CSF 434/534: Advanced Network and System Security

Week 04 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes

Bluejacking and Bluesnarfing

Bluejacking and Bluesnarfing

Bluejacking

- ☑ Sending of unsolicited messages to another device via Bluetooth
  - ☑ No mobile carrier required!
- ☑ Typical functional distance is about 10 meters
  - ☑ More or less, depending on antenna and interference
- ☑ Bluejack with an address book object
  - ☑ Instead of contact name, write a message
    - □ "You are Bluejacked!"
  - ☑ "You are Bluejacked! Add to contacts?"
- ☑ Third-party software may also be used
  - ☑ Blooover, Bluesniff

Bluejacking and Bluesnarfing

Bluesnarfing

- ☑ Access a Bluetooth-enabled device and transfer data
  - ☑ Contact list, calendar, email, pictures, video, etc.
- ☑ First major security weakness in Bluetooth
  - ☑ Marcel Holtmann in September 2003 and Adam Laurie in November 2003
  - ☑ This weakness was patched
- ☑ Serious security issue
  - ☑ If you know the file, you can download it without authentication

RFID and NFC Attacks

RFID and NFC Attacks

RFID (Radio-frequency identification)

- It's everywhere
  - Credit / debit cards
  - Access badges
  - Inventory/Assembly line tracking
  - Pet/Animal identification
  - Anything that needs to be tracked
- Radar technology
  - Radio energy transmitted to the tag
  - RF powers the tag, ID is transmitted back
  - Bidirectional communication
  - Some tag formats can be active/powered

RFID and NFC Attacks

RFID Attacks

- Data capture
  - View communication
  - Replay attack
- Spoof the reader
  - Write your own data to the tag
- Denial of service
  - Signal jamming
- Decrypt communication
  - Many default keys are on The Google

RFID and NFC Attacks

Near field communication (NFC)

- Two-way wireless communication
  - Builds on RFID, which was one-way
- Payment systems
  - Google wallet and MasterCard partnership
- Bootstrap for other wireless
  - NFC helps with Bluetooth pairing
- Access token, identity "card"
  - Short range with encryption support

RFID and NFC Attacks

NFC Security Concern

- Remote capture
  - It's a wireless network
  - 10 meters for active devices
- Frequency jamming
  - Denial of service
- Relay / Replay attack
  - Man in the middle
- Loss of NFC device control
  - Stolen/lost phone

Wireless Disassociation Attacks

Wireless Disassociation Attacks

It started as a normal day

- Surfing along on your wireless network
  - And then you're not
- And then it happens again
  - And again
- You may not be able to stop it
  - There's (almost) nothing you can do
  - Time to get a long patch cable
- Wireless disassociation
  - A significant wireless denial of service (DoS) attack

Wireless Disassociation Attacks

802.11 management frames

- 802.11 wireless includes a number of management features
  - Frames that make everything work
  - You never see them
- Important for the operation of 802.11 wireless
  - How to find access points, manage QoS, associate/ disassociate with an access point, etc.
- Original wireless standards did not add protection for management frames
  - Sent in the clear
  - No authentication or validation

Wireless Disassociation Attacks

Protecting against disassociation

- IEEE has already addressed the problem
  - 802.11w - July 2014
- Some of the important management frames are encrypted
  - Disassociate, deauthenticate, channel switch announcements, etc.
- Not everything is encrypted
  - Beacons, probes, authentication, association
  - Cart before the horse
- 802.11w is required for 802.11ac compliance
  - This will roll out going forward

Cryptographic Attacks

Cryptographic Attacks

Cryptographic attacks

- You’ve encrypted data and sent it to another person
  - Is it really secure?
  - How do you know?
- The bad guy doesn’t have the combination (the key)
  - So they break the safe (the cryptography)
- Finding ways to undo the security
  - There are many potential cryptographic shortcomings

Cryptographic Attacks

Known plaintext attack (KPA)

- Attacker has both the plaintext and the encrypted data
  - If you know the original plaintext, you may be able to find a “wedge” that is revealed in the ciphertext
  - The known plaintext is the crib
- WWII Enigma cipher
  - Easier to break if you knew some plaintext
  - Daily weather report (wetter)
  - Numbers were common (eins)
  - Royal Air Force would “seed” the North Sea with mines
  - Future messages would reference the harbor name

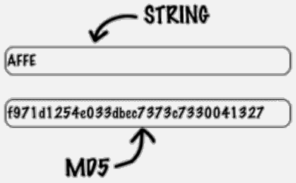
Cryptographic Attacks

The password file

- Different across operating systems
- Different hash methods
- Linux Account Hashes
  - Jumper Bay:1001::42e2f19c31c9ff73cb97eb1b26c10f54:::
    Carter:1007::cf4eb977a6859c76efd21f5094ecf77d:::
    Jackson:1008::e1f757d9cdc06690509e04b5446317d2:::
    O'Neill:1009::78a8c423faedd2f002c6aef69a0ac1af:::
    Teal'c:1010::bf84666c81974686e50d300bc36aea01:::

