Introduction and Security Principles

ITIS 6200/8200 Fall 2023

Today’s Cunning Plan (First half): Introductions & Logistics

- Staff introductions
- Course overview:
  - What will you learn in this class?
- Course logistics
  - Lectures, office hours, exams, and grading
  - Resources and communication platforms
  - Collaboration and academic integrity
  - Inclusive learning
  - Stress management and mental health
  - Ethics
  - Non-discrimination

Staff Introductions

Who Am I? Professor Xiang (shaang) (he/him)

- Did my undergrad in China
  - Electronic Engineering
- Did a PhD at University of Virginia (UVa)
  - Research focus: formal methods; dependability
  - Advisors: John Knight
- Did a 5 year Postdoc at Harvard University
  - Research focus: formal methods for security; information flow analysis; Cyber-physical systems
  - Advisors: Stephen Chong
- First-year assistant professor in SIS
  - First time teaching a complete class, so your feedback/advice/complaints are appreciated!

Our TAs!

- Vineeth Mylavarapu (Linkedin, email)
  - Master Student of Cyber Security

- Tarun Grandhi (Linkedin, email)
  - Master Student of Computer Science

Course Overview

Learning Objectives

- Understand **fundamental** concepts of security
- Understand security vulnerabilities, threats and their significance
- Understand how attacks work in practice
- Understand security properties, and build computer systems with robust security properties

- What mistakes *not to make!*

Course Outline

- Introduction to Security
  - What are some general philosophies when thinking about security?
- Cryptography
  - How do we securely send information over an insecure channel?
- Web Security
  - What are some attacks on the web, and how do we defend against them?
- System Security
  - What are some attacks on computer systems, and how do we defend against them?
- Assurance of Security
  - How to establish/prove security properties for computer systems? (My research)
- Miscellaneous Topics
  - Useful, interesting, or fun topics. Maybe some guest lectures! e.g., CPS security

Extra Tools and Skills

- Some non-security-related skills you can take away from this class:
- Cryptography
  - Becoming a better consumer: be able to analyze security products and pick the right security tools for your software
- Web Security
  - Software engineering: understand how websites are built and how your web browser interacts with remote web servers
- System Security
  - Architecture and OS: understand how the memory works and how your software applications interact with OS and hardware
- Assurance of Security
  - Mathematical notations, system modeling, and proof methods

Prerequisites

No prior course requirement; but the following skills help

- Familiarity with basic mathematical notation and proof structures
  - Relevant for cryptography
  - Relevant for assurance of security
- Familiarity with memory layouts and assembly
  - Relevant for system security
- An ability to pick up new programming languages quickly
  - Projects may need it

Course Logistics

Enrollment

- Course staff does not control enrollment; we have to follow department policy
  - For course registration issues, please contact Katie Watson at katie.watson@charlotte.edu

Course Structure: Lectures

- This is a in-person class, you are expected to be here!
- Attendance is not taken
- Tuesday/Thursday, 10:00–11:15 AM
- Using electronic devices not allowed except for learning purposes

Course Structure: Office Hours

- Space to ask questions about content, get help with projects, raise concerns with the course, etc. with a TA or instructor
- All office hours start next week (week of August 28)
- My office hours will be in person
  - Tu,Th 1:45-3:00pm, Woodward Hall 330d
- TA's office hours be available both in-person and online
  - Vineeth Mylavarapu: Monday 7-8pm; COED-065, College of Education
  - Tarun Grandhi: Wednesday 6-7pm; Woodward Hall, 309

- Office hours details are available in a Google calendar at:
  - The canvas site
  - And my webpage: https://www.jianxiang.info/teaching/ITIS6200/2023fa/officehours.html

Platforms

- Canvas
  - Course information, e.g., schedule, office hours, policies
  - Distributions / submission of assignments and projects
  - Post questions at Discussion forum
- Email
  - itis6200-staff@uncc.edu for questions and issues related to assignments, course content, etc.. The course staff will closely monitor this email.
  - **sending email to individual course staff will delay a response**.
  - It may take up to 48 hours to respond

Textbooks

No textbook is required, but if you would like additional references, we recommend:

- Security Engineering by Ross Anderson
- Cryptography Engineering by Ferguson, Schneier, and Kohno
- Introduction to Computer Security by Matt Bishop
- Computer Security: Principles and Practice by William Stallings
- Computer Security: Art and Science by Matt Bishop
- Security in Computing by Charles P. Pfleeger
- Introduction to Computer Security by Michael Goodrich and Roberto Tamassia
- Computer Security, a freely available course textbook from UC Berkerly.

