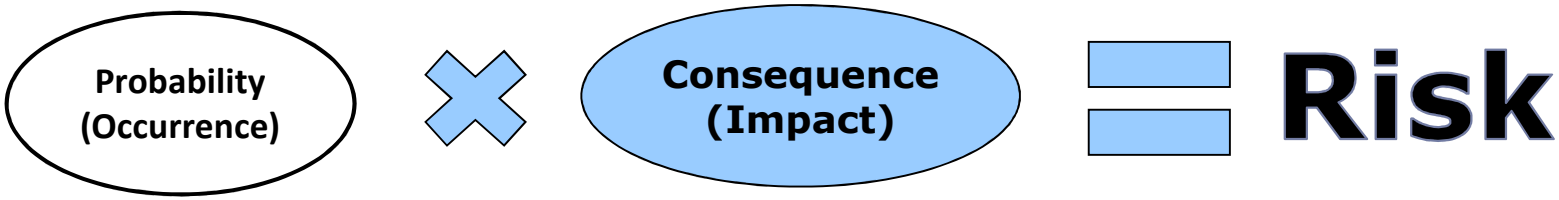
Information Risk Management



Risk Management

Information Security Risk

- ISO 27005 Information Security Risk Management
- Potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization
  - Note: *It is measured in terms of combination of likelihood of an event and its consequence*



Analiza rizika…

- Jednačina rizika
  - Rizik = Pretnja × Ranjivost × Vrednost imovine
    - Pretnja = protivnik (haker), situacija (zemljotres, požar) ili splet okolnosti (greška operatera) sa mogućnošću i/ili namerama da eksploatiše ranjivost.
    - Ranjivost = slabost u nekoj vrednosti, resursu ili imovini koja može biti iskorišćena, tj. eksploatisana.
    - Vrednost imovine = mera vremena i resursa potrebnih da se neka imovina zameni ili vrati u svoje prethodno stanje (= cena zamene).

Analiza rizika…

- Osetljivost sistema na neki događaj
  - finansijski gubitak koji pretrpi neka organizacija ako se taj događaj desi.
- Izloženost sistema nekom događaju (rizik)
  - Osetljivost na događaj X verovatnoća dešavanja
  - Verovatnoće se opisuju pomoću intervala u kom se očekuje jedno dešavanje događaja.
    - verovatnoća dešavanja požara je jedanput u 40 godina,
    - verovatnoća dešavanja operatorske greške kojom se uništava jedna datoteka iznosi jedanput u 4 godine

Likelihood of Risk

- The table shows the standard options for the likelihood of risk. These range from no chance of occurring up to certain to occur.

Likelihood	Equivalent Probability
No Chance Of Occurring	0%
Unlikely To Occur	5 – 45%
As Likely As Not	45 – 55%
Likely	55 – 95%
Almost Certain	95 – 99%
Certain To Occur	100%

Impact of the Risk

- The table below gives the categories of the impact if the risk does occur. This is a 6 level table that should give enough flexibility to categorise all risks that occur within the project.

Assessment of Impact	Grading
Little Impact, Nuisance Only	1
Medium Loss	2
Manageable Loss	3
In Range Of Largest Previous Loss	4
Serious Loss	5
Catastrophic	6

Upravljanje rizikom

- Proces uravnotežavanja troškova zaštite od rizika i troškova izloženosti riziku.
  - Mali troškovi zaštite
    - Visoka izloženost
    - Nizak nivo sigurnosti
  - Veliki troškovi zaštite
    - Nizak nivo izloženosti
    - Visok nivo sigurnosti
- Cilj: naći ravnotežu između ulaganja i efekata

Upravljanje rizikom…

- Nakon analize i procene rizika, mogu se preduzeti mere da bi se:
  - Eliminisao rizik - potpuno otklonio
  - Umanjio rizik - umanjio na prihvatljivu meru
  - Preneo rizik - preneo na drugu organizaciju, recimo osigurao kod osiguravajeće kompanije
  - Prihvatio rizik - odluka da se određeni nivo rizika može prihvatiti i pretrpeti

