Sigurnost mobilnih aplikacija

Vlatko Košturjak

AGENDA

- **Uvod**
- **Sigurnost aplikacija**
- **Sigurnost mobilnih aplikacija**
  - **Razlike**
  - **Preporuke**
  - **Ispravan pristup**
- **Sažetak**
- **Pitanja i odgovori**

30 minuta

Nekoliko pitanja za početak

- **Koliko se sigurnosnih incidenata preventiralo?**
- **Koliko se sigurnosnih incidenata prepoznalo u 24 sata od njihove pojave?**
- **Da li se opseg sigurnosnog incidenta mogao prepoznati odmah prilikom pojave?**
- **U koliko se slučajeva počinitelj pronašao?**
- **U koliko se slučajeva počinitelj procesirao?**

Preventiva jedino rješenje

… i najjeftinije! ;)

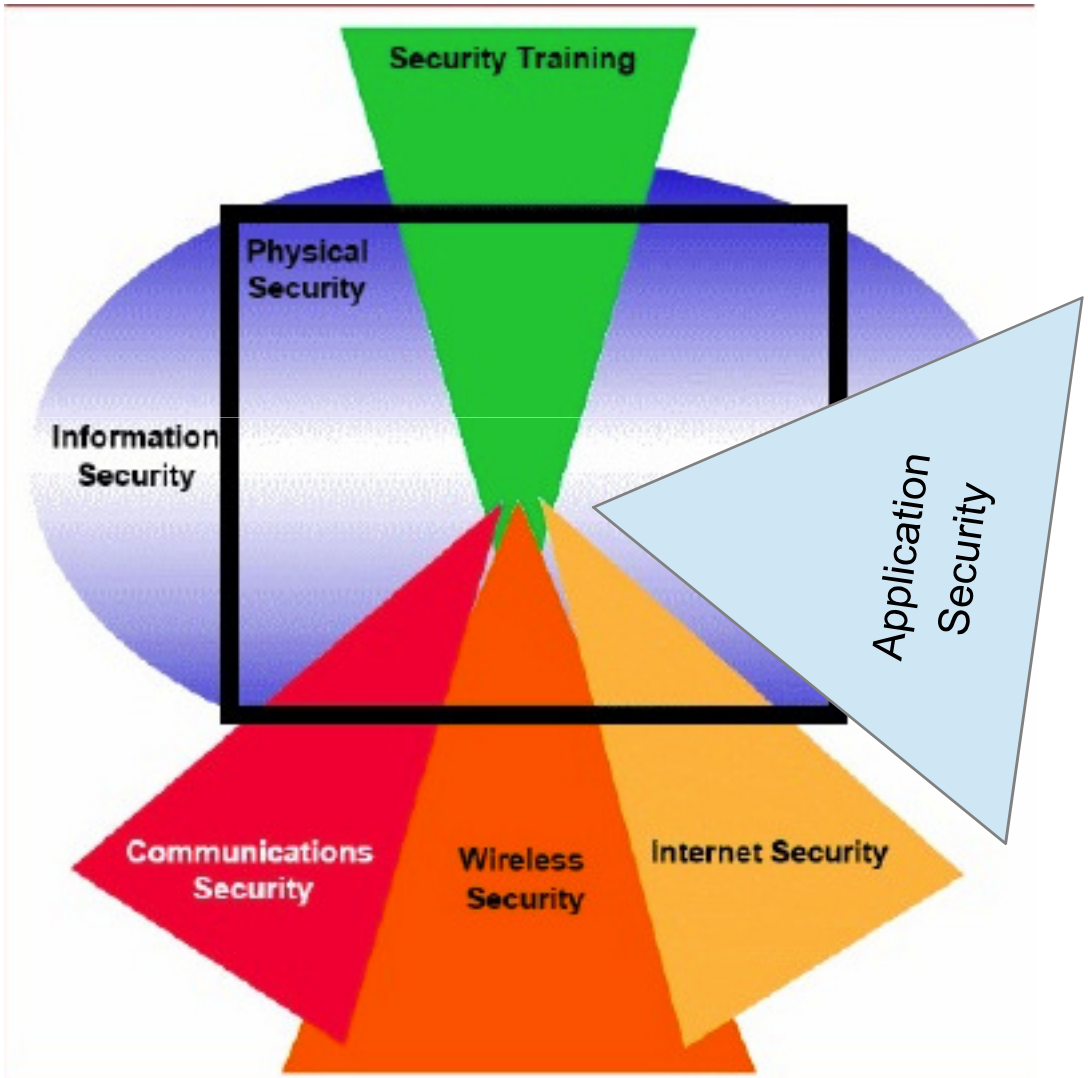
Nekoliko pitanja za početak

- **Koliko ste puta sigurnosno krpali aplikaciju zbog početnog lošeg dizajna?**
- **Koliko bi toga riješio ispravan pristup od početka dizajna aplikacije?**

Hm

Isplati se misliti na sigurnost odmah na početku...

