Principles of Security

CMPSC 403 Fall 2021

September 2, 2021

Security Mindset

Computer Security

- **Computer security** studies how systems behave in the presence of an adversary (actively tries to cause the system to misbehave).

Attacker Mindset

- **Thinking like an attacker**
  - Understand techniques for circumventing security
  - Look for ways security can break, not why it will not break
  - Look for weakest links, assumptions security depends on
- Practice!
  - When interact with a system, think about what it means to be secure and how it might be exploted

Think like an Attacker

- **Think Along:**

- How would you break into Alden?
- How would identify who was at Jan 6th event?
- How would you steal an email password?

Defender Mindset

- **Thinking like a defender**
  - Understand what is defended and against whom
  - Benefits vs. Costs (no system will be completely secure)
- Security Policy
- Threat Model
- Risk Assessment
- Countermeasures

Principle 1: Threat Models

Threat Models

- Who are the adversaries? What are their motives? Capabilities?
- What type of attacks do we need to prevent?
- What type of attacks should we ignore?

Know Your Threat Model

- **Threat model**: A model of who your attacker is and what resources they have
- It all comes down to people: The attackers
  - No attackers = No problem!
  - One of the best ways to counter an attacker is to attack their reasons
- Why do people attack systems?

Money

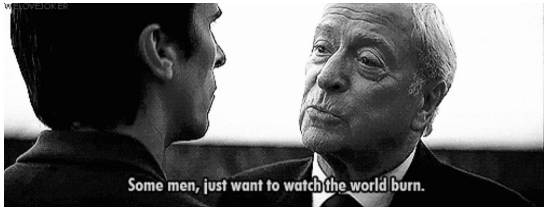
Advertisers

Politics

Anonymous

NSA

Fun



To watch the world burn

Example of Threat Modeling

Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	Magical amulets? Fake your own death, move into a submarine? YOU'RE STILL GONNA BE MOSSAD'ED UPON

Figure 1: Threat models

James Mickens "This World of Ours"

Security Principle: Know Your Threat Model

- **Think Along: Personal security**
- Who and why might someone attack *you*?

Trusted Computing Base

- **Trusted computing base (TCB)**: The components of a system that security relies upon
- Question: What would you want from a TCB?
- Properties of the TCB:
  - Correctness
  - Completeness (can't be bypassed)
  - Security (can't be tampered with)
- Generally made to be as small as possible
  - A smaller, simpler TCB is easier to write and audit.
  - **KISS principle**: Keep It Simple, Stupid

Assessing Risk: Controlled Paranoia

- What will a security breach cost?
  - Direct costs: money, property, safety, …
  - Indirect costs: reputation, future customers, …
- How likely are these costs?
  - Probability of attacks
  - Probability of success

Countermeasures

- Technical countermeasures
- Non-technical countermeasures
  - Policy, law, training, incentives, ...

