ORACLE®

Postupy a technologie pro budování bezpečných aplikací

Aleš Novák
Oracle

Situace

- Pro tvorbu aplikací v internetu převažují webové (web 2.0) technologie
  - Použití cloud computingu tento trend posiluje
- Exploze aplikací na mobilních klientech
- Zabezpečení aplikací se často řeší po jejich nasazení.

Ohrožení

- Phishing
- Session hijacking
- Man in the Middle
- Man in the Browser
- Kontrola formátování XML; kontrola velikosti XML; XPath a XQuery injection; SQL injection; XML encapsulation; XML viruses
- Skenování odchozích zpráv na citlivé informace
- Detekce XML bomb
- Schema a DTD validace

- SQLInjection
- Cross Site scripting
- Message replay
- Filtrování SOAP operací
- Filtrování SOAP attachments (např. viry)
- HTTP header and query string analysis
- Filtrování IP adres
- Traffic throttling – DoS, DDoS

Co s tím?

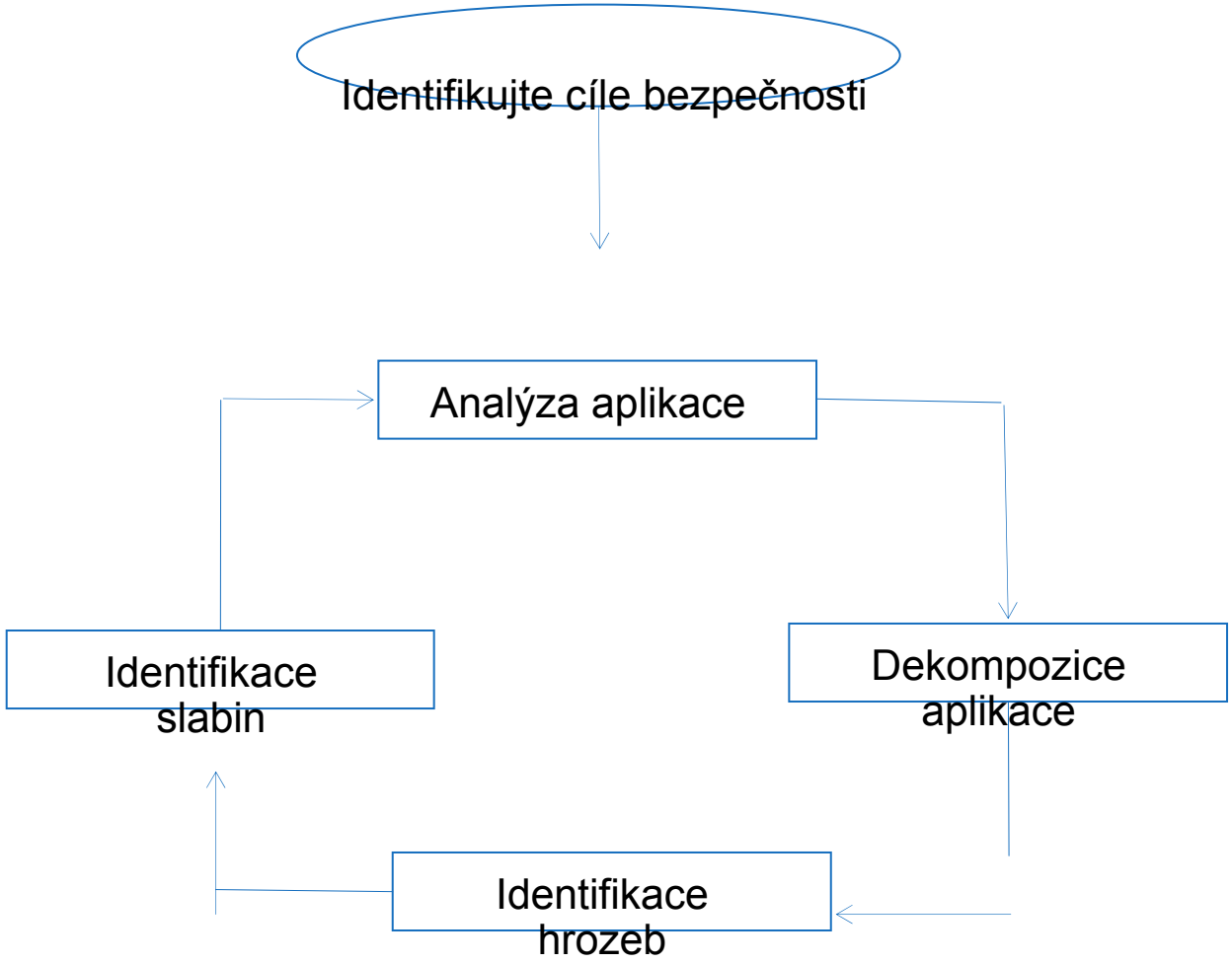
- Dáme tam firewall.

