Introduction to Computer and Network Security

CS-3113: PRINCIPLES OF CYBER SECURITY

BENJAMIN R. ANDERSON

Computers are Tools

Computers assist us in our work, expand our thinking, and provide entertainment

Because computers are used everywhere, they are used to commit crimes

Preventing, detecting, and prosecuting computer crime is a challenge

Sophos 2022 Threat Report

https://assets.sophos.com/X24WTUEQ/at/b739xqx5jg5w9w7p2bpzxg/sophos-2022-threat-report.pdf

I encourage you to read (or at least skim) the report, but here are some key quotes:

- As one of the most potentially damaging and costly types of malware attacks, ransomware remains the kind of attack that keeps most administrators up at night, a Keyser Söze of the internet.
- This ransomware-as-a-service (or RaaS) model has changed the landscape in ways we couldn't predict.
- [Re: Cobalt Strike] In fact, the Beacons do such a good job, criminals only need to make minor modifications to the source code in order to leverage the Beacon as a foothold on an infected machine.
- Since the 2010s, breakthroughs in neural network vision and language technologies have disrupted the way we practice defensive cybersecurity. For example, most security vendors now use vision and language inspired neural network technologies to help detect threats.

Sophos 2022 Threat Report

Another quote:

In past years, we were able to break down attacks into two broad categories. The first: shotgun attacks, in which the threat actors might spam absolutely everyone, or use search engine optimization (SEO) techniques to drive search engine users to malicious web pages. And second: highly targeted attacks, in which the attackers have done some homework and go into the attack with foreknowledge about the target organization, the people who make up that organization, and which of those people might be juicy targets.

But in 2021, we saw the emergence of a hybrid category: a broad-based attack meant to lure in lots of people, but that only fires off when the unlucky people who stumble into the trap meet certain criteria. This may seem counterintuitive, but from the criminals' perspective, it makes some sense: they can block malware analysts from continuing to probe their servers, and they also reduce suspicion by keeping the number of attacks relatively low, under the radar that might otherwise tip off security researchers or IT admins to a wider campaign.

Sophos 2022 Threat Report

More quotes:

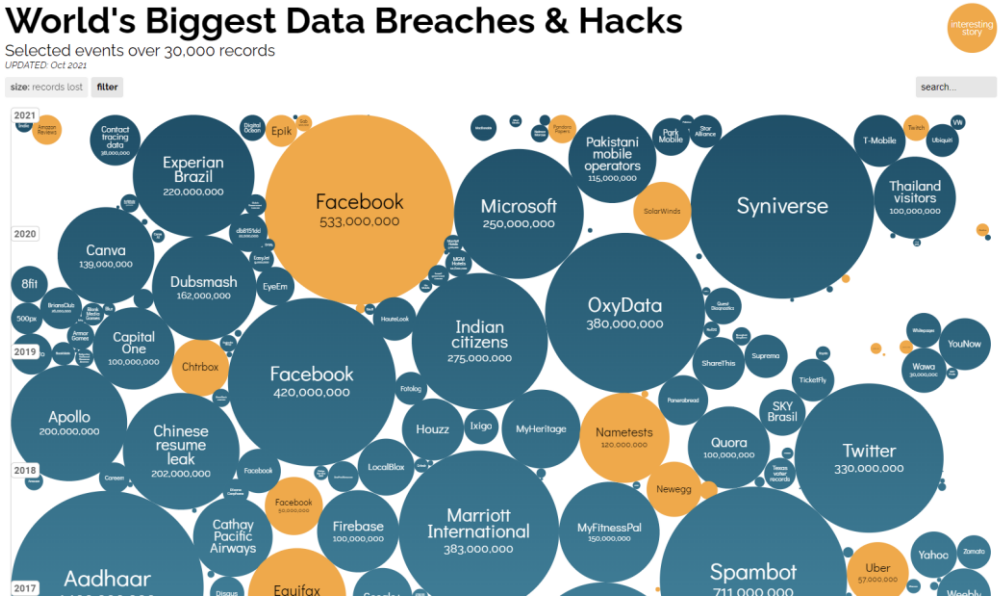
- More than in any previous year, in 2021 it felt like almost every week we were confronted with a major cyberattack that threatened thousands of large enterprises or organizations. From the SolarWinds hack and the ransomware attack that forced the Colonial Pipeline to shut down, to a massively disruptive Revil ransomware attack over the July 4 U.S. holiday weekend, the infrastructure that underpins business on the internet seemed to be under constant threat.
- Ransomware attackers have not ignored the potentially lucrative targets that have Linux servers. A ransomware family called RansomEXX appeared in 2021. It attempts to replicate in the Linux space the success of ransomware attacks targeting Windows endpoints.
- One ransomware we encountered in 2021 targeted the VMware ESXi platform and came in the form of a Python script
- Internet-of-things (IoT) devices that run a feature-limited “busybox” Linux shell also remain a target for worms that deliver cryptominers and other nuisance malware to commodity devices like routers or network-attached storage.