Kontrola pristupa

- Kontrole pristupa zasnovane na:
  - nečemu što osoba zna (na primer, PIN broj ili lozinka)
  - nečemu što osoba ima (na primer, sigurnosna identifikaciona kartica, hardverski token)
  - nečemu što osoba jeste (biometrija zasnovana na fizičkim karakteristikama)
  - nečemu što osoba radi (biometrija zasnovana na karakteristikama ponašanja)

Kontrola pristupa

- Sigurnost zasnovana na dva faktora
  - korišćenje najmanje dva od četiri elementa, da bi se odobrio pristup.
    - Npr: korisniku se dozvoli pristup kada unese lozinku i kad se proveri otisak prsta.
- Sigurnost zasnovana na četiri faktora
  - upotreba sva četiri elementa.
- Danas se za proveru identiteta najčešće koristi samo jedan faktor (lozinka)

Biometrija

- Biometrija
  - grčki: bios – život, metron – mera)
  - skup metoda za identifikovanje pojedinaca na osnovu bioloških karakteristika i/ili karakteristika ponašanja
    - biološke karakteristike: otisak prsta, snimak rožnjače oka, crte lica, geometrija šake, DNK
    - karakteristike ponašanja: glas, potpis
  - najčešće se koristi za proveru identiteta

Biometrija…

- Najobičniji biometrijski sistem se sastoji od pet komponenti:
  - senzor - sakuplja podatke i pretvara ih u digitalnu formu
  - algoritam izračunavanja signala - stvara biometrijsku mapu
  - skladište podataka - sadrži početne biometrijske mape sa kojim se nove upoređuju
  - algoritam za proveru podudaranja - upoređuje biometrijske mape iz predhodne dve komponente

Biometrija…

- Karakteristike biometrijskih metoda:
  - jedinstvenost – jednoznačnost identifikacije
  - trajnost – dužina zadržavnja karakteristike
  - prikupljivost – lakoća dobija uzoraka
  - izvodljivost – u kojoj je meri moguće u praksi implementirati navedene biometrijske metode i
  - prihvatljivost – u kojoj je meri implementacija moguća a da se pri tome ne naruše ljudska prava.

Biometrija – otisci prstiju

- Površina kože na prstima je pokrivena sitnim brazdama koje se nazivaju papilarnim linijama.
  - Papilarne linije jednoznačno identifikuju osobu i nepromenljive su.
  - Ne posmatra se pun otisak, već karakteristične značajne tačke otisaka prstiju. Razlozi:
    - u forenzici se često ne nađu potpuni otisci prstiju već delovi (trag)
    - ušteda vremena

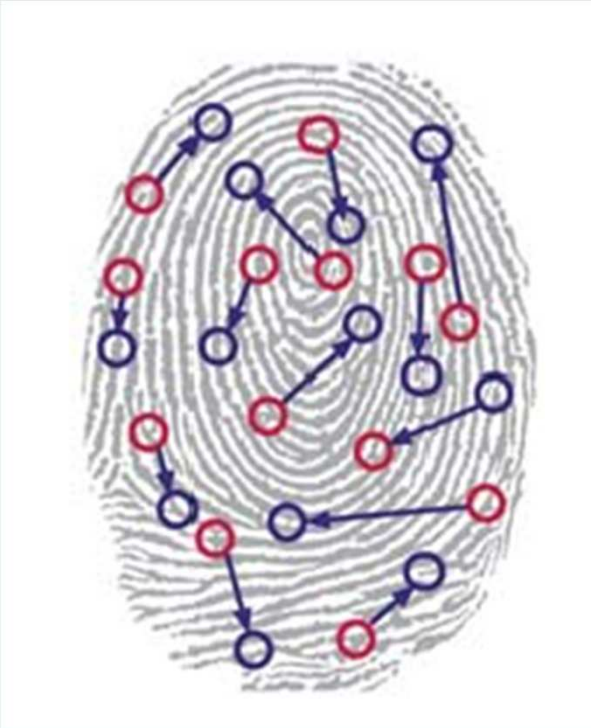
Biometrija – otisci prstiju…

- Otisak se opisuje karakterističnim tačkama
  - globalne
    - osnovni uzorci papilarnih linija (lukovi, spirale, petlje)
    - referentni centar, delta (tačka prvog grananja)
    - papilarni broj
  - lokalne (minutacije)
    - tačke koje se markiraju na krajevima, granama i razdvajanju papilarnih linija.
    - minutacije su glavni nosioci identifikacije
    - dve osobe ne mogu imati više od 8 zajedničkih minutacija.

