CSCI-UA.9480
Introduction to Computer Security

Session 0
Introduction and Threat Modeling

Prof. Nadim Kobeissi

Introduction

Welcome!

0a

Welcome to your new course!

Open discussions.

- We can adopt a seminar style and focus more on practical work.
- Feel free to ask questions any time.
- You can do the readings before or after class.

Important notes.

- Don’t miss sessions. This is an intensive course: demanding assignments, packed sessions, strict grading.
- Pioneers from all over the world will come give you invited talks.
- Assignments are due on the day of, *before* class.

About me.

- Originally studied philosophy, got into applied cryptography as a passion.
- First project: Cryptocat (while in undergrad.)
- Moved to Paris in 2015 to pursue Ph.D. in computer security and applied cryptography. I specialize in designing and formally verifying cryptographic protocols.
- Peer-reviewed publications, etc.
- Personal website: https://nadim.computer

Goals of this course.

- Understand the basic principles of:
  - Computer security.
  - Cryptographic constructions underlying modern computer security.
- Learn practical skills:
  - Design secure systems.
  - Write secure code.
  - Exploit insecure code.
- Acquire important knowledge in:
  - Applied cryptography.
  - Designing and breaking secure systems.
  - Operating system security.
  - Network security.
  - Web security.
  - Security economics.

Course layout.

- Parts:
  - 1. Cryptography
  - 2. Network Security
  - 3. Software Security
  - 4. Web Security
  - 5. Security and Society
- Graded items:
  - Class participation (10%)
  - Three problem sets (20%)
  - Two practical assignments (20%)
  - Midterm exam (25%)
  - Final exam (25%)
- **Keep the course website bookmarked: https://computersecurity.paris**

Course guidelines.

- Bring a laptop to every class but only open it when asked.
- No smartphones during class.
- No eating in class.
- Academic integrity: there's no need to cheat. My job is to help you learn and succeed.
- Absences must be justified with a doctor's note or similar.
- *"Leaving class to go to the bathroom or yawning in class is considered rude in France."* No problem in my class: please yawn and go to the bathroom all the time.
- Check your syllabus for the whole list of guidelines.

Typifying Attacks

“Cybersecurity, computer security or IT security is the protection of computer systems from theft of or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.”
– Wikipedia.

“Security engineering is about building systems to remain dependable in the face of malice, error, or mischance. As a discipline, it focuses on the tools, processes and methods needed to design, implement and test complete systems, and to adapt existing systems as their environment evolves.”

– Ross Anderson.

“Applied cryptography is the science and practice of designing and implementing real-world systems that derive their practical security guarantees primarily from mathematically ‘hard’ foundations, and only miscellaneously from access control.”

– Me? I hope this is accurate.

Today's reality.

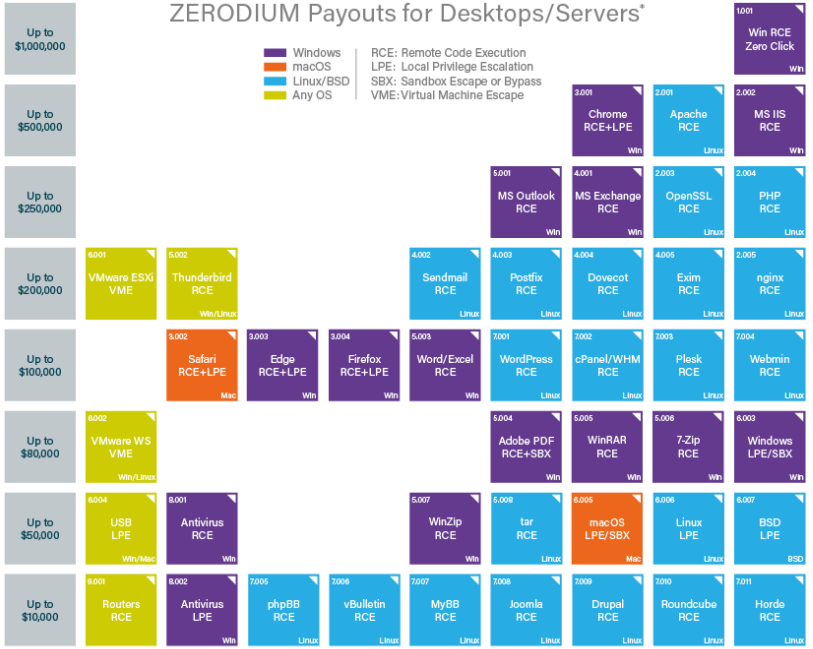
There's a lot of buggy software out there...

Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2017

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013
Time Leaders

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	842
2	Linux Kernel	Linux	OS	453
3	Iphone Os	Apple	OS	387
4	Imagemagick	Imagemagick	Application	357
5	Mac Os X	Apple	OS	299
6	Windows 10	Microsoft	OS	268
7	Windows Server 2016	Microsoft	OS	252
8	Windows Server 2008	Microsoft	OS	243
9	Windows Server 2012	Microsoft	OS	235
10	Debian Linux	Debian	OS	230
11	Windows 7	Microsoft	OS	229
12	Windows 8.1	Microsoft	OS	225

...and bugs don't sell for cheap.



Today's reality.

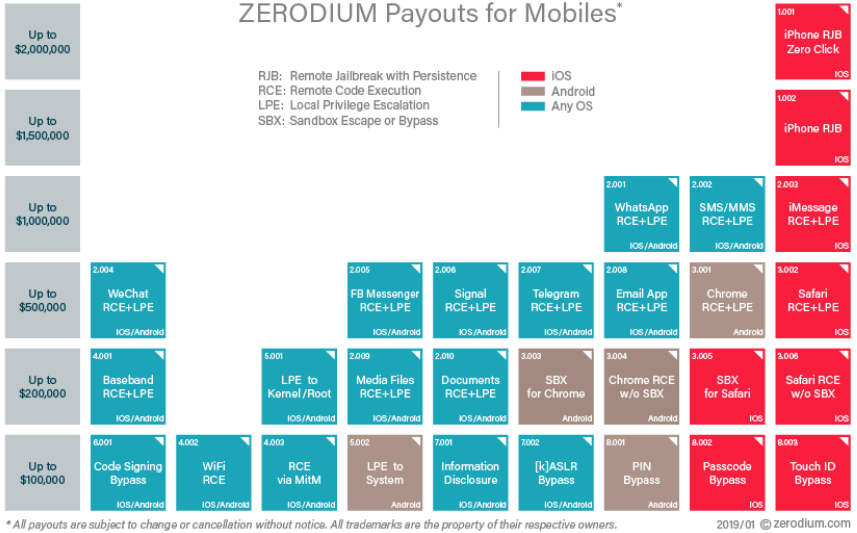
There's a lot of buggy software out there...

Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2017

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013
Time Leaders

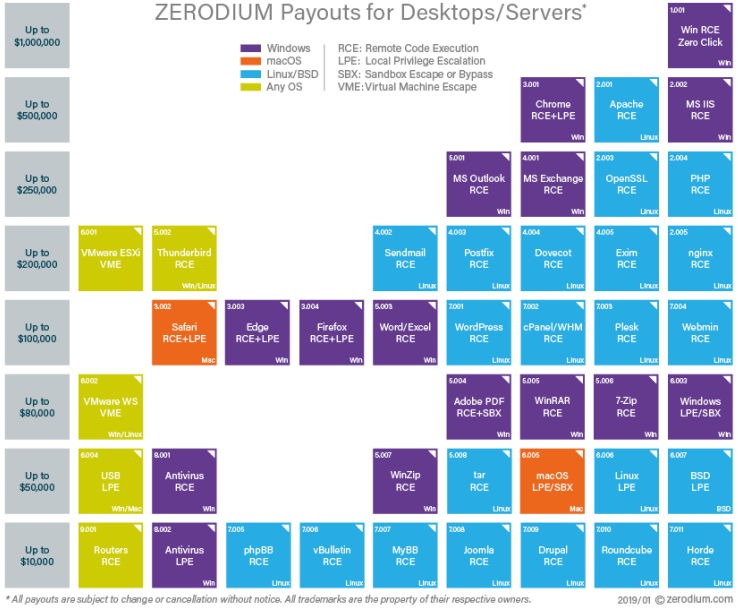
	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	842
2	Linux Kernel	Linux	OS	453
3	Iphone Os	Apple	OS	387
4	Imagemagick	Imagemagick	Application	357
5	Mac Os X	Apple	OS	299
6	Windows 10	Microsoft	OS	268
7	Windows Server 2016	Microsoft	OS	252
8	Windows Server 2008	Microsoft	OS	243
9	Windows Server 2012	Microsoft	OS	235
10	Debian Linux	Debian	OS	230
11	Windows 7	Microsoft	OS	229
12	Windows 8.1	Microsoft	OS	225

...and bugs don't sell for cheap.

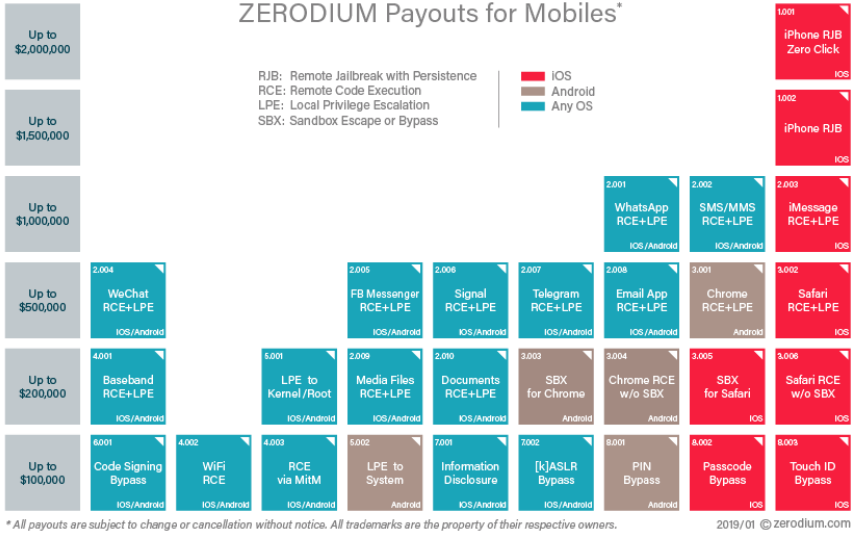


Can you think of any types of attacks?

On these platforms?



Or on these?



Example: WannaCry Ransomware

Threat Modeling

The bird’s eye view.

0c

Kerckhoff's principle.

Originated in cryptography...

- The security of a cipher should rely only on the secrecy of the key and not on the secrecy of the cipher.
- This came about in 1883, back when military encryption machines could be stolen by the enemy, leading to decryption.

...but can be generalized to security systems.

- Assume the attacker knows the system.
- However, the attacker doesn't have:
  - Access control.
  - Authentication.
  - Ability to modify the system, etc.

Threat model for a bank.

Threats to consider for a bank.

- *Inside threat*: Main threat to bank bookkeeping is petty theft by bankers (1% get fired each year for this.)

- *Outside threat*: ATM machines. How to handle authentication? Prevent tampering? Secure communications?

Threat model for a bank.

Some more threats to consider.

- *Online banking*: Users could be susceptible to trickery (phishing) or could have their account hijacked by exploiting bugs in the bank's web applications or in their browser (XSS.)

- *High-value messaging systems*: Internal communications, regularizing balances between branches, etc.

Threat model for a bank.

Let’s talk about “security theater.”