Cryptographic Attacks

Rainbow tables



- An optimized, pre-built set of hashes
  - Doesn't need to contain every hash
  - The calculations have already been done
- Remarkable speed increase
  - Especially with longer password lengths
- Need different tables for different hashing methods (MD5 / SHA1)
  - Windows is different than MySQL
- Rainbow tables won't work with salted hashes
  - Additional random value added to the original hash
  - e.g (password + random bit/byte sequence)

Cryptographic Attacks

Dictionary attacks

- People use common words as passwords
  - You can find them in the dictionary
- If you're using brute force, you should start with the easy ones
  - password, ninja, football
- Many common wordlists available on the 'net
  - Some are customized by language or line of work
- This will catch the low-hanging fruit
  - You'll need some smarter attacks for the smarter people

Cryptographic Attacks

Brute force

- The password is the key
  - Secret phrase
  - Stored hash
- Brute force attacks - Online
  - Keep trying the login process
  - Very slow
  - Most accounts will lockout after a number of failed attempts
- Brute force the hash - Offline
  - Obtain the list of users and hashes
  - Calculate a password hash, compare it to a stored hash
  - Large computational resource requirement

Cryptographic Attacks

Birthday attack

- In a classroom of 23 students, what is the chance of two students sharing a birthday?
  - 23 students - about 50%
  - For a class of 30, the chance is about 70%
- In the digital world, this is a hash collision
  - A hash collision is the same hash value for two different plaintexts
  - Find a collision through brute force
- The attacker will generate multiple versions of plaintext to match the hashes
  - Protect yourself with a large hash output size

Cryptographic Attacks

Collisions

- Hash digests are supposed to be unique
  - Different input data should never create the same hash
- MD5 hash
  - Message Digest Algorithm 5
  - First published in April 1992
  - Collisions identified in 1996
- December 2008: Researchers created CA certificate that appeared legitimate when MD5 is checked
  - Built other certificates that appeared to be legit and issued by RapidSSL

Cryptographic Attacks

Downgrade attack

- Instead of using perfectly good encryption, use something that’s not so great
  - Force the systems to downgrade their security
- 1995 - SSL/TLS vulnerability - FREAK - Factoring RSA Export Keys
  - Public key pairs can be limited to 512 bits or less
    - 1990 U.S. cryptography export regulations
- Weak keys could be forced during the SSL handshake
- Modern systems can easily brute force the small keys
- Vulnerability was patched

Cryptographic Attacks

Weak implementations

- Weak encryption
  - One weak link breaks the entire chain
- 802.11 WEP
  - The RC4 key can be recovered by gathering enough packets
  - The algorithm didn’t sufficiently protect the key
- DES - Data Encryption Standard
  - Relatively small 56-bit keys
  - Modern systems can brute force this pretty quickly

Cryptographic Attacks

Replay attacks

☑ Some cryptographic algorithms are more susceptible than others to a replay attack

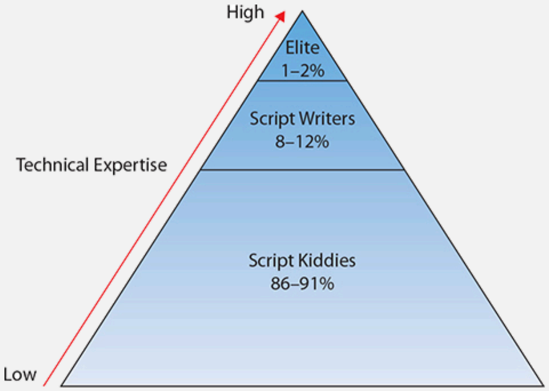
☑ A hash with no salt, no session ID tracking, no encryption

☑ Replay countermeasure may be part of the cryptography

☑ Kerberos and Kerberos derivatives include time stamps

☑ Anything after the time to live (TTL) is discarded

Threat Actors



Threat Actors

Threat actors and attributes

☑ The entity responsible for an event that has an impact on the safety of another entity

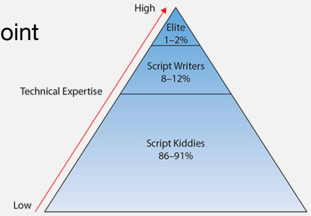
- ☑ Also called a malicious actor

☑ Broad scope of actors

- ☑ And motivations vary widely

☑ Intelligence can come from everywhere

- ☑ Open source intelligence is a massive starting point



Threat Actors

Script kiddies

☑ Runs premade scripts without any knowledge of what's really happening

- ☑ Not necessarily a youngster

☑ Can be internal or external

- ☑ But usually external

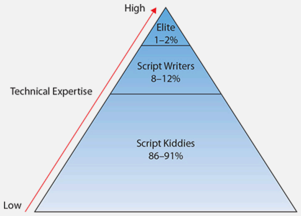
☑ Not very sophisticated

☑ No formal funding

- ☑ Looking for low hanging fruit

☑ Motivated by the hunt

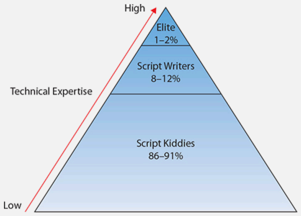
- ☑ Working the ego, trying to make a name



