Imperial College London

Network and Web Security

Threat Modelling

Dr Sergio Maffeis
Department of Computing
Course web page: https://331.cybersec.fun

Threat modelling

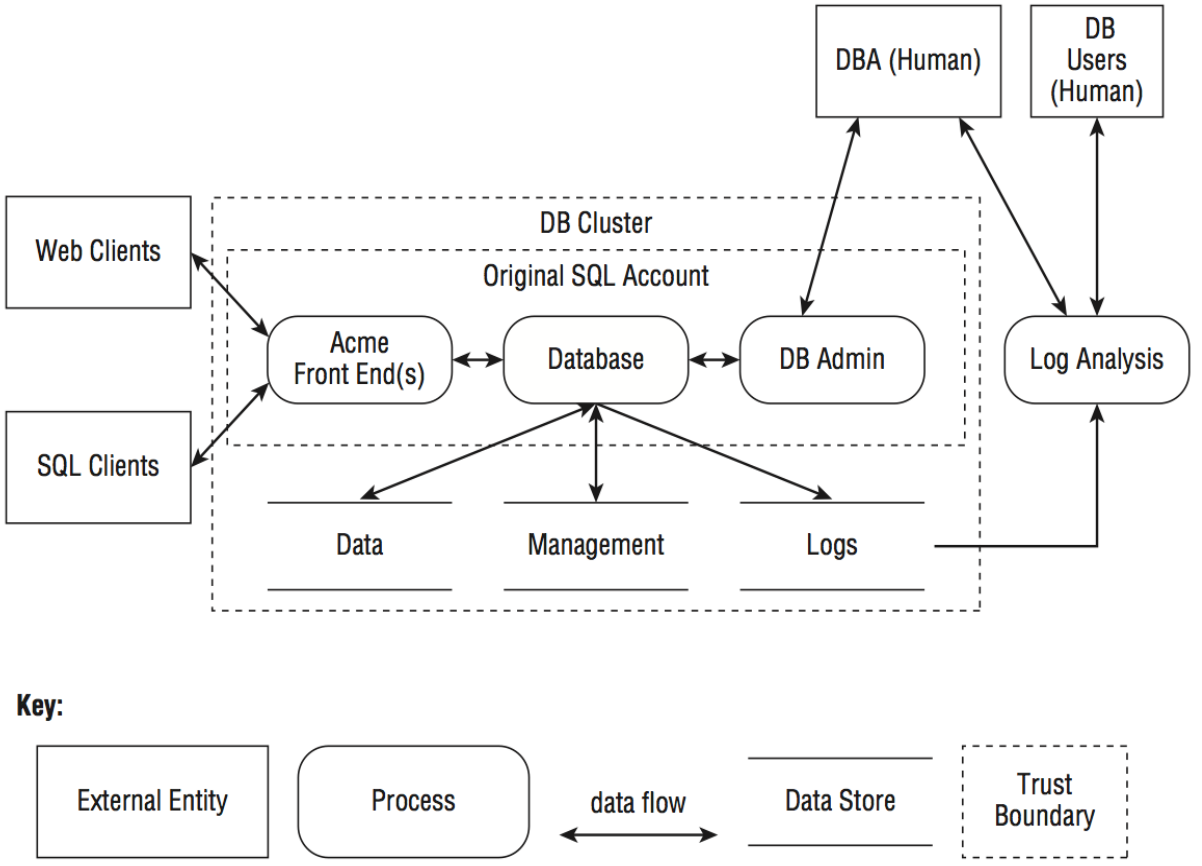
Imperial College London

- Guides decision making
  - Who are the attackers, what are their goals
  - What attacks are likely to occur
  - What security assumptions does the system rely on
  - Where to invest the security budget (time, effort, money)
- Performed on model of the system
  - Free from implementation and deployment details
  - Secure design: issues can be addressed before a system is built
  - Can guide the security review of a deployed system
- More an art than a science
  - Threat modelling is a practical activity
  - Experience is key
  - There is no single way to do it right
- Three key steps
  - Model the system
  - Identify threats (STRIDE/Attack trees)
  - Evaluate and address threats (DREAD, META)

