Security Principles

Announcement: Texas...
- If you have family or friends affected by the Texas flooding...
  - The university has resources to help:
    I don’t know what they are but if you need help finding them,
    I’ll help you find them
  - But resist the temptation to head back now...
    - We want you to succeed and perhaps the best thing is to do well in this semester
    - Plus the logistics in Texas are going to be awful for *months*

Announcement: Logistics
- Sign up on GradeScope
  - Course sign-in code is 9RWWP2
  - Course page is https://gradescope.com/courses/10071
- Project 1 will be issued next Monday
  - Will either be solo or with a single partner, its up to you
    - You don’t need to keep the same partner on subsequent projects

Security Rating: A Real Safe
- TL-15:
  - An expert with common tools will take 
    $\geq 15$ minutes to break in
Security Rating: A Stronger Safe

- TL-30:
  - The same expert and tools now takes 30 minutes

Security Rating: Now We Are Talking

- TRTL-30
  - 30 minute to break with tools and/or a cutting torch

Security Rating: Maximum Overkill...

- TXTL-60:
  - 60 minutes with tools, torches, and up to 4 oz of explosives!
  - Far easier to use "Rubber Hose Cryptanalysis" on someone who knows the combination

Security Rating: 😂😂😂😂😂😂😂😂😂...

- This is legally a "gun safe"
- Meets the California requirements for "safe" storage of a handgun
- But it is practically snake oil:
  - Cylindrical locks can often be opened with a Bic pen
  - Some safes like this open if you just drop them a foot!
- So why do people buy this?
  - It creates an illusion of security
  - It meets the legal requirement for security
Lesson: Security is economics

- More security (generally) costs more
  - If it costs the same or less and doesn’t impose other costs, you’d always go with "more security"
- Standards often define security
  - The safe standards from Underwriters Laboratories
  - If you are selling a real safe to a customer who knows what they are buying, you have to meet these standards
  - The "gun safe" standards from the California Department of Justice
What is this program *able* to do?

Can it leak your files elsewhere?

Can it delete all of your files?

Can it send spam?

Can it add a new executable to your search path?

**YES. Why?**

What does this program *need* to be able to do?

Maybe:
- access screen
- manage a directory of downloaded files
- access config & documentation files
- open connections for a given set of protocols
- receive connections as a server
Check for Understanding

- We’ve seen that laptop/desktop platforms grant applications a lot of privileges
- Quiz: Name a platform that does a better job of least privilege

So What Do You Think Here?

Allow “Adult Cat Finder” to access your location while you use the app?
We use your location to find nearby adorable cats.

Don’t Allow  Allow

Thinking About Least Privilege

- When assessing the security of a system’s design, identify the Trusted Computing Base (TCB).
  - What components does security rely upon?
- Security requires that the TCB:
  - Is correct
  - Is complete (can’t be bypassed)
  - Is itself secure (can’t be tampered with)
- Best way to be assured of correctness and its security?
  - KISS = Keep It Simple, Stupid!
  - Generally, Simple = Small
- One powerful design approach: privilege separation
  - Isolate privileged operations to as small a component as possible

Web browser

“Drive-by malware”: malicious web page exploits browser bug to infect local files
The Chrome browser

Goal: prevent “drive-by malware”, where a malicious web page exploits a browser bug to infect local files

TCB (for this property)

The Chrome browser

70% of vulnerabilities are in the rendering engine.

1M+ lines of code

A Failure of Complete Mediation

Every required action needs to be checked for authenticity, integrity and authorization

Ensuring Complete Mediation

- To secure access to some capability/resource, construct a reference monitor
  - Single point through which all access must occur
    - E.g.: a network firewall
  - Desired properties:
    - Un-bypassable (“complete mediation”)
    - Tamper-proof (is itself secure)
    - Verifiable (correct)
  - (Note, just restatements of what we want for TCBs)
  - One subtle form of reference monitor flaw concerns race conditions …
Time of Check to Time of Use Vulnerability

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. dispense $w to user

TOCTTOU = Time of Check To Time of Use

A Hundred Million Dollar TOCTTOU Bug...

- Ethereum is a cryptocurrency which offers "smart" contracts
- Program you money in a language that makes JavaScript and PHP look beautiful and sound
- The DAO (Distributed Autonomous Organization) was an attempt to make a distributed mutual fund in Ethereum
  - Participants could vote on "investments" that should be made
  - Of course nobody actually had any idea what to do with the "investments" but hey, it's the DAO! Gotta get in on the DAO!
- The DAO supported withdrawals as well
  - What is the point of a mutual fund that you couldn't take your money out of?

A "Feature" In The Smart Contract

- To withdraw, the code was:
  - Check the balance, then send the money, then decrement the balance
- But sending money in Ethereum can send to another program written by the recipient
- So someone "invested", then did a withdraw to his program
- Which would initiate another withdraw...

public void buyItem(Account buyer, Item item) {
    if (item.cost > buyer.balance) {
        return; /* they can't afford it */
        buyer.possessions.put(item); /* provide item */
        buyer.possessionsUpdated(); /* freshen screen */
        buyer.balance -= item.cost; /* deduct cost */
        buyer.balanceUpdated(); /* freshen screen */
    }
}
Welcome to a Nuclear Bunker

Two Man Control: Each Needs To Turn the Key

Desired Security Property: Only Want To Destroy The World On Purpose

“Separation of responsibility.”
Summary: Notions Regarding Managing Privilege

- Least privilege
  - The notion of avoiding having unnecessary privileges
- Privilege separation
  - A way to achieve least privilege by isolating access to privileges to a small Trusted Computing Base (TCB)
- Separation of responsibility
  - If you need to have a privilege, consider requiring multiple parties to work together (collude) to exercise it

Impact of a Password Policy

- When you send information to the Internet, it might be possible for others to see that information. Do you want to continue?
  - Yes
  - No

- When you see a dialog box like this, click 'Yes' to make it go away. It available, click the checkbox first to avoid being bothered by it again.
  - Yes
  - No
Security Keys and Human Factors

- This is a security key for storing key material for an encrypted military phone

Summary: Dealing with Users

- Psychological acceptability
  - Will users abide a security mechanism, or decide to subvert it?

- Consider human factors
  - Does a security mechanism assume something about human behavior when interacting with the system that might not hold, even in the absence of conscious decisions by the users to subvert
“Only as secure as the weakest link.”

- "A door lock is only as strong as the window"
“Don’t rely on security through obscurity.”

- Because otherwise the raptors will get you...
- Obscurity does help but you need to design your system so that it fails...
- Kerckhoffs's Principle:
  - A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.
- Shannon's Maxim:
  - The enemy knows the system
“Trusted path.”

- Users need to know they are talking with the legit system
- System needs to know its talking with the legit user
- These channels need to be unspoofable and private
  - ATM skimmers are a failure of the trusted path
“Use fail-safe defaults.”

• But it can often be hard to determine
• Default for access here is reasonable...
  • Deny all except for an allowed user list
• But when the power goes out...
  • Should the lock fail shut?
    Should the lock fail open?
Common Assumptions When Discussing Attacks

• (Note, these tend to be pessimistic ... but prudent)
• Attackers can interact with our systems *without particular notice*
  • Probing (poking at systems) may go unnoticed ...
  • ... even if highly repetitive, leading to crashes, and easy to detect
• It’s easy for attackers to know general information about their targets
  • OS types, software versions, usernames, server ports, IP addresses, usual patterns of activity, administrative procedures

Common Assumptions, con’t

• Attackers can obtain access to a copy of a given system to measure and/or determine how it works
  • Shannon’s Maxim: “The Enemy Knows the System”
• Attackers can make energetic use of automation
  • They can often find clever ways to automate
• Attackers can pull off complicated coordination across a bunch of different elements/systems
• Attackers can bring large resources to bear if req’d
  • Computation, network capacity
  • But they are not super-powerful (e.g., control entire ISPs)

Common Assumptions, con’t

• If it helps the attacker in some way, *assume they can obtain privileges*
  • But if the privilege gives everything away (attack becomes trivial), then we care about unprivileged attacks
• The ability to robustly detect that an attack has occurred *does not replace desirability of preventing*
  • Infrastructure machines/systems are well protected (hard to directly take over)
  • So a vulnerability that requires infrastructure compromise is less worrisome than same vulnerability that doesn’t

Common Assumptions, con’t

• Network routing is hard to alter ... other than with physical access near clients (e.g., “wifi/coffeeshop”)
  • Such access helps fool clients to send to wrong place
  • Can enable Man-in-the-Middle (MITM) attacks
• We worry about attackers who are lucky
  • Since often automation/repetition can help “make luck”: If its 1 in a million, just try a million times!
• Just because a system does not have apparent value, *it may still be a target*
  • “Lets break into the Casino network... Through the fishtank”
• Attackers are mostly undaunted by fear of getting caught
  • There are exceptions