

**Sigurnost operacijskih sustava i aplikacija**

# **Modeliranje prijetnji: STRIDE**

Vedran Ćutić, 4.4.2025.

# Pregled predavanja

- Pitanja za ispite
- Motivacija
- Model STRIDE
- Elementi modela
- Koraci STRIDE-a
- Dijagram protoka podataka
- Microsoftov alat za modeliranje prijetnji
- Analiza sustava digitalnog bankarstva modelom STRIDE
- Prednosti i mane modela STRIDE
- Zaključak
- Literatura

# Pitanja za ispite

- Nabrojite i ukratko opišite svaku kategoriju modela prijetnji STRIDE.
- Koji su koraci projekta metodom modeliranja prijetnji STRIDE.
- Navedite prednosti i mane metode modeliranja prijetnji STRIDE.
- Kako napadači koriste *Spoofing* i *Denial of Service* te koje su metode zaštite?
- Zašto su granice povjerenja važne u dijagramima protoka podataka i kako one pomažu u identificiranju prijetnji?

# Motivacija

- Razvoj softvera složen je postupak i stoga postoje mnoge mogućnosti iskorištavanja ranjivosti softvera
- Mnogi povjerljivi podaci izloženi napadima
- Prepoznavanje kritičkih ranjivosti sustava i reagiranje prije incidenta
- Standardizirana metoda prepoznavanja potencijalnih prijetnji
- Otkrivanje sigurnosnih zahtjeva sustava i smanjivanje rizika
- Implementacija zaštitnih mjera

# Model STRIDE

- Microsoft 1999.
  - Nedostatak znanja o računalnoj sigurnosti
  - Poticaj na osviještenost o sigurnosti
- Developer-focused
- Prevencija umjesto naknadnih popravaka
- Prilagodljiv modernim arhitekturama

# Elementi modela

Prijetnja	Ugroženi sigurnosni princip	Opis prijetnje
Pretvaranje identiteta (eng. Spoofing)	Autentičnost	Krađa identiteta
Uplitanje (eng. Tampering)	Integritet	Izmjena podataka
Odbijanje (eng. Repudiation)	Neporecivost	Poricanje aktivnosti
Povreda informacija (eng. Information disclosure)	Povjerljivost	Neautorizirani pristup osjetljivim informacijama
Uskraćivanje usluge (eng. Denial of Service)	Dostupnost	Preopterećenje sustava
Podizanje prava (eng. Elevation of privilege)	Autorizacija	Zloupotreba prava namijenjenih privilegiranim korisniku

# Pretvaranje identiteta (eng. *Spoofing*) S

- Lažno predstavljanje čime se dobiva pristup povjerljivim podacima
- E-mail, telefonskim pozivom, porukama, web stranicama, IP, ARP, GPS, DNS
- **Zaštita:**
  - Višefaktorska autentifikacija(**MFA**)
  - Filtriranje e-pošte
  - Edukacija korisnika

# Uplitanje (eng. *Tampering*)

**T**

- Neovlaštena manipulacija podacima
- Man-in-the-middle
- SQL injection
- Zaštita:
  - Nadzor integriteta datoteka (eng. *File Integrity Monitoring*)
  - WAF (Web Application Firewall)



# Odbijanje (eng. *Repudiation*)

**R**

- Poricanje izvršavanja neovlaštene operacije
- Nedostatak logova
- Zaštita:
  - Digitalni potpisi
  - Nepromjenjivi (eng. *immutable*) logovi

# Povreda informacija (eng. *Information disclosure*)

- Neovlašteno ili nenamjerno otkrivanje osjetljivih podataka
- Primjeri
  - Poruke grešaka otkrivaju osjetljive podatke – potrebno osigurati da poruke budu generičke
  - Otkrivanje direktorija i njihove strukture
  - Slučajno objavljivanje povjerljivih podataka poput API ključeva na GitHub tijekom razvoja

# Uskraćivanje usluge (eng. *Denial of Service*) D

- Postupak preopterećenja mreže prometom ili zahtjevima → smanjenje performanse ili onemogućavanje pristupa
- Distribuirani napad uskraćivanja usluge (**DDoS**)
- Zaštita:
  - Napredni sustavi nadgledanja prometa
  - **AWS Shield** ili **Cloudflare DDoS**
  - Ograničavanje zahtjeva