Sigurnost



ISECOM

Koliko je različito od web ili desktop aplikacija?

- Ne, previše :)
  - Klijent strana je različita
- Pozitivne strane
  - Sustav dozvola i razdvajanja
  - Vrijeme detekcije izgubljenog
- Negativne strane
  - Lako Izgubiti
  - Općeniti sustav dozvola
  - Ograničeni resursi

SIGURNOST PLATFORME

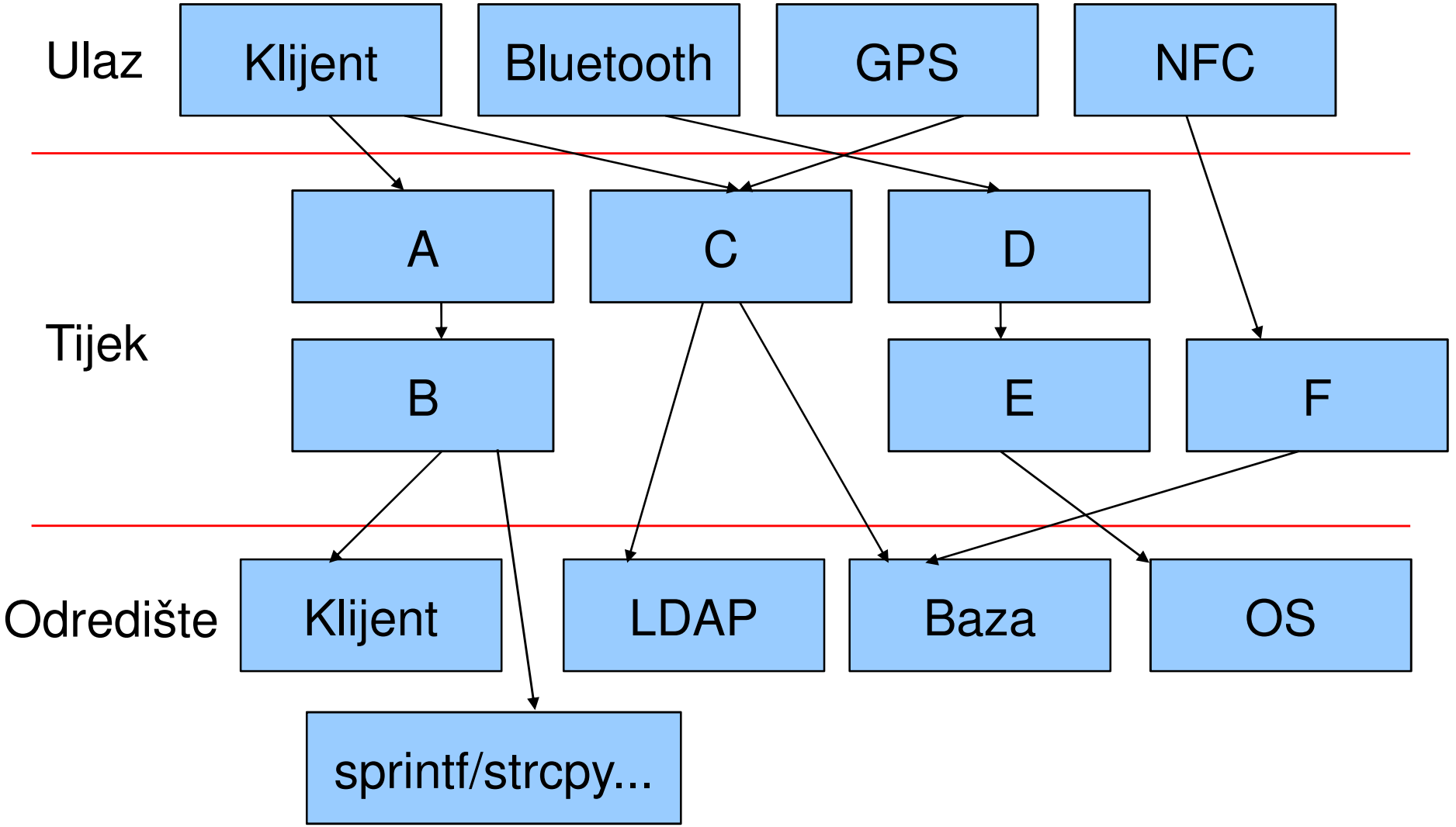
- Sigurnost hardverske platforme
- Sigurnost softverske platforme
  - Aplikacijski poslužitelj
  - Operativni sustav
  - Upravljački programi
  - Servisi
  - Pohrana
    - SQL
    - LDAP
    - XML
    - ...