Biometrija – otisci prstiju…

- Postoji pet različitih osobina minutacija:
  - vrsta minutacije, na primer:
    - papilarni kraj – nagli prekud papilarne linije
    - grananje (bifurkacija) – grananja linije u više novih
    - papilarne linije koje se dele na dve, a zatim se ponovo spajaju u sopstvenu izvornu liniju
  - orijentacija – smer u kome "gleda" minutacija
  - zakrivljenost – brzina promene smera minutacije
  - udaljenost papilarnih linija u okolini minutacije
  - koordinate u odnosu na središnju tačku ili deltu.

Biometrija – otisci prstiju…



Biometrija – za ili protiv?

- Fizički
  - Realna situacija: 2005. u Maleziji su odsekli prst vlasniku automobila za čije je pokretanje bilo neophodno očitati otisak prsta.
- Privatnost
  - LK sa biometrijskim podacima?
  - Zloupotreba prikupljenih podataka za lažiranje pri izvođenju ilegalnih operacija
    - neugodnosti za pojedinca koji je predmet zloupotrebe.

Konvencija o cyber-kriminalu

- Veće Evrope je u novembru 2001. donelo konvenciju kojom je pokušalo dati smernice u borbi protiv računarskog kriminala.
  - krivična dela protiv tajnosti, nepovredivosti i dostupnosti podataka
  - krivična dela poput prevare i faslifikovanja uz pomoć računara
  - krivična dela koja se odnose na sadržaj podataka
    - npr. distribuciju i širenje dečje pornografije
  - kršenje autorskih i srodnih prava.

Konvencija o cyber-kriminalu…

- Krivična dela protiv tajnosti, nepovredivosti i dostupnosti podataka
  - neovlašćen pristup (čl. 2)
  - neovlašćeno presretanje podataka (čl. 3)
  - menjanje sadržaja, brisanje ili oštećenje podataka (čl. 4)
  - ometanja normalnog rada računara (čl. 5)
  - proizvodnja, prodaja, distribucije ili upotreba uređaja projektovanih u svrhu počinjenja nekog od prethodno navedenih krivičnih dela (čl. 6)

Konvencija o cyber-kriminalu…

- Krivična dela protiv tajnosti, nepovredivosti i dostupnosti podataka

Zemlje	čl. 2	čl.3	čl.4	čl. 5	čl. 6
Nemačka	X	✓	✓	✓	✓
Austrija	✓	✓	✓	X	X
V. Britanija	✓	✓	✓	✓	✓
SAD	✓	✓	✓	✓	✓
Francuska	✓	✓	✓	✓	✓
Švedska	X	X	✓	✓	X
Japan	✓	✓	✓	X	X
Kina	✓	✓	✓	✓	✓
Srbija	✓	✓	✓	✓	✓
Slovenija	✓	✓	✓	✓	X
Hrvatska	✓	✓	✓	✓	✓

Zakonodavstvo u Srbiji - bezbednosti računarskih podataka

- Krivična dela protiv bezbednosti računarskih podataka:
  - Oštećenje računarskih podataka i programa
  - Računarska sabotaža
  - Pravljenje i unošenje računarskih virusa
  - Računarska prevara
  - Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka
  - Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži
  - Neovlašćeno korišćenje računara ili računarske mreže

Zakonodavstvo u Srbiji - intelektualna svojina

- Krivična dela protiv intelektualne svojine:
  - Povreda moralnih prava autora i interpretatora
  - Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava
  - Neovlašćeno uklanjanje ili menjanje elektronske informacije o autorskom i srodnim pravima
  - Povreda pronalazačkog prava
  - Neovlašćeno korišćenje tuđeg dizajna

Zakon o elektronskom potpisu

- Narodna skupština Republike Srbije usvojila je 14. decembra 2004. Zakon o elektronskom potpisu (pod ovim se podrazumeva digitalni potpis).
  - Nakon toga su donešena podzakonska akta i počela primena

  - 1. Da li Srbija ima sertifikaciona tela (CA) i koja?
  - 2. Zašto su sertifikati mnogih e-bank portala samopotpisani od strane banke?

