Embedded Security

EECE 5698-08: Special Topics:

Cyber-Physical Security of IoT Systems in the Age of AI

Lecture 2: Threat Modeling

Prof. Kevin Fu

September 8, 2025

https://spqrlab1.github.io/emsec/

Today's Learning Goals

- How to proactively and methodically reason about embedded security with threat modeling
- How to read a research paper
- Lab safety

Pop Quiz

- Write your name on paper

Pop Quiz: Pick two of A, B, and C

Which two are NOT the four questions in Shostack's Four-Question Framework for Threat Modeling?

A) What assets do we have? What are the threats? How can we mitigate them? Did we verify the fixes?

B) What are we working on? What can go wrong? What are we going to do about it? Did we do a good job?

C) What could fail? What threats exist? How severe are they? Who is responsible?

Last Time: Security is a Negative Property of a System

- **Confidentiality**
- **Integrity**
- **Availability**
- Authentication
- Non-repudiation
- …
- What isn’t a security property?
    - Encryption: mechanism to provide confidentiality and sometimes, but not always, integrity and authentication
    - Hashing and blockchains (they are mechanisms, not properties, often misused)
    - Digital signatures and message authentication codes: mechanisms to provide authentication
- Not orthogonal! :-(

What is Threat Modeling?

- A systematic approach to identifying and mitigating security risks
- Anticipate potential threats before they occur
- Why bother? Identify design and implementation issues early.

Why Threat Modeling Matters

- Prevent security vulnerabilities
- Reduce costs by addressing risks early
- Improve system design and user trust

Key Principles

- Identify assets
- Understand potential threats
- Prioritize based on risk impact

The Four Key Questions for Threat Modeling

1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good job?

The Process of Threat Modeling

1. Define scope and context
2. Identify potential threats
3. Evaluate and prioritize risks
4. Mitigate and validate

Question 1: What Are We Working On?

- Identify assets and components
- Define trust boundaries
- Use structured diagrams to clarify system design

Identifying Assets

- Examples: Data, devices, and processes.
- Importance: Assets drive the scope of threat modeling.

Question 2: What Can Go Wrong?

- Attack Trees: Explore paths an attacker might take
- Kill Chains: Analyze stages of an attack
- STRIDE (more on this later)

