Computer Security

Security Risks

- Computerized systems are often susceptible to more security risks than non-computerized alternatives
- On the other hand, there are things computers can do that are infeasible or uneconomical by hand
- Both using and not using computers carries risks (how do you back up paper medical records?)

Theft by Computer

- Scale
- Repetition
- Frequently, more people have access to more data

Scale

- Computers can store *lots* of data
- High-capacity storage media are very small and very cheap
- High-bandwidth connectivity is very common
- Both insiders and outsiders can steal much more data by computer than manually

Large-Scale Manual Information Thefts

- Of course, large-scale manual thefts have taken place
- In the late 1960s, Israel stole the complete plans for the French Mirage 5 fighter: 250,000 documents, weighing over 3 tons. . . (https://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=152)
- Daniel Ellsberg gave the “Pentagon Papers”—47 volumes, 7,000 pages—to the NY Times and other newspapers (1971)
- The “Media 9” broke into an FBI field office, stole all of the files, and sent copies to reporters (1971)
- But it’s easier by computer—think Edward Snowden

Repetition

- You can steal a lot of money at once, or you can steal a little bit, repeatedly
- “Bite fraud” versus “nibble fraud” (AKA “salami fraud”)
- Purported nibble fraud: when calculating interest payments, always round down to the lower cent; add the fractions of a cent—from many accounts—to the fraudster’s account

Access

- Locking down things too finely is difficult—users don’t understand how to do it
- The operating systems and networks may not permit the kind of controls you want
- It’s very easy to forget to revoke permissions when people leave the company or switch job roles
- Attacks

Attacks

- Many kinds!
- Technical attacks
  - Network protocol or system design
  - Cryptographic (rare)
  - Bugs
- Social attacks (phishing, spear-phishing, etc.)
- Combination attacks

Typical Penetration

- Initial penetration, via a bug or phishing for credential theft
  ☞ Sometimes, social engineering is used
- Internal scanning for “interesting” systems
- Lateral movement, via bugs or stolen credentials

Three Crucial Questions

- What are you trying to protect?
- Who is your enemy?
- What are your enemy's powers?

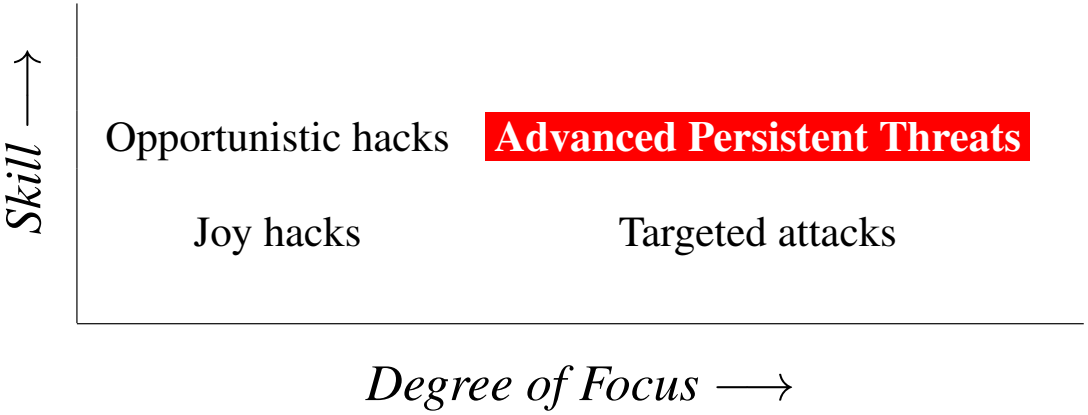
Enemy Goals

- Theft of information
- Damage
- Extortion
- Ransom (via encrypted files)
- Vandalism
- Bragging
- Access to your resources
- Voyeurism
- More? Probably...

Enemies

- (Teenage?) joy hackers
- Low-level criminals (phishers, spammers, etc.)
- Organized crime
- Insiders
- Industrial spies
- Foreign governments
- Or, of course, combinations

The Threat Matrix



Joy Hackers

- Many are “script kiddies”; some are very competent.
- ☞ The scripts are very sophisticated.
- The hackers share tools more than the good guys do.

Are Joy Hackers a Problem?

- What would it cost you to rebuild a machine?
- What would your CEO say if you ended up on the front page of the NY Times?
- What if they're working for someone else?
- N.B. Their target selection has improved.

Opportunistic Attacks

- They’re good, often very good—but they don’t care whom they get
- Most viruses, spam emails, phishing emails, etc., fall into this category
- First you shoot the arrows, then you paint your target. . .

Hacking for Profit

- The hackers have allied themselves with the spammers and the phishers
- The primary motivation for most current attacks is *money*
- The market has worked—the existence of a profit motive has drawn new talent into the field
- We are seeing, in the wild, sophisticated attacks
- We're seeing less pure vandalism
- Many of today's worms and viruses are designed to turn victim computers into "bots" or cryptocurrency miners
- Turning off the Internet isn't profitable. . .

Organized and Disorganized Crime

- In many cases, hacking is just another venue for ordinary criminal activity
- The same people who hack steal also credit card numbers, launder money, etc.
- Some are even former drug dealers

Equifax

- Equifax is a *credit reporting firm*
- The site was penetrated in early March, 2017
- The attackers entrenched themselves and started looking around internally
- On May 13, they started stealing data
- By the time they were detected and access was shut down, they stole information on more than 145,000,000 Americans
- What happened?

(What's a Credit Reporting Firm?)

- Collects information used to assess how risky people are as borrowers
- Have massive databases on more or less everyone
- Governed by the Fair Credit Reporting Act (15 U.S.C. §1681)
- You're the data, not the customer; you can't opt out of being in their database
- Banks, etc., are their customers
- The data is valuable to criminals for identity theft
  ☞ but many analysts think that a government was behind that hack
- N.B. Credit bureaus go back to the mid-19th century

Struts

- On March 6, a bug was disclosed and fixed in the Apache Struts framework
- By March 9, the bug was actively being exploited by hackers
- Equifax Security was aware of this, and on March 8 ordered their systems patched
- This email wasn't heeded, and an internal network scan a week later failed to detect an unpatched system—why isn't clear
- The hackers had better scans. . .

SamSam

- Manually launched, highly targeted *ransomware*
- Ransomware: encrypts your disk; demands payment (in Bitcoin) for the decryption key
- SamSam is aimed at hospitals, government agencies, etc.
- It's spread in a variety of ways, mostly by looking for open vulnerable services, e.g., RDP (Remote Desktop Protocol)
- ☞ Recent prominent ransomeware victim: Colonial Pipeline
- If you have good backups, you can restore from them instead—but that might be more expensive than paying up

Lessons

- A good IT infrastructure matters—why didn't Equifax *know* where its web servers were and what they ran?
- Good IT management matters—why wait a week to do the scan, and why not follow up with local sysadmins who didn't report successful patches
- Good internal monitoring matters—don't rely on your firewall

Targeted Attacks

- Often an insider
- They'll do lots of research on *you*
- May send "spear-phishing" emails

Phishing versus Spear-Phishing

- Phishing: bulk email about, e.g., your account at some bank
- Spear-phishing: highly targeted email based on what particular individuals are believed to be susceptible to

☞ Email about hiring to someone in HR

☞ “Would you review this paper?” to an academic

☞ Often purports to be from someone known to the recipient

A Sample Phishing Message

From: iCloud <service@intlapple.com>
To: Recipients <service@intlapple.com>
Subject: Your Apple ID was used to sign in to iCloud via a web browser.?
Date: February 5, 2016 at 7:48 54AM

Dear Customer,

Your Apple ID was used to sign in to iCloud via a web browser.

Date and Time: February 04, 2016, 10:13 PM +10:00
Browser: Firefox
Operating System: Windows

If the information above looks familiar, you can disregard this email.

If you have not signed in to iCloud recently and believe someone may have accessed your account, go to Apple ID Login now and change your password as soon as possible.

Apple Support

The Phishing Link

Dear Customer,

Your Apple ID was used to sign in to iCloud via a web browser.

Date and Time: February 04, 2016, 10:13 PM +10:00
Browser: Firefox
Operating System: Windows

If the information above looks familiar, you can disregard this email.

If you have not signed in to iCloud recently and believe someone may have accessed your account, go to Apple ID Login now and change your password as soon as possible.

Apple Support

http://labotoansu.com.vn/logs/1PHP.php?
mailbox=INBOX&actionID=105FromSubmit=true&FOLDER=SF_INBOX&dub=1

Stolen Credentials

- Generally, these are passwords
- If you reuse passwords, they can be stolen from one site and used on another
- “Strong” passwords prevent guesses at passwords—and don’t matter nearly as much if you *never* reuse passwords
- A better defense: *multi-factor authentication*, typically by some sort of “token” you have to use in addition to your password
- It could be an app on your phone, e.g., the Duosec app we all use here
- (Also done by email or text message, but those aren’t as secure)

Security Tokens

An RSA SecurID token

A Yubikey FIDO2 token

Inside Jobs

- Insiders know what you have.
- Insiders often know the weak points.
- Insiders are on the inside of your firewall.
- Etc., etc., etc.

☞ What if your system administrator turns to the Dark Side?

Industrial Espionage

- Less than 5% of attacks are detected. Professionals who are after you won't use your machine to attack other companies, and that's how successful penetrations are usually found.
- Professionals are more likely to use non-technical means, too: social engineering, bribery, wiretaps, etc.
- Professionals tend to know what they want.

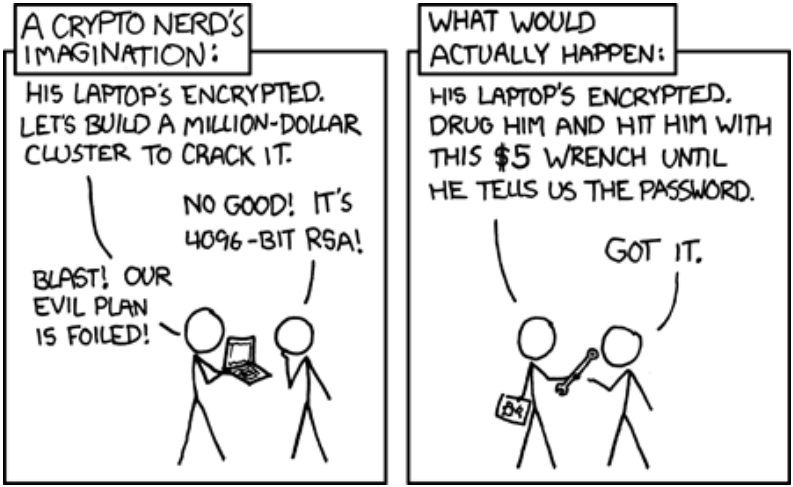
Advanced Persistent Threats

- Generally a codename for governments
- ☞ In the US, it usually means China or Russia
- Get in, often by clever means
- Do what's necessary
- *Stay hidden*!

Spies

- Governments may want your technology.
- Some governments lend tangible support to companies in their own countries.
- Spies tend to be sophisticated, well-funded, etc.
- Governments can attack cryptosystems
- Is cyberwarfare a threat?

Why the Attacker Matters



(http://www.xkcd.com/538/)

The Threat Level

- What sorts of activities are taking place?
- What could happen?
- Is it real or is it hype?

Types of Activity

Cyberespionage	Spying, but by computer
Cyberattack	Offensive attack; may or may not be an act of war
Preparing the Battlefield	Penetrate a crucial system and stay there, against possible future need

The NSA

- According to the Snowden revelations, the NSA has engaged in large-scale, sophisticated system and network penetrations
- Massive spying on Internet backbone links
- Highly targeted attacks against specific countries and individuals–even tampering with computers during shipment
- Supposedly worked with Israel to develop Stuxnet, attack software that damaged Iran's uranium enrichment centrifuges
- Who's better, the NSA or the Russians?

Stuxnet

- Extremely sophisticated malware—jumped airgaps to attack
- Highly targeted—would attack *only* the centrifuge plant
- (Would spread elsewhere, but not cause damage)
- Attacked Programmable Logic Controllers (PLCs), specialized interfaces to industrial equipment
- Attackers had detailed knowledge of the plant—how?
- Used five “zero-days”—holes for which there was no known defense
- Persisted for years; related to other malware found in the wild

SolarWind—A Supply Chain Attack

- SolarWind makes a popular enterprise-scale network management software system
- Many large enterprises, including government agencies, use it
- Someone, purportedly the SVR (Russian foreign intelligence), hacked SolarWind and planted a “back door” in the software package
- When their customers updated their software, the SVR had ready access to all of these enterprise networks
- Other attackers have been targeting popular open source software packages, including to install crypto-currency mining packages

What's a Cyberwar?

- No one knows—we've never had one
- Some experts doubt there could be a strategic-grade cyber attack—the effects are too upredictable
- There don't seem to be any feasible defenses
- Could deterrence work? It's hard—all too often, we don't know who the attacker is
- "I have seen too many situations where government officials claimed a high degree of confidence as to the source, intent, and scope of a [cyber]attack, and it turned out they were wrong on every aspect of it. That is, they were often wrong, but never in doubt." (DoJ official)
- (But attribution is getting better)
- It's also hard to know your opponents' capabilities

What Might One Be Like?

- Disrupt the power grid (the CIA claims that extortionists have done this abroad—others dispute that)
- Scramble financial records
- Interfere with transportation
- Blow up pipelines (the report of the CIA doing that to the Soviets in 1982 does not appear to be true)

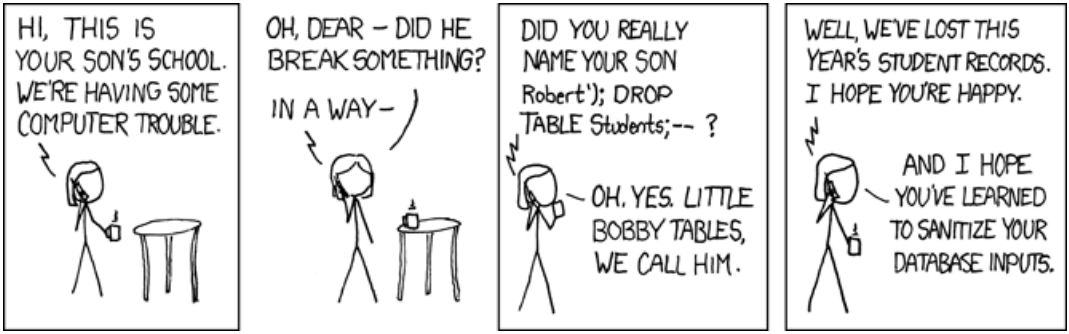
Is this Plausible?

- Some experts doubt all this
- There's no profit in cyberwar—and it may be more valuable to spy on your enemies than to destroy their communications networks
- Besides, recovery is often not that difficult, and defenders will be busy, too

Back to Bugs. . .

- The most common way to penetrate a system
- As we've discussed, eliminating all bugs is very hard
- Defending against attackers exploiting such bugs is even harder
- Einstein said "Nature is subtle but not malicious". Attackers are subtle *and* malicious

Subtle Bugs



(http://xkcd.com/327/)

Where Are We Now?

- The most visible current threat is ransomware
- Much of it seems to be originating in Russia
- Payment is via Bitcoin or other cryptocurrency
- Recent wrinkle: if you don’t pay up, the attackers also leak your files to the world

Striking Back?

- One prominent ransomware gang has apparently been shut down by a counter-attack
- It may have been the FBI and US Cybercommand, possibly with foreign allies
- The FBI recovered decryption keys, too

What About “Hack-Back”?

- Should private companies be allowed to strike back at their attackers?

What About “Hack-Back”?

- Should private companies be allowed to strike back at their attackers?
- Do they know who the attackers really are?

What About “Hack-Back”?

- Should private companies be allowed to strike back at their attackers?
- Do they know who the attackers really are?
- Is it ethical?

What About “Hack-Back”?

- Should private companies be allowed to strike back at their attackers?
- Do they know who the attackers really are?
- Is it ethical?
- Is it legal?

What About “Hack-Back”?

- Should private companies be allowed to strike back at their attackers?
- Do they know who the attackers really are?
- Is it ethical?
- Is it legal?
  ☞ U.S. Constitution: “The Congress shall have Power To. . . grant Letters of Marque and Reprisal”

So What's the Problem?

- We've created a very fragile world
- The investment necessary to acquire significant attack abilities is relatively low
- "If builders built buildings the way programmers build programs, then the first woodpecker that came along would destroy civilization" (Gerald Weinberg)

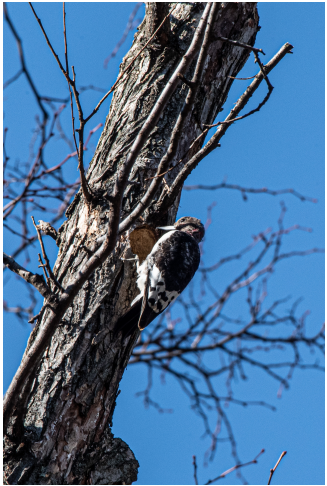
Internal Security

- A single firewall at the front door isn't sufficient (and probably hasn't been since 1997)
- You need internal segmentation
- You need internal intrusion detection
- You need internal logging

What Do We Do?

- Work on program correctness (but we're not going to succeed any time soon)
- Work on usability—too often, it's been ignored
- Multi-factor authentication
- Look for another path to safety, such as "resilient systems"

Questions?



(Red-headed woodpecker, Central Park, February 22, 2020)