Threat Actors

Hacktivist

- A hacker with a purpose
  - Social change or a political agenda
  - Often an external entity
- Can be remarkably sophisticated
  - Very specific hacks
  - DoS, web site defacing, release of private documents, etc.
- Funding is limited
  - Some organizations have fundraising options



Threat Actors

Organized crime

- Professional criminals
  - Motivated by money
  - Almost always an external entity
- Very sophisticated
  - Best hacking money can buy
- Crime that’s organized
  - One person hacks, one person manages the exploits, another person sells the data, another handles customer support
- Lots of capital to fund hacking efforts

Threat Actors

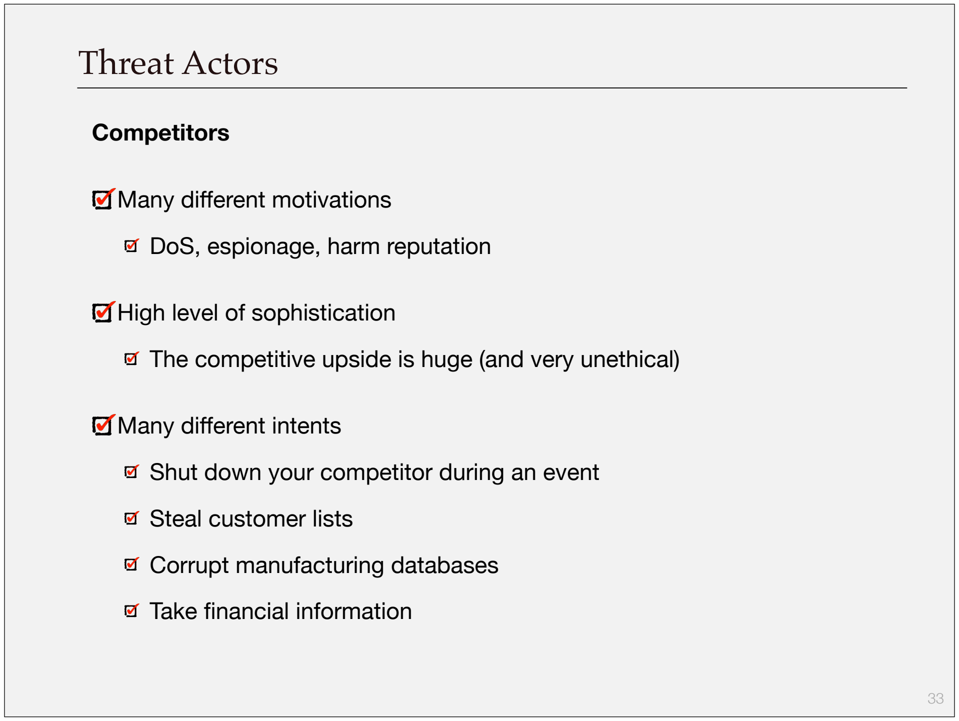
Nation states / APT (Advanced persistent threat)

- Governments
  - National security, job security
  - Always an external entity
- Highest sophistication
  - Military control, utilities, financial control
  - United States and Israel destroyed 1,000 nuclear centrifuges with the Stuxnet worm
- Constant attacks
  - Advanced Persistent Threat (APT)
- Massive resources available