Copyright, patenti i licence

- Autorsko pravo
  - štiti originalnu implementaciju i način prikaza neke ideje, a ne samu ideju!
  - može se zaštititi izvorni i izvršni kôd, uputstva i dokumentacija u digitalnom ili pisanom obliku.
  - ne štiti algoritme, metode i matematičke postupke korišćene u realizaciji softvera
    - štiti od neovlašćenog kopiranja ili oponašanja koda, ali ne štiti od konkurencije koja samostalno i nezavisno (bez uvida u izvorni kôd konkurencije) razvija sličan softver

Copyright, patenti i licence

- Patent
  - Za razliku od autorskog prava koje štiti prezentaciju ideje i oblik izražavanja, patent štiti samu ideju
  - Dakle, patent štiti ideje, algoritme i matematičke postupke korišćene u programu, a ne sam kôd
    - zabranjuje objavu bilo kakvog sličnog rada, pa makar bio i nezavisno razvijen
    - visoka cena njihovog izdavanja i dugo vreme koje mora proći od predaje zahteva pa do eventualnog odobrenja za objavljivanje patenta

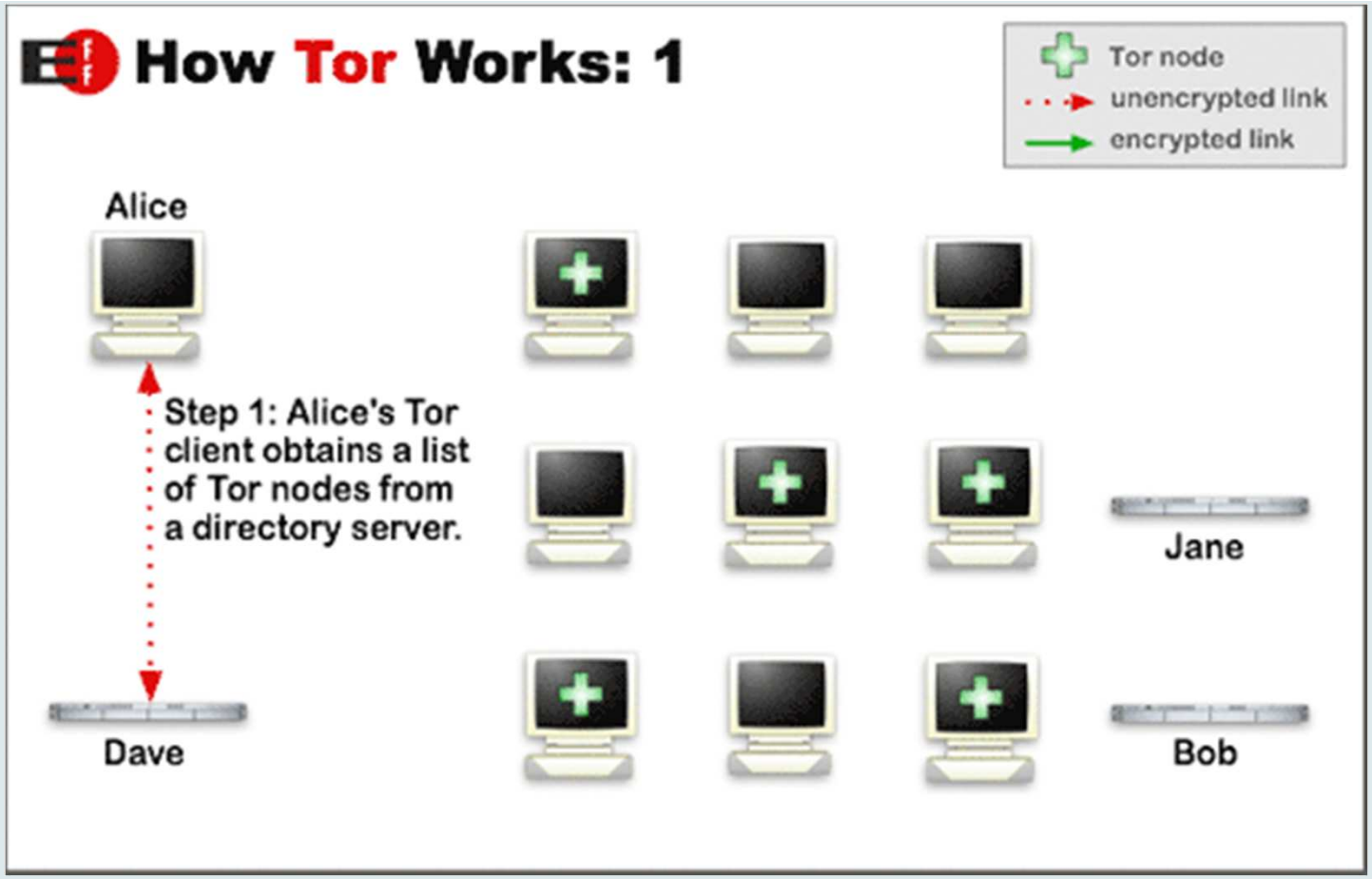
Copyright, patenti i licence…

- Podela softvera
  - public domain
  - open source
    - razlika između public domain i open source softvera?
  - freeware
  - shareware / trialware
  - adware
  - commercialware

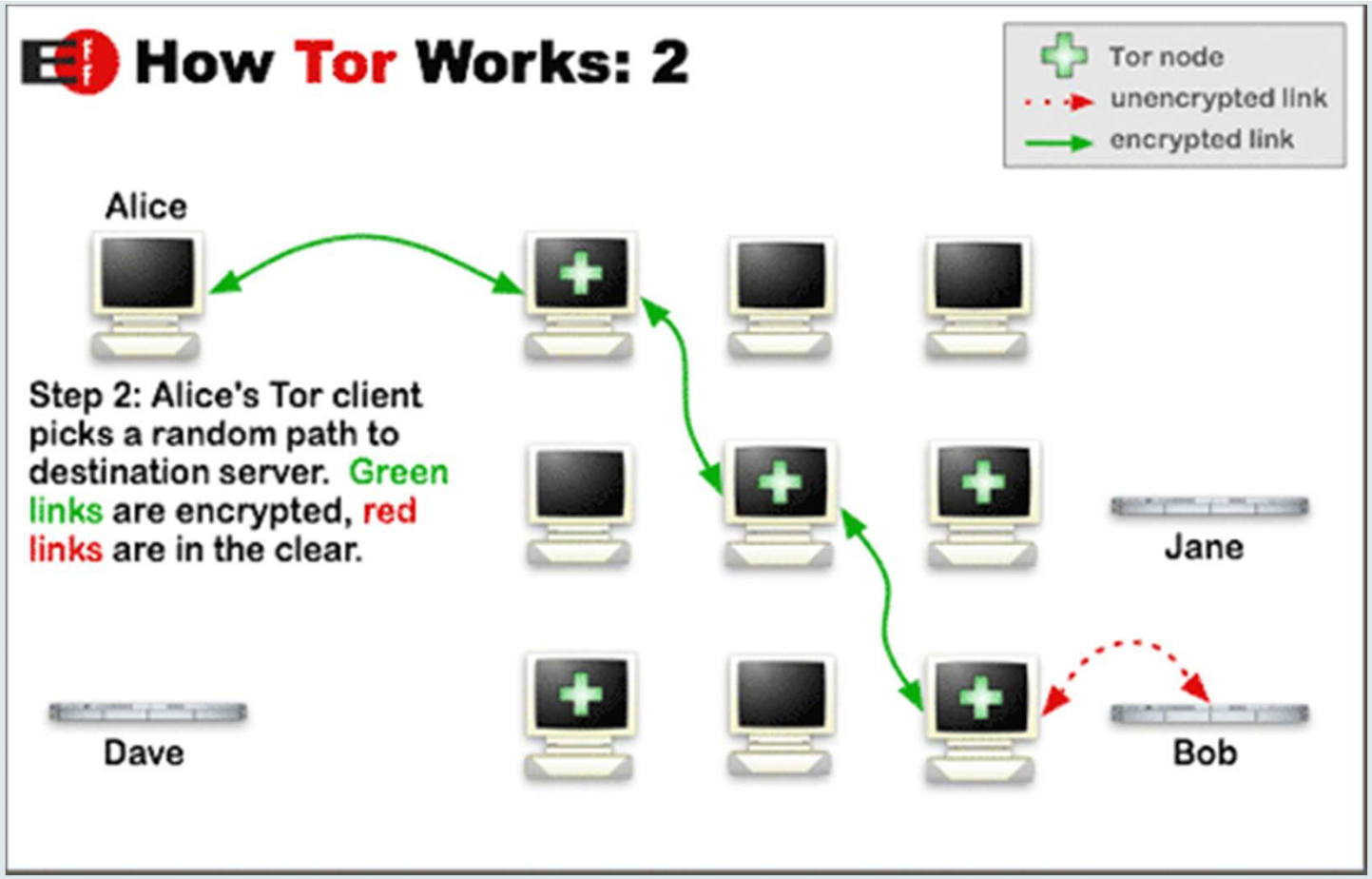
Društveni aspekti sigurnosti

- Privatnost
  - važna za one koji ne žele da svima pokažu „svoju ličnu kartu“
  - Electronic frontier foundation
  - videti: TOR (tor.eff.org)
    - mreža šifrovanih kanala, obezbeđuje visok nivo anonimnosti
    - podiže tor klijent (i opciono, ukoliko dozvolite) server koji radi kao anonymous proxy
      - whatsmyip.com – proverite sa tor-om i bez njega
  - Savremeni Web čitači (*browsers*) imaju opciju *private / incognito browsing*

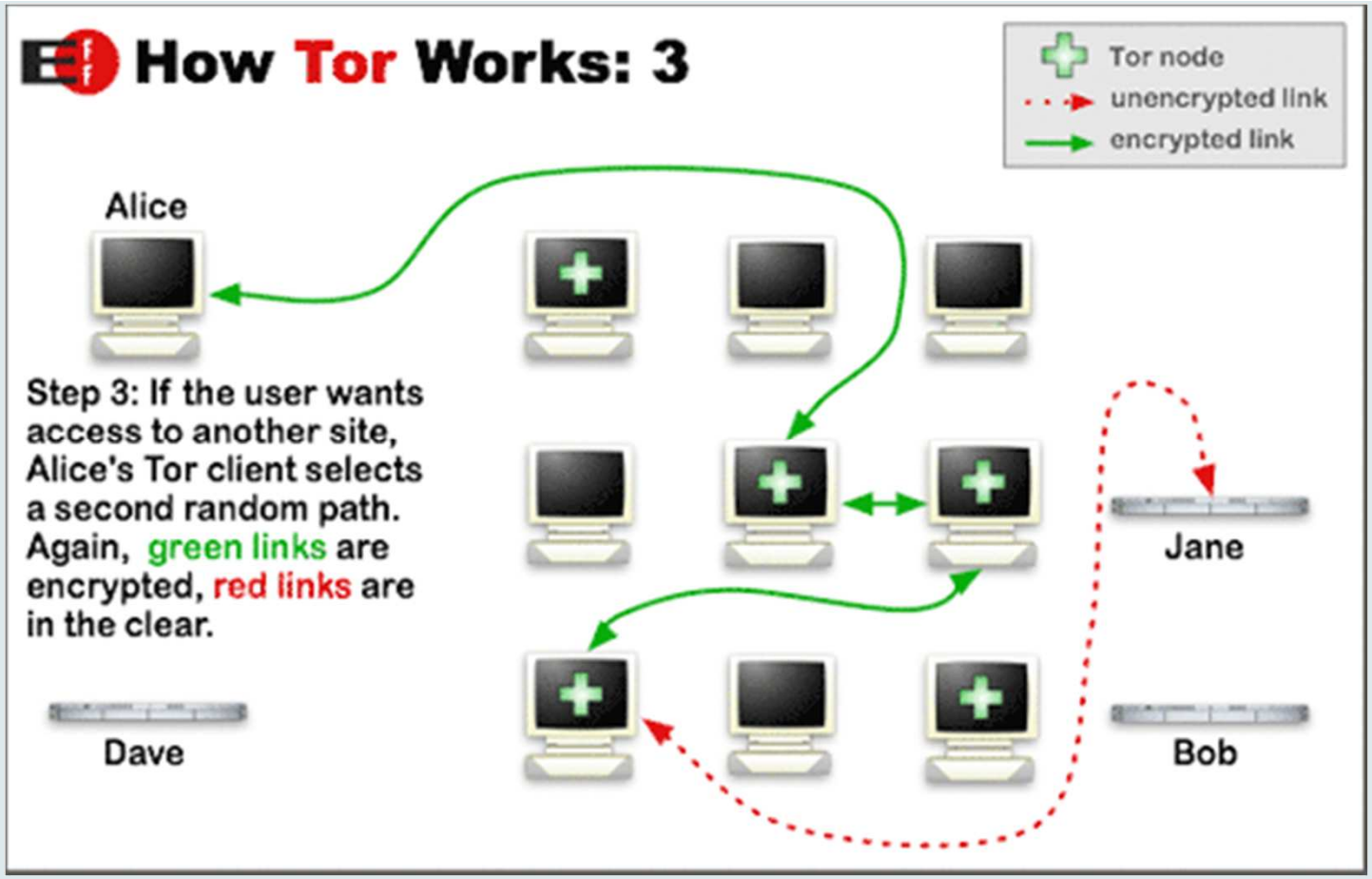
TOR



TOR



TOR



Društveni aspekti sigurnosti

- Steganografija
  - utiskivanje jedne poruke u drugu na neki način pri čemu utisnuta poruka ostaje skrivena
  - primer – utiskivanje poruke u sliku
    - Npr. za utiskivanje informacije o vlasničkim pravima u sliku (engl. *watermarking*)
    - Prednost u odnosu na kriptografiju: ne zna se da je poruka skrivena

Društveni aspekti sigurnosti…

- Sloboda izražavanja i cenzura
  - Zabranjeni materijal može da obuhvati lokacije sa sledećim sadržajem (shodno vladajućem režimu):
    - materijal nepodesan za decu i omladinu
    - govor mržnje usmeren na različitie etničke, religiozne, seksualne i druge grupe
    - informacije o demokratiji i demokratskim vrednostima
    - istorijski materijali koji protivreče zvaničnoj verziji vlade
    - priručnici za ilegalne aktivnosti kao što su obijanje brava, pravljenje oružja, eksploziva i eksplozivnih naprava, razbijanje šifara i slično.

Društveni inženjering

- Probijanje sigurnosti iskorišćenjem ljudskog faktora
  - nedostatka svesti o veličini problema sigurnosti
  - nemara i grešaka
  - neobaveštenosti i neobrazovanosti

- Knjige
