Sigurnost operacijskih sustava i apikacija

Modeliranje prijetnji

Martin Subotić, 4.4.2025.

Pitanja

- Što je modeliranje prijetnji?
- Koji je glavni razlog korištenja modeliranja prijetnji?
- Koji su zadaci eksperta modeliranja prijetnji?
- Koji su koraci tipičnog projekta modeliranja prijetnji?
- O čemu govori manifest modeliranja prijetnji?

Motivacija

- Aplikacija koja ne mari za zaštitu od prijetnji će podleći tim prijetnjama
  - Eliminiranje ranjivosti **prije** ulaska u produkciju
- Rano prepoznavanje ranjivosti sustava – ne čeka se napad
- Granice sigurnog korištenja sustava
  - Korisnik mora znati u kojim slučajevima je aplikacija sigurna, a u kojim nije
  - Određivanje granica sistema

Modeliranje prijetnji

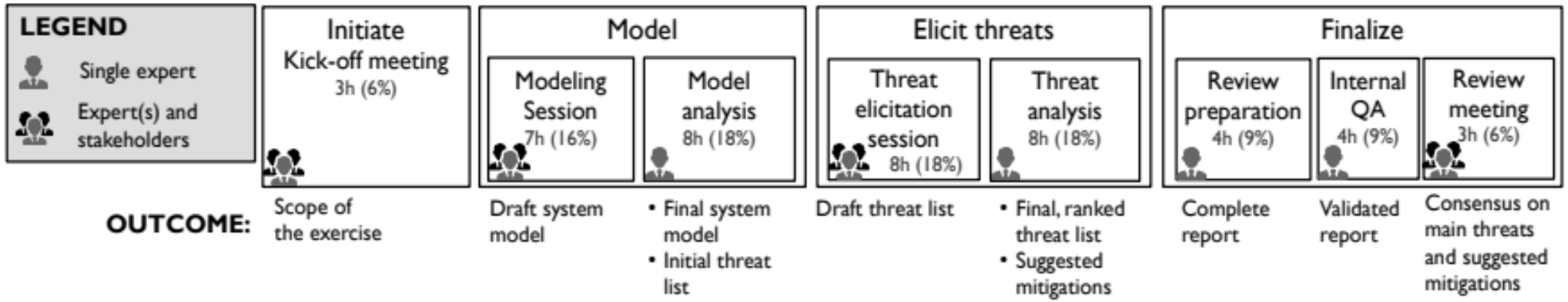
- Pojam bez jedinstvene definicije
- Proces korišten za analiziranje potencijalnih napada i prijetnji
- Pruža strukturiran način za osiguravanje softvera
  - Uključuje razumijevanje napadača i potencijalno poželjnih sredstava sustava
- Arhitektura se analizira, ranjivosti se otkrivaju i poduzimaju se mjere mitigacije

U praksi

- 4 pitanja vrijedna postavljanja
  1. Na čemu radimo?
  2. Što može poći po krivu?
  3. Što možemo napraviti u vezi toga?
  4. Jesmo li napravili dovoljno dobar posao?
- Najvažniji član projekta modeliranja prijetnji sustava je ekspert modeliranja prijetnji
  - Vodi projekt modeliranja prijetnji
  - Upoznaje dionike i ostale na projektu s prijetnjama
  - Postiže se dijeljeno razumijevanje oko sigurnosnih rizika
- Jedno modeliranje nekad nije dovoljno
  - Vođenje dokumentacije projekta je bitno u slučaju ponovnog provođenja projekta **VRLO PREPORUČIVO!**

Koraci modeliranja prijetnji

1. Određivanje ciljeva projekta s dionicima
2. Kreiranje modela sustava
3. Otkrivanje prijetnji i njihovo analiziranje
4. Pregled rangiranih prijetnji te provjera kvalitete rezultata s dionicima