Threat Modeling

- **Think Along: Should you lock your door?**

- Assets
- Adversaries
- Risk Assessment
- Countermeasures
- Cost/benefit

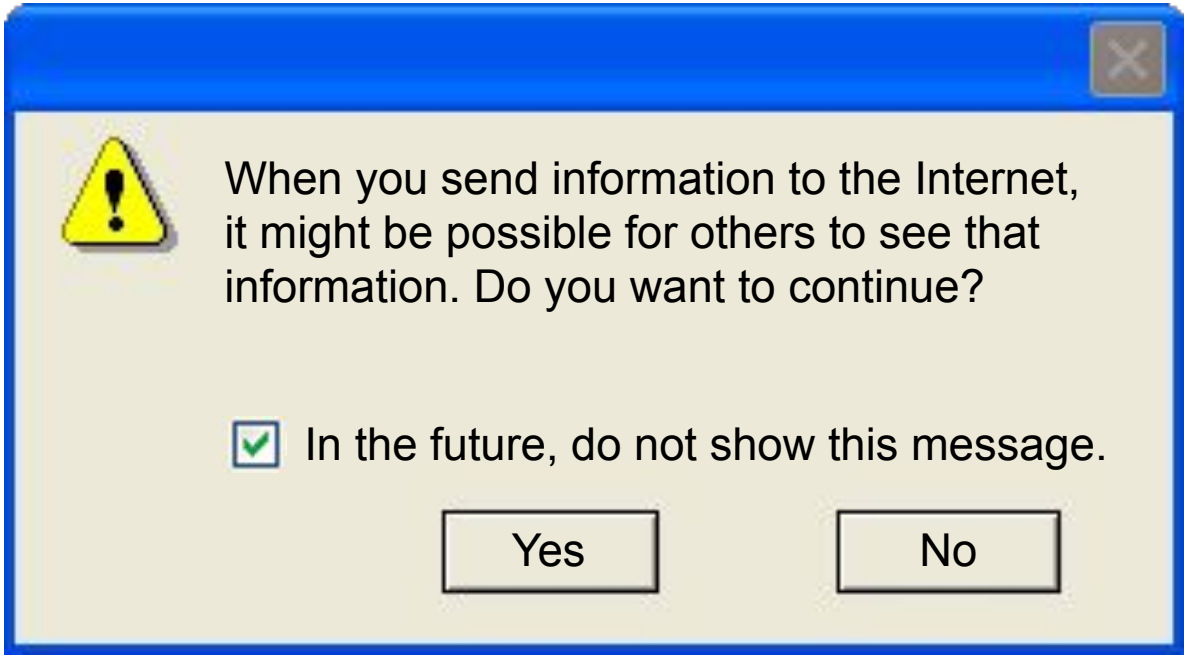
Principle 2: Consider Human Factors

It All Comes Down To People

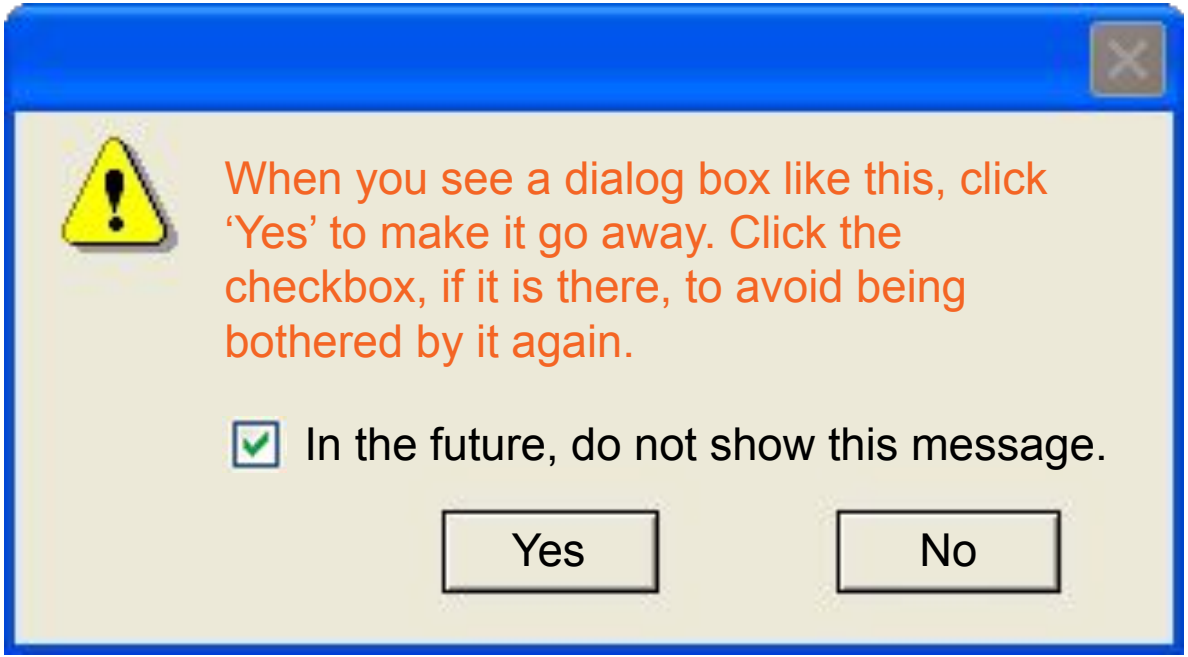
- The users
  - Users like convenience (ease of use)
  - If a security system is unusable, it will be unused
  - Users will find way to subvert security systems if it makes their lives easier
- The programmers
  - Programmers make mistakes
  - Programmers use tools that allow them to make mistakes (e.g. C and C++)
- Everyone else
  - Social engineering attacks exploit other people's trust and access for personal gain
- Consider the tools presented to users, and make them *fool*-proof

Physical security keys are designed to look like keys because humans are trained to protect keys

Warning Dialogs

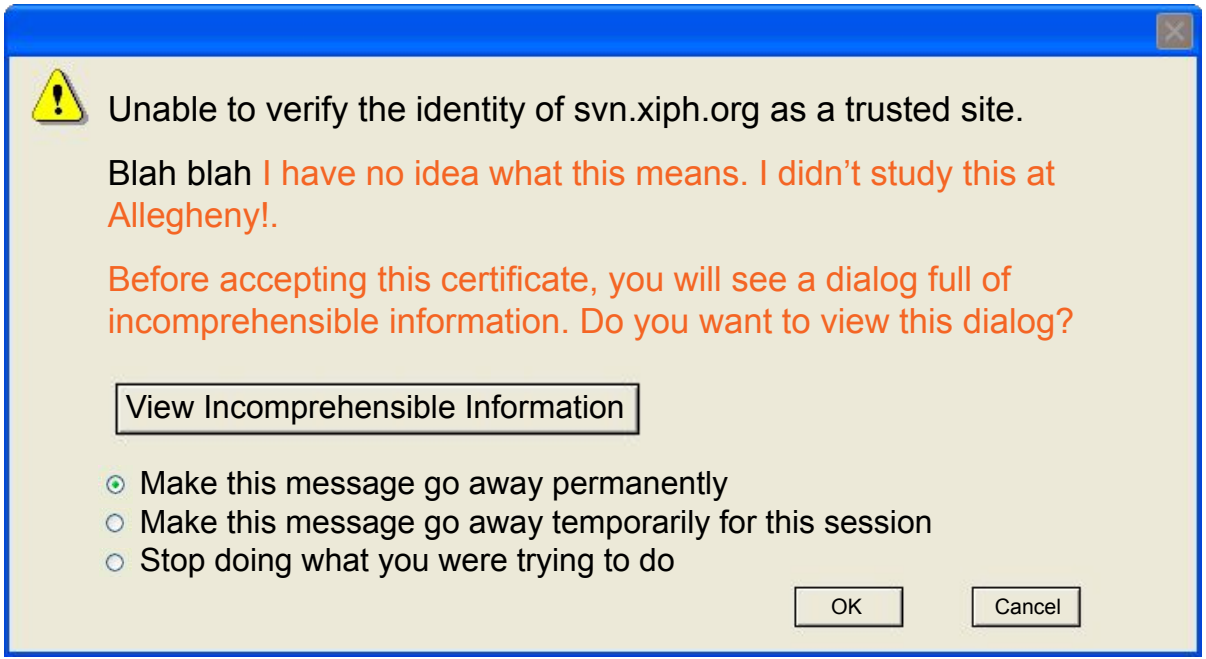


Warning Dialogs



Warning Dialogs

Warning Dialogs



Takeaway: Consider human factors