Threat Actors

Insiders

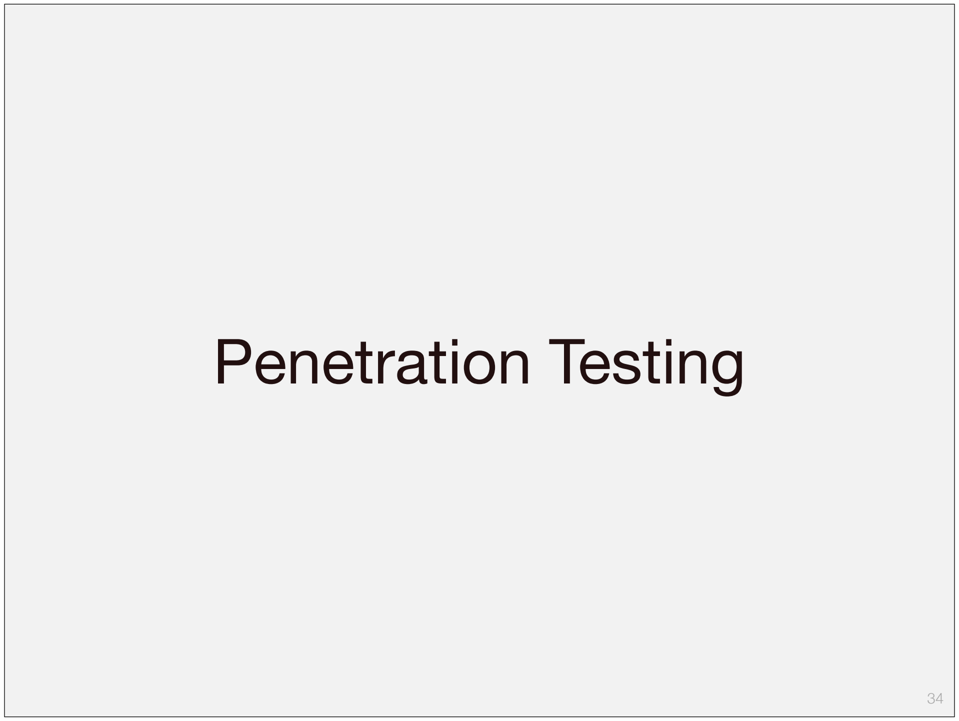
- More than just passwords on sticky notes
  - Some insiders are out for no good
- Sophistication may not be advanced, but the insider has institutional knowledge
  - Attacks can be directed at vulnerable systems
  - The bad guy knows what to hit
- Extensive resources
  - Eating away from the inside



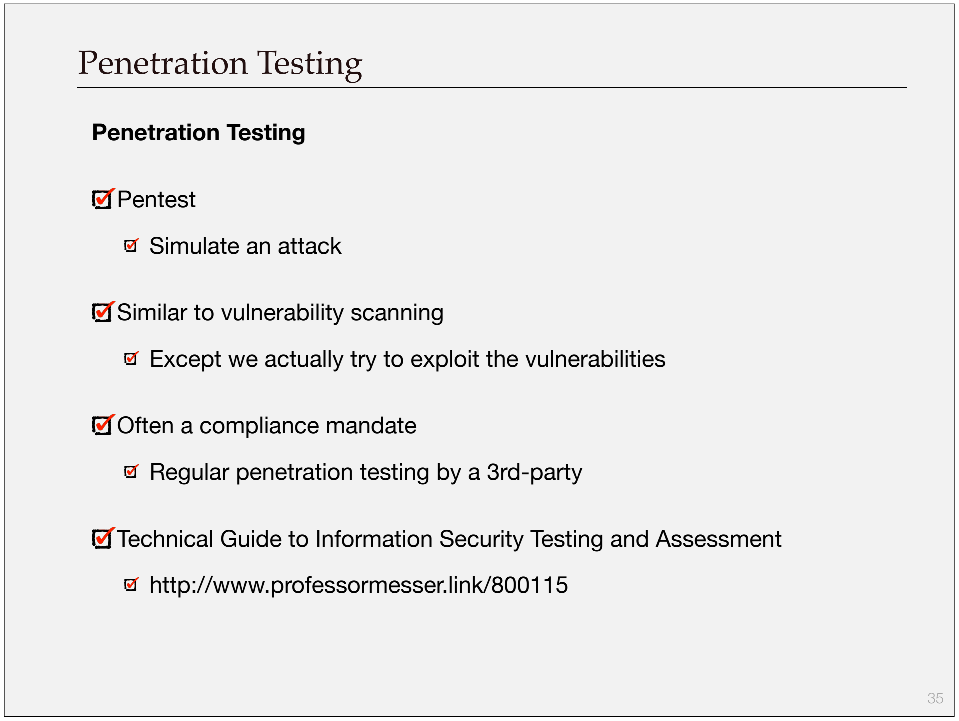
Threat Actors

Competitors

- ☑ Many different motivations
  - ☑ DoS, espionage, harm reputation
- ☑ High level of sophistication
  - ☑ The competitive upside is huge (and very unethical)
- ☑ Many different intents
  - ☑ Shut down your competitor during an event
  - ☑ Steal customer lists
  - ☑ Corrupt manufacturing databases
  - ☑ Take financial information



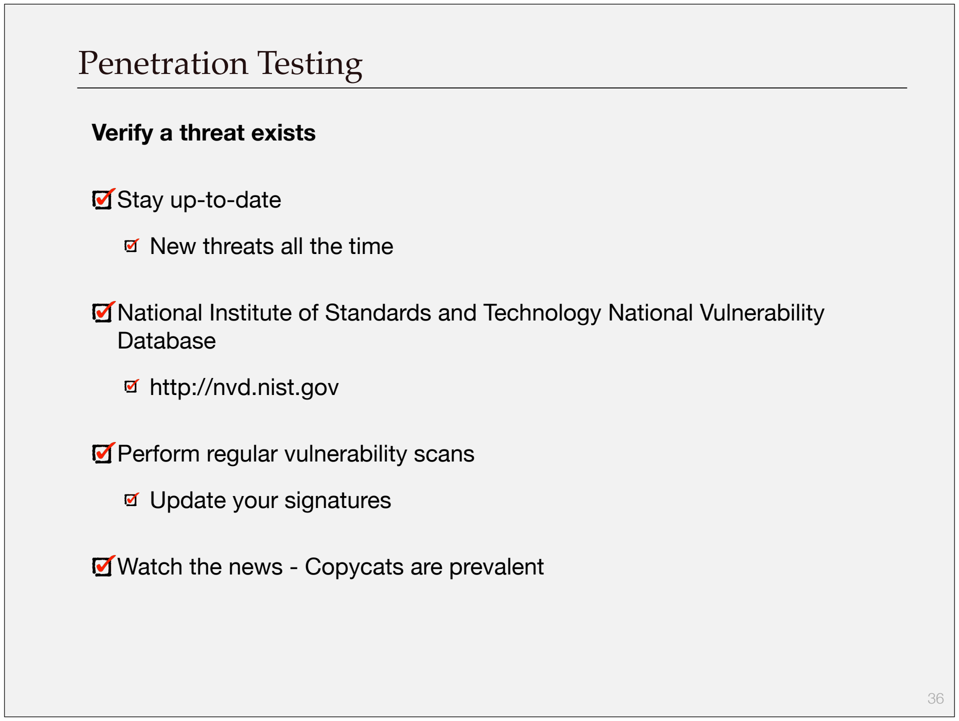
Penetration Testing



Penetration Testing

Penetration Testing

- ☑ Pentest
  - ☑ Simulate an attack
- ☑ Similar to vulnerability scanning
  - ☑ Except we actually try to exploit the vulnerabilities
- ☑ Often a compliance mandate
  - ☑ Regular penetration testing by a 3rd-party
- ☑ Technical Guide to Information Security Testing and Assessment
  - ☑ http://www.professormesser.link/800115



Penetration Testing

Verify a threat exists

- ☑ Stay up-to-date
  - ☑ New threats all the time
- ☑ National Institute of Standards and Technology National Vulnerability Database
  - ☑ http://nvd.nist.gov
- ☑ Perform regular vulnerability scans
  - ☑ Update your signatures
- ☑ Watch the news - Copycats are prevalent

Penetration Testing

Passive reconnaissance

- ☑ Learn as much as you can from open sources
  - ☑ There’s a lot of information out there
  - ☑ Remarkably difficult to protect or identify
- ☑ Social media
- ☑ Corporate web site, online forums, Reddit
- ☑ Social engineering, dumpster diving
- ☑ Business organizations

Penetration Testing

Active reconnaissance

- ☑ Trying the doors
  - ☑ Maybe one is unlocked
  - ☑ Don’t open it yet
  - ☑ Relatively easy to be seen
- ☑ Ping scans, port scans
- ☑ DNS queries
- ☑ OS scans, OS fingerprinting
- ☑ Service scans, version scans

Penetration Testing

Exploiting vulnerabilities

- ☑ Try to break into the system
  - ☑ Be careful; this can cause a denial of service or loss of data
  - ☑ Buffer overflows can cause instability
  - ☑ Gain privilege escalation
- ☑ You may need to try many different vulnerability types
  - ☑ Password brute-force
  - ☑ Social engineering
  - ☑ Database injections
  - ☑ Buffer overflows
- ☑ You’ll only be sure you’re vulnerable if you can bypass security
  - ☑ If you can get through, the bad guys can get through

Penetration Testing

The process

- ☑ Initial exploitation
  - ☑ Get into the network
  - ☑ A challenging hurdle (most of the time)
- ☑ Persistence
  - ☑ Once you’re there, you need to make sure there’s a way back in
  - ☑ Set up a backdoor
  - ☑ Build user accounts, change or verify default passwords
- ☑ The pivot
  - ☑ The foothold point
  - ☑ The inside of the network is often relatively open
  - ☑ Jump from here to the rest of the network

Penetration Testing

Black box, white box, and grey box

- ☑ How much do you know about the test?
  - ☑ Many different approaches
- ☑ Black box
  - ☑ The pentester knows nothing about the systems under attack
  - ☑ “Blind” test
- ☑ White box
  - ☑ Full disclosure
- ☑ Grey box
  - ☑ A mix of black and white
  - ☑ Focus on certain systems or applications

Vulnerability Scanning

Vulnerability Scanning

Vulnerability scanning

- ☑ Usually minimally invasive, unlike a penetration test
- ☑ Port scan - Poke around and see what’s open
- ☑ Identify systems and security devices
- ☑ Test from the outside and inside
  - ☑ Don’t dismiss insider threats
- ☑ Gather as much information as possible
  - ☑ We’ll separate wheat from chaff later