Model the system

Imperial College London

- Use consistent visual syntax
- Alternative approaches
  - Focus on assets: password, credit card numbers, …
  - Focus on attackers: hacker, criminal, secret service
  - **Focus on system architecture**
- Data-Flow Diagrams (DFD)
  - Depict flow of information across system components
  - External entities are out of control
  - Trust boundaries help establish what *principal* controls what
  - Attacks tend to cross trust boundaries



(*Threat Modeling*, Shostack, 2014)

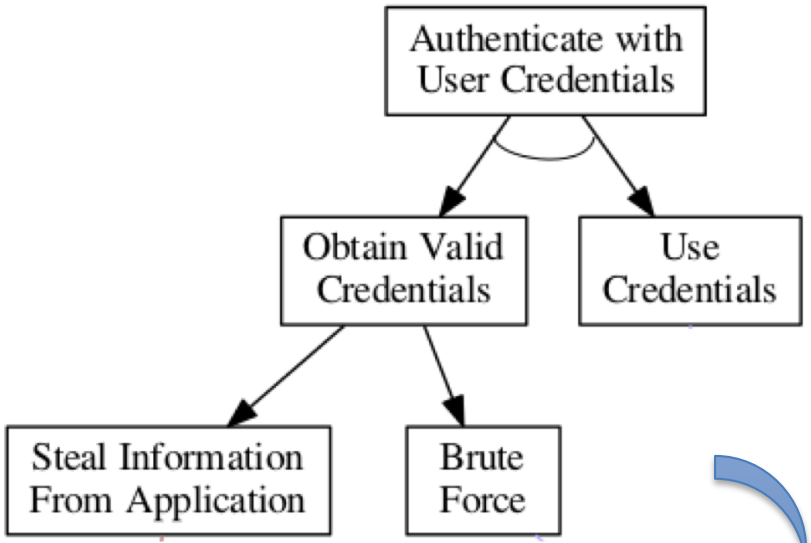
Identify threats: STRIDE

Imperial College London

- For each element in a DFD, ask “What can go wrong?”
  - **S**poofing: pretending to be something/somebody else
  - **T**ampering: modifying without permission
  - **R**epudiation: denying to have done something
  - **I**nformation Disclosure: revealing information without permission
  - **D**enial of Service: prevent a system from providing a (timely) service
  - **E**levation of Privilege: achieve more than what is intended
- Some threats may belong to more than one category
- Document threats by writing risk-based security tests (where possible).
- *Elevation of Privilege*: a card game based on STRIDE methodology
  - Was widely used at Microsoft, which now has moved on to a dedicated threat modelling tool: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