- What is the value of having giant stone walls or solid marble tables?
- Whole books have been written about “security theater” (Bruce Schneier most notably).

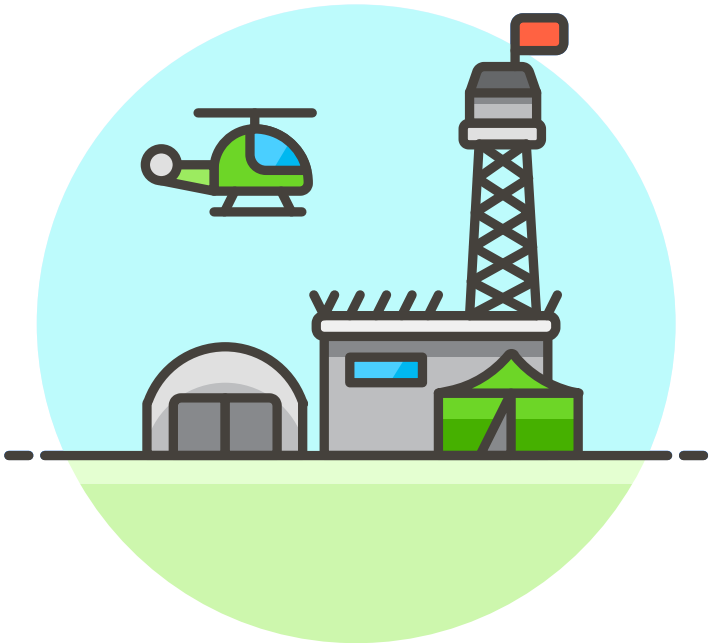
Did you know?

ATMs were the first large-scale commercial deployment of cryptography and helped establish a number of standards.

Threat model for a military base.

Threats to consider for a military base.

- Prevent enemies from jamming your radars while jamming theirs.
- Denial of service prevention takes a higher priority.



Test your knowledge!

What is the better way to protect nuclear weapons from unauthorized access?

- ☐ **A**: Store them in a secret location.
- ☐ **B**: Require multiple authentication methods spread across multiple people.
- ☐ **C**: Dismantle the weapons, thereby removing the need to protect them.

Test your knowledge!

What is the better way to protect nuclear weapons from unauthorized access?

- ☐ **A**: Store them in a secret location.
- ☑ **B**: Require multiple authentication methods spread across multiple people.
- ☐ **C**: Dismantle the weapons, thereby removing the need to protect them.

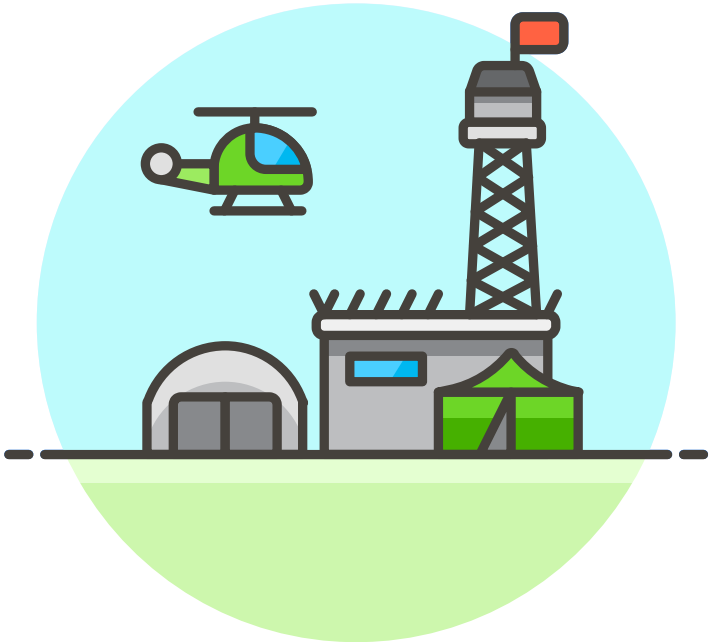
Threat model for a military base.