The Open Web Application Security Project (OWASP)

- www.owasp.org
- Podává přehled hrozeb

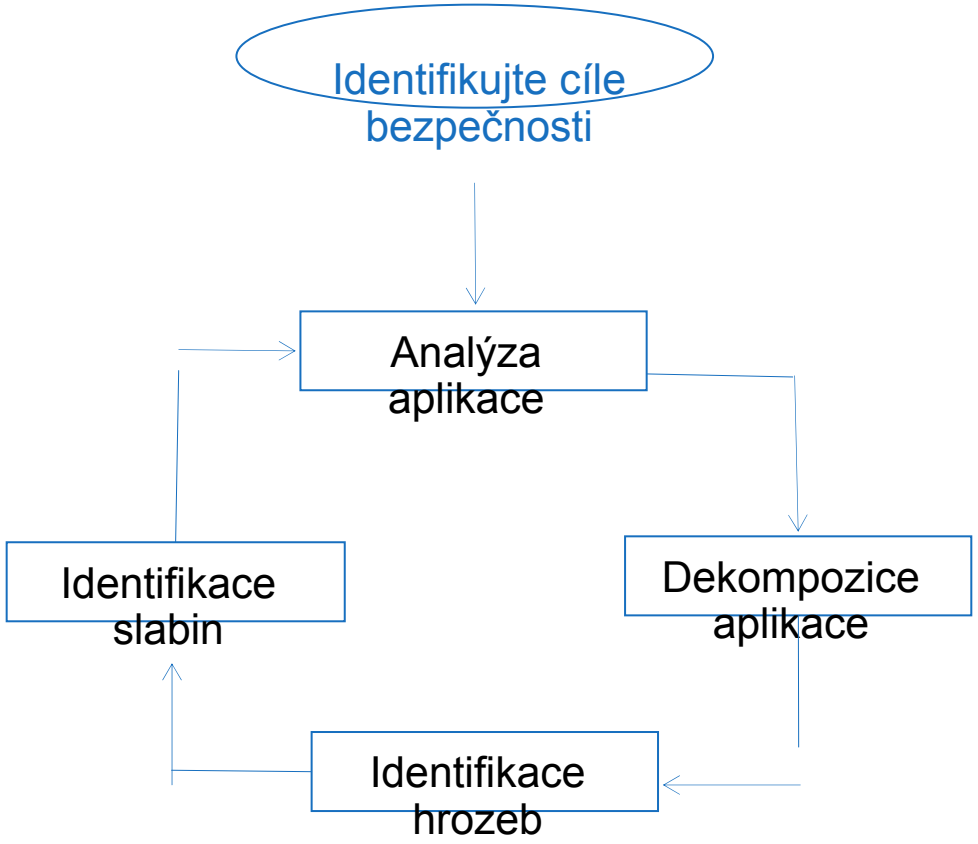
- Doporučení – udělejte analýzu aplikace. Konkrétně „Threat Risk Modeling“