Vulnerability Scanning

Scan types

- ☑ Scanners are very powerful
  - ☑ Use many different techniques to identify vulnerabilities
- ☑ Non-intrusive scans
  - ☑ Gather information, don’t try to exploit a vulnerability
- ☑ Intrusive scans
  - ☑ You’ll try out the vulnerability to see if it works
- ☑ Non-credentialed scans
  - ☑ The scanner can’t login to the remote device
- ☑ Credentialed scan
  - ☑ You’re a normal user, emulates an insider attack

Vulnerability Scanning

Identify vulnerability

- ☑ The scanner looks for everything
  - ☑ Well, not everything ~
  - ☑ The signatures are the key
- ☑ The vulnerabilities can be cross-referenced online
  - ☑ Almost all scanners give you a place to go
  - ☑ National Vulnerability Database: http://nvd.nist.gov/
  - ☑ Microsoft Security Bulletins
- ☑ Some vulnerabilities cannot be definitively identified
  - ☑ You'll have to check manually to see if a system is vulnerable
  - ☑ But the scanner gives you a heads-up

Vulnerability Scanning

Vulnerability scan results

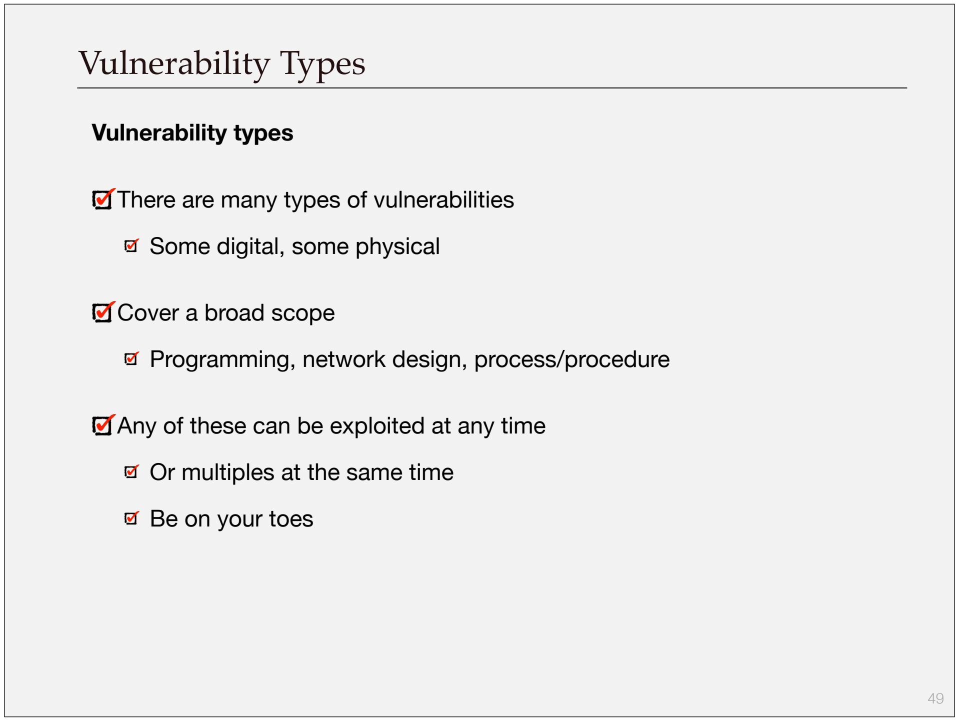
- ☑ Lack of security controls
  - ☑ No firewall, no anti-virus, no anti-spyware
- ☑ Misconfigurations - Open shares, guest access
- ☑ Real vulnerabilities
  - ☑ Especially newer ones, occasionally the old ones

Vulnerability Scanning

Dealing with false positives

- ☑ False positives
  - ☑ A vulnerability is identified that doesn't really exist
- ☑ This is different than a low-severity vulnerability
  - ☑ It's real, but it may not be your highest priority
- ☑ False negatives
  - ☑ A vulnerability exists, but you didn't detect it
- ☑ Update to the latest signatures
  - ☑ If you don't know about it, you can't see it
  - ☑ Work with the vulnerability detection manufacturer
  - ☑ They may need to update their signatures for your environment