No matter what platform you run – the Bad Guys are looking to take advantage!

Large Data Breaches

Information is Beautiful hosts a graphic showing the biggest data breaches and hack by year:

- https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- The graphic is interactive.
  - Mousing-over gives you a summary
  - Clicking brings you to a news story with more information



Levels of Threat

Not all threats are equal

- Some threat actors are very sophisticated and have tremendous capabilities
- Others have little experience and understanding of security and are looking for easy ways to exploit systems

We need to look at the different levels of threats that exist and understand what each consists of and how capable the adversaries are.

Levels of Threat

Three broad categories:

- Unstructured threats
  - The organization structure is very low. Attacks are typically mounted by a single person or a small, loosely affiliated group.
    - "Script Kiddies"
    - Disgruntled employees
- Structured threats
  - Organized groups of attackers. Attackers aware of who they are attacking, targets are specifically chosen and may include insider attacks.
    - Organized crime
    - Hacking groups (Hacktivists)
- Highly-structured threats
  - Attackers devote large amounts of time to attack a target. Attacks in this category may occur over years and if successful, may not be exploited until some point in the future when it is more advantageous to the attacker.
    - Nation states
    - Ideological groups
    - Terrorists

Levels of Threat

As the sophistication of threats increases, the cost to defend against them increases

Important Note

- A sophisticated attacker doesn't always use their sophisticated tools
- If they can use a simple phishing email to achieve their goals, they will use that instead of a zero-day attack
- This can make it more difficult to identify the specific attacker

Nation State Attacks

Also referred to as “Advanced Persistent Threat” or APT

- You can find a list of APT groups and other information on the MITRE ATT&CK™ Groups Pages
- https://attack.mitre.org/groups/

This is not new – attacks by APT groups have been going on for over a decade

- The earliest listed attacks by MITRE are from 2008
- APT29 (attributed to Russia’s Foreign Intelligence Service (SVR)) targeted government networks in Europe and NATO member countries.
- APT29 is also tied to the compromise of the Democratic National Committee starting in summer 2015

Nation State Attacks

Other notable attacks:

- November 2014: Sony Pictures Hack (North Korea)
  - 47,000 employees affected: SSNs, DOBs, addresses, etc.
  - 5 unreleased movies leaked (most notably – *The Interview*)
- February 2015: Anthem (China – “Deep Panda”)
  - Affected 78.8 million people
  - Revealed PII and may have included medical information
- June 2015: U.S. Office of Personnel Management (China)
  - Largest government data breach
  - 22.5 million individuals affected
  - Background investigation data stolen: SSNs, DOBs, addresses, etc.
- December 2015: Ukraine Power Grid Attack (Russia – “Sandworm”)
  - Resulted in power outages for roughly 230,000 consumers in Ukraine for 1-6 hours
  - It is the first publicly acknowledged successful cyberattack on a power grid.

Nation State Attacks

Other notable attacks:

- 2016: Democratic National Committee (Russia)
  - Obtained access to email servers
- September 2020: U.S. Elections (Russia)
  - Microsoft reported Strontium had attacked “more than 200 organizations including political campaigns, advocacy groups, parties, and political consultants”
- February 2022: Ukraine (Russia)
  - DDoS of Ukraine Defense Ministry
  - DDoS of banking apps and ATMs

Nation State Sponsored Hackers

Nation states can also utilize criminal hacking groups (or even legitimate groups – in their own country) to enhance their capabilities

- China's military-based cyber team (Unit 61398) – APT1 – used multiple resources:
  - Specialized military units
  - Experts from civilian organizations
  - External entities comprised of hacking-for-hire mercenaries
  - Non-government affiliated personas
- This allowed APT1 to obtain plans, drawings and key project details for a variety of cutting edge technology programs

