Lecture 1:
The Security Mindset

Ryan Cunningham
University of Illinois
ECE 422/CS 461 – Fall 2017
Security News

• Black Hat and DEFCON about 1 month ago
• Xerub releases decryption key for iOS secure enclave
• MalwareTech (Marcus Hutchins) pleads not guilty, faces 40 years in jail
• Chrome extensions hijacking on the rise
• Maersk Shipping reports $300M loss from ransomware attack
COURSE POLICIES
WARNING!

• This class is hard.
• Requires comfort with:
  1. Assembly code
  2. Architecture
  3. Operating systems
  4. Networking
  5. Scripting
  6. Web programming
Course Websites

• Course website: wiki.illinois.edu/wiki/display/CS461ECE422fall2017/
• Piazza: piazza.com/illinois/fall2017/cs461ece422
• Subversion: subversion.engr.illinois.edu/svn/fa17-cs461
• Append your netid to get to your personal svn directory
Grading

• 50% Programming Projects (MPs)
• 20% Midterm Exam (October 13\textsuperscript{th})
• 30% Final Exam (tentatively December 15\textsuperscript{th})
TO DO

• Register on Piazza
• Find an MP partner
SECURITY MINDSET
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
• Can also mean the measures and controls that ensure these properties
• Security is weird, as we don’t explicitly study other properties
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.
Assets

Things we want to protect:

- Hardware
- Software
- Data
- Communication facilities

Adversary

Someone who attacks or threatens our assets

Vulnerabilities

- A flaw or weakness in a system. Can cause system to become
  - Corrupt
  - Leaky
  - Unavailable
**Threats/attacks**

- **threat** - the potential to exploit a vulnerability
- **attack** - exploiting a vulnerability to violate security of an asset

http://www.mtv.com/movies/photos/g/Guardians_Clip/Guardians_Ball.gif
Countermeasures

Things we do to reduce threats, vulnerabilities, or attacks by preventing, minimizing, or taking corrective action

http://tvtropes.org/pmwiki/pmwiki.php/Film/GuardiansoftheGalaxy
Risk

An expectation of loss, expressed as the probability that an adversary will exploit a vulnerability with a harmful result
Why Study Attacks?

• Identify vulnerabilities so they can be fixed.
• Create incentives for vendors to be careful.
• Learn about new classes of threats.
  – Determine what we need to defend against.
  – Help designers build stronger systems.
  – Help users more accurately evaluate risk.
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.
Exercise

• How might we break into Siebel Center?
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?

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

1. Confidentially
2. Integrity
3. Availability
   • Additional objectives
     – Authenticity
     – Accountability
Security Policies

• What assets are we trying to protect?
• What properties are we trying to enforce?
• The CIA Triad:
  – Confidentiality
  – Integrity
  – Availability
• Additional properties:
  – Authenticity
  – Accountability
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.
Security Costs

• 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
Design principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability
- Isolation
- Encapsulation
- Modularity
- Defense in depth
- Minimize *attack surface*
- Least astonishment
Exercise

• How should you secure your bike?
  – Assets?
  – Adversaries?
  – Risk assessment?
  – Countermeasures?
  – Costs/benefits?
Exercise

• How should you secure your home/apartment/dorm room?
  – 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


Questions?