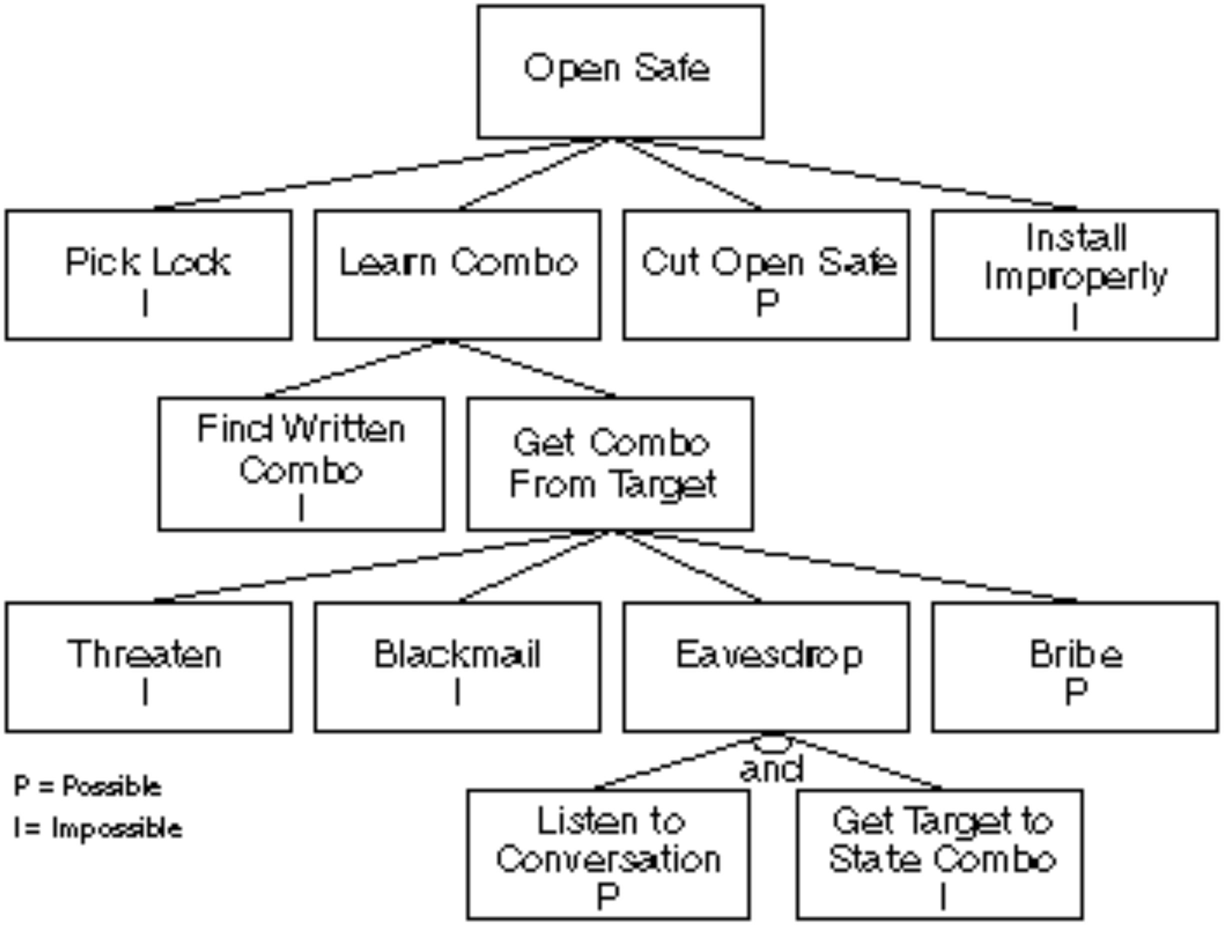
Identifying Threats: Methods

- Raw brainstorming
- Historical analysis
- Leveraging frameworks

Attack Trees

- Inspired by Fault Trees, but for security
- Top-down approach: Map attacker actions and outcomes
- Helps identify weak points in systems
- Use for prioritizing threats and mitigation strategies
- Pro: forces writing of assumptions
- Con: Can never be complete, adversary adapts

Attack Tree Example



Credit: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

STRIDE Framework

- Spoofing.
- Tampering.
- Repudiation.
- Information Disclosure.
- Denial of Service.
- Elevation of Privilege.

Question 3: What Are We Going to Do About It? Risk Management

1. Eliminate
2. Mitigate
3. Accept
4. Transfer

Risk Evaluation and Prioritization

- Likelihood
- Impact
- Mitigation costs
- ~~Probability~~

Validation and Review

- Test mitigations
- Update model as systems evolve

Mitigation Strategies

- Secure coding standards
- Encryption and access control
- Regular vulnerability assessments

Question 4: Did We Do a Good Job? (Evaluation methods)

- Internal reviews
- Security assessments and red teaming
- Updating models based on field feedback

Metrics and Evaluation

- Prioritize threats by likelihood and impact or exploitability, not probability
- Use scoring systems like DREAD or CVSS
  - Common Vulnerability Scoring System (CVSS): method used to supply a qualitative measure of severity.
  - But what can go wrong with CVSS?

https://nvd.nist.gov/vuln-metrics/cvss

https://learn.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers

Common Challenges

- Complexity of systems
- Lack of stakeholder involvement
- Evolving threat landscape

Tools for Threat Modeling

- Microsoft Threat Modeling Tool
- OWASP Threat Dragon
- IriusRisk Platform

Threat Modeling Summary

- Threat modeling helps identify, prioritize, and mitigate risks
- Incorporate it early and iteratively in your projects

How to Read a Paper

- ✓ Read critically
- ✓ Read creatively
- ✓ Take notes
- ✓ Comprehend the core thesis
- ✓ Compare with related work
- ✗ Trash the work

It’s trivial to find flaws in a paper; it’s hard to find the hidden gems.

2. How to Read a Paper

Jon Crowcroft, Cambridge

Based on CCR Article by Keshav (Waterloo)

- http://www.cl.cam.ac.uk/~jac22/talks/jon-cfip.ppt

Stand on the Shoulders of Giants

And do not stand on their toes

You read other papers so that

- You are learning what papers are like
- You are current in the field
- You may be writing survey (literature review)
- You want to find what to compare with
- We propose a 3 pass reading approach

Pass 1

- Structural overview of paper
  - Read abstract/title/intro
  - Read section headings, ignore bodies
  - Read conclusions
  - Scan references noting ones you know

Pass 1 output

- You can now say
  - Is this a system, theory or simulation paper (category defines methodology)
    - Check system measurement methodology
    - Check expressiveness/fit for purpose of formalism
    - Check simulation assumptions
  - What other papers/projects relate to this?
  - Are the assumptions valid?
  - What are the key novel contributions
  - Is the paper clear?
- Takes about 5 minutes
- 95% of reviewers will stop at pass 1 :-(
  - See Section 3 of this (on writing papers)

Pass 2

- Check integrity of paper
  - Look at figures/diagrams/exes/definitions
  - Note unfamiliar references
  - Do not check proofs yet
- Takes around 1 hour
- You should be able to summarise the paper to someone else now
- If it is unclear, you may need to pasuse overnight

Pass 3

- Virtually re-implement the paper
  - Challenge all assumptions
  - Think adversarially about experiments, proofs, simulation scenarios
  - Takes 4-5 hours
- You should be able to reconstruct paper completely now

Reading batches of papers

- E.g. for literature survey excercise
  - pick topic (hot or cold), and search on google scholar or citeseer for 10 top papers
  - Find shared citations and repeated author names - key papers (look at citation count/ impact too)
  - Go to venues for these papers and look at other papers

Homework and Next

- Homework:
  - Before Monday's lecture, read **"On the Importance of Checking Cryptographic Protocols for Faults"** by Boneh et al., EuroCrypt 1997
  - Discuss the topic freely on Piazza; use your new paper reading skills
- Next:
  - Thursday: Your first in-lab exercises!
  - Monday lecture: Refresher on signals and systems