Webové služby a bezpečnosť

Jan Jusko

Obsah

- Druhy bezpečnosti
- Základné pojmy
- Modelovanie hrozieb
- Metriky závažnosti zraniteľností
- Protiopatrenia

Webové služby a bezpečnosť

- nasadenie väčšinou vo veľkom merítku
- citlivé aplikácie
  - e-commerce, e-health, sociálne siete
- dynamické prostredie s heterogénnymi platformami
- propagované výhody SOA sú často rizikom pre bezpečnosť
  - lepšia prístupnosť dát, dynamická konfigurácia, autonómne jednotky

Druhy bezpečnosti

- Komplexnejšie ako zabezpečenie serverov
- rôzne pohľady na bezpečnosť
  - bezpečnosť správy
  - bezpečnosť servera
  - bezpečnosť klienta
  - súkromie (?)

Bezpečnosť správ

- bezpečnosť v oblasti správ pracuje s troma aspektami
  - utajenie
  - integrita
  - dostupnosť

Bezpečnosť správ (II)

- kryptografia
  - symetrické (DES, AES), asymetrické šifry (RSA)
  - digitálne podpisy
  - certifikáty

Bezpečnosť klienta

- využitie service discovery
- musíme zaručit, že klient prijíma autentické a správne udaje
- jednoznačná identifikácia poskytovateľa
- phishing

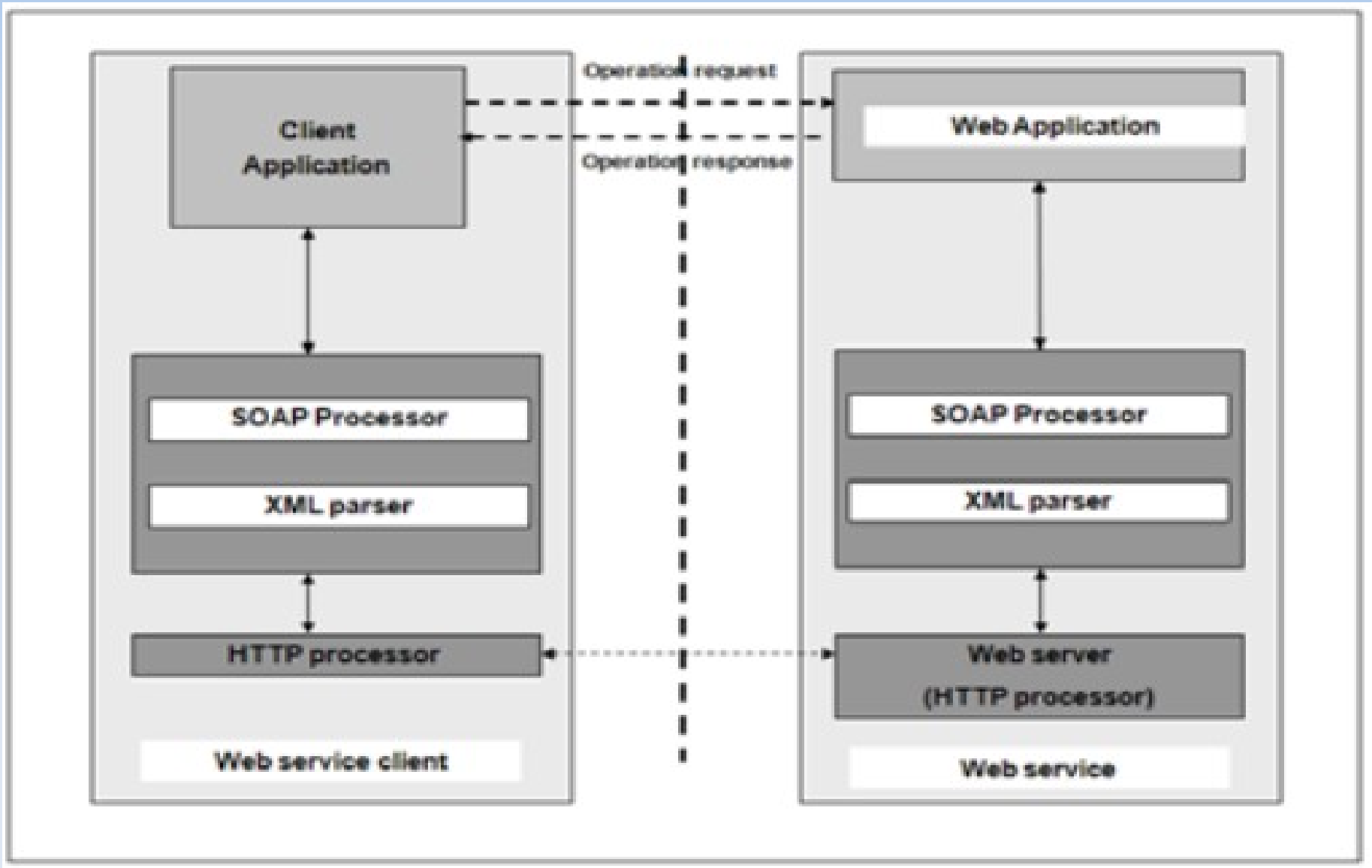
Bezpečnosť servera

- server (poskytovateľ služby) musí chrániť svoje prostriedky a dáta
  - identifikácia
  - autentifikácia
  - autorizácia
- identifikácia bezpečnostných rizík
  - modelovanie hrozieb

Bezpečnosť servera

- jedná sa o ochranu celého aplikačného servera, vrátane HTTP servera, XML parsera atp.
  - tieto sú však implementované tretími stranami
  - úloha je teda ochrániť serverovú aplikáciu
- bezpečnosť sa zohľadňuje už pri návrhu služby
  - iteračne sa upravuje podľa potreby, vrátane fázy implementácie a prevádzky

Štruktúra servera



Bezpečnosť servera (II)

- Základné definície
  - **hrozba** (threat)
  - **zraniteľnosť** (vulnerability)
  - **útok**
  - **cena útoku**
  - **incident**
  - **protiopatrenie**

Bezpečnosť servera (III)

- druhy zraniteľností
  - softwarové zraniteľnosti
    - chyba návrhu
    - chyba implementácie
  - konfiguračné zraniteľnosti
    - spustené zbytočné služby
    - nesprávna konfigurácia

Klasifikácia zraniteľností

- zranitelnosti je možné rozdeliť do niekoľkých tried
  - Validácia vstupov, autentikácia, autorizácia, konfigurácia, kryptografia, audit/logovanie, kontrola výnimiek...
- Tieto triedy indikujú hrozby, ktoré z nich pramenia

Modelovanie hrozieb

- metodológia na identifikovanie, ohodnotenie a zdokumentovanie hrozieb, útokov, zraniteľností a protiopatrení
  - dá sa aplikovať na rôzne časti celého systému
- Cieľom je minimalizovať bezpečnostné rizika počas návrhu, implementácie a prevádzky služby
- Iteračný proces
  - je zložité odhaliť všetky bezpečnostné hrozby naraz

Modelovanie hrozieb (II)

- Postup
  - identifikácia *assets*
  - definícia cieľov bezpečnosti
  - návrh architektúry aplikácie
  - bezpečnostný profil
  - identifikácia hrozieb a rizík
  - dokumentácia hrozieb a rizík
  - ohodnotenie hrozieb

Identikácia assets

- dáta, ktorými aplikácia disponuje
- dáta, ktoré nemá aplikácia priamo, ale riadi k nim prístup
- nehmotné assets, ako napr. reputácia

Bezpečnostné ciele

- Závisia na stupni požadovaného utajenia, integrity a dostupnosti
- Závisia aj na dopade prieniku do systému a zneužitia *assets*

