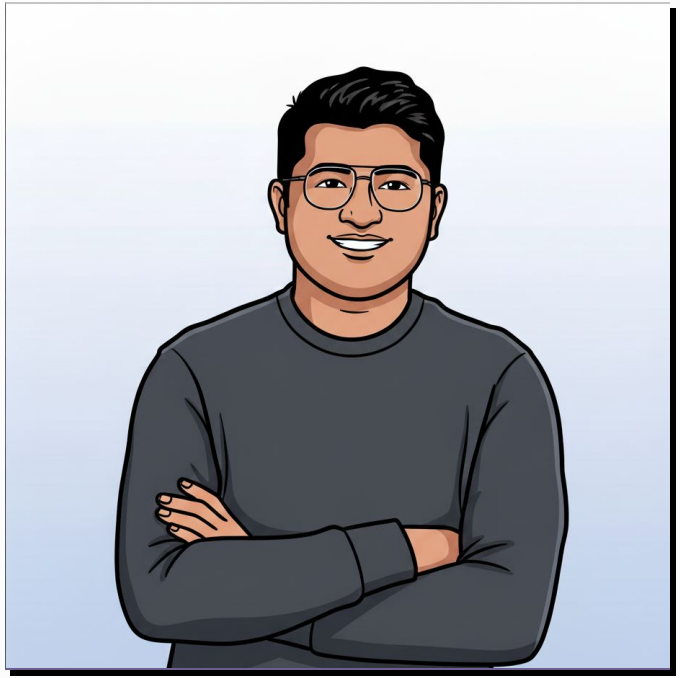
THREAT MODELLING OPENSSL BASED SYSTEMS

NARAYAN RAM NARAYANAN

._n2r_.

08 - October - 2025

Next



ABOUT

Hi! I am **Narayan Ram Narayanan**
I also go by ***._n2r_.***

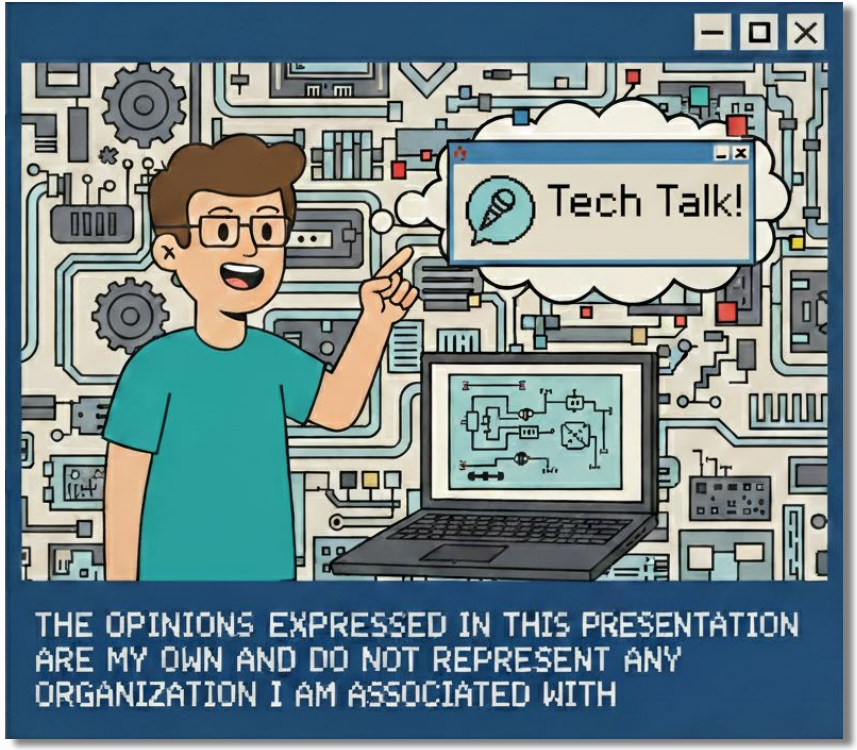
Cybersecurity Engineer @ EchoStar

Passionate about
- Linux
- Applied Cryptography
- Information Security

Back

Next

DISCLAIMER



Back

Next

CONTENTS

Back

Next

OBJECTIVE

- Understand **What** Threat Modelling is, **How** to do it and **Why** it is needed.
- Understand difference between **STRIDE** and **LINDDUN** frameworks.
- **Threat Model** SSL threats using **STRIDE/LINDDUN**.