Cyber Arms Race

Nation-states have advanced “cyber weapons” to use against their adversaries

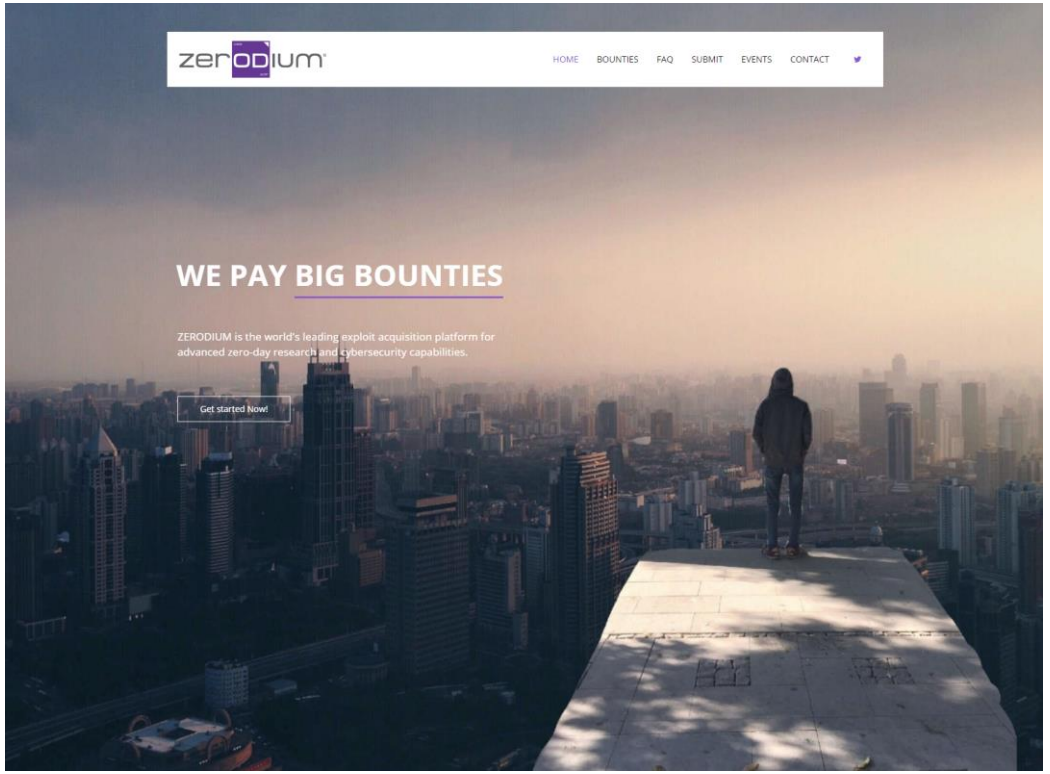
Essentially they develop, buy, or have zero-day exploits that they can use, if necessary

- China has rules that vulnerabilities must be reported to the government (and no one else)
- U.S. Cyber Command, in their Technical Challenge Problem Set 2020 looked for:
  - “the ability to rapidly develop means to exploit those vulnerabilities before a patch can be developed or distributed and applied by the adversaries.”
- The Shadow Brokers published several leaks in 2016 that contained several zero-day exploits
  - These were alleged to come from the “Equation Group” a group suspected to work for the National Security Agency

Cyber Arms Race

Zerodium (formerly Vupen) is, according to their website https://zerodium.com/ :

- “the world’s leading exploit acquisition platform for advanced zero-day research and cybersecurity capabilities”
- Their customers are: “government institutions (mainly from Europe and North America) in need of advanced zero-day exploits and cybersecurity capabilities”



Organized Crime Attacks

December 2013: Target

- 40 million credit/debit card accounts stolen
- Estimated cost to Target: $252 million
- Dozens of class action lawsuits filed on behalf of banks, consumers, and other stakeholders
- Settled a $10 million class action lawsuit with individual cardholders
- This is the reason Target moved to chip-reader credit card systems earlier than other retailers

May 2021: Colonial Pipeline (DarkSide group)

- Ransomware attack
- As a protective measure they halted pipeline operations
- Impacted oil and gas deliveries to 17 states and the District of Columbia
- Colonial Pipeline paid the ransom of 75 Bitcoin ($4.4 million)
- The Department of Justice (DOJ) recovered 63.7 Bitcoin ($2.3 million) from the ransom payment
  - The price of Bitcoin had crashed around that time
  - The DOJ had previously compromised the private keys of the Bitcoin wallets