Threat Model Flow



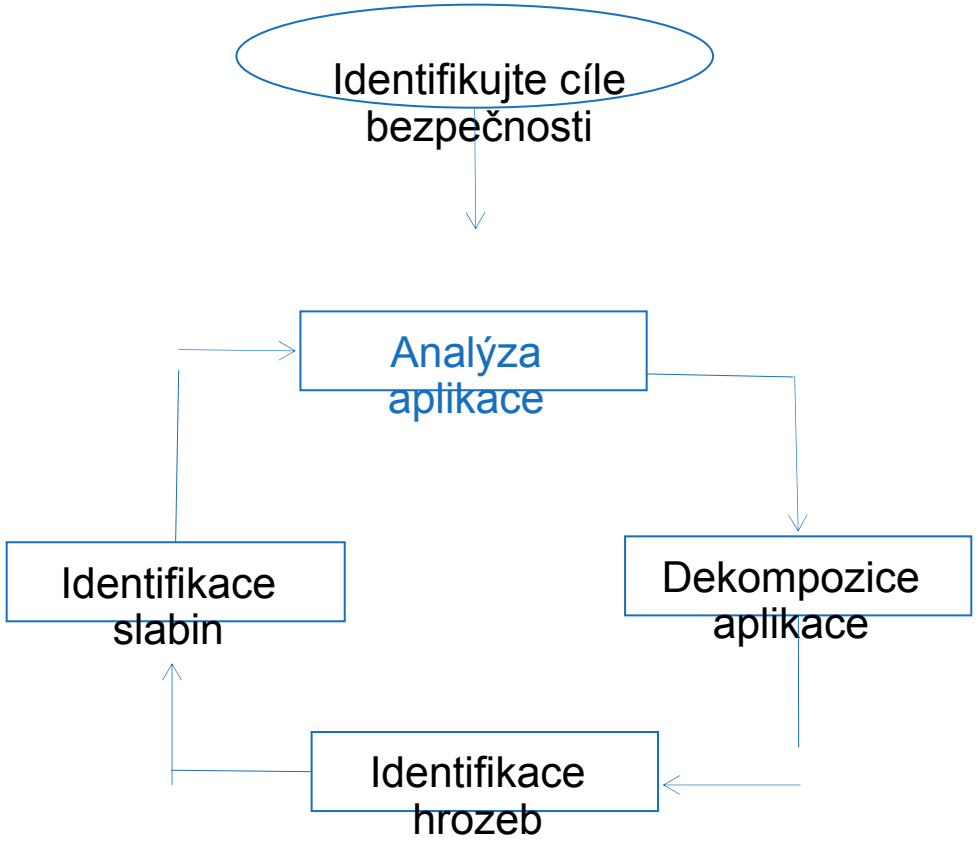
Cíle bezpečnosti

- Zamezit:
  - Krádež identity
  - Ohrožení reputace
  - Finanční ztráty
  - Regulace, zákony
  - Dostupnost