Back

Next

THREAT MODELLING

Back

Next

WHAT ?

What is a Threat Model ?

Threat

The possibility that something bad or harmful could happen.

Model

A description used to help represent or visualize something that cannot be directly observed.

Threat Model

A description used to help represent or visualize the possibility that something bad or harmful could happen.

WHY ?

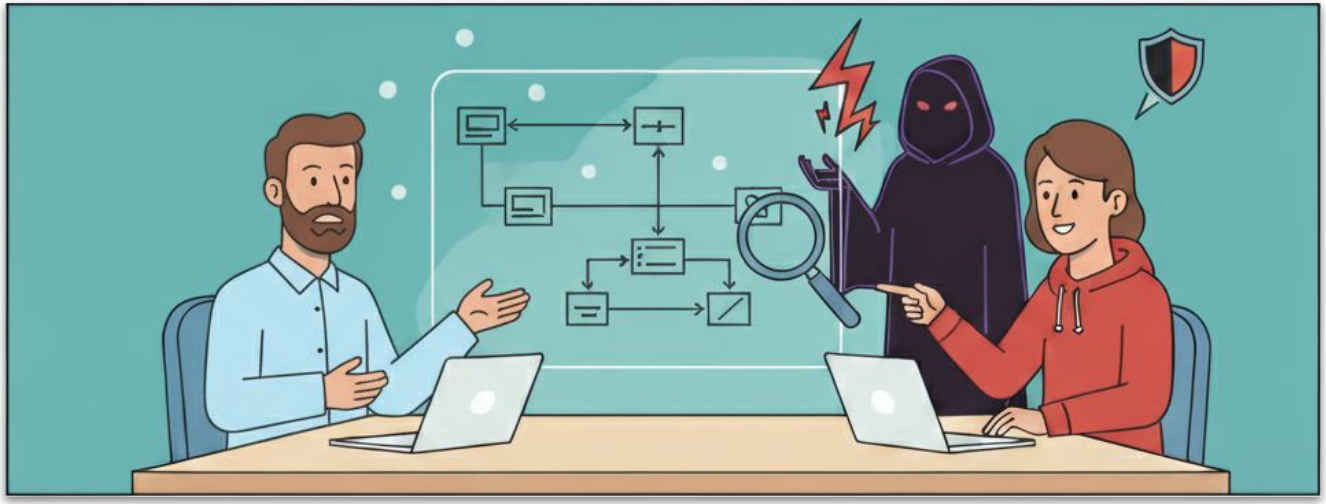
Threat modeling helps us **proactively** find and fix security flaws before they are exploited.

Why should we Threat Model OpenSSL ?

- **Foundation of Trust**
  - One of the most widely used cryptographic libraries.
  - It secures countless web servers, VPNs, and applications.

- But its **ubiquity** makes it a **high value target**.
  - **Supply Chain Risk:** A vulnerability in OpenSSL is a vulnerability in your system, even if your own code is perfect.

WHO ?



Developers, Security Engineers, Product Managers

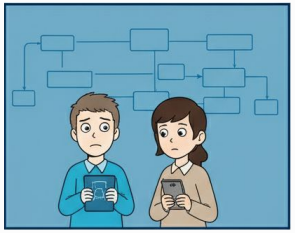
Back

Next

HOW ?