The History of Hacking

Hacking is not something that started with the creation of the Internet

It has been around for much longer than that

It hasn't, however, always been considered a "bad" thing as the term "hack" has meant different things during the history of computers

The History of Hacking

Phase One: “The Early Years”

- 1960s and 1970s
- Originally, hacker referred to a creative programmer who wrote clever code
- The first operating systems and computer games were written by hackers
- The term hacking was a positive term
- Hackers were usually high-school and college students

Example: Dennis Ritchie and Ken Thompson

- Known online as dmr and Ken, they created the UNIX operating system in 1969
- UNIX was written in the C programming language to help port it to different computer platforms
- Linux is a “descendent” of UNIX (via Minix and GNU)

There was even a special term for people who hacked the telephone system to gain access, or make free phone calls: ***Phreakers***

- This was a shortened form of “Phone Hackers” (and it sounds cool)
- At this time, long-distance calls could cost over $1.00/minute

The History of Hacking

Phase Two: Hacking gets a negative meaning

- 1970s through 1990s.
- Authors and the media used the term hacker to describe someone who used computers, without authorization, sometimes to commit crimes
- Early computer crimes were launched against business and government computers
- Adult criminals began using computers to commit their crimes

Example: Kevin Mitnick (Alias: Condor)

- The first hacker to have his face immortalized on an FBI "Most Wanted" poster
- Gained unauthorized access to a computer system at Digital Equipment Corporation (DEC) when he was 16 years old.
  - Copied the companies software, and was convicted in 1988
  - Sentenced to 12 months in prison, and 3 years of supervised release
- Hacked into Pacific Bell and became a fugitive for over 2 years
- Arrested again in 1995 – and pled guilty in 1999
  - Sentenced to 5 years in prison
  - When under supervised release, he was not allowed to touch a computer until 2003
- Wrote the book *The Art of Deception*
- ***Source***: *https://en.wikipedia.org/wiki/Kevin_Mitnick*

The History of Hacking

Phase Two: Hacking gets a negative meaning

Example: Robert Morris (Alias: rtm)

- Father was the chief scientist at the National Computer Security Center (part of the National Security Agency)
- In 1988, while a student at Cornell University, wrote an internet worm (now called “The Morris Worm”)
- Infected thousands of machines, and did $millions in damage
- First person indicted under the Computer Fraud and Abuse Act
- Sentenced to 3 years of probation, 400 hours of community service, and a fine of $10,050 and the costs of his supervision.
- He is now a professor at MIT and a partner at Y Combinator
- ***Source**:* *https://en.wikipedia.org/wiki/Robert_Tappan_Morris*

The History of Hacking

Phase three: The Web Era

- Beginning in the mid-1990s
- This era saw the introduction of the PC, the Internet, and the World Wide Web (and AOL)
- The increased use of the Internet for school, work, business transactions, and recreation makes it attractive to criminals with basic computer skills
- Crimes include the release of malicious code (viruses and worms)
- Unprotected computers can be used, unsuspectingly, to accomplish network disruption or commit fraud
- Hackers with minimal computer skills can create havoc by using malicious code written by others

The History of Hacking

Phase three: The Web Era

- The rise of Hacktivism – hacking to achieve social or political ends
  - This kind of hacking can range from mild to destructive activities
  - Some consider hactivism as modern-age civil disobedience
  - Others believe hactivism denies others their freedom of speech and violates property rights
- Anonymous is probably the most well-known hacktivist group

Anonymous Emblem

From: https://en.wikipedia.org/wiki/Anonymous_(hacker_group)#/media/File:Anonymous_emblem.svg

