

# Sigurnost Podataka: Kratak Izlet u Svet Mobilnih Racunara i Komunikacija

Boris Dragovic, PhD

Security Research Area Head

CREATE-NET

[Boris.Dragovic@create-net.org](mailto:Boris.Dragovic@create-net.org)

# Sadržaj



- ✓ Postavljanje scene
- ✓ Sigurnosni izazovi i faktori
- ✓ Tradicionalni pristup zaštiti...
- ✓ ... i zasto on ne zadovoljava izazov
- ✓ Sugestija resenja
- ✓ Generalizacija

# Okruzenje



YUINFO 2007

# Trziste mobilnih uredjaja

- ✓ 1.019 milijarde mobilnih telefona isporuceno u 2006. (IDC)
  - ✓ 55% rasta u odnosu na 2005.
- ✓ 80+ miliona “smart” telefona
  - ✓ 42% rast u odnosu na 2005.
- ✓ 5.5 miliona PDA
  - ✓ -28.5% u odnosu na 2005.
- ✓ 878 miliona “mobilnih radnika” do 2009.

# Sigurnost podataka - principi



- ✓ Tajnost (Confidentiality)
- ✓ Integritet (Integrity)
- ✓ *Dostupnost* (Availability)
  - ✓ Bilo kad i bilo gde
  - ✓ Sustinska u svetu mobilnih racunara i komunikacija

# Od fixnih ka mobilnim sistemima

- ✓ Prirodno neprijateljsko okruzenje
  - ✓ Koncept fizickog perimetra gubi smisao
- ✓ Dinamicnost, nepredvidivost konteksta
- ✓ Raznolikost platformi (sw/hw)
  - ✓ I komunikacionih tehnologija
- ✓ Dostupnost servisa i podataka
- ✓ Ogranicenost resursa
- ✓ Korisnik kao centar slike

# Osvrt na rizike



- ✓ *Znacajni pomeraaj fokusa u odnosu na tradicionalne sisteme*
  - ✓ *Uz nove tipove rizika*
- ✓ **Curenje (leakage) informacija**
  - ✓ *Izgubljeni uređaji, Wireless, EM emanacije*
- ✓ **Interakcije sa nepoznatim entitetima**
  - ✓ **Poverenje i reputacija (Trust & reputation)**

# Curenje informacija (Leakage)

- ✓ Gubitak uređaja popularan primer
  - ✓ Ocigledan i lako se kvantifikuje
- ✓ Realni rizik i od
  - ✓ Emanacija (EM, RF, optickih), Audio/Video analize & rekonstrukcije, wireless kanala itd.
  - ✓ ... i jos mnogo drugih
- ✓ Znatno izrazenije “slučajno” curenje
  - ✓ Kompleksnost sredine vs. kongnitivni kapacitet
  - ✓ Tesko se identifikuje, kvalifikuje i kvantifikuje

# Gubljenje uređaja - kratak osvrt

- ✓ # izgubljenih uređaja u taksi vozilima
- ✓ London, 6 meseci tokom 2005.
  - ✓ 63135 mobilnih telefona, 5838 PDA i 4973 laptopa ostavljeno
- ✓ San Francisco + Baltimore/WA, 2006.
  - ✓ 8856 mobilnih telefona, 2566 PDA i 370 laptopa ostavljeno
- ✓ Oko 50% biznis klijenata

# Uloga konteksta

- ✓ Kontekst određuje karakteristike rizika
- ✓ *U mobilnim okruženjima kontekst je ključno dinamičniji i teško predvidiv*
  - ✓ Samim tim i implicirani rizik
- ✓ *Menadžment i način manipulacije podacima implicitno određuje nivo zaštite datom kontekstu*