The 4 Question Framework

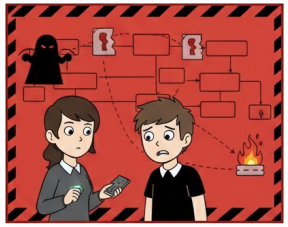
01



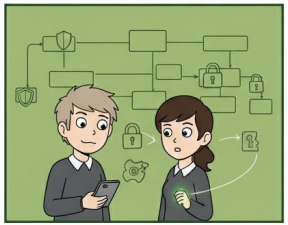
What are we working on?

02

What can go wrong?



03



What can we do about it?

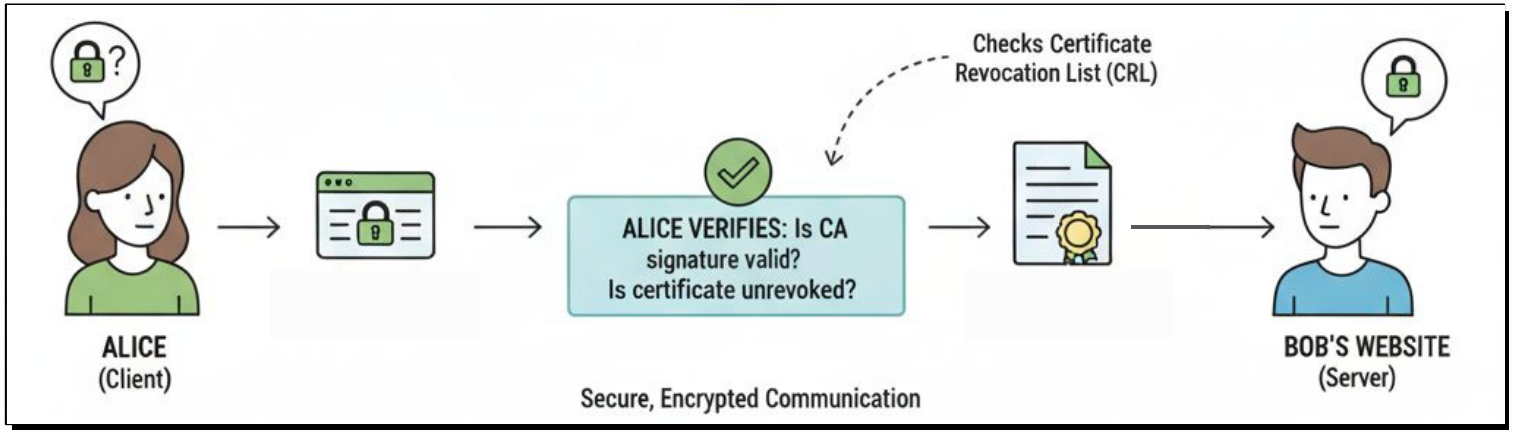
04

Did we do a good job?

Back

Next

What are we going to work on ?



Case Study (PKI, HTTPs)