The History of Hacking

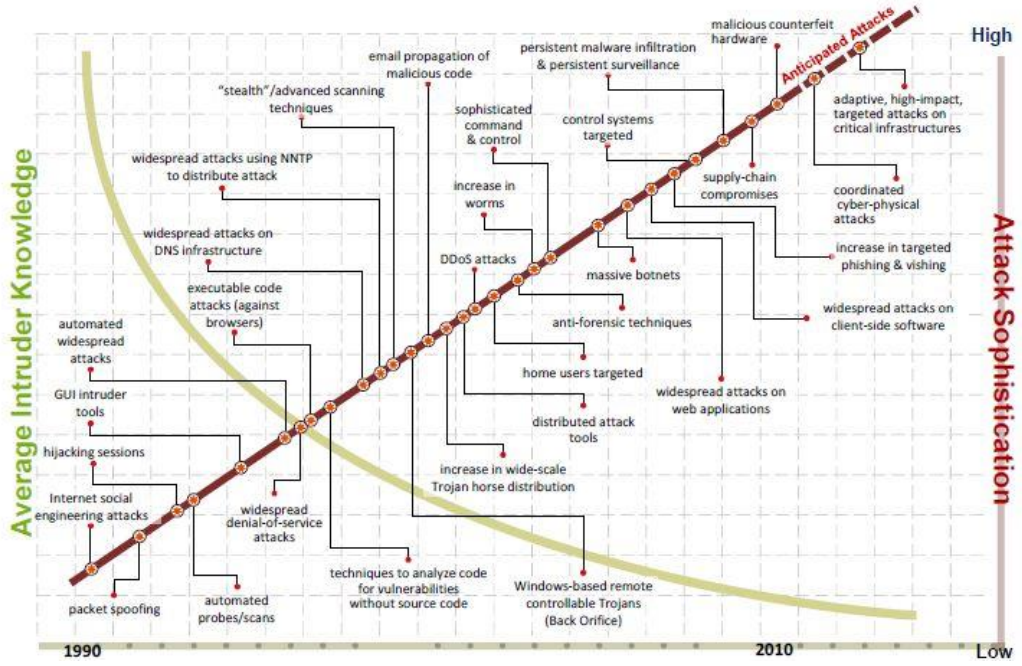
Phase Four: The Mobile Era

- Been increasing for 10+ years (depending on how you define it)
- Started with “dumb” cell phones with limited capabilities and took off with smart phones
- Also includes tablets, eReaders, scanners, and other smart devices
- Malicious apps are constantly being developed and distributed
  - Even “beneficial” apps want access to a lot of personal data
  - App stores have to regularly purge these apps
- Given the rapid development cycle of mobile devices, features often outpace security

Hacker Knowledge vs Attack Sophistication

Notice the two trend lines

- The green line shows the knowledge required by hackers is going down over time
  - You can Google for things you don't know
- Tools are gaining in sophistication
  - Tools like Nmap and Metasploit abstract out the complexity
- An attacker no longer needs a deep understanding of a system, protocol, or application
  - They can provide information to a tool and click "Hack"



HD Moore's Law

Moore's Law

- Computer power grows at the rate of doubling about every 2 years

HDMoore's Law

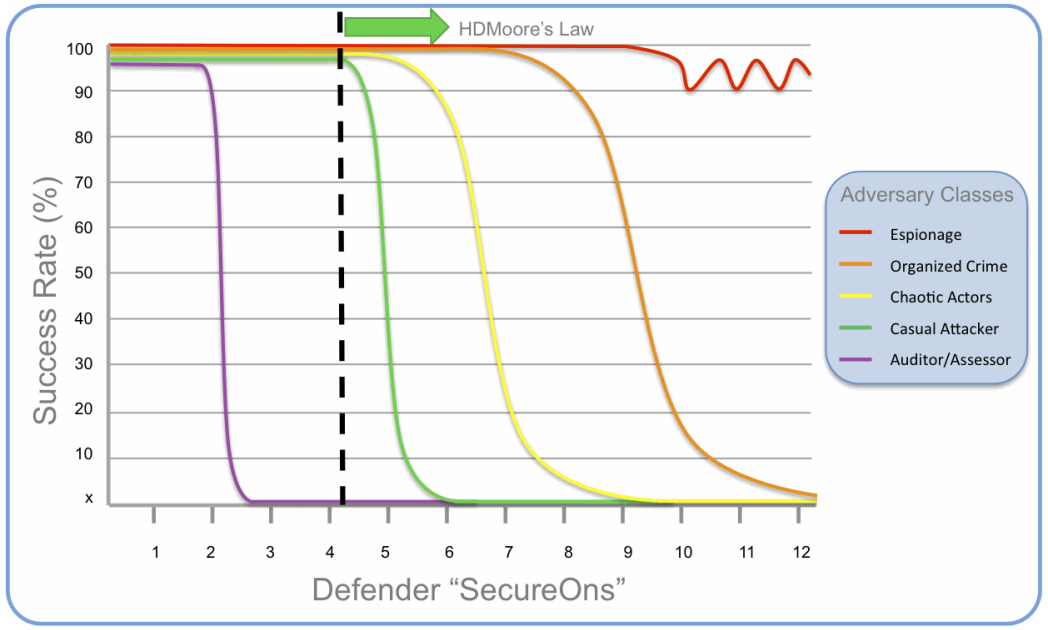
- Casual Attacker power grows at the rate of Metasploit