# Podizanje prava (eng. *Elevation of privilege*) E

- Korisnik ili proces dobije veća prava pristupa nego što mu je namijenjeno
- Vertikalni i horizontalni napadi
- Zaštita:
  - Princip najmanjih prava

# Koraci STRIDE-a

## 1. Dizajn modela sustava







- Dijagrami protoka podataka modela

## 2. Identificiranje potencijalnih prijetnji i ranjivosti

- Modelom STRIDE identificiraju se potencijalne prijetnje na svakom elementu sustava

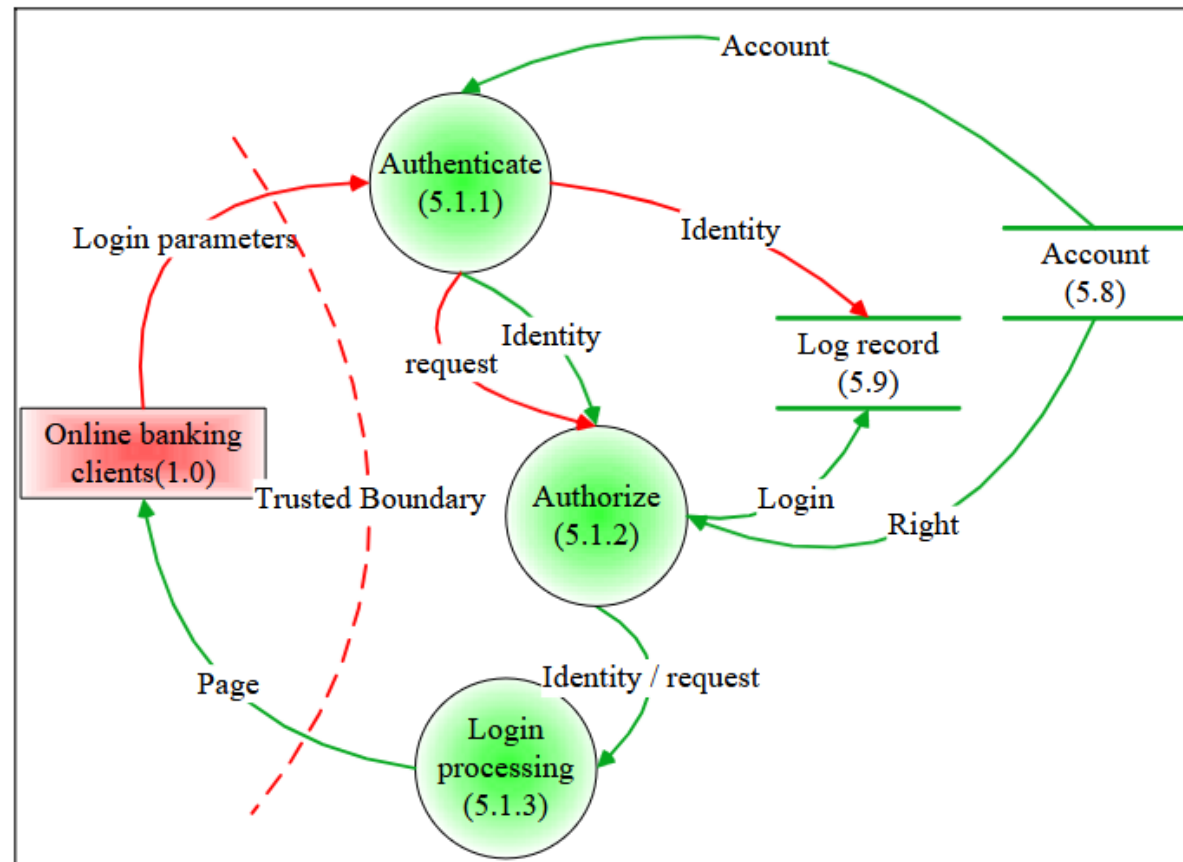
## 3. Implementacija sigurnosnih zaštita za smanjivanje rizika od prijetnji

# Dijagram protoka podataka (eng. *Data Flow Diagram*)

Symbol	Elements Name	Description
	External Interactor	Input to the system
	Process	Transforms or manipulates data
	Multiple Process	Transforms or manipulates data
	Data Storage	Location that stores temporary or permanent data
	Data Flow	Depicts data flow from data stores, processes or interactors
	Boundary	Machine, physical, address space or trust boundary.