Identify threats: attack trees

Imperial College London



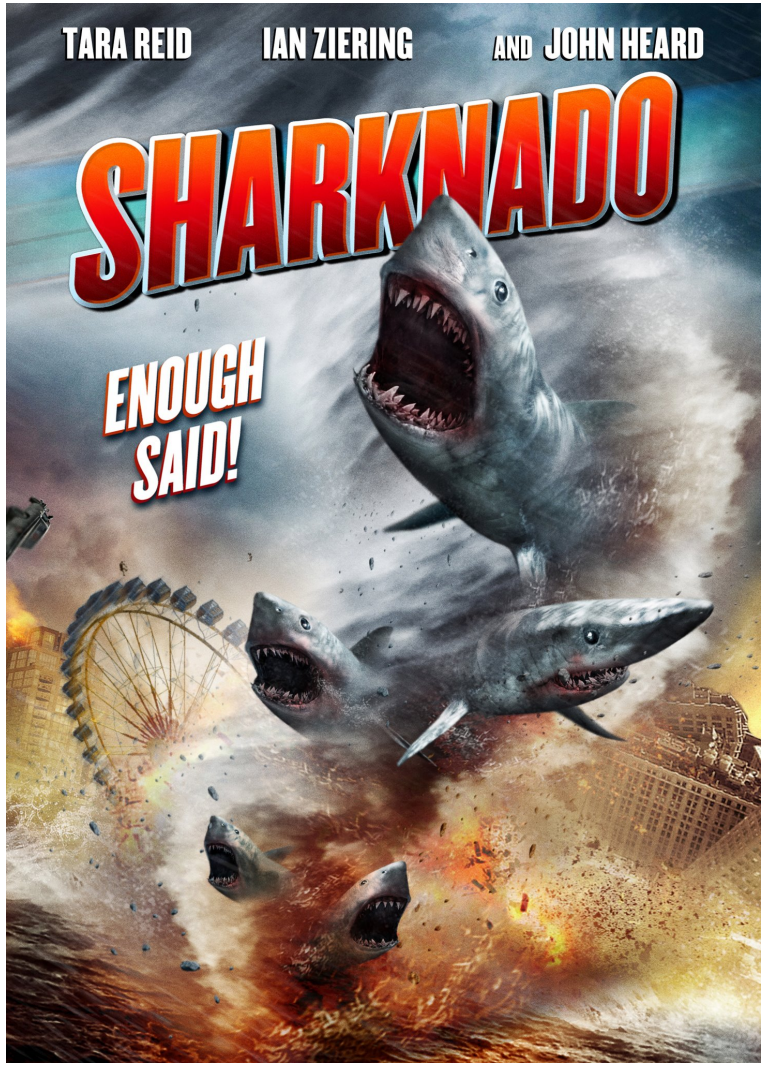
- Authenticate with credentials
  - + Obtain Valid Credentials
    - − Steal information from application
    - − Brute Force
  - + Use credentials

- Tree structure
  - Root node represent the goal of the attack, or the asset being compromised
  - Children are steps to achieve goal
  - Leaves are concrete attacks
  - By default sibling nodes represent *sufficient* steps to achieve the goal (step 1 **or** step 2)
  - Special notation for siblings that represent *necessary* steps (step 1 **and** step 2)
  - Trees have alternative textual notation
- Attack trees are an alternative to STRIDE
  - For each element in a DFD, if the goal of an attack tree is relevant, start traversing the tree to identify possible attacks
  - Attack trees capture domain-specific expertise and can be reused on different DFDs

Focus on realistic threats

Imperial College London

- Denial of service caused by sharks lifted from ocean by massive tornado
- Nuclear power plant
  - USB stick infected with Stuxnet
  - Earthquake followed by tsunami
- Email account
  - Password-guessing attack
  - Breach in online provider
  - Keylogger on user machine
- What threats should be considered depends on
  - System being modelled
  - Value of the assets being protected
  - Security budget



Evaluate threats

Imperial College London

- There are many approaches to evaluating threats
  - Qualitative: based on insight, previous experience, expectations
  - Quantitative: based on numerical score
- Beware of formulae that quantify risk
  - It's difficult to estimate realistic parameters
    - Companies are now forced to release breach data in many jurisdictions, so it may become easier
  - Black Swan problem: extremely rare events are hard to predict and quantify
- **DREAD**
  - Score each threat between 5 (lowest) and 15 (highest)
  - Designed at Microsoft, now used also by other companies

Evaluate threats

Imperial College London

	Rating	High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

(MSDN 2003)

Address each threat

Imperial College London

- Recommend a response: **META**
  - **M**itigate: make a threat harder to exploit
    - Threat: spoofing via password brute-forcing
    - Mitigations:
      - Require longer, more random passwords
      - Lock account after 3 failed attempts
      - Use biometrics instead (too expensive?)
  - **E**liminate: typically, remove the feature that was exposed to the threat
    - Longer passwords don't eliminate spoofing
    - Giving up on user accounts does (clash with business objectives?)
  - **T**ransfer: let another party assume the risk
    - We still want user accounts: "Log in with Facebook"
    - Cost: Facebook gets info about your customers
    - Technological risk may be transferred, but legal responsibility may remain
  - **A**ccept: when other options are impossible or impractical
    - Nothing can prevent a lucky hacker from guessing a password on first try
    - Important to keep track that the threat remains valid
- Cost-benefit analysis of each response depends on business objectives
- Document your response: a good way is to use project issue tracker