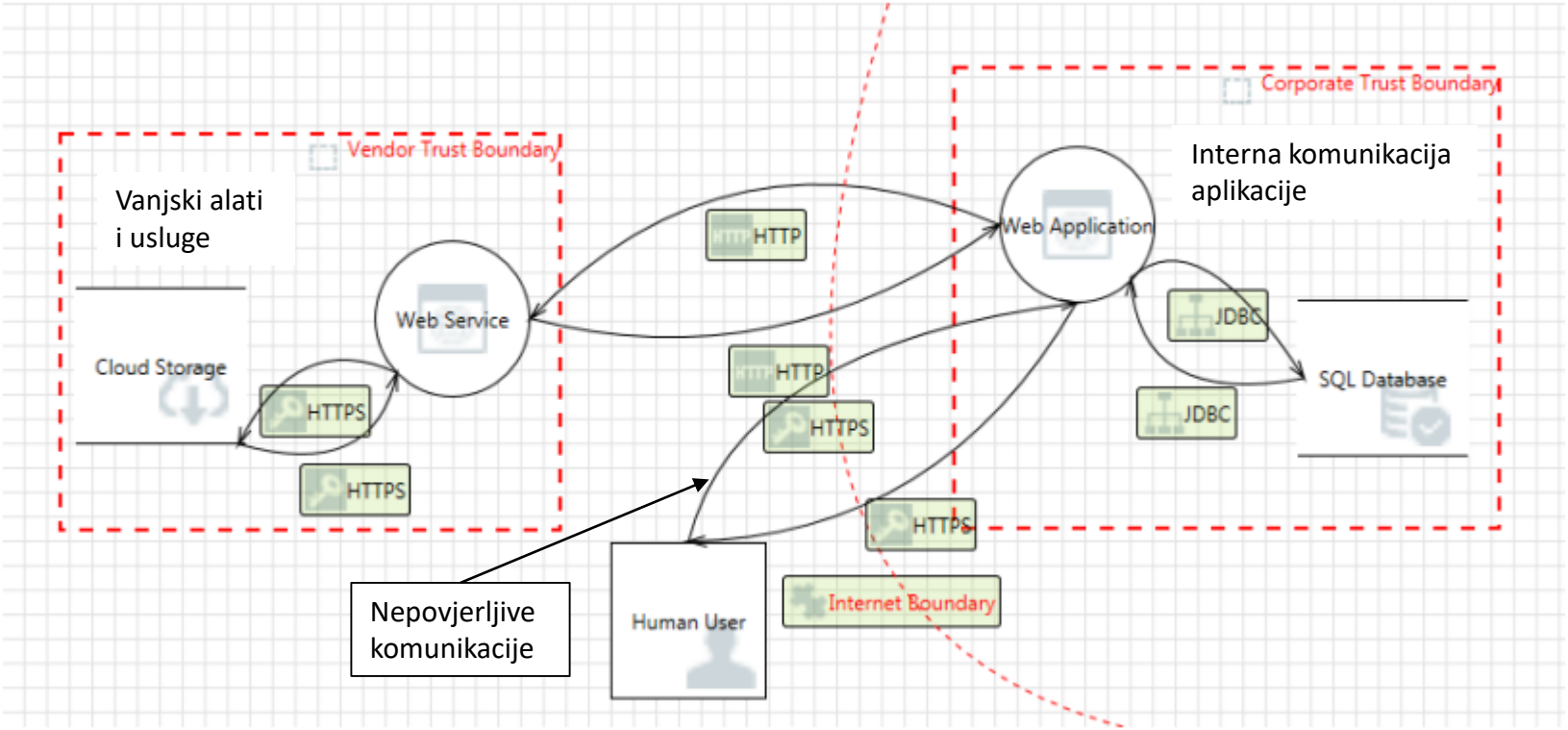
Slika 1: Generični koraci modeliranja prijetnji

Tipovi modeliranja prijetnja

- Ručno i automatsko modeliranje prijetnji
- Formalno i grafičko modeliranje
  - Formalno – temeljeno na matematičkim modelima
  - Grafičko – putem grafova napada ili tablica
- Većinom se koriste ručne metode koje grafički prikazuju prijetnje
- Modeli
  - STRIDE
  - PASTA
  - Stabla napada
  - Persona non Grata
  - LIDDUN

Dijagram toka podataka

- Ukazuje na povezanosti različitih dijelova sustava
  - Kakvi napadi zahvaćaju koje dijelove sustava
  - Gdje je komuniciranje smatrano sigurnim, a gdje nije



Slika 2: Dijagram toka podataka web aplikacije

Tok podataka i granice povjerenja

- Točke unosa
  - dijelovi korisničkog sučelja gdje korisnik unosi podatke koji se pohranjuju
  - Priključne točke i fizički portovi koje treba zaštititi
- Privilegirani kod
  - Pristupa sigurnim resursima
  - Obavlja privilegirane operacije
- Granice povjerenja
  - Označavaju gdje su sigurni, a gdje nesigurni resursi
  - Operacije također mogu biti sigurne i nesigurne
  - Oprezno s kodom izvan granice sigurnosti