# Dijagram protoka podataka

- Granice povjerenja omogućuju identifikaciju ranjivih točki u sustavu gdje su moguće potencijalne sigurnosne ranjivosti
- Primjer dijagrama protoka podataka za sustav digitalnog bankarstva



# Microsoftov alat za modeliranje prijetnji

- Besplatan alat koji omogućuje modeliranje prijetnji programerima i stručnjacima računalne sigurnosti
- Temeljen na STRIDE-u
- Jednostavno i intuitivno „*drag-and-drop*” korisničko sučelje
- Automatsko generiranje potencijalnih prijetnji



New Threat Model\* - Microsoft Threat Modeling Tool (Preview)

File Edit View Settings Diagram Reports Help

Diagram 1

```
sequenceDiagram
    participant HU as Human User
    participant WS as Web Server
    participant GDS as Generic Data Store
    HU->>WS: Commands
    WS-->HU: Responses
    WS->>GDS: Configuration
    GDS-->WS: Results
```

Stencils

- Generic Process
  - OS Process
  - Thread
  - Kernel Thread
  - Native Application
  - Managed Application
  - Thick Client
  - Browser Client
  - Browser and ActiveX Plugins
  - Web Server
  - Windows Store Process
  - Win32 Service
  - Web Application

Element Properties

Diagram

Name: Diagram 1

[Add New Custom Attribute](#)

Messages - No issues found

Description	Severity	Diagram	Ignore
-------------	----------	---------	--------

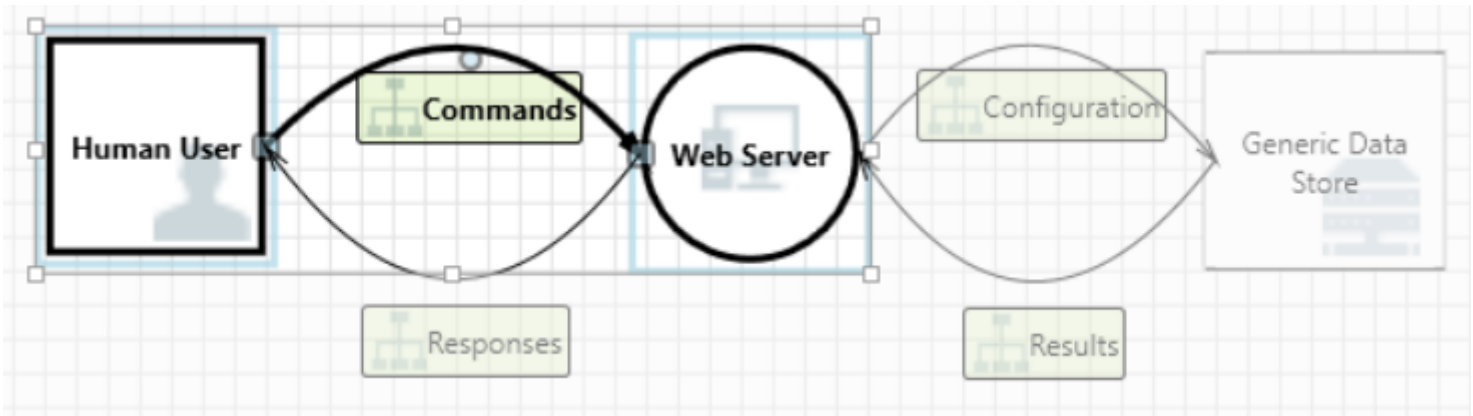
Messages - No issues found | Notes - no entries

Korisničko sučelje Microsoft alata  
za modeliranje prijetnji

ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Priority
1	Diagram 1		Generated	Not Started	Cross Site Scr...	Tampering	The web serv...		Commands	High
2	Diagram 1		Generated	Not Started	Elevation Usi...	Elevation Of...	Web Server...		Commands	High
3	Diagram 1		Generated	Not Started	Spoofing of D...	Spoofing	Generic Data...		Configuration	High
4	Diagram 1		Generated	Not Started	Potential Exc...	Denial Of Ser...	Does Web Se...		Configuration	High
5	Diagram 1		Generated	Not Started	Spoofing of S...	Spoofing	Generic Data...		Results	High
6	Diagram 1		Generated	Not Started	Cross Site Scr...	Tampering	The web serv...		Results	High
7	Diagram 1		Generated	Not Started	Persistent Cr...	Tampering	The web serv...		Results	High
8	Diagram 1		Generated	Not Started	Weak Access...	Information...	Improper dat...		Results	High
9	Diagram 1		Generated	Not Started	Spoofing the...	Spoofing	Human User...		Commands	High