# Sasvim obicni primeri...

- ✓ Razliciti konteksti
  - ✓ Kancelarija, javno mesto, kongresna sala...
- ✓ Izbor komunikacionih kanala
  - ✓ Wi-Fi vs. Bluetooth vs. IrDA
- ✓ Prikaz informacija
  - ✓ javni vs. laptop vs. PDA displej
- ✓ Unos podataka
  - ✓ ATM vs. laptop vs. PDA

# Bakina kuhinja

- ✓ Karakteristike tradicionalnog pristupa zaštiti podataka
  - ✓ Staticka procena/analiza rizika (u kontekstu)
    - ✓ I postavljanje adekvatne zaštite
  - ✓ Princip postavljanja *perimetra* sto blize izvoru opasnosti
    - ✓ Skaliranje perimetra kroz racunarsku evoluciju
    - ✓ Odn. gubitak smisla
- ✓ Ali...

# Rezultat



- ✓ Tradicionalan pristup zaštiti podataka primenjen *per se* negira (u većini slučajeva) benefecije mobilnosti
  - ✓ Primarno dostupnost
  - ✓ Kreira svojevrсни paradoks
  - ✓ Prvobitno osmisljen za različit sistem prioriteta rizika

# Prioritetna karakteristika

- ✓ ... koja se mora ocuvati (u mobilnim sistemima) je

## DOSTUPNOST

- ✓ ... zahteva visoko kompromisna i dinamička *SOCIO-TEHNICKA* rešenja
  - ✓ krucijalna razlicitost u odnosu na tradicionalne sisteme

# Gde je greska?



- ✓ Staticko resenje za dinamički problem
  - ✓ Generalizovana analiza rizika
  - ✓ Nemogućnost adaptacije
- ✓ Parcijalna, nepotpuna zaštita podataka
  - ✓ Enkripcija (skladištenje, transport), Access Control
  - ✓ Ali... **Rizici vrebaju kontinualno!**
- ✓ Znacajna kolatelarna šteta perimetra
  - ✓ Dostupnost podataka

# Mozda resenje lezi u...

- ✓ Inverziji tradicionalnog pristupa postavljanja perimetra
  - ✓ Od izvora opasnosti ka ugrozenom resursu - informaciji; informacija kao centar slike
- ✓ Dinamickoj proceni i adaptaciji riziku
  - ✓ Uz aktivno balansiranje nivoa zastite kroz izbor alternativnih manipulativnih metoda
- ✓ Sigurnost kao kompromis (nivo zastite vs. dostupnost) a ne kao apsolutna vrednost
  - ✓ Good-enough security

# Postavljanje perimetra



- ✓ Tehnicki problem na vise nivoa
  - ✓ Sistemskom/Aplikativnom
  - ✓ ... Moze se ostvariti postepeno
    - ✓ Sa odredjenim gubicima u granularnosti i finoci balansa izmedju dostupnosti i zastite
  - ✓ Kompletno resenje zahteva redizajn sw/hw arhitekture
    - ✓ Prilicno radikalno

# Dinamicka adaptacija

- ✓ Socio-tehnicki problem
  - ✓ Dinamicka analiza rizika u okruzenju
    - ✓ Tehnicki problem: metricke jedinice, mapiranje i analiza rizika itd.
  - ✓ Adaptacija
    - ✓ Tehnicki: procena nivoa zastite, metricke jedinice i modeli, mehanizmi adaptacije
    - ✓ Socio: transparentnost u ponasanju sistema

# Nivo zastite vs. *Dostupnost*

- ✓ Nivo zastite - tehnicki problem
  - ✓ Metricke jedinice, modeli
- ✓ Dostupnost - socio-tehnicki problem
  - ✓ Subjektivni faktori u percepciji dostupnosti
  - ✓ Personalizacija

# Generalizacija



- ✓ Izložene ideje imaju potencijalne beneficije izvan sveta “mobilnosti”
- ✓ Npr. outsourcing servisa u industriji i komercijalnom sektoru
  - ✓ E-mail, skladištenje podataka itd.
  - ✓ npr. Google korporativni servisi



**That's All Folks!**