Course Structure: Exams

- Closed book exams
- Midterm
  - Tentatively Thursday, Sep 28th, 10:00-11:15 AM
- Final
  - Thu 14-Dec, 8:00 - 10:30am

Grading Structure (Tentatively)

- Homework: 40%
  - Complete individually
  - For now, 4 homework in total
- Projects: 15%
  - Complete individually
  - For now, 2 projects in total
- Midterm: 20%
- Final: 20%
- Participation: 5%
  - Includes attendance and participation in class and office hours, and contributing to online discussion
- (Late policy next)

Class Policies: Late policy

- Submission
  - Must be submitted on Canvas.
  - Assignments are due by 11:59PM on the due date.
- Late policy
  - No late submissions, except for special circumstances such as accident, illness or death in the immediate family, in which case you must give us notice or proof. Late submissions will be discussed on a case-by-case basis.
  - To request late submissions, please send emails to itis6200-staff@uncc.edu.

Class Policies: Inclusive Learning

- Are you facing barriers in school due to a disability?
  - Office of Disability Services
  - University Center for Academic Excellence
- Our goal is to teach you the material in our course. The more accessible we can make it, the better.

Class Policies: Collaboration

- Asking questions and helping others is encouraged
  - Discussing course topics with other is welcome!
  - But make sure you can walk through the problems yourself
  - The answers you submit for evaluation must be results of your own efforts.
- Limits of collaboration
  - Don’t share solutions with each other
  - You should never see or have possession of anyone else’s solutions—including from past semesters
  - Do not look on the web or generative AI for solutions (unless we say so in the assignment and projects)

Class Policies: Academic Integrity

- Academic integrity policies
  - **Any form of cheating will receive 0 point in that task and be reported to the University.**
  - If you are ever in doubt, ask the course staff to clarify what is and isn't appropriate.
  - Students have the responsibility to know and follow the requirements of University Policy 407: The Code of Student Academic Integrity.
  - Do not pass solutions to problem sets nor accept them from another student.
  - Do not post course materials (including problem sets, solutions, exams, etc.) to websites or course-content archives.
  - No cheating will be tolerated! Copying from previous semesters, other students, or the Internet are prohibited!

Ethics

- In this class, you will learn a lot about attacks out of necessity
  - To be able to defend against the attacker, you must learn the techniques that attackers use
- It is usually okay to break into your own systems
  - This is a great way to evaluate your own systems
- It is usually okay to break into someone else's systems with their explicit permission
- It is **grossly unethical** and **exceedingly criminal** to break into someone else's systems without their permission

Non-Discrimination

- No student will be discriminated against in this class based on age, race, nationality, religion, sexual orientation, gender identity/expression, veteran's status, country of origin, or group affiliation.

- Any student who does not behave in a respectful manner may be asked to leave the classroom.

- Students with continuous or repeated disrespectful behavior will be referred to the Office of Student Conduct or the Title IX Office.

Stress Management and Mental Health

- If you feel overwhelmed, there are options
  - Academically: Ask on Canvas, talk to staff in office hours, set up a meeting with staff to make a plan for your success this semester
  - Non-academic:
    - The Center for Counseling and Psychological Services line 704-687-0311 is a support line (with after hour support) for students who have mental health concerns, whether they are in immediate distress or not, on-campus or elsewhere.

Today’s Cunning Plan (Second half): Intro to Security

- Introduction to security
  - What is security
  - Why is security important
  - **Security principles**

What is security?

What is security?

Enforcing a desired property *in the presence of an attacker*

data confidentiality

user privacy

data and computation integrity

authentication

availability

…

Why is security important?

- It is important for our
  - physical safety
  - confidentiality / privacy
  - functionality
  - protecting our assets
  - successful business
  - a country’s economy and safety
  - and so on…

Why is security important?