9 Threats Displayed, 9 Total

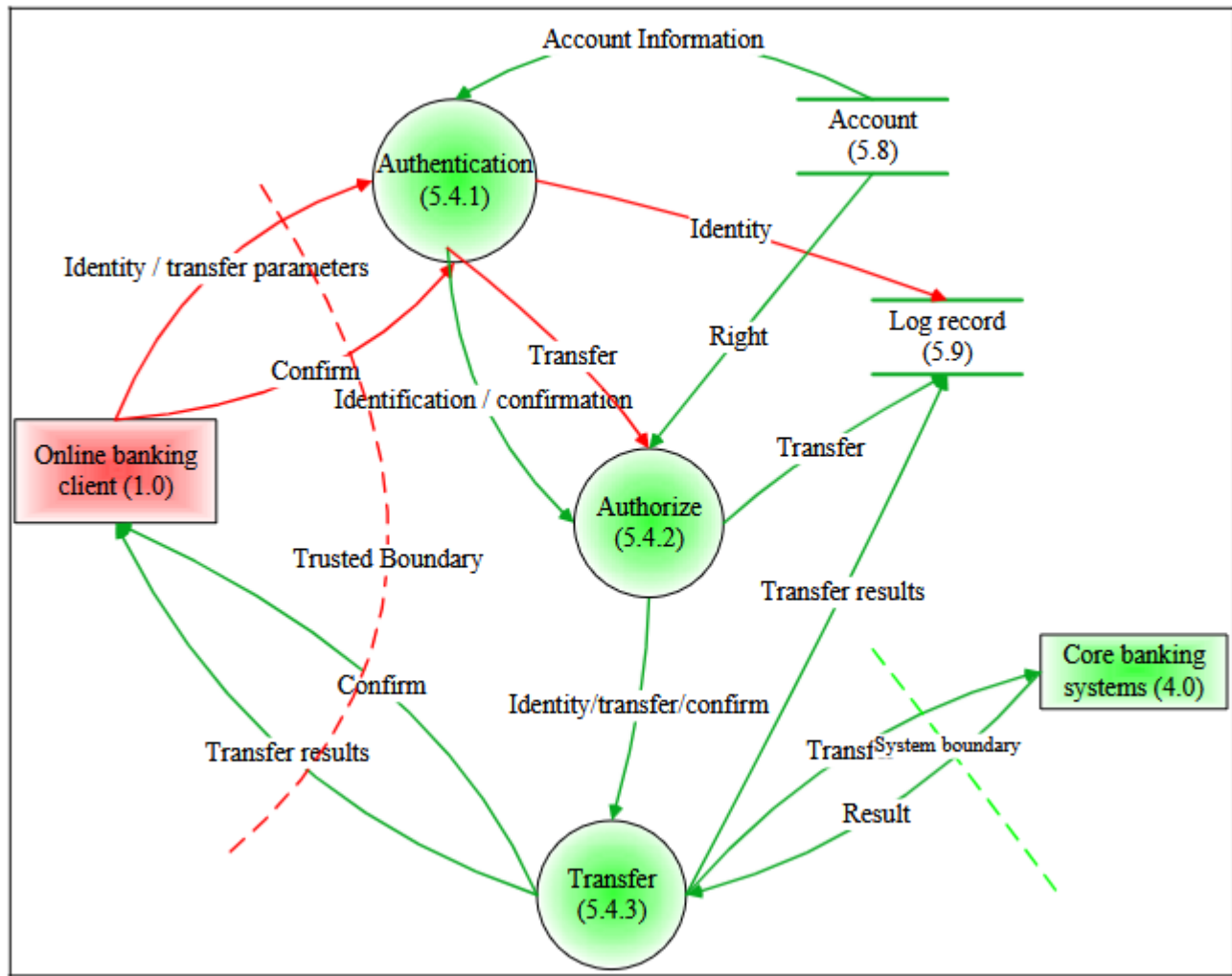
Popis prijetnji



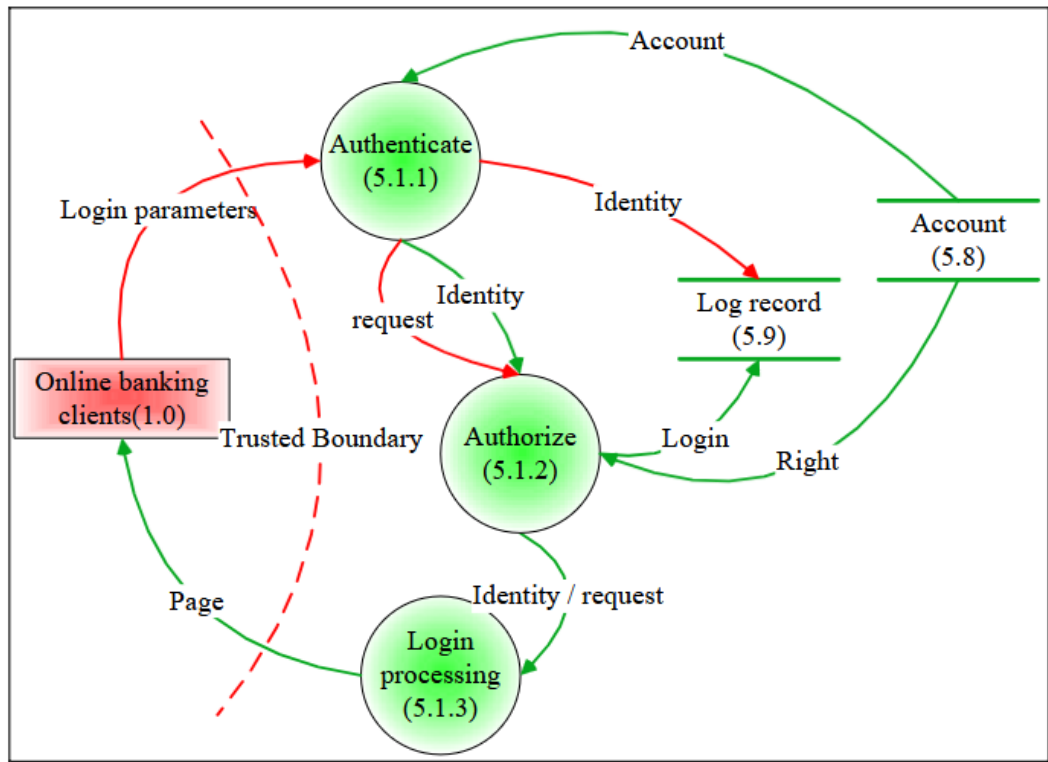
Interakcije

# Analiza sustava digitalnog bankarstva modelom STRIDE

- Sustav mora implementirati stroge sigurnosne zahtjeve zbog povezanosti s internetom
- Vanjski entiteti:
  1. Web/mobilna aplikacija - korisnik
  2. API – B2B/B2C (PayPal, KEKS Pay...)
  3. Administracija
  4. Banka



Dijagram protoka podataka procesa transakcije



Dijagram protoka podataka prijavljivanja korisnika

Kategorije	1. Aplikacija - korisnik	2. API	3. Administracija	Zaštita
<b>SPOOFING</b>	<ul style="list-style-type: none"> <li>- Krivotvorenje identiteta</li> <li>- Sigurnost lozinki (slaba ili nesigurno spremljena)</li> </ul>	<ul style="list-style-type: none"> <li>- B2B stranica je lažna („scam” ili „phishing” stranica)</li> </ul>	<ul style="list-style-type: none"> <li>- Krivotvorenje identiteta admina</li> </ul>	<ul style="list-style-type: none"> <li>- MFA</li> <li>- Edukacija korisnika</li> </ul>
<b>TAMPERING</b>	<ul style="list-style-type: none"> <li>- Napadač ugrađuje zloćudni kod – mijenja korisničke zahtjeve, pristupa povjerljivim informacijama</li> <li>- SQL injection</li> </ul>	<ul style="list-style-type: none"> <li>- B2B stranica sadrži zloćudni kod</li> </ul>	<ul style="list-style-type: none"> <li>-</li> </ul>	<ul style="list-style-type: none"> <li>- Digitalni potpisi transakcija</li> <li>- Validacija unosa</li> </ul>
<b>REPUDIATION</b>	<ul style="list-style-type: none"> <li>- Nedostatak potpisivanja i logiranja transakcija</li> <li>- Korisnici poriču transakcije</li> </ul>	<ul style="list-style-type: none"> <li>- Nedostatak potpisivanja i logiranja transakcija</li> </ul>	<ul style="list-style-type: none"> <li>- Admin briše logove</li> </ul>	<ul style="list-style-type: none"> <li>- Nepromjenjivi logovi</li> <li>- Digitalni potpisi transakcija</li> </ul>