Why not A?

- Kerckhoff's principle.
- Single point of compromise.

Why not C?

- The security engineer rarely decides the requirements.



Threat model for a home.

Let’s try to come up with one.

- What are the risks?
- Who are the adversaries?
- What are the systems?
- What are the points of failure?
- What are the failure scenarios and their impact?

Now that you have your threat model, you can reason about the systems you must design and implement.

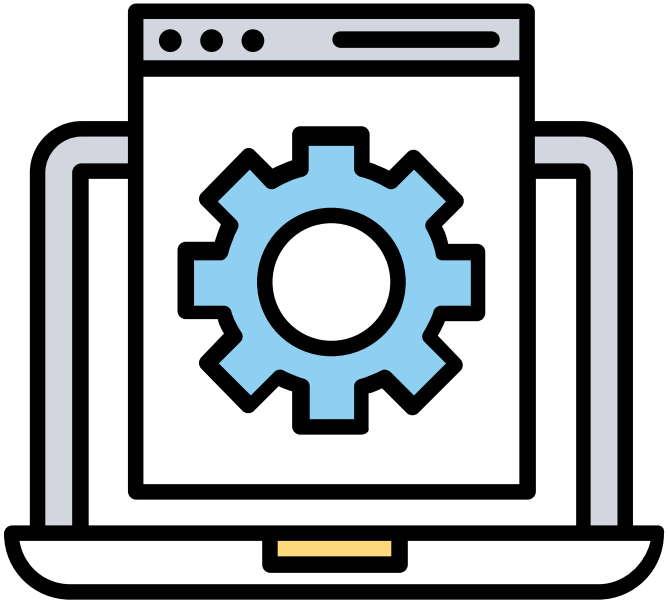
Defining Security Systems

An overview to get you started.

“Systems?”

Now that you have your threat model, you can reason about the systems you must design and implement.

- But what are systems?
- Cryptographic protocols: TLS.
- Operating system: Linux.
- Application: WhatsApp.
- Embedded hardware: iPod.



“Alice and Bob?”

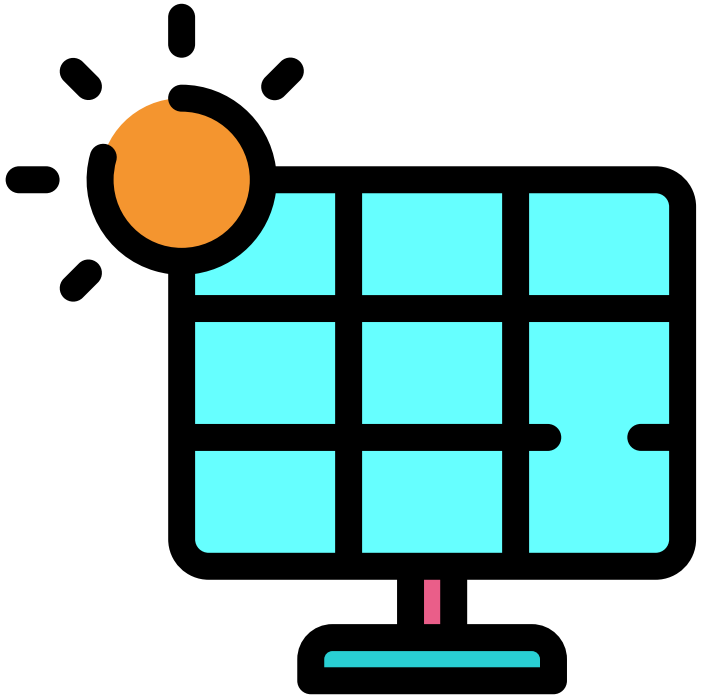
In *protocols*, we reason about:

- Principals: Alice, Bob.
- Security goals: confidentiality, authenticity, forward secrecy...
- Use cases and constraints.
- Attacker model.
- Threat model.