H.D. Moore created Metasploit – a penetration testing platform

- Included in Kali Linux

Source and more information:

- https://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/



Types of Attacks

Types of Attacks:

- Fabrication
- Interception
- Interruption
- Modification

Learn more about these attack by reading: *Section 1.4 Attacks – Types of Attacks*

- https://eng.libretexts.org/Courses/Delta_College/Information_Security/01%3A_Information_Security_Defined/1.4_Attacks_-_Types_of_Attacks

You will be responsible for knowing the information on that page

- (Don’t worry – it isn’t very long)

Security Weaknesses

Security weaknesses can be found in the computer systems used by:

- Government (classified and unclassified)
- Businesses
- Personal computing systems (including mobile devices)

In other words, they can be found in ANY computer, no matter what its purpose. Causes of security weakness include:

- Underlying characteristics of the Internet
  - A website needs to be publicly available, so it is open to DDoS attacks
- Human nature
  - People can be tricked into doing things, or not even realize anything is wrong
- Inherent complexity of computer systems
  - Things may be overlooked, or systems may be used in ways not expected by their designers

What can we do?

Security can be improved by:

- Ongoing education and training to recognize the risks
  - System designers and developers
  - Also the end user
- Better system and network design
  - Secure protocols and network topologies
- Use of security tools and systems
  - Use tools to look for vulnerabilities before an attacker finds them
- Challenging "others" to find flaws in systems
  - Bug bounty programs
- Writing and enforcing laws that don’t hinder research and advancement

Who Needs To Worry About Cybercrime?

We may have heard that we can prevent cyberbullying, but what about cybercrime?

We all know that we can prevent wildfires because Smokey has told us we can – but what about cybercrime?

We all have to work together to prevent it!

Security Tools and Systems

A list of security tools and systems we will cover more in class:

- Encryption
- Anti-Virus Software
- Firewalls
- Intrusion Detection/Prevention Systems
- Vulnerability/Penetration Testing
- Patches
- Backups
  - When was the last time you created a backup of your data?
  - When was the last time you made sure you could RESTORE that backup?

Saltzer and Schroeder's Security Design Principles

Many security issues are a result of poor coding techniques which lead to flaws in the program which can result in a security hole that can be exploited

Saltzer and Schroeder came up with a list of 8 security design principles that, if followed, would help programmers reduce the number of errors and design more secure software

1. Economy of mechanism – A simple design is easier to test and validate
2. Fail-safe defaults –In computing systems, the safe default is generally "no access" so that the system must specifically grant access to resources
3. Complete mediation – Access rights are completely validated every time an access occurs
4. Open design –secure systems, including cryptographic systems, should have unclassified designs
5. Separation of privilege – A protection mechanism is more flexible if it requires two separate keys to unlock it, allowing for two-person control and similar techniques to prevent unilateral action by a subverted individual
6. Least privilege – Every program and user should operate while invoking as few privileges as possible
7. Least common mechanism – Users should not share system mechanisms except when absolutely necessary
8. Psychological acceptability – users won't specify protections correctly if the specification style doesn't make sense to them

Saltzer and Schroeder's Security Design Principles

Later they added 2 related principles

1. Work factor – Stronger security measures pose more work for the attacker
2. Compromise recording – The system should keep records of attacks, even if it can't block them. This allows for other mitigations to be utilized (Ex. Alert people about a loss of PII)

In this class we will be examining these in more detail, but through a similar list of design principles that NSA has developed

This will be the topic beginning in the next lesson and continuing for several lessons after that

Cyber Threat Defender

Developed by the Center for Infrastructure Assurance and Security (CIAS) at UTSA

Collectable card game (also available as an electronic download)

Players have to build their networks while defending against attacks

Targeted at middle- and high-school students

Available here: https://cias.utsa.edu/ctd.php