- Consider: Physical Safety

The Washington Post

Link

FBI probe of alleged plane hack sparks worries over flight safety

Drew Harwell *May 18, 2015*

PCWorld

Link

Pacemaker hack can kill via laptop

Jeremy Kirk *October 21, 2012*

Why is security important?

- Consider: Privacy/Confidentiality

eSecurity Planet

Link

91 Percent of Healthcare Organizations Suffered Data Breaches in the Past Two Years

Jeff Goldman *May 12, 2015*

Money

Link

Data Breach Tracker: All the Major Companies That Have Been Hacked

Karavbrandeisky *October 30, 2014*

In 2020, there were over 1001 breaches, affecting the data of 155,000,000 individuals

Why is security important?

- Consider: National security

THE WALL STREET JOURNAL.

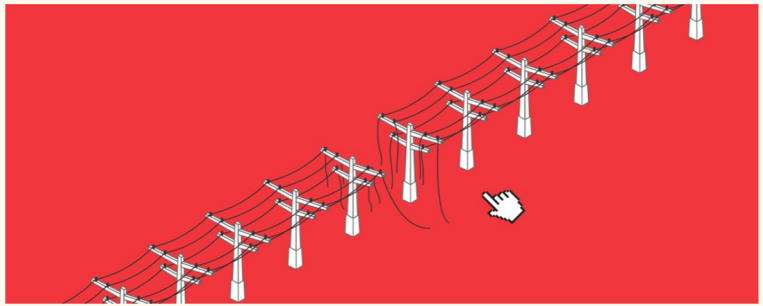
Link

America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It

Rebecca Smith and Rob Barry

January 10, 2019

A Wall Street Journal reconstruction of the worst known hack into the nation's power system reveals attacks on hundreds of small contractors



What is hackable?

- Everything!
  - Especially things connected to the Internet
  - Assume that every system is a target
  - A casino was hacked because a fish-tank thermometer was hacked within the network

SLATE

Link

For the First Time, Hackers Have Used a Refrigerator to Attack Businesses

Julie Bort *January 17, 2014*

Security Principles

Security Principles

- Security principles
  1. Know your threat model
  2. Consider human factors
  3. Security is economics
  4. Detect if you can’t prevent
  5. Defense in depth
  6. Least privilege
  7. Separation of responsibility
  8. Ensure complete mediation
  9. Don’t rely on security through obscurity
  10. Use fail-safe defaults
  11. Design in security from the start

Know Your Threat Model

The Parable of the Bear Race

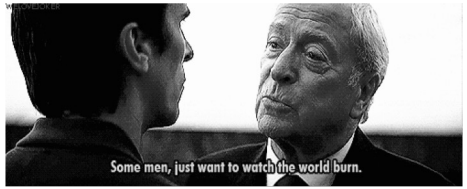
Blue slides are stories and case studies; the key is the **takeaways**

"I don't have to outrun the bear. **I just have to outrun you.**"

Takeaway: You often just need to have "good enough" defense to make attackers turn somewhere else.

Security Principle: 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
  - Politics
  - Fun
  - Watching the world burn



Security Principle: Know Your Threat Model

- Consider: Personal security
- Who and why might someone attack *you*?
  - Criminals might attack you for money
  - Teenagers might attack you for laughs or to win online games
  - Governments might spy on you to collect intelligence
  - Intimate partners might spy on you
    - This is a surprisingly dangerous threat model!

Threat Model: Common Assumptions for Attackers

- Assume the attacker…
  - Can interact with systems without notice
  - Knows general information about systems (operating systems, vulnerabilities in software, usually patterns of activity, etc.)
  - Can get lucky
    - If an attack only succeeds 1/1,000,000 times, the attacker will try 1,000,000 times!
  - May coordinate complex attacks across different systems
  - Has the resources required to mount the attack
  - Can and will obtain privileges if possible

Trusted Computing Base

- **Trusted computing base (TCB)**: The components of a system that security relies upon
- 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.