PASTA

- Proces za napad i analizu prijetnji
  - The Process for Attack and Threat Analysis
- Sjedinjavanje poslovnih i tehničkih zahtjeva
- Koristi u svojim koracima razne metode kao što su stabla napada i DFD (Data flow diagram)

Slika 3: Koraci PASTA-e

PASTA - koraci

1. Definiranje ciljeva
   - Poslovnih i sigurnosnih
2. Definiranje tehničkog opsega
   - Granice tehničkog okruženja, grade se arhitekturalni dijagrami
   - Zabilježavanje infrastrukture
3. Dekompozicija aplikacije
   - Slučajevi korištenja, granice povjerenja i dijagram toka aplikacije
4. Analiza prijetnji

   Scenarij napada i sigurnosni planovi

5. Analiza Ranjivosti
   - Praćenje ranjivosti
   - Mapiranje ranjivosti pomoću stabla prijetnji
   - Analiza dizajna koristeći slučajeve korištenja
6. Modeliranje napada
   - Analiza površine napada
   - Razvoj stabla napada
7. Analiza rizika i utjecaja
   - Utjecaj rizika na poslovanje
   - Prepoznavanje protumjera i analiza ostalih rizika
   - Načini mitigacije rizika

Persona non Grata

- Motivacije i vještine napadača
- Modeliranje arhetipovi ljudi koji bi napadali
  - Burno otpušteni član odjela kripto-sigurnosti
  - Smijenjeni visokopozicionirani menadžer kojem neke dozvole nisu uskraćene
  - Novozaposleni senior koji dolazi iz protivničke firme
- Lagana (i rijetka) implementacija, ali zaustavlja samo mali dio napadača
- Ljudi su oni koji su prave prijetnje

Automatiziranje modeliranja prijetnji

- Obično ručni posao
- moguće automatizirati samo dio posla
- OWASP Threat Modeling project
- Microsoft Threat Modeling tool

Manifest modeliranja prijetnji

- Kreirali ga iskusni eksperti u listopadu 2020.
- Skraćena verzija kolektivnog znanja modeliranja prijetnji
- „Ideologija” programiranja
  - Vodič kroz principe modeliranja prijetnji
- Vrijednosti:
  - Kultura uviđanja i ispravljanja dizajnerskih problema
  - Surađivanje i povezanost s kolegama
  - Put ka razumijevanju sigurnosti
  - Aktivno modeliranje prijetnji
  - Kontinuirano unaprjeđivanje

Pozitivni i negativni uzorci modeliranja prijetnji

- Uzorci koje je poželjno pratiti
  - Sistematski pristup
  - Informirana kreativnost
  - Raznolikost pogleda na projekt
  - Korisni alati
- Uzorci koje je poželjno izbjegavati
  - Junak modeliranja prijetnji
  - Prekomjerno fokusiranje na tehnikalije modela
  - Savršena reprezentacija problema

Zaključak

- Modeliranje prijetnji – labavo definiran pojam
- Potrebno je povećanje svijesti o sigurnosnim benefitima modeliranja prijetnji
  - Više informiranje o raznim metodama modeliranja prijetnji
  - I prije svega **NAČIN RAZMIŠLJANJA** koji će razumjeti kako koristiti određene metode i alate
  - Modeliranje prijetnji ne bi trebalo biti samo lista provjera kojih treba ispuniti

Literatura

- Wenjun Xiong, Robert Lagerström. „Threat modeling – A systematic literature review” Computers & Security 84 (2019): 53-69.
- Yskout, Koen, et. Al „Threat modeling: form infancy to maturity.” 2020 IEEE/ACM 42nd International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER). IEEE, 2020.
- Shevchenko, Nataliya, et al. Threat modeling: a summary of available methods. Carnegie Mellon University Software Engineering Institute Pittsburg United States, 2018.
- Shostack, Adam. „Experiences Threat Modeling at Microsoft.” MODSEC@ MoDELS 2008 (2008): 35.
- Threat modeling manifesto: www.threathmodelingmanifesto.org

Dodatna literatura

- Mellado Daniel, Blanco Carlos, e: Sanchez Luis, Fernandez-Medina Eduardo:„A systematic review of security requirements engineering”, Computer Standards & Interfaces: Vol. 32, Issue 4, June 2010, pg 153-165
- OWASP-ovi alati https://owasp.org/www-project-threat-model
- Microsoft Threat Modeling tool https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool