Principles of Security

CMPSC 403 Fall 2021

September 7, 2021

Take the Reflection Quiz 2

Check Discord for the link

Principle 3: Security is Economics

Security is Economics

- Cost/benefit analyses often appear in security
  - The cost of your defense should be less than the cost of attacks happening
  - 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
  - iPhone security vulnerabilities are often sold for ~$1M on the market

Physical Safes

- We want our safes to stop people from breaking in, so let's measure them by how long it takes an expert to break into one:

TL-15 ($3,000)
15 minutes with common tools

TL-30 ($4,500)
30 minutes with common tools

TRTL-30 ($10,000)
30 minutes with common tools and a cutting torch

TXTL-60 (>$50,000)
60 minutes with common tools, a cutting torch, and up to 4 oz of explosives

Takeaway: Security is economics

Principle 4: Detect If You Can't Prevent

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!

Response: Mitigation and Recovery

- Assume that bad things will happen! You should plan security in way that lets you to get back to a working state.

1. **Think Along**: Flooding/tornado
2. **Think Along**: Ransomware

Detection but no Response

- Bitcoin transactions are irreversible. If you are hacked, you can not recover your Bitcoins.

- **Takeaway:** Prevention is great, but depending only on prevention can be *brittle*: When prevention fails, the system fails catastrophically.

Bloomberg

Link

Hacked Bitcoin Exchange Says Users May Share $68 Million Loss

Lulu Yilun Chen and Yuji Nakamura — *August 5, 2016*

HOME > BUSINESS TECH

BUSINESS TECH CAR TECH BUSINESS TECH PHONES/TABLETS/MOBILE TECH APPS/SOFTWARE GADGETS

Coinbase User Accounts Emptied After Hackers Gained Access to Their Crypto Wallets | Couple Discovered $168K Crypto Stolen

Urian B., Tech Times | 25 August 2021, 03:08 am

Ads by Google

Hackers return nearly half of the $600 million they stole in one of the biggest crypto heists

PUBLISHED WED, AUG 11 2021•1:33 AM EDT | UPDATED THU, AUG 12 2021•4:57 PM EDT

Arjun Kharpal @ARJUNKHARPAL | Ryan Browne @RYAN_BROWNE_

SHARE

Principle 5: Defense in Depth

Defense in Depth

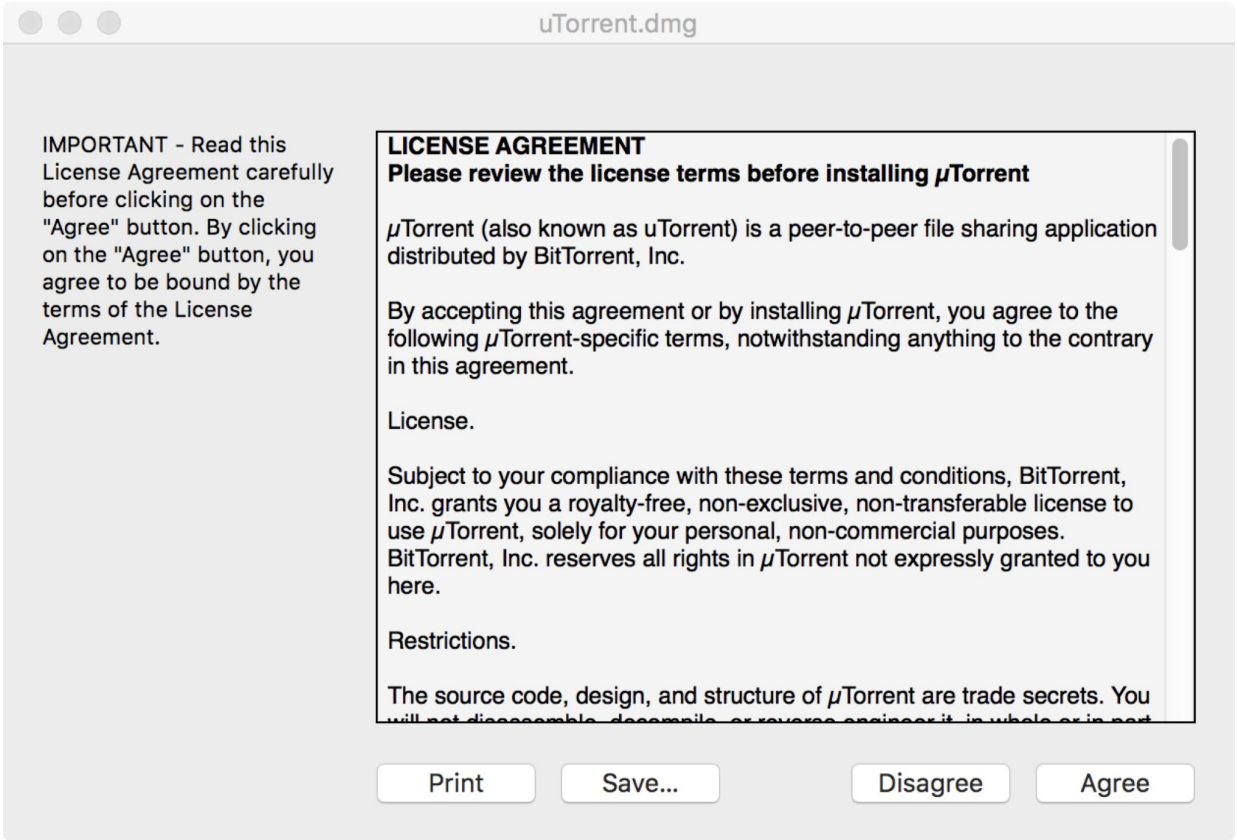
- Multiple types of defenses should be layered together
- An attacker should have to breach all defenses to successfully attack a system
  - Ideally the strength of the defenses compounds somehow
- However, remember: security is economics
  - Defenses are not free.
  - Diminishing returns: Defenses are often less than the sum of their parts
    - 2 walls is much better than 1 wall
    - 101 walls is not much better than 100 walls

Principle 6: Least Privilege

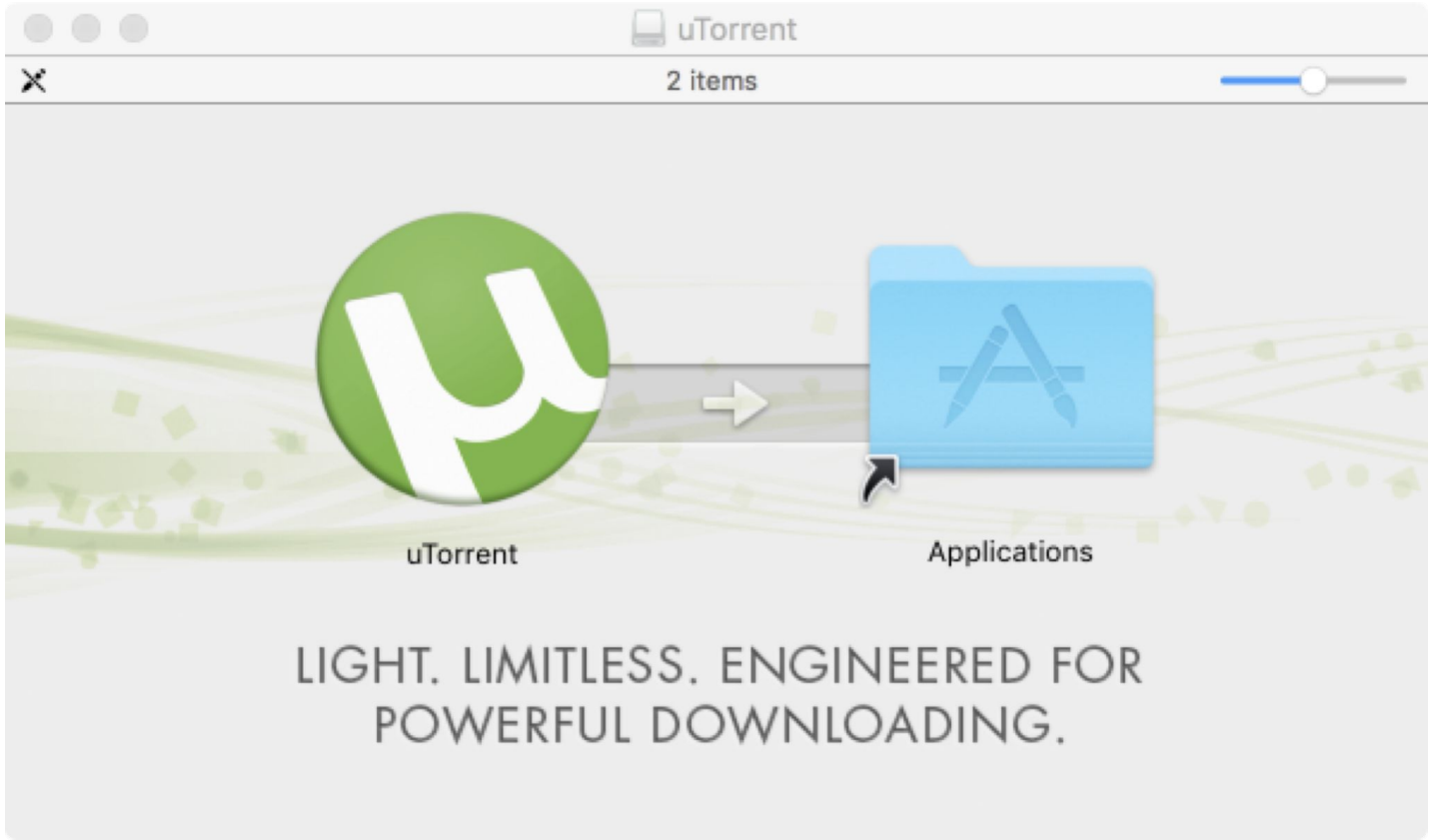
Least Privilege

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

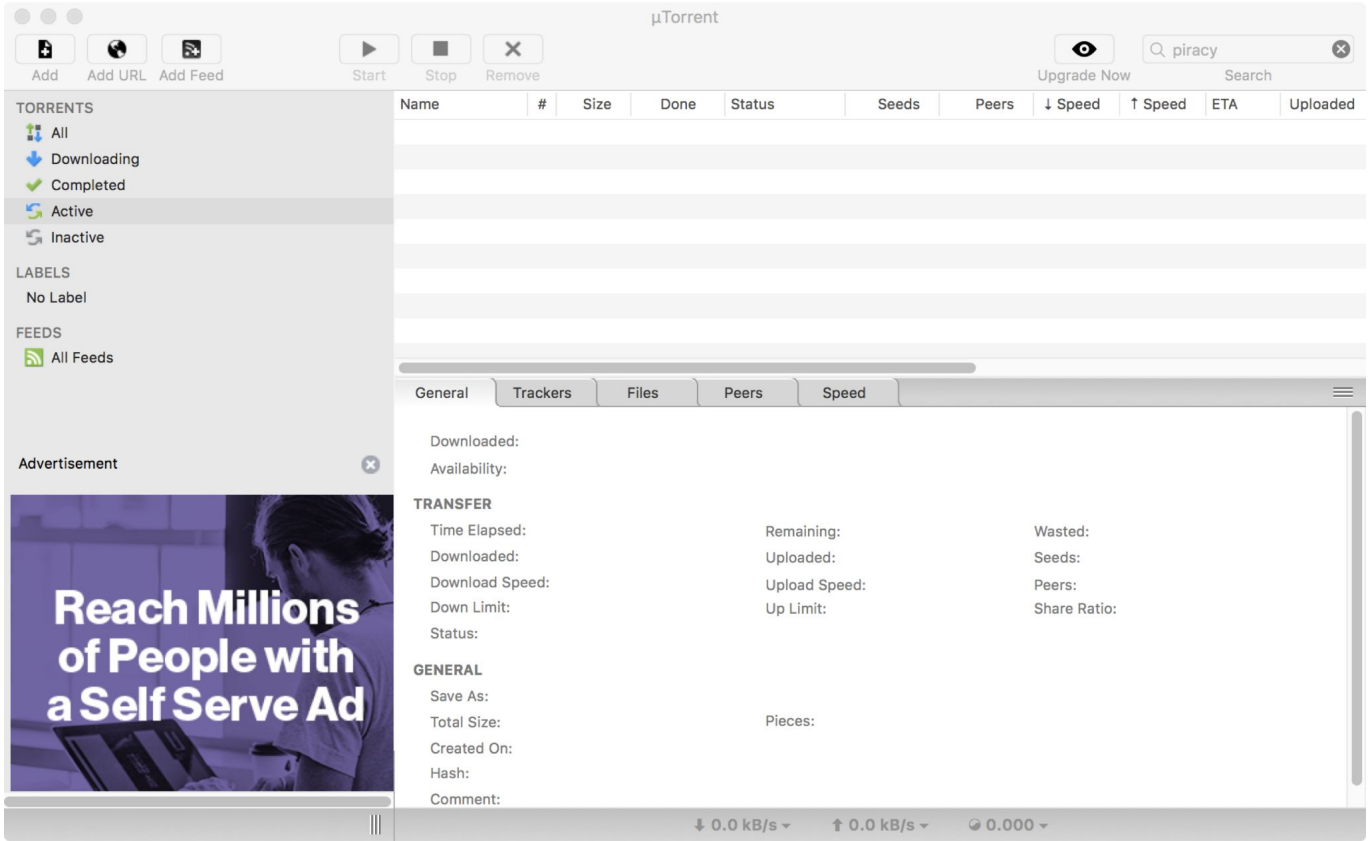
uTorrent


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

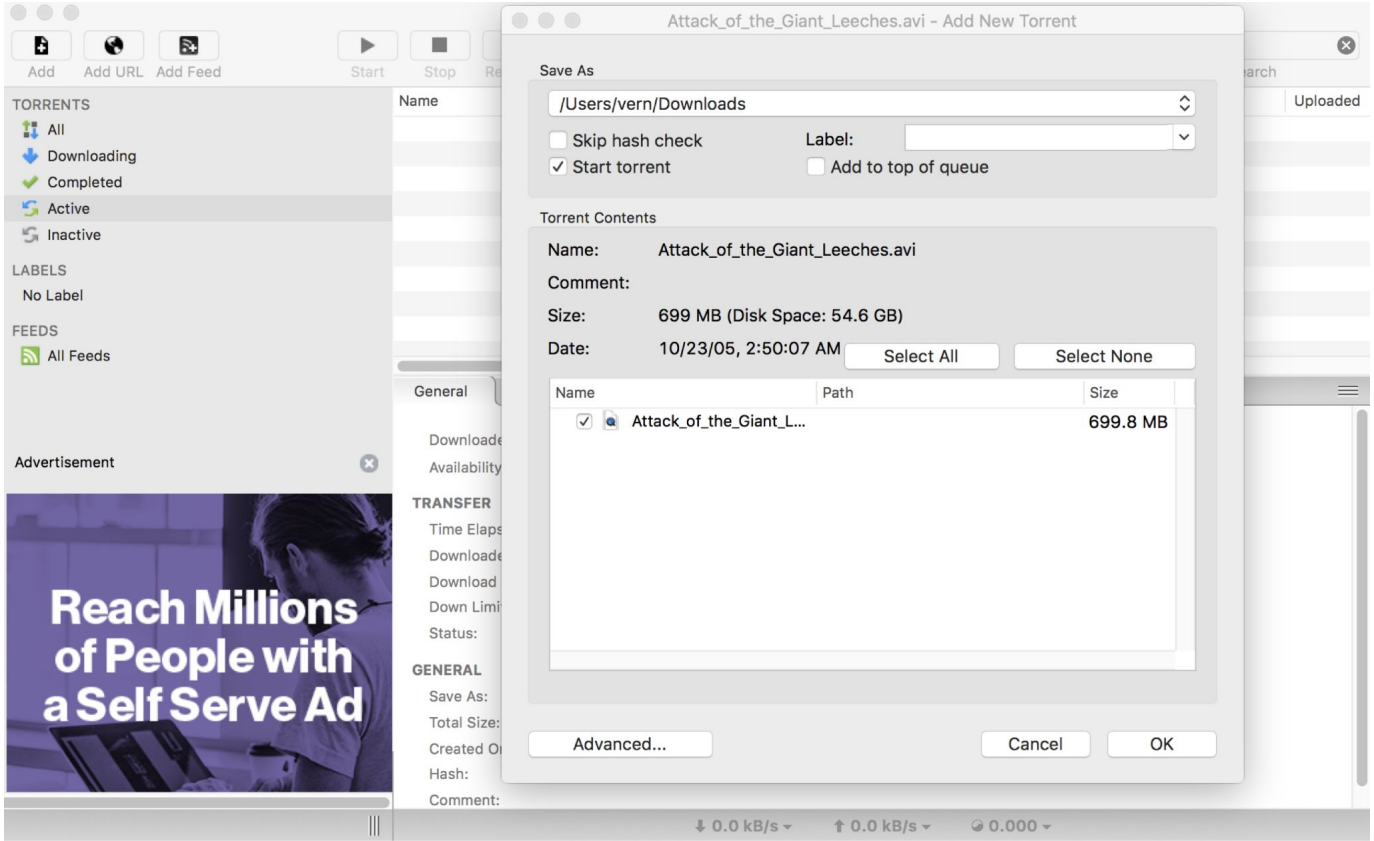
uTorrent


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

uTorrent


µTorrent
Add
Add URL
Add Feed
Start
Stop
Remove
Upgrade Now
piracy
Search
TORRENTS
All
Downloading
Completed
Active
Inactive
LABELS
No Label
FEEDS
All Feeds
Name
#
Size
Done
Status
Seeds
Peers
↓ Speed
↑ Speed
ETA
Uploaded
General