Consider Human Factors

Security Principle: 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
- It all comes down to people: The programmers
  - Programmers make mistakes
  - Programmers use tools that allow them to make mistakes (e.g. C and C++)
- It all comes down to people: Everyone else
  - Social engineering attacks exploit other people's trust and access for personal gain

Physical security keys use the fact that humans are trained to safeguard keys

Security is Economics

Security Principle: Security is Economics

- Cost/benefit analyses often appear in security: The expected benefit of your defense should be proportional to the expected cost of attack
  - More security (usually) costs more
  - If the attack costs more than the reward, the attacker probably won't do it
- Example: You don't put a $10 lock on a $1 item…
  - … unless a $1 item can be used to attack something even more valuable
- Example: You have a brand-new, undiscovered attack that will work on anybody's computer. You wouldn't expose it on a random civilian

Detect If You Can’t Prevent

Burglar Alarms

- Security companies are supposed to detect home break-ins
  - Problem: Too many false alarms. Many alarms go unanswered
  - Placing a sign helps deter burglars from entering at risk of being caught…
    - … even if you don't have an alarm installed!
- **Takeway**: Prevent attacks when you can, but detect them if you can't

Security Principle: Detect if You Can't Prevent

- **Deterrence**: Stop the attack before it happens
- **Prevention**: Stop the attack as it happens
- **Detection**: Learn that there was an attack (after it happened)
  - If you can't stop the attack from happening, you should at least be able to know that the attack has happened.
- **Response**: Do something about the attack (after it happened)
  - Once you know the attack happened, you should respond
  - Detection without response is pointless!

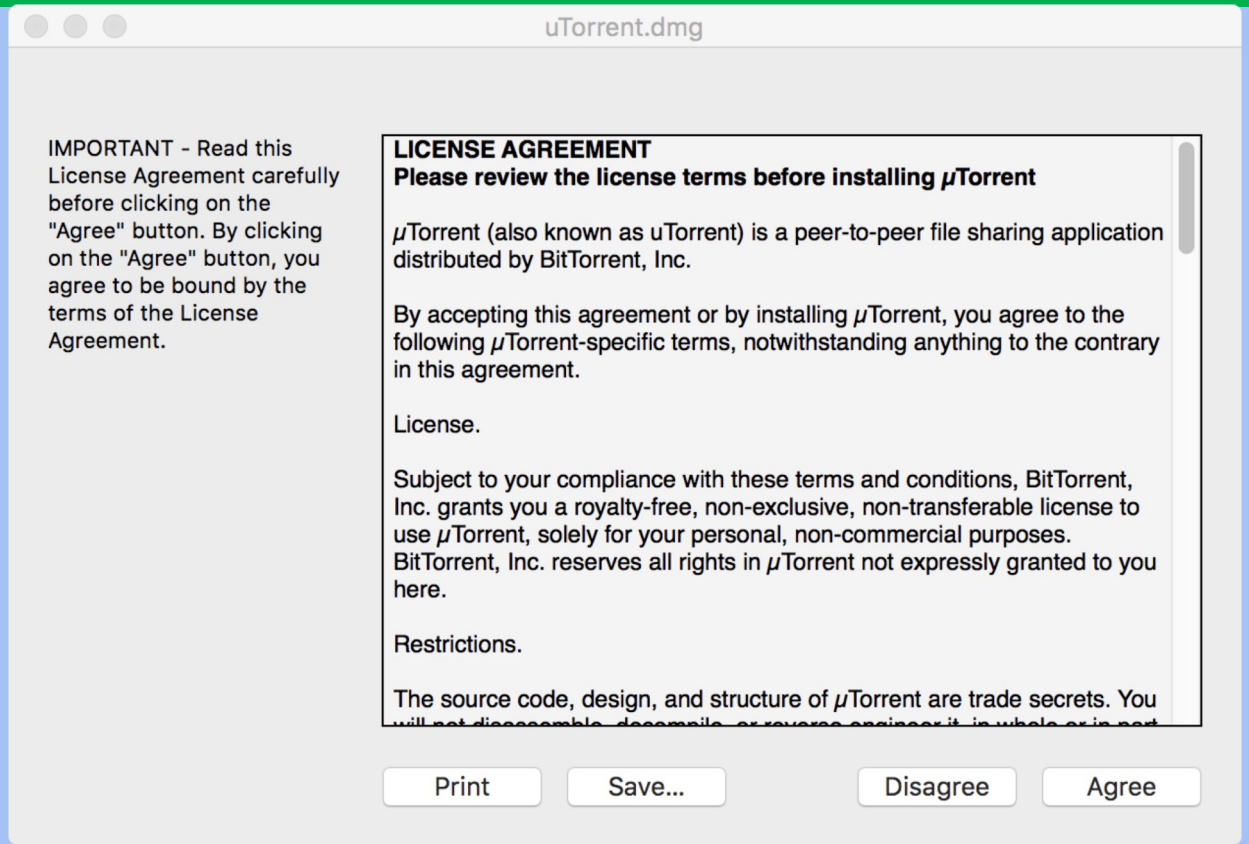
Defense in Depth

Security Principle: Defense in Depth

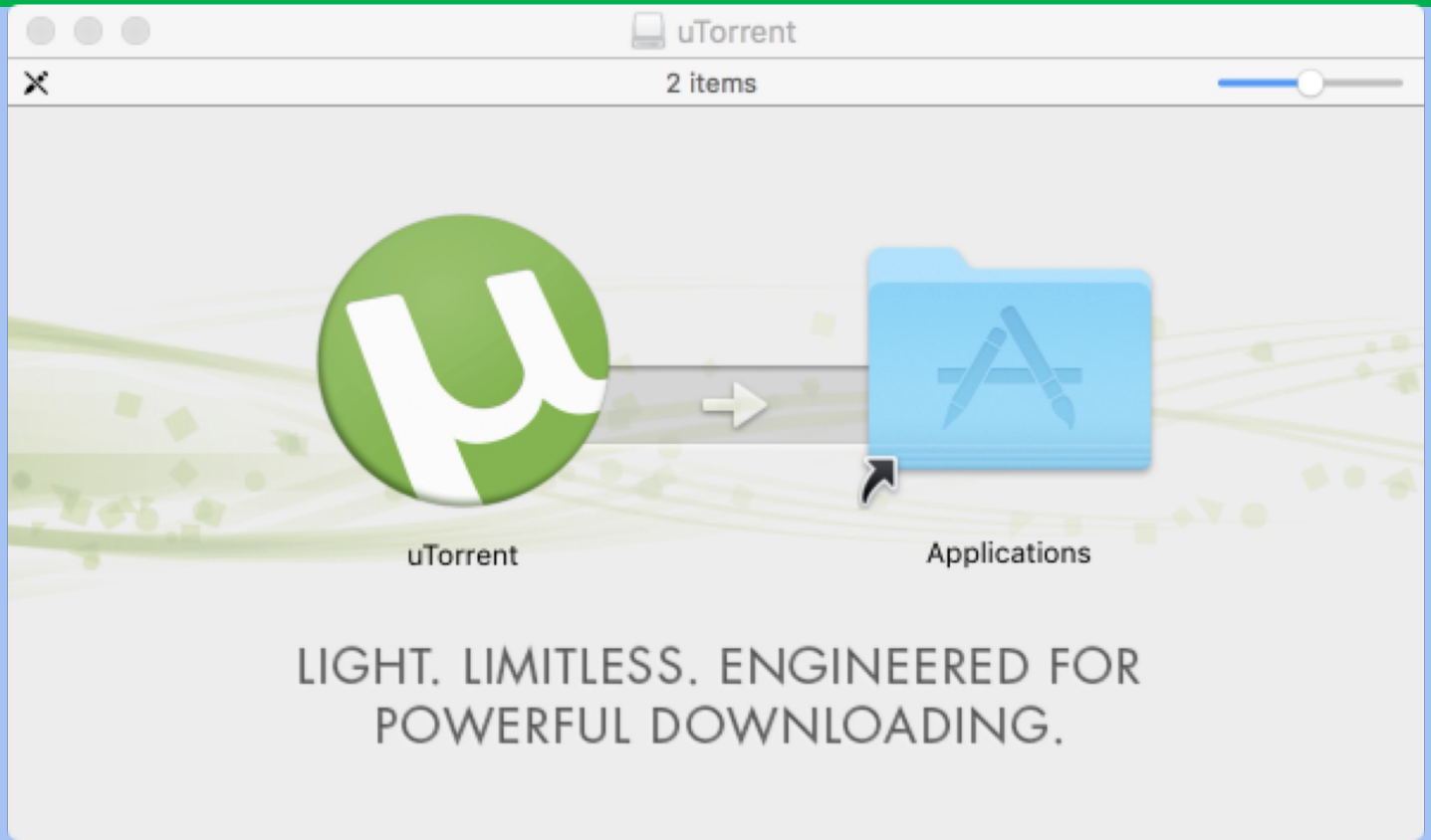
- Multiple types of defenses should be layered together
- An attacker should have to breach all defenses to successfully attack a system
- However, consider **security is economics**
  - Defenses are not free.
  - Defenses are often less than the sum of their parts

Least Privilege

uTorrent

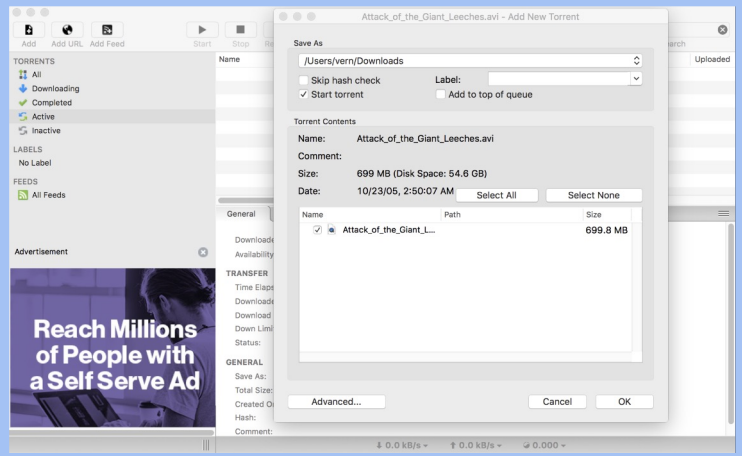

uTorrent.dmg
IMPORTANT - Read this License Agreement carefully before clicking on the "Agree" button. By clicking on the "Agree" button, you agree to be bound by the terms of the License Agreement.
LICENSE AGREEMENT
Please review the license terms before installing µTorrent
µTorrent (also known as uTorrent) is a peer-to-peer file sharing application distributed by BitTorrent, Inc.
By accepting this agreement or by installing µTorrent, you agree to the following µTorrent-specific terms, notwithstanding anything to the contrary in this agreement.
License.
Subject to your compliance with these terms and conditions, BitTorrent, Inc. grants you a royalty-free, non-exclusive, non-transferable license to use µTorrent, solely for your personal, non-commercial purposes. BitTorrent, Inc. reserves all rights in µTorrent not expressly granted to you here.
Restrictions.
The source code, design, and structure of µTorrent are trade secrets. You
Print
Save...
Disagree
Agree

uTorrent


uTorrent
2 items
uTorrent
Applications
LIGHT. LIMITLESS. ENGINEERED FOR
POWERFUL DOWNLOADING.

uTorrent

- What was this program able to do?
  - Leak your files
  - Delete your files
  - Send spam
  - Run another malicious program
- What does this program need to be able to do?
  - Access the screen
  - Manage some files (but not all files)
  - Make some Internet connections (but not all Internet connections)
- **Takeaway**: Least privilege