OWASP TOP 10
Opća i mobilna usporedba

- Injection
- Cross Site Scripting (XSS)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross Site Request Forgery (CSRF)
- Security misconfiguration
- Failure to Restrict URL Access
- Unvalidated Redirects and Forwards
- Insecure Cryptographic Storage
- Insufficient Transport Layer Protection

- Insecure Data Storage
- Weak Server Side Controls
- Insufficient Transport Layer Protection
- Client Side Injection
- Poor Authorization and Authentication
- Improper Session Handling
- Security Decisions Via Untrusted Inputs
- Side Channel Data Leakage
- Broken Cryptography
- Sensitive Information Disclosure

Tijek podatka u aplikaciji



Prvi koraci

- Prikupljanje i analiza poslovnih potreba i zahtjeva
- Analiza poslovnih rizika i prijetnji
  - Analiza rizika i prijetnji mobilne aplikacije
    - Osjetljivi aplikativni podaci
      - Lozinke, Ključevi, Povjerljivi podaci
    - Jednoznačni idenifikatori mobilnog uređaja
      - IMEI, IMSI, …
    - Osobni podaci
      - Adresar, E-mail, Popis poziva, …
    - Osjetljivi podaci
      - Lozinke, Ključevi, …

Aplikacijski zahtjevi

- **Funkcionalni zahtjevi**
  - **Ispunjava poslovne zahtjeve**
- **Nefunkcionalni zahtjevi**
  - **Performanse**
  - **Sigurnost**
  - **Kompatibilnost**
  - **Usability**
  - **…**

OWASP Top 10 Mobile Security Controls

- **Identify and protect sensitive data on the mobile device**
- **Handle password credentials securely on the device**
- **Ensure sensitive data is protected in transit**
- **Implement user authentication,authorization and session management correctly**
- **Keep the backend APIs (services) and the platform (server) secure**
- **Secure data integration with third party services and applications**
- **Implement controls to prevent unauthorized access to paid-for resources (wallet, SMS, phone calls etc.)**
- **Ensure secure distribution/provisioning of mobile applications**
- **Carefully check any runtime interpretation of code for errors**

Ponešto o provjeri unosa

- Osnovni problem ispravne implementacije
- Aplikacija
  - Provjera na poslužiteljskoj strani
  - Provjera što je dozvoljeno (Whitelisting)
- (Web) Application Firewall (WAF)
  - Provjera što nije dozvoljeno (blacklisting)
  - Normalizacija prometa
  - Detekcija zaobilaženja

OR 1=1
OR 9=9
OR 2<3
O/**/R 2<3
...

Test prihvatljivosti

- **Pristup**
  - **Black box**
  - **Gray box**
  - **White Box**
  - **…**
- **Način**
  - **Penetracijski test**
  - **Analiza izvornog koda**
  - **…**

Nekoliko ideja za proaktivnost

- **Umetanje proaktivnih parametara i varijabli**
  - **Jedina svrha = detekcija promjene**
- **Korištenje sigurnih opcija kod protokola**
  - **Verifikacija certifikata**
  - **HTTP zaglavlja**
  - **Atributi**
  - **…**
- **Višeslojna zaštita**

Dobre pretpostavke

- Pretpostavka
  - Napadač je pronašao i iskoristio ranjivost
  - Višeslojna zaštita
- Prijava sigurnosnog problema
  - Kontakt
  - Odgovorne osobe
  - Prioriteti
- Suradnja
  - Incident Response Plan (IRP)
  - Opseg i kontakti

Sažetak

- Analiza rizika
- Nefunkcionalni zahtjevi
- Sigurnost platforme
- Sigurnost protokola
- Sigurnost mobilne aplikacije
- Testiranje i stalno praćenje
- Edukacija

Edukacija je važan faktor

CFO asks CEO: *“What happens if we invest in developing our people & then they leaves us?”*

CEO: *“What happens if we don't, and they stay?”*

Matt Umholtz

Hvala na pažnji