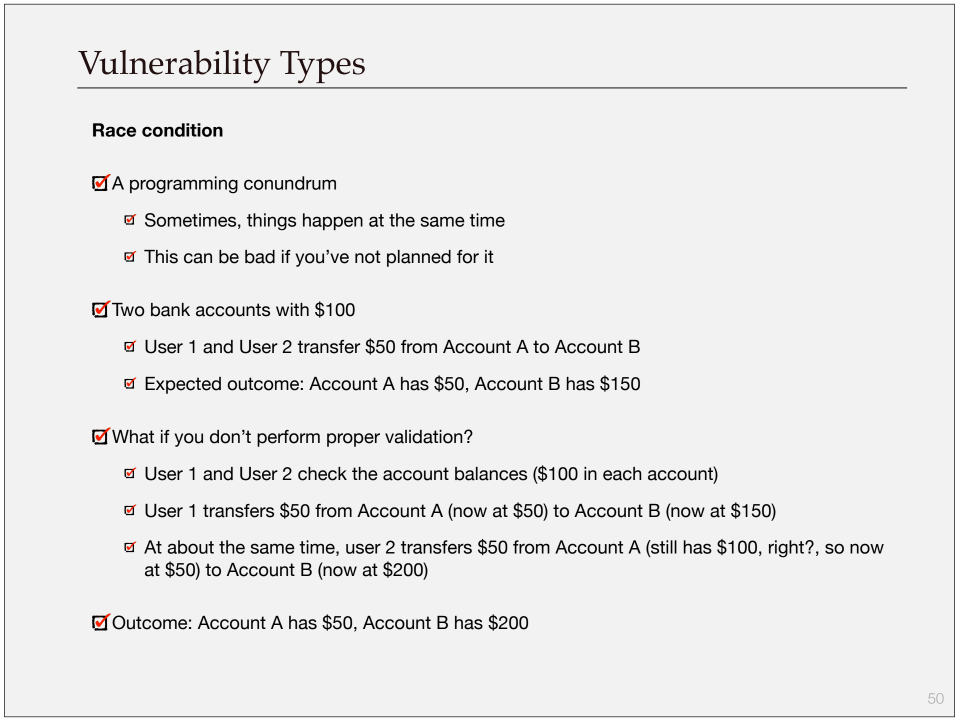
Vulnerability Types



Vulnerability Types

Vulnerability types

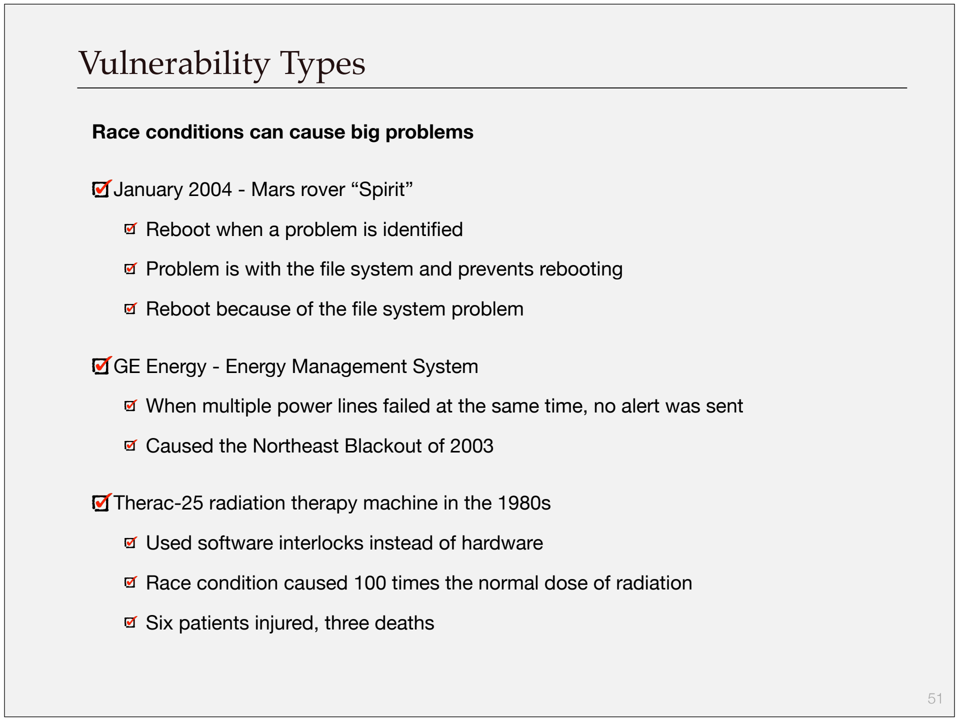
- There are many types of vulnerabilities
  - Some digital, some physical
- Cover a broad scope
  - Programming, network design, process/procedure
- Any of these can be exploited at any time
  - Or multiples at the same time
  - Be on your toes