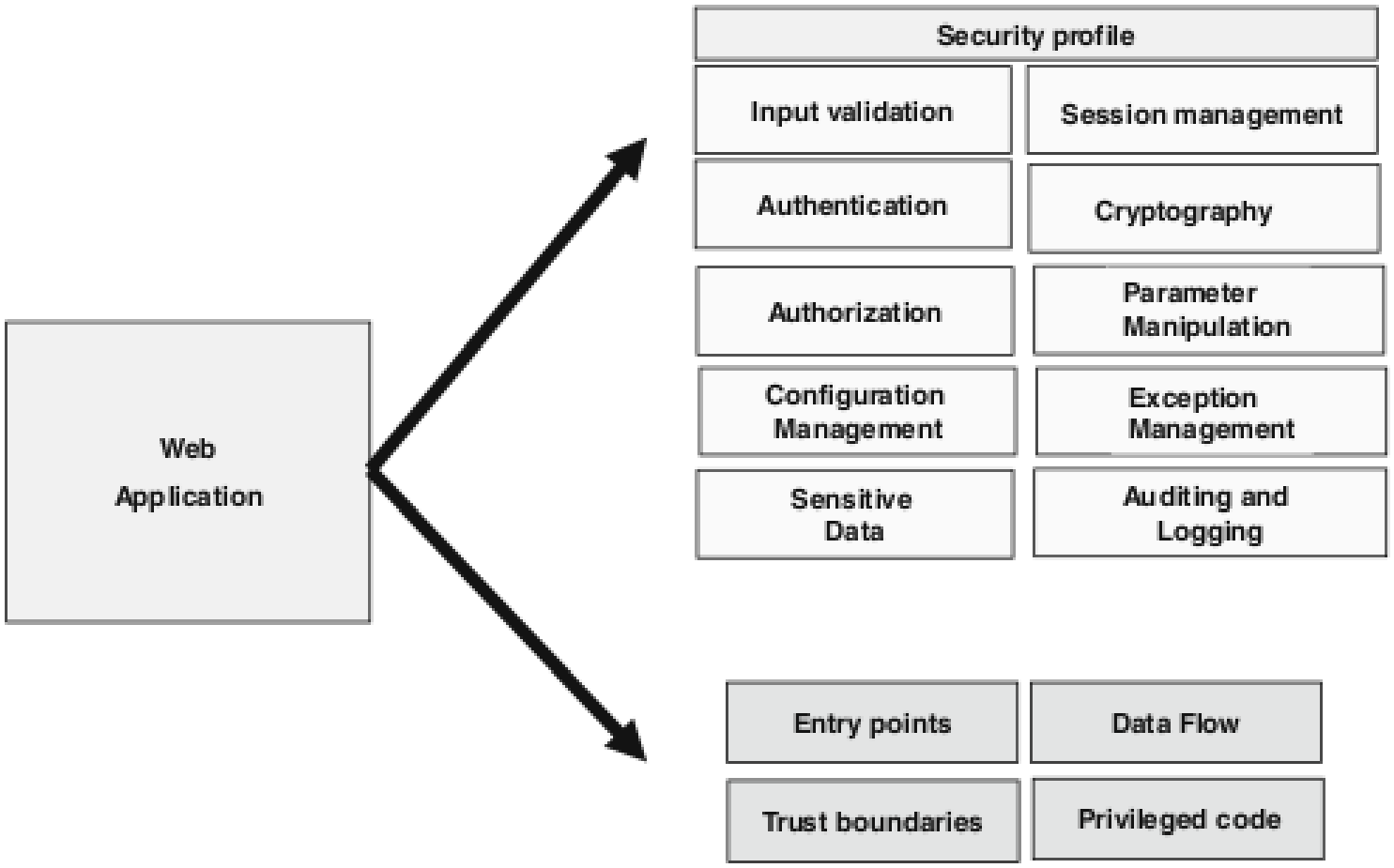
Architektúra aplikácie

- Identifikácia a zdokumentovanie
  - funkčností, ktoré bude aplikácia ponúkať
  - Architektúry aplikácie
  - fyzického nasadenia a konfigurácie
  - modulov, ktoré bude využívať

Bezpečnostný profil

- Popisuje dátove toky, privilegovaný kód, vstupné a výstupné body aplikácie
- Určuje perimeter aplikácie
- Popisuje, ktoré bezpečnostné funkcie sa budú implementovať (používať)

Bezpečnostný profil (II)



Hrozby a riziká

- Identifikácia hrozieb typických pre bezpečnostné funkcie, ktoré sa budú implementovať
- popisuje bežné postupy napadnutia
- výstupom tohto kroku sú najpravdepodobnejšie typy útokov, ktoré hrozia systému
- Rôzne kategórie hrozieb a rizík
  - spoofing, tampering, repudiation, DoS, privilege elevation (STRIDE)

Hrozby a riziká (II)

- Používajú sa aj stromy útokov
  - koreň – všeobecný útok
  - list – útok, ktorý sa uz nedá bližšie špecifikovať
  - veľké množstvo ciest
- Vzory útokov
  - Popisujú útok (potrebné znalosti, postup, predpoklady, cieľ, …)
- Katalógy rizík

Ohodnotenie hrozieb

- Určenie vážnosti zranitelnosti
- Určuje ju niekoľko faktorov
  - Zložitosť vykonania útoku, potrebné nástroje na útok, vážnosť dopadu na systém
- Neexistencia jednotnej metriky
  - Rôzne *assets* majú rozdielnu hodnotu pre rôzne organizácie

Metriky hrozieb

- Existuje niekoľko metrík na ohodnotenie hrozieb
  - Microsoft […] Severity Rating System
  - US-CERT vulnerability metrics
  - CVSS
  - SANS

Metriky - US-CERT

- Kvantitatívna metrika, 0 – 180, nelineárna
- Závisí od reportingu užívateľov
- Kritériá:
  - miera rozšírenia vedomostí o zranitelnosti
  - risk pre internetovú infraštruktúru
  - počet ohrozených systémov
  - dopad exploitu
  - zložitosť útoku
  - nutné podmienky na zneužitie exploitu

Metriky - SANS

- Critical, high, moderate & low
- Kritériá
  - miera rozšírenia napadnutého produktu
  - jedná sa o server alebo klienta
  - vyskytuje sa zranitelnosť pri základnej konfigurácii
  - ovplyvnené assets a infraštruktúra
  - verejná dostpnosť exploit kódu
  - zložitosť útoku

Protiopatrenia

- STRIDE definuje základné protiopatrenia
- Môžu mať formu procesov, odporúčaní
- Počas vývoja
  - analyzátory kódu, penetračné testy, scannery zraniteľností
- Počas nasadenia
  - správna konfigurácia
- Počas behu
  - IDS, IPS
  - scannovanie zraniteľností