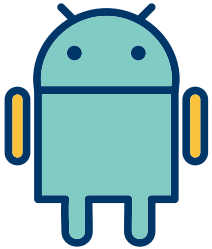
“Application Security.”

In *applications* and many *user-facing systems*, we reason about:

- User compromise: device compromise, impersonation, phishing…
- Server compromise: leaks, database hacks…
- Usability and security.



Link each icon to the correct label.



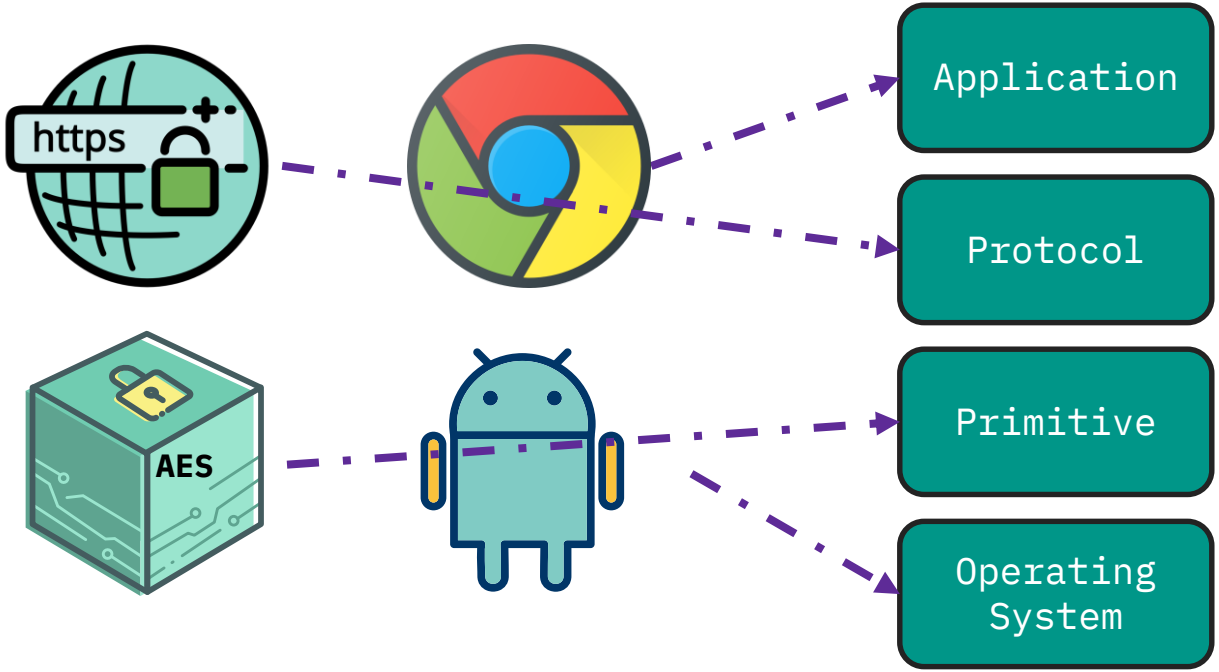
Application

Protocol

Primitive

Operating System

Link each icon to the correct label.



Each layer is exposed to different attacks.

- Systems layer:
  - Access control violations.
  - Privilege escalation.
  - Memory corruption.
- Primitives layer:
  - Side channels.
  - Cryptographic breaks.
  - Implementation errors.
- Protocol layer:
  - Implementation errors.
  - Design errors.
  - Outdated specifications.
  - Active attacks.
- Application layer:
  - User error or manipulation.
  - Bugs in the code.

End of introductory session.

I hope you now have a clear picture of what our class is about:

- Introducing fundamental computer security concepts.
- Introduce security engineering and analyze it from an attacker's perspective.
- Design and break real-world systems.
- Understanding security's role in society and ethics' role in security.

Next time: Cryptography

The building blocks of modern security systems.