Trackers
Files
Peers
Speed
Downloaded:
Availability:
TRANSFER
Time Elapsed:
Remaining:
Wasted:
Downloaded:
Uploaded:
Seeds:
Download Speed:
Upload Speed:
Peers:
Down Limit:
Up Limit:
Share Ratio:
Status:
GENERAL
Save As:
Total Size:
Pieces:
Created On:
Hash:
Comment:
Advertisement
Reach Millions of People with a Self Serve Ad
0.0 kB/s
0.0 kB/s
0.000

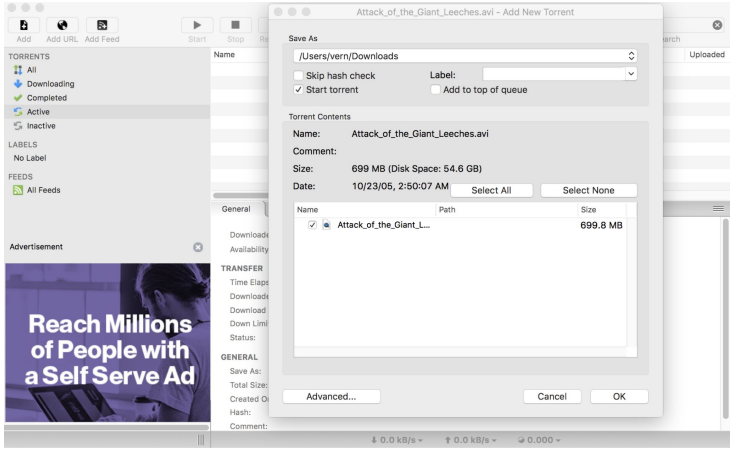
uTorrent


Add
Add URL
Add Feed
Start
Stop
TORRENTS
All
Downloading
Completed
Active
Inactive
LABELS
No Label
FEEDS
All Feeds
Advertisement
Reach Millions of People with a Self Serve Ad
Name
Uploaded
General
TRANSFER
GENERAL
Save As:
Total Size:
Hash:
Comment:
0.0 kB/s
0.0 kB/s
0.000
Attack_of_the_Giant_Leeches.avi - Add New Torrent
Save As
/Users/vern/Downloads
Skip hash check
Start torrent
Label:
Add to top of queue
Torrent Contents
Name: Attack_of_the_Giant_Leeches.avi
Comment:
Size: 699 MB (Disk Space: 54.6 GB)
Date: 10/23/05, 2:50:07 AM
Select All
Select None
Name
Path
Size
Attack_of_the_Giant_L...
699.8 MB
Advanced...
Cancel
OK

uTorrent

Flaw in Popular µTorrent Software Lets Hackers Control Your PC Remotely

- 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**: <u>Least privilege</u>