  - Bruce Schneier - “Secrets & Lies - Digital Security in a Networked World”
  - Kevin Mitnick - “Umeće provale”, prevod, Mikro knjiga

Literatura

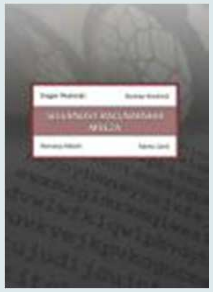
- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **"Sigurnost računarskih sistema i mreža"**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

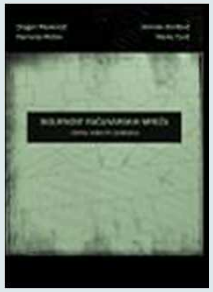
- Za predavanje 14:
  - Poglavlje 14: Organizacione, fizičke i pravne metode zaštite, društveni aspekti

Literatura - nastavak

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - priručnik za laboratorijske vežbe"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - zbirka rešenih zadataka"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html





Dodatna literatura

- **Applied Cryptography**
  Bruce Schneier
  John Wiley & Sons, 1995

- **Cryptography and Network Security**
  William Stallings
  Prentice Hall, 1998

- **The CISSP Prep Guide – Mastering the Ten Domains of Computer Security**
  Ronald L. Krutz, Russell Dean Vines
  John Wiley & Sons, 2001

  Druge knjige i razni *online* resursi

- ***Napomena:*** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

?