Back

Next

PKI - Reference

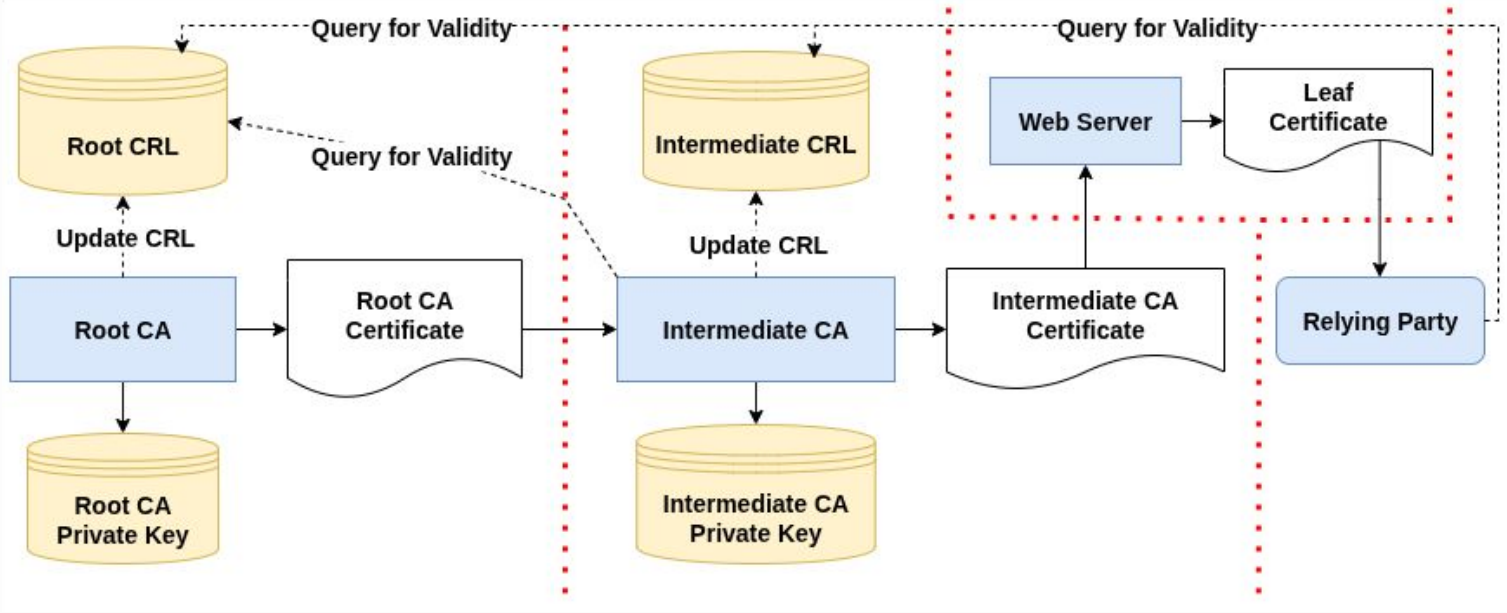
We will analyze a two tier PKI responsible for issuing certificates to web servers.

OpenSSL powers the cryptographic operations of the Certificate Authorities.

Core Security Trust Components:

- **Offline Root CA (Root Certificate Authority)**
  The ultimate source of trust. It only signs the Intermediate CA's certificate and is then taken offline for security.
- **Online Intermediate CA (Intermediate Certificate Authority)**
  The workhorse of the PKI. It issues, signs, and manages certificates for end-entities.
- **OCSP (Online Certificate Status Protocol)/CRL (Certificate Revocation List) Server**
  Provides certificate status information (revoked or valid) to clients.
- **Relying Party**
  A client (web browser) that needs to validate a server's certificate before trusting it.

DFD - Data Flow Diagram



Key Interaction: A Relying Party trusts a web server's certificate because it was signed by the Intermediate CA, which in turn was signed by the trusted Root CA.

Back

Next

What can go wrong ?

Security Oriented Threat Modelling Framework

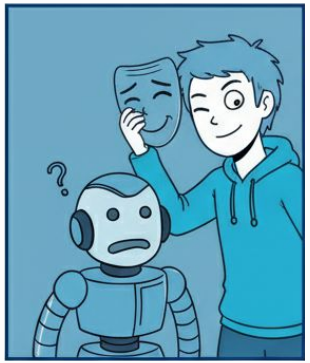
STRIDE

Spoofing, **T**ampering, **R**epudiation, **I**nformation Disclosure,
Denial of Service, **E**levation of Privilege

Back

Next

STRIDE



Spoofing

An attacker impersonates a legitimate user, server or Certificate Authority (CA)

Tampering

Unauthorized modification of data, such as a client request, server response

Repudiation

An entity falsely denies an action, and the system lacks reliable logs or cryptographic proof to refute it.

Back

Next

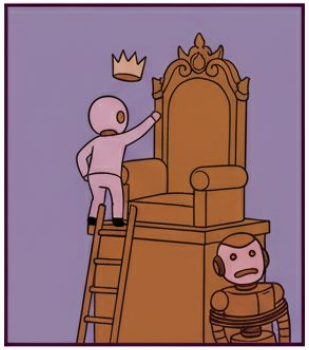
STRIDE

Information Disclosure

The unauthorized release of sensitive information

Denial of Service

Attacker prevents legitimate users from accessing the system or resources



Elevation of Privilege

An unprivileged user gains unauthorized, higher-level access or capabilities.