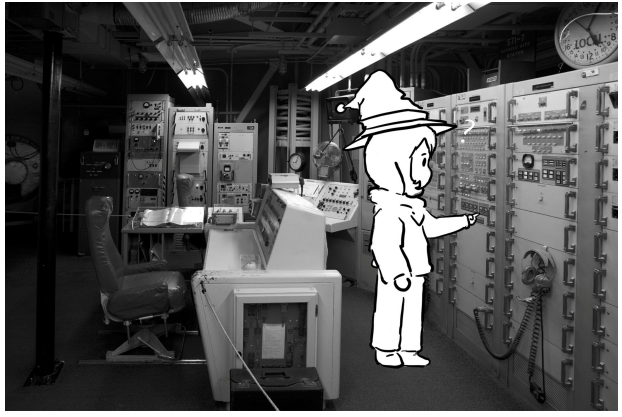


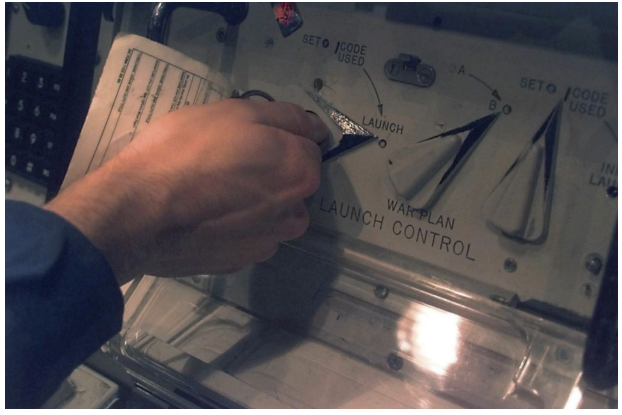
Principle 7: Separation of Responsibility

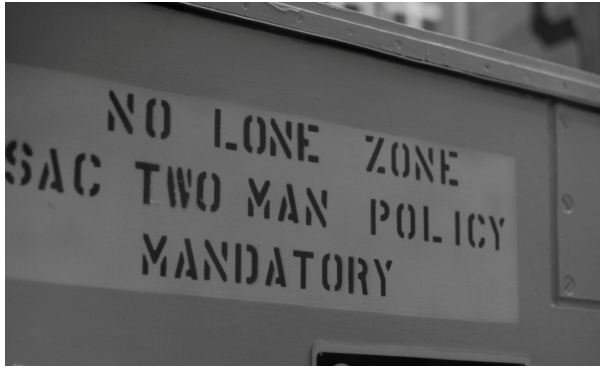
Separation of Responsibility

- Also known as distributed trust
- 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

Welcome to a Nuclear Bunker







Think Along: Movie Theater

- Why do two different employees handle tickets?
  - One sells them, other one checks them and lets you in

Principle 8: Ensure Complete Mediation

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

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

Time

```
withdrawal(5)
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
```

```
withdrawal(5)
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
```

The machine gives you $10!

Principle 9: Don’t Rely on Security Through Obscurity

Don’t Rely on Security Through Obscurity

- Also known as Shannon’s Maxim
- Also known as Kerckhoff’s Principle

Highway Signs

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`**.

Highway Signs

Note: **Do not do this.**

Don’t Rely on Security Through Obscurity

- Don’t do security through obscurity. 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 knows the default password.

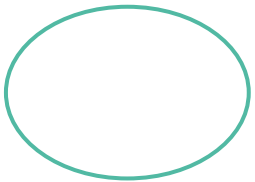
Principle 10: Use Fail-Safe Defaults

Think Along: Room Access

- ALIC rooms are secured by electronic card keys
- **What do you do if the power goes out?**

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



Principle 11: Design in Security from the Start

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!

Summary: Security Principles

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