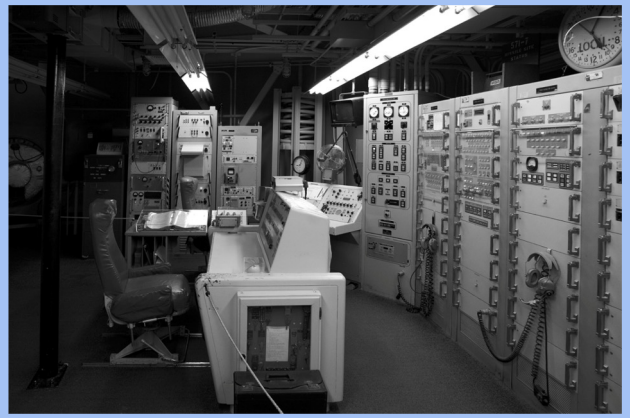


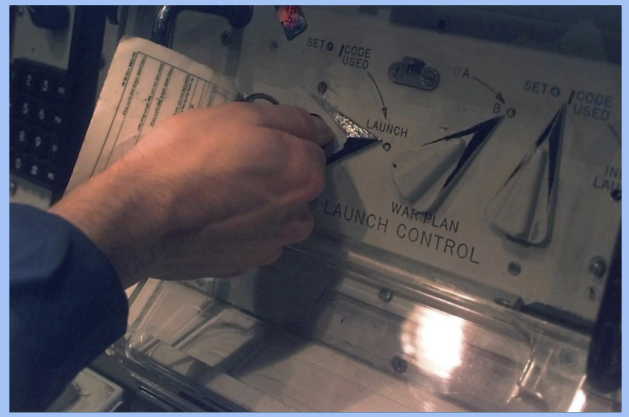
Security Principle: Least Privilege

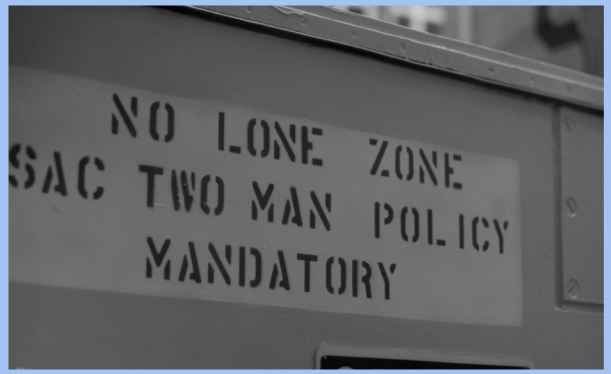
- Consider what permissions a entity or program *needs* to be able to do its job correctly
  - If you grant unnecessary permissions, a malicious or hacked program could use those permissions against you

Separation of Responsibility

Welcome to a Nuclear Bunker







Security Principle: Separation of Responsibility

- If you need to have a privilege, consider requiring multiple parties to work together (collude) to exercise it
  - It’s much more likely for a single party to be malicious than for all multiple parties to be malicious and collude with one another

Ensure Complete Mediation

Spot the Issue

Security Principle: Ensure Complete Mediation

- Ensure that every access point is monitored and protected
- **Reference monitor**: Single point through which all access must occur
  - Example: A network firewall, airport security, the doors to the dorms
- Desired properties of reference monitors:
  - Correctness
  - Completeness (can't be bypassed)
  - Security (can't be tampered with)
  - Should be part of the TCB
- A common failure of ensuring complete mediation involving race conditions