Kategorije	1. Aplikacija - korisnik	2. API	3. Administracija	Zaštita
<b>INFORMATION DISCLOSURE</b>	<ul style="list-style-type: none"> <li>- Malware krade povjerljive informacije, snima ekran ili bilježi unos tipkovnice</li> <li>- Poruke grešaka otkrivaju detalje</li> </ul>	<ul style="list-style-type: none"> <li>- Malware unutar API-ja</li> </ul>	-	<ul style="list-style-type: none"> <li>- Enkripcija podataka</li> <li>- Generičke poruke o greškama</li> </ul>
<b>DENIAL OF SERVICE</b>	<ul style="list-style-type: none"> <li>- Preopterećenje mreže</li> <li>- Nepravilni parametri uzrokuju prekomjerno korištenje memorije/CPU</li> <li>- Zaključavanje korisničkih računa i prestanak rada aplikacije</li> </ul>	<ul style="list-style-type: none"> <li>- Preopterećenje kanala uzrokuje pad sustava za obradu transakcija</li> <li>- DDoS</li> </ul>	- Preopterećenje mreže	<ul style="list-style-type: none"> <li>- Ograničavanje broja zahtjeva</li> <li>- Cloudflare DDoS zaštita</li> </ul>
<b>PRIVILEGE ESCALATION</b>	<ul style="list-style-type: none"> <li>- Zaobilaženje autentikacije promjenom URL parametara</li> <li>- Loše definirane kontrole pristupa (korisnik dobiva administratorske ovlasti)</li> </ul>	-	-	<ul style="list-style-type: none"> <li>- Princip najmanjih prava</li> </ul>

# Prednosti i mane modela STRIDE

- Prednosti
  - Strukturirana analiza prijetnji
  - Može se koristiti u svim fazama razvoja softvera.
  - Koristi dijagrame protoka podataka što ga čini jednostavnim za razumijevanje i omogućava vizualizaciju prijetnji
- Mane
  - Vremenski zahtjevno, analizira svaki element dijagrama protoka podataka zasebno
  - Neće uvijek identificirati sve prijetnje

# Zaključak

- Model STRIDE je kvalitetan, intuitivan i prilagodljiv oblik modeliranja prijetnji koji pomaže u razvoju novih tehnologija
- Strukturiran oblik i mogućnost automatske provjere prijetnji, ubrzava cijeli proces analize rizika, ovo omogućuje programerima da:
  - Više vremena posvete implementaciji sigurnosnih zahtjeva umjesto naknadnom ispravljanju incidenata
  - Poboljšaju kvalitetu proizvoda



# Literatura

- Microsoft Threat Modeling Tool
  - <https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats>, Pristupljeno: 1. travnja 2025.
- Članci
  - Software Secured - STRIDE threat modeling, Poveznica: <https://www.softwaresecured.com/post/stride-threat-modelling>, Pristupljeno: 27. ožujka 2025.
  - Practical devsecops – What is STRIDE threat model, Poveznica: <https://www.practical-devsecops.com/what-is-stride-threat-model/>, Pristupljeno: 30. ožujka 2025.
  - Palo Alt Networks – Elevation of privilege risks, Poveznica: <https://www.paloaltonetworks.com/cyberpedia/data-flow-diagramhttps://www.ikarussecurity.com/en/security-news-en/elevation-of-privilege-eop-risks-methods-and-protective-measures/>, Pristupljeno: 30. ožujka 2025.
  - Reversing Labs – Phishing and Spoofing, Poveznica: <https://www.reversinglabs.com/glossary/phishing/>, Pristupljeno: 30. ožujka 2025.

# Literatura

- Istraživanja

- Van Landuyt, Dimitri, and Wouter Joosen. "A descriptive study of assumptions in STRIDE security threat modeling." *Software and Systems Modeling* (2022): 1-18.
- Xin, Tong, and Ban Xiaofang. "Online banking security analysis based on STRIDE threat model." *International Journal of Security and Its Applications* 8.2 (2014): 271-282.
- Scandariato, Riccardo, Kim Wuyts, and Wouter Joosen. "A descriptive study of Microsoft's threat modeling technique." *Requirements Engineering* 20 (2015): 163-180.

# Hvala!