Lecture 01 – The Security Mindset

Michael Bailey
University of Illinois
ECE 422/CS 461 – Spring 2018

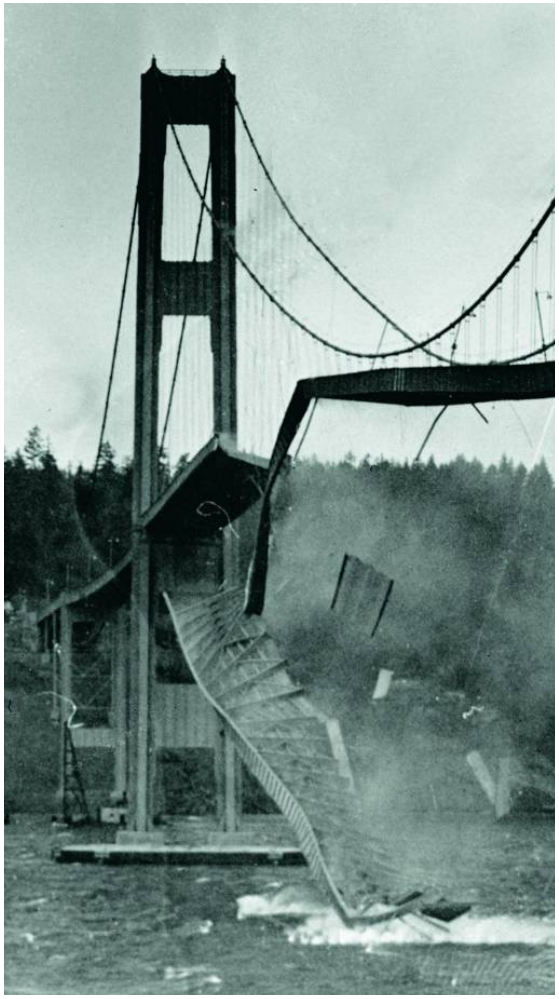
Goals for this Course

- Critical thinking
  - How to think like an attacker
  - How to reason about threats and risks
  - How to balance security costs and benefits
- Learn to be a security-conscious citizen

What is Computer Security?

- Security is a property (or more accurately a collection of properties) that hold in a given system under a given set of constraints
  - Where a system is anything from hardware, software, firmware, and information being processed, stored, and communicated.
  - and constraints define an adversary and their capabilities.
- Can also mean the measures and controls that ensure these properties
- Security is weird, as we don't *explicitly* study other properties
  - Correctness
  - Performance

What's the Difference?



Meet the Adversary

"Computer security studies how systems behave in the presence of an adversary."

- The adversary
  - a.k.a. the attacker
  - a.k.a. the bad guy

* An intelligence that actively tries to cause the system to misbehave.

“Know your enemy.”

- Motives?
- Capabilities?
- Degrees of access?

Thinking Like an Attacker

- Look for weakest links – easiest to attack.
- Identify assumptions that security depends on. Are they false?
- Think outside the box: Not constrained by system designer's worldview.

Practice thinking like an attacker:
For every system you interact with, think about what it means for it to be secure, and image how it could be exploited by an attacker.

Exercises

- Breaking into Siebel?

Thinking as a Defender

- Security policy
  - What are we trying to protect?
  - What properties are we trying to enforce?
- Threat model
  - Who are the attackers?
  - What are their Capabilities? Motivations?
- Risk assessment
  - What are the weaknesses of the system?
  - How likely?
- Countermeasures
  - Technical vs. nontechnical?
  - How much do they cost?


PARANOIA
Yes. Tiny rodents with surveillance equipment ARE watching you.

Challenge is to think rationally and rigorously about risk. *Rational paranoia.*

Security Policies

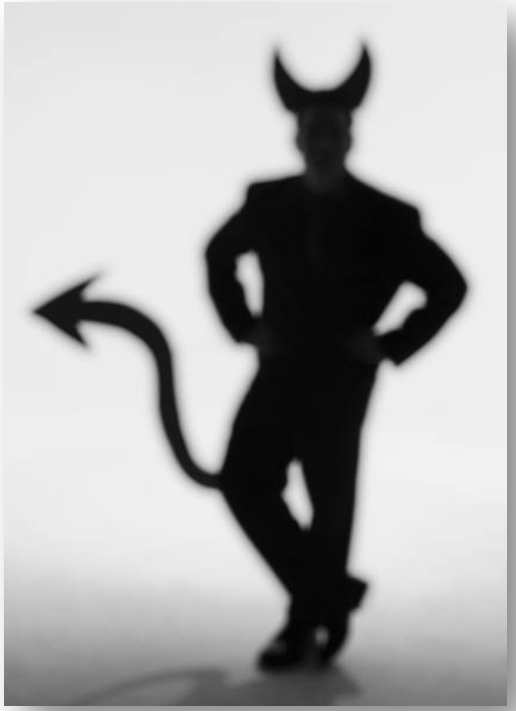
- What assets are we trying to protect?

- What properties are we trying to enforce?
  - Confidentiality
  - Integrity
  - Availability
  - Privacy
  - Authenticity

  ⋮

Threat Models

- Who are our adversaries?
  - Motives?
  - Capabilities?



- What kinds of attacks do we need to prevent?
  (Think like the attacker!)

- Limits: Kinds of attacks we should ignore?

Assessing Risk

- What would security breaches cost us?
  - Direct costs: Money, property, safety, ...
  - Indirect costs: Reputation, future business, well being, …
- How likely are these costs?
  - Probability of attacks?
  - Probability of success?
- Remember: rational paranoia

Countermeasures

- Technical countermeasures
- Nontechnical countermeasures
  - Law, policy (government, institutional), procedures, training, auditing, incentives, etc.
- No security mechanism is free
  - Direct costs: Design, implementation, enforcement, false positives
  - Indirect costs: Lost productivity, added complexity
- Challenge is rationally weigh costs vs. risk
  - Human psychology makes reasoning about high cost/ low probability events hard

Exercises

- Should you lock your bike?
  - Assets?
  - Adversaries?
  - Risk assessment?
  - Countermeasures?
  - Costs/benefits?

The Security Mindset

- Thinking like an attacker
  - Understand techniques for circumventing security.
  - Look for ways security can break, not reasons why it won't.
- Thinking like a defender
  - Know what you're defending, and against whom.
  - Weigh benefits vs. costs: No system is ever completely secure.
  - "Rational paranoia!"

To Learn More …

- The Security Mindset. https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html
- https://freedom-to-tinker.com/blog/felten/security-mindset-and-harmless-failures/
- https://cubist.cs.washington.edu/Security/2007/11/22/why-a-computer-security-course-blog/

Questions?