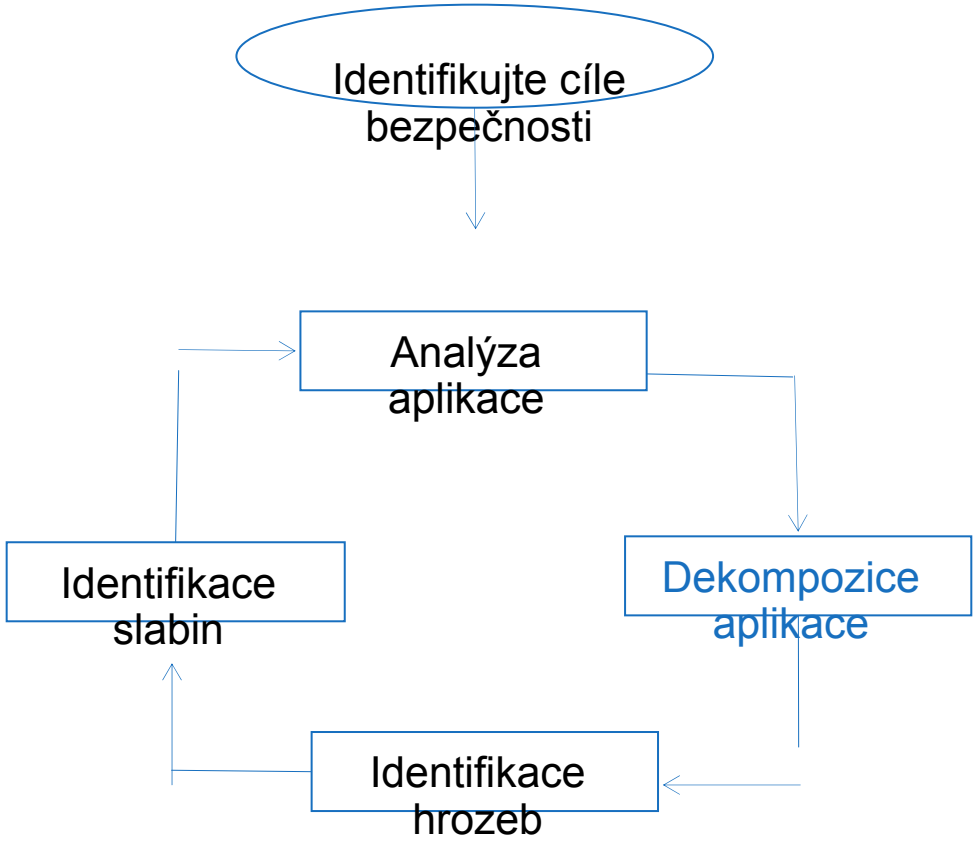
Analýza aplikace

- Komponenty
  - UML
- Datové toky
- Trust boundaries



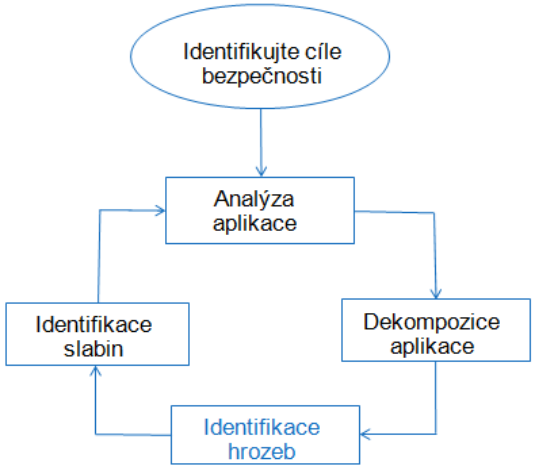
Dekompozice

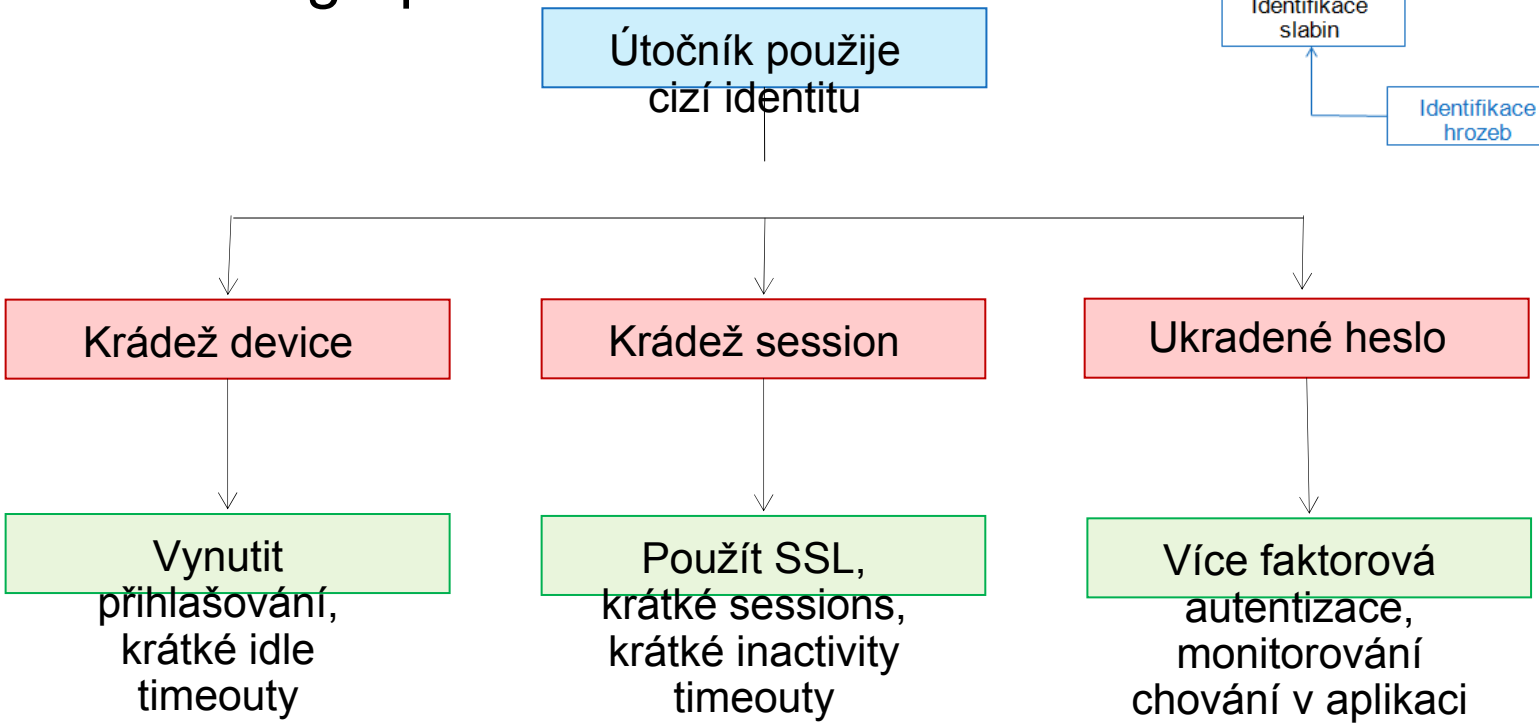
- Detailní analýza funkčních modulů
- Dělají validaci dat? Ukládají data? Audit?



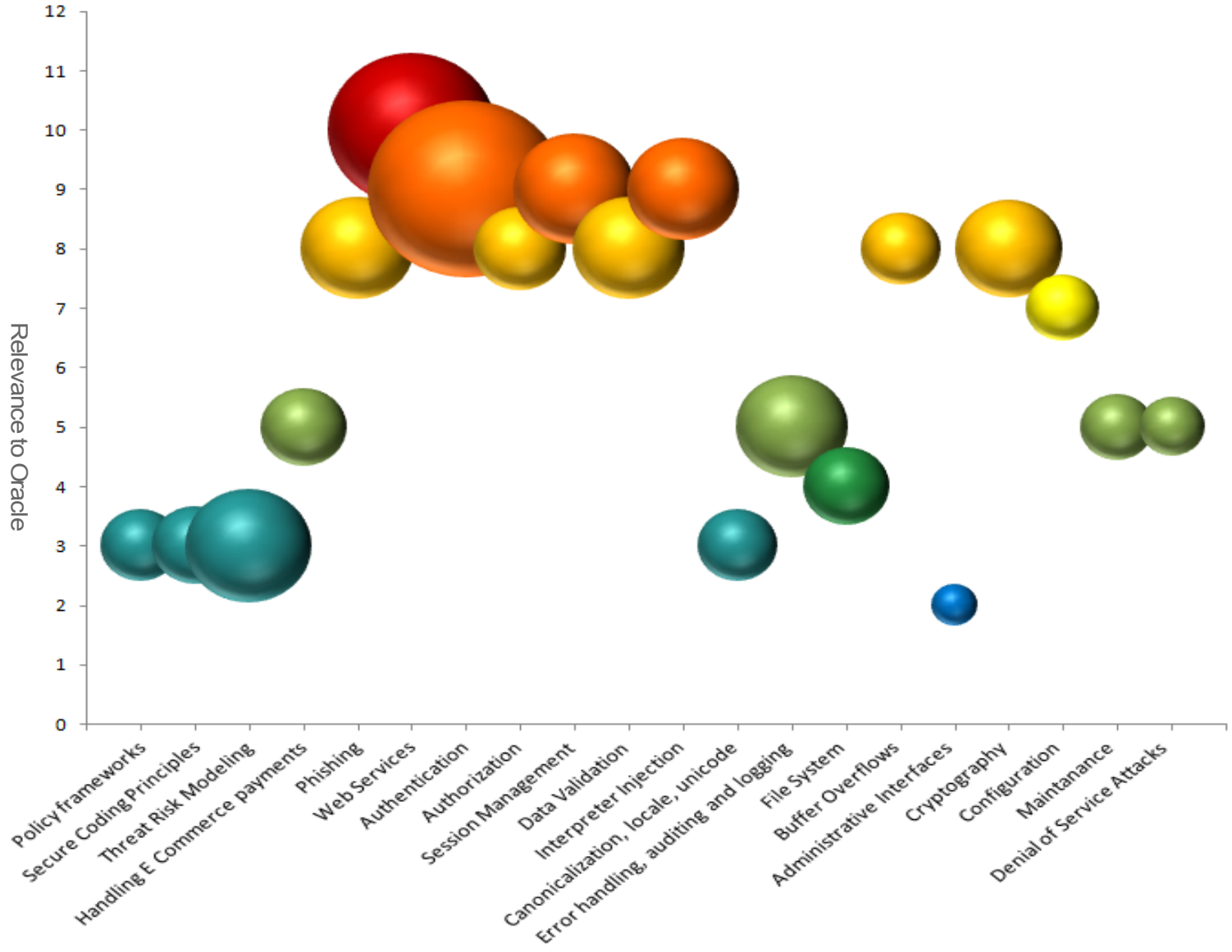
Hrozby

- Threat graph





Hrozby a jejich pokrytí technologiemi Oracle



Klíčové softwareové technologie

- Oracle Identity a Access Management
  - Autentizace
  - Autorizace
  - Správa sessions
  - Vícefaktorová autentizace
  - Monitorování chování v aplikacích
  - Audit
  - Správa životního cyklu identit
- Oracle Middleware
  - Java, Weblogic, bezpečné web servery
- Aplication Development Framework

Oracle systems

- SPARC T4
  - Krypto akcelerace
  - Využívá ji Solaris
  - Využívá ji Java
  - SSL, encryption, digest, signatures, vše „zdarma“
- Virtualizace, LDOMs, Zones
- RBAC, Solaris Trusted Extensions
- ZFS

- Exalogic
- Exadata

Shrnutí

- Spousta rizik
- Nad bezpečností je třeba se zamyslet
- Oracle poskytuje špičkové technologie od HW po Software a služby
- Oracle Consulting dodává bezpečnostní projekty