The cars drove around the barrier

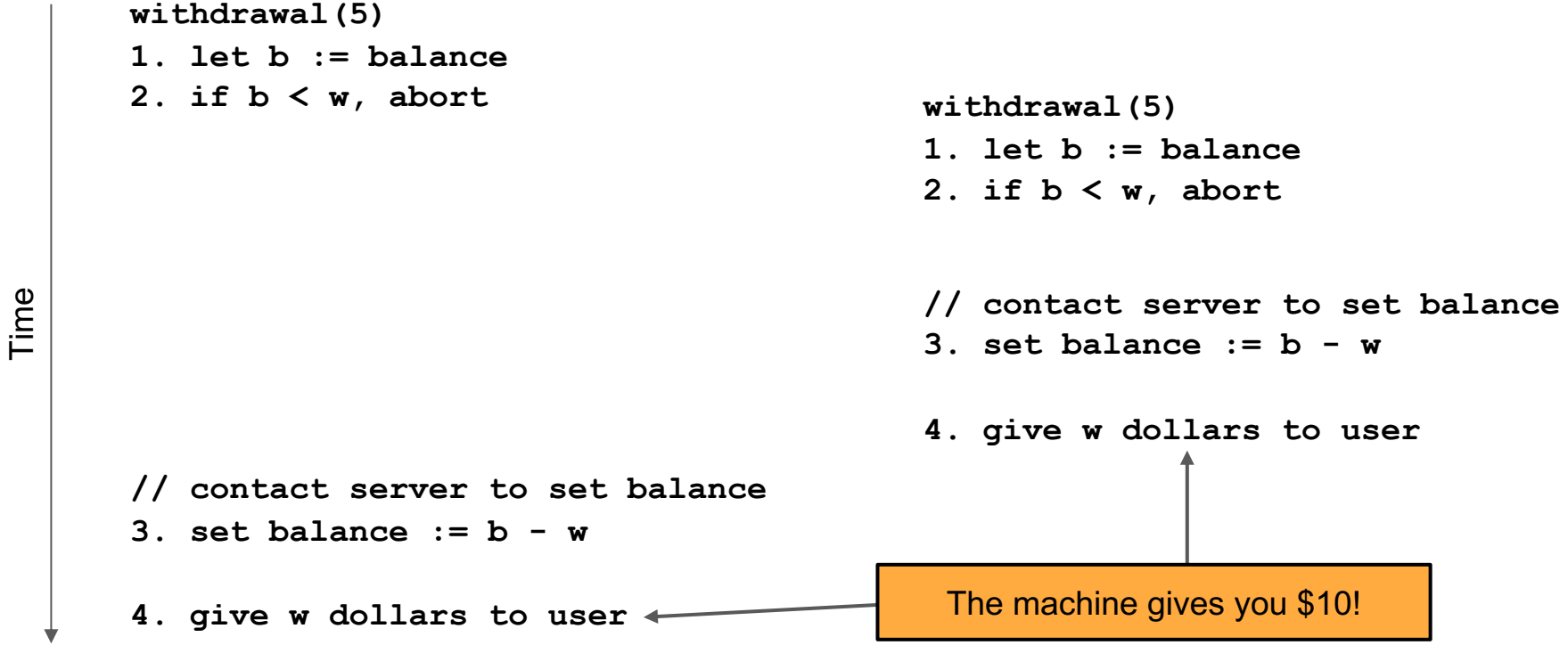
Time-of-Check to Time-of-Use

- A common failure of ensuring complete mediation involving race conditions
- Consider the following code:

```
procedure withdrawal(w)
        // contact central server to get
balance
        1. let b := balance

        2. if b < w, abort

        // contact server to set balance
        3. set balance := b - w

        4. give w dollars to user
```

Suppose you have $5 in your account. How can you trick this system into giving you more than $5?

Time-of-Check to Time-of-Use



Don’t Rely on Security Through Obscurity

Accident on Motorway

Here's a highway sign.

Here's the hidden computer inside the sign.

Here's the control panel. Most signs use the default password, **DOTS**.

Caution! Zombies Ahead!!!

Takeaway: Shannon's maxim/Don't rely on security through obscurity

Security Principle: Shannon's Maxim

- **Shannon's maxim**: "The enemy knows the system"

- You should never rely on obscurity as part of your security. Always assume that the attacker knows every detail about the system you are working with (algorithms, hardware, defenses, etc.).

Assume the attacker knows where the "secret" control panel is located, and has read the manual with instructions on resetting the password.

Use Fail-Safe Defaults

Guarded rooms

- The rooms are guarded by electronic card keys
- What do you do if the power goes out?
  - **Fail closed**: No one can get in if the power is out
  - **Fail open**: Anyone can get in if the power goes out
- What's the best option to choose for closets with expensive equipment? What about emergency exit doors?
- **Takeaway**: Use fail-safe defaults

Security Principle: Use Fail-Safe Defaults

- Choose default settings that “fail safe,” **balancing security with usability when a system goes down**
  - This can be hard to determine

Design in Security from the Start

Security Principle: Design in Security from the Start

- When building a new system, include security as part of the design considerations rather than patching it after the fact
  - A lot of systems today were not designed with security from the start, resulting in patches that don't fully fix the problem!
- Keep these security principles in mind whenever you write code!

Security Principles: Summary

- **Know your threat model**: Understand your attacker and their resources and motivation
- **Consider human factors**: If your system is unusable, it will be unused
- **Security is economics**: Balance the expected cost of security with the expected benefit
- **Detect if you can't prevent**: Security requires not just preventing attacks but detecting and responding to them
- **Defense in depth**: Layer multiple types of defenses
- **Least privilege**: Only grant privileges that are needed for correct functioning, and no more
- **Separation of responsibility**: Consider requiring multiple parties to work together to exercise a privilege
- **Ensure complete mediation**: All access must be monitored and protected, unbypassable
- **Shannon's maxim**: The enemy knows the system
- **Use fail-safe defaults**: Construct systems that fail in a safe state, balancing security and usability.
- **Design in security from the start**: Consider all of these security principles when designing a new system, rather than patching it afterwards