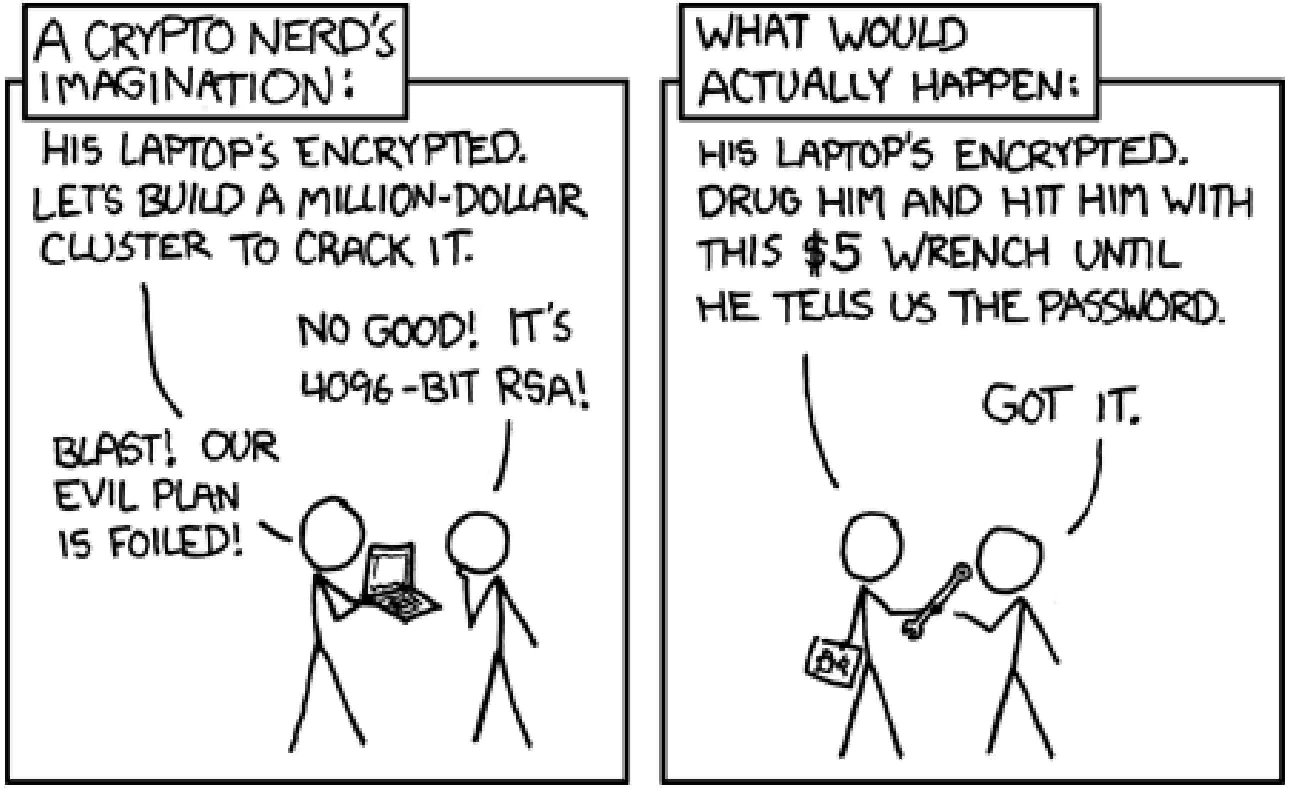
Threat Modelling

An introduction


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

What if?

Wouldn’t it be better to find security issues before you write a line of code?

Ways to find Security Issues

- Static Analysis
- Fuzzing
- Penetration Test
- Vulnerability Disclosures
- Bug Bounty Programe

..and Threat Modelling

- Think about security issues **early**!
- Understand your requirements better
- Prevent bugs before writing a single line of code

What is Threat Modelling?

Threat modelling works to **identify**, **communicate**, and **understand threats and mitigations** within the context of protecting something of **value**.

A threat model is a **structured representation** of all the information that affects the security of an application. In essence, it is a view of the application and its environment through the **lens of security**.

What does a Threat Model consist of?

A threat model typically includes:

- Description of the subject to be modelled
- Assumptions that can be checked or challenged in the future as the threat landscape changes
- Potential threats to the system
- Actions that can be taken to mitigate each threat
- A way of validating the model and threats, and verification of success of actions taken

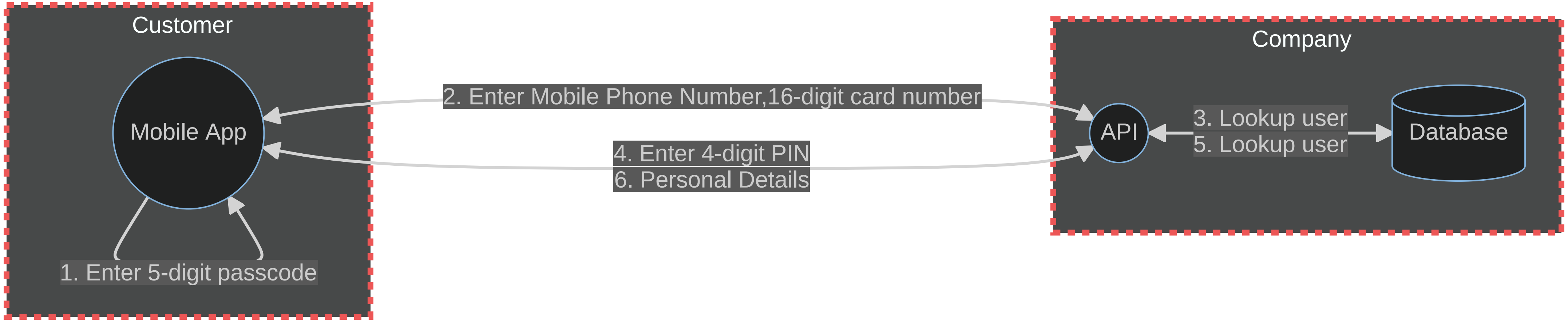
When do you do a Threat Model?

Threat modelling is best applied **continuously** throughout a software development project!

Updating threat models is advisable after events such as:

- A new feature is released
- Security incident occurs
- Architectural or infrastructure changes

How


Customer
Mobile App
1. Enter 5-digit passcode
2. Enter Mobile Phone Number,16-digit card number
4. Enter 4-digit PIN
6. Personal Details
Company
API
3. Lookup user
5. Lookup user
Database

References

- Lecture on Threat Modeling with STRIDE
- OWASP Threat Modelling
- Threat Modelling Cheat Sheet
- Threat Modelling Cookbook
- pytm: A Pythonic framework for threat modeling
- mermaid: Mermaid lets you create diagrams and visualisations using text and code
- MITRE ATT&CK: A knowledge base of adversary tactics and techniques
- MITRE D3FEND: A knowledge graph of cybersecurity countermeasures