Back

Next

Discussion

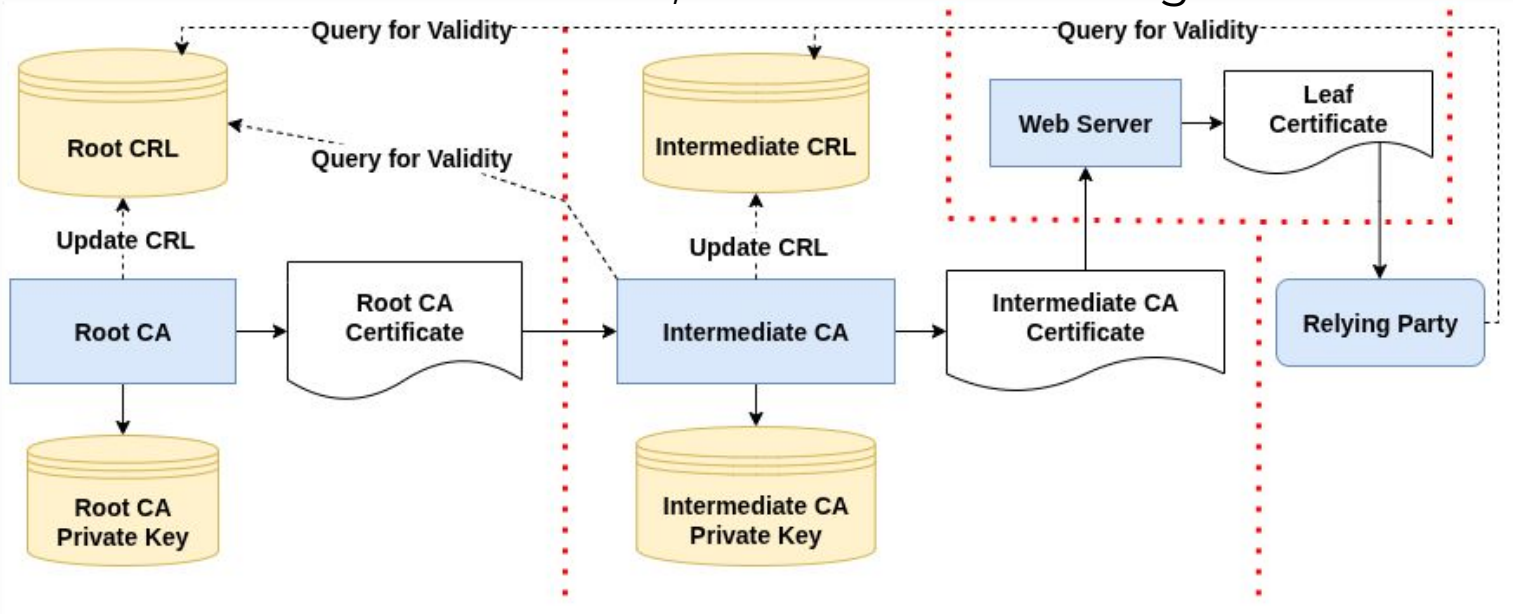
- Can we threat model the **Intermediate CA** using STRIDE ?
- Can we threat model the **Relying Party** using STRIDE?

Back

Next

STRIDE

Spoofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, **E**levation of Privilege



Back

Next

What can go wrong ?

Privacy Oriented Threat Modelling Framework

LINDDUN

Linkability, **I**dentifiability, **N**on-Repudiation, **D**etectability,

Data Disclosure, **U**nawareness, **N**on-Compliance

Back

Next

LINDDUN

Linkability

Can data items (even anonymous ones) be linked to one another to build a profile?

Identifiability

Can a data subject be identified from the collected data, even if it's pseudonymous?

Back

Next

Non - Repudiation

Can a user plausibly deny having performed a certain action or interaction?

Detectability

Can an attacker merely detect the existence of an item of interest without seeing the content?

LINDDUN

Data Disclosure

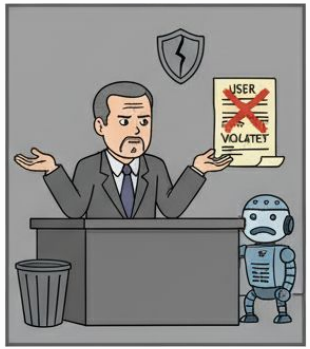
Is personal data excessively collected, stored, processed, or exposed

Unawareness

Does the system hide what it's doing with your information, and do you have any control over it?

Back

Next



Non - Compliance

Does the processing violate privacy regulations or system policies (e.g., GDPR, CCPA)?

Discussion

SCENARIO:
Our PKI issues certificates to employees for email signing and device authentication.

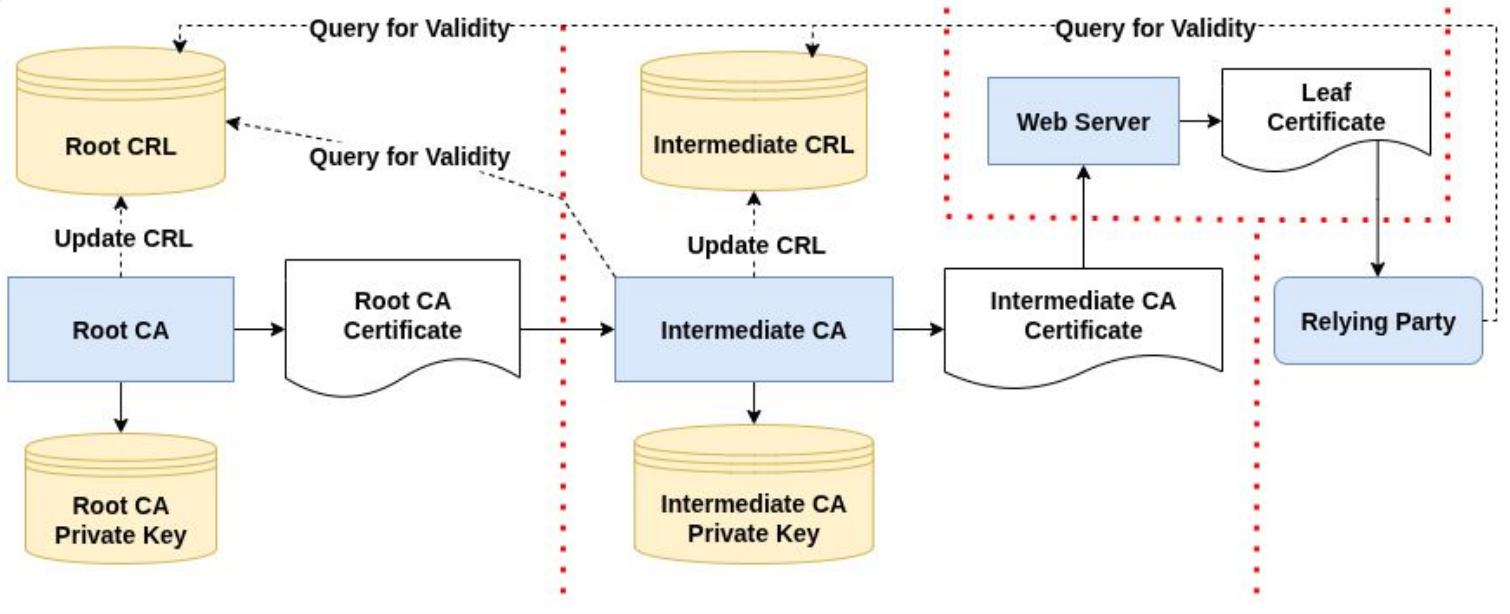
- Can we threat model the above scenario using LINDDUN ?

Back

Next

LINDDUN

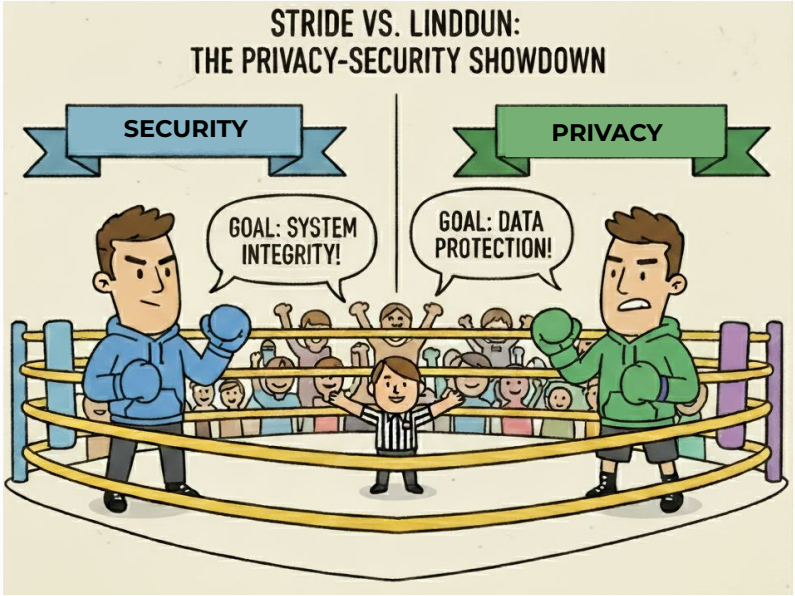
Linkability, **I**dentifiability, **N**on-Repudiation, **D**etectability,
Data Disclosure, **U**nawareness, **N**on-Compliance



Back

Next

FAQs

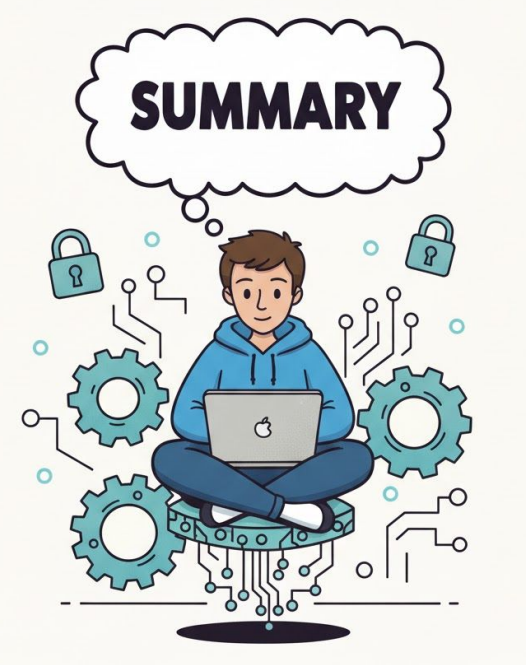


1. What's the biggest misconception between the two threat model?
2. How do the threat modeling approaches differ?
3. What's the tradeoff between accountability and privacy in PKI?

Back

Next

Summary



- What is Threat Modelling?
- Why is it important?
- Who should do it?
- How to do it?

- Threat Modelling Frameworks
  - STRIDE
  - LINDDUN

- Threat Model - 2 Tier PKI

Back

Next

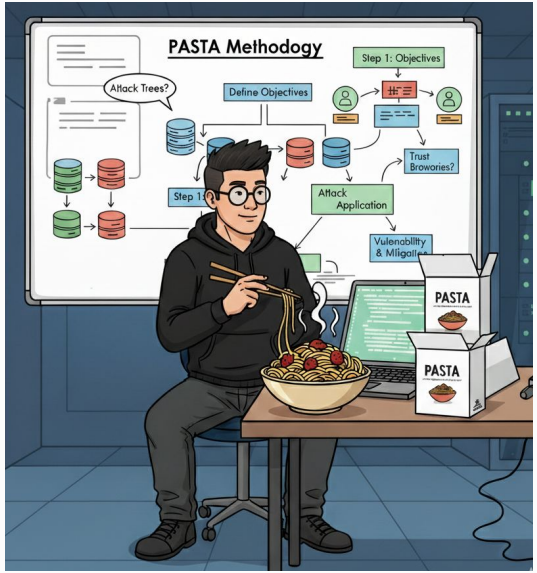
Next Steps

Implement security controls based on Threat Model.
Regularly update them as the system evolves.

PASTA

Process for Attack Simulation and Threat Analysis
Risk Centric Threat Model

1 : Definition of the Objectives
2 : Definition of the Technical Scope
3 : Application Decomposition and Analysis
4 : Threat Analysis
5 : Vulnerability/Weakness Analysis
6 : Attack Modeling and Simulation
7 : Risk and Impact Analysis

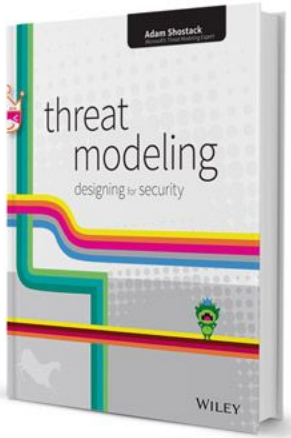


Back

Next

References

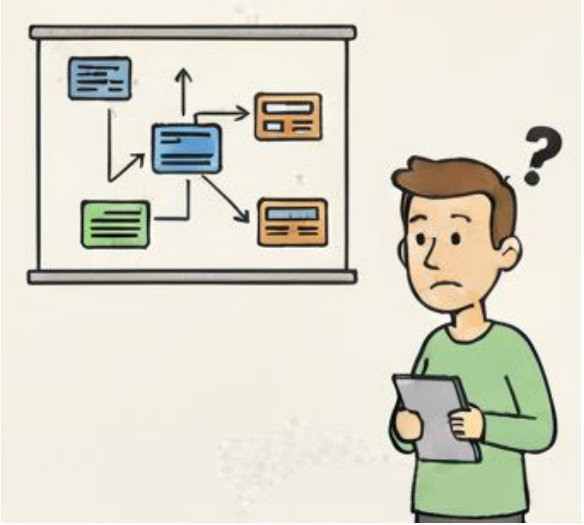
- OWASP Threat Modeling Process
- Threat Modelling Manifesto
- Threat Modeling: Designing for Security
  - EoP - Elevation of Privilege [Game]
- LINDDUN
  - LINDDUN - GO [Game]
- Threat Modelling Blog
- PASTA Threat Modelling
- PKI Fundamentals
- Microsoft Threat Modelling Tool
- OWASP Threat Dragon



Back

Next

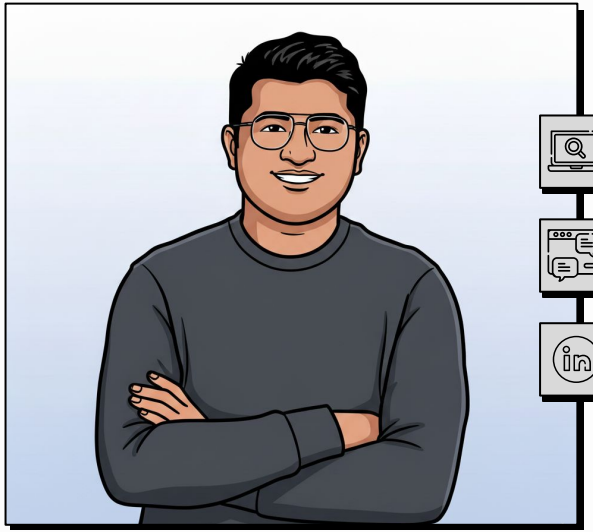
QUESTIONS?



Back

Next

CONTACT



https://narayanram-n2r.github.io/

narayanramn2r@proton.me

https://www.linkedin.com/in/n2r/

Back