Vulnerability Types

Race condition

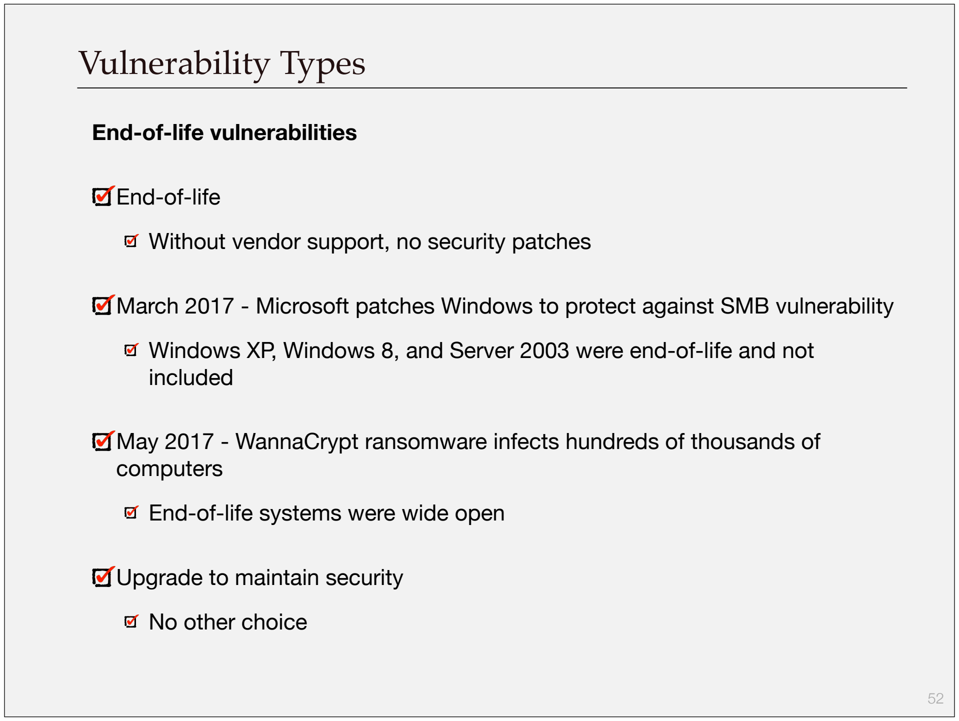
- A programming conundrum
  - Sometimes, things happen at the same time
  - This can be bad if you've not planned for it
- Two bank accounts with $100
  - User 1 and User 2 transfer $50 from Account A to Account B
  - Expected outcome: Account A has $50, Account B has $150
- What if you don't perform proper validation?
  - User 1 and User 2 check the account balances ($100 in each account)
  - User 1 transfers $50 from Account A (now at $50) to Account B (now at $150)
  - At about the same time, user 2 transfers $50 from Account A (still has $100, right?, so now at $50) to Account B (now at $200)
- Outcome: Account A has $50, Account B has $200



Vulnerability Types

Race conditions can cause big problems

- January 2004 - Mars rover "Spirit"
  - Reboot when a problem is identified
  - Problem is with the file system and prevents rebooting
  - Reboot because of the file system problem
- GE Energy - Energy Management System
  - When multiple power lines failed at the same time, no alert was sent
  - Caused the Northeast Blackout of 2003
- Therac-25 radiation therapy machine in the 1980s
  - Used software interlocks instead of hardware
  - Race condition caused 100 times the normal dose of radiation
  - Six patients injured, three deaths



Vulnerability Types

End-of-life vulnerabilities

- End-of-life
  - Without vendor support, no security patches
- March 2017 - Microsoft patches Windows to protect against SMB vulnerability
  - Windows XP, Windows 8, and Server 2003 were end-of-life and not included
- May 2017 - WannaCrypt ransomware infects hundreds of thousands of computers
  - End-of-life systems were wide open
- Upgrade to maintain security
  - No other choice

Vulnerability Types

Lack of vendor support

- ☑ Security requires diligence
  - ☑ The potential for a vulnerability is always there
- ☑ Vendors are the only ones who can fix their products
  - ☑ Assuming they know about the problem
  - ☑ And care about fixing it
- ☑ Trane Comfortlink II thermostats
  - ☑ Control the temperature from your phone
  - ☑ Trane notified of three vulnerabilities in April 2014
  - ☑ Two patched in April 2015, one in January 2016

Vulnerability Types

Improper input handling

- ☑ Many applications accept user input
  - ☑ We put data in, we get data back
- ☑ All input should be considered malicious
  - ☑ Check everything. Trust nobody.
- ☑ Allowing invalid input can be devastating
  - ☑ SQL injections, buffer overflows, denial of service
- ☑ It takes a lot of work to find input that can be used maliciously
  - ☑ But they will find it

Vulnerability Types

Improper error handling

- ☑ Errors happen
  - ☑ And you should probably know about it
- ☑ Messages should be just informational enough
  - ☑ Avoid too much detail
  - ☑ Network information, memory dump, stack traces, database dumps
- ☑ This is an easy one to find and fix
  - ☑ A development best-practice

Vulnerability Types

Misconfiguration/weak configuration

- ☑ Very easy to leave a door open
  - ☑ The hackers will always find it
- ☑ September 2015 - Patreon is compromised
  - ☑ Used a debugger to help troubleshoot site issues
  - ☑ Was left exposed to the Internet
  - ☑ Effectively allowed for remote code executions
  - ☑ Gigabytes of customer data was released online
- ☑ June 2017 - 14 million Verizon records exposed
  - ☑ Third-party left an Amazon S3 data repository open
  - ☑ Researcher found the data before the bad guys

CSF 434/534: Advanced Network and System Security

Week 04 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes