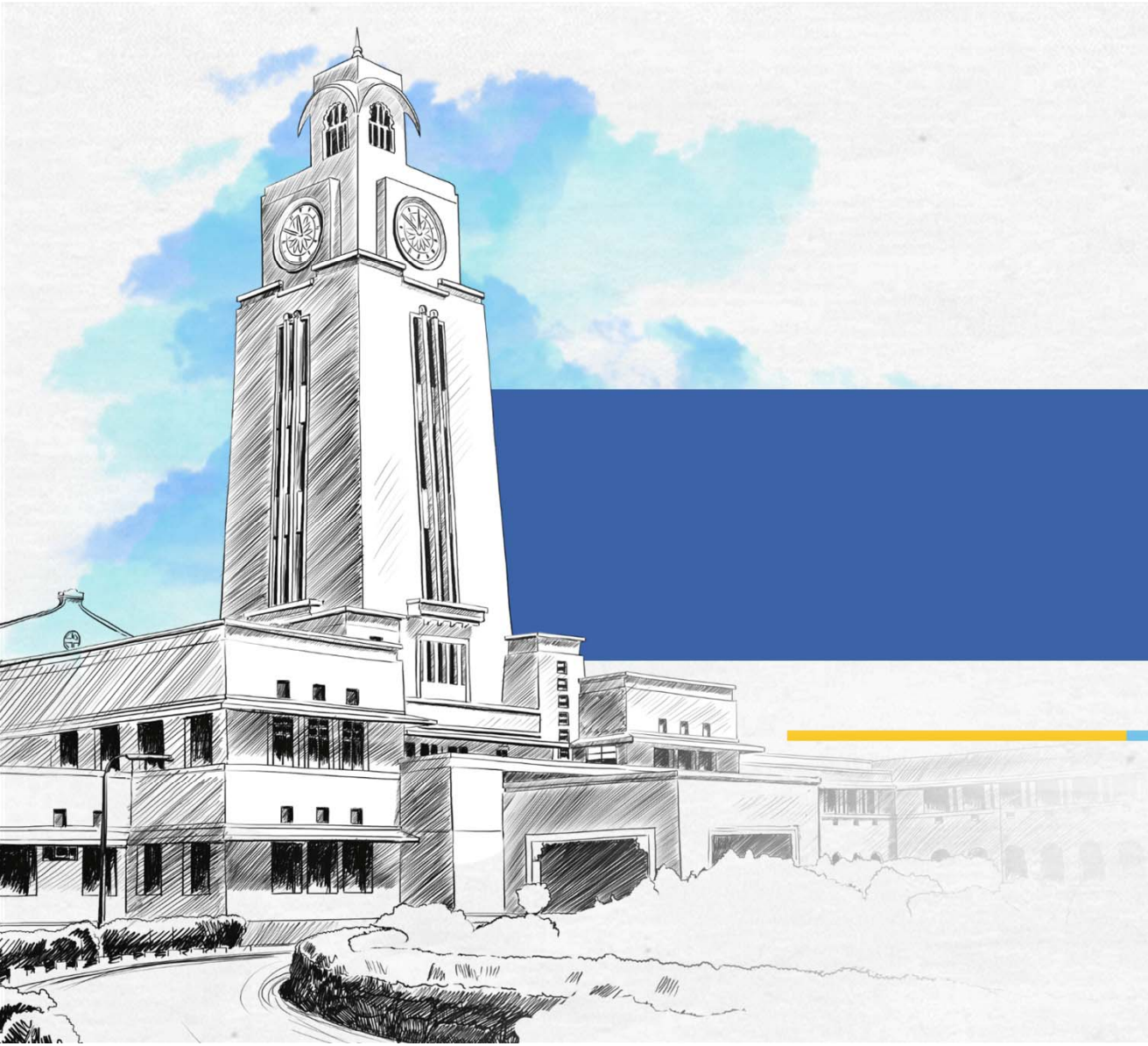


BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Cyber Threat Landscape and Common Cyber Attacks

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Cyber Threat Landscape and Common Cyber Attacks

innovate achieve lead

Agenda

- The Threat Landscape
- Understanding Vulnerabilities
- Common Cyber Attacks
  - Stages and Patterns
  - Targeted and Non-targeted Attacks
  - Reducing exposure to Cyber Attacks
- Essential Cyber Security Controls
  - Boundary firewalls and Internet gateways
  - Secure configuration
  - Whitelisting and execution control
  - User access control
  - Password policy
  - Content checking

The Threat Landscape

The Threat Landscape

innovate achieve lead

Scenario

- Before we take a look at the cyber security threat landscape, let's look at this scenario
- Cybercrime Up 600% Due To COVID-19 Pandemic
- There is a rise in sophisticated phishing emails due to COVID-19
- Malicious actors are posing as the CDC or WHO representatives (see next slide)
- These emails are designed to deceive and trick recipients into taking an action:
  - E.g., clicking a malicious link, or opening an attachment with a virus

CDC = Center for Disease Control and Prevention
WHO = World Health Organization

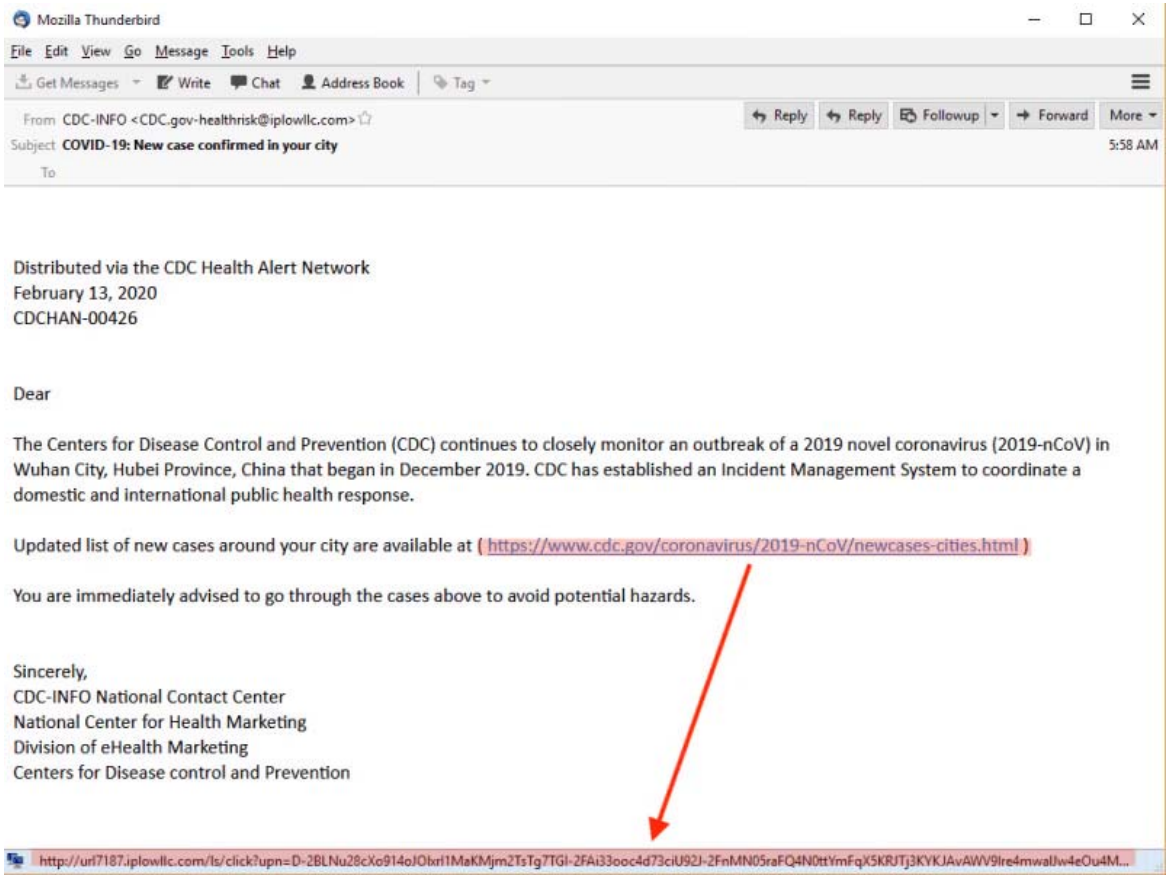
https://purplesec.us/resources/cyber-security-statistics/

The Threat Landscape

innovate achieve lead

Scenario

CDC = Center for Disease Control and Prevention
WHO = World Health Organization



https://purplesec.us/resources/cyber-security-statistics/

The Threat Landscape

innovate achieve lead

Key Industry Trends

- The cyber threat landscape is complex and constantly changing
- Cybersecurity has never been more important than before
- COVID-19 has forced companies to create remote workforces and operate off cloud-based platforms
- The rollout of 5G has made connected devices more connected than ever
- Some industry trends to watch for in 2021 and beyond
  - Remote workers will continue to be a target for cybercriminals
  - As a side effect of remote workforces, cloud breaches will increase
  - The cybersecurity skills gap will remain an issue
  - As a result of 5G increasing the bandwidth of connected devices, IoT devices will become more vulnerable to cyber attacks

https://www.varonis.com/blog/cybersecurity-statistics/

The Threat Landscape

innovate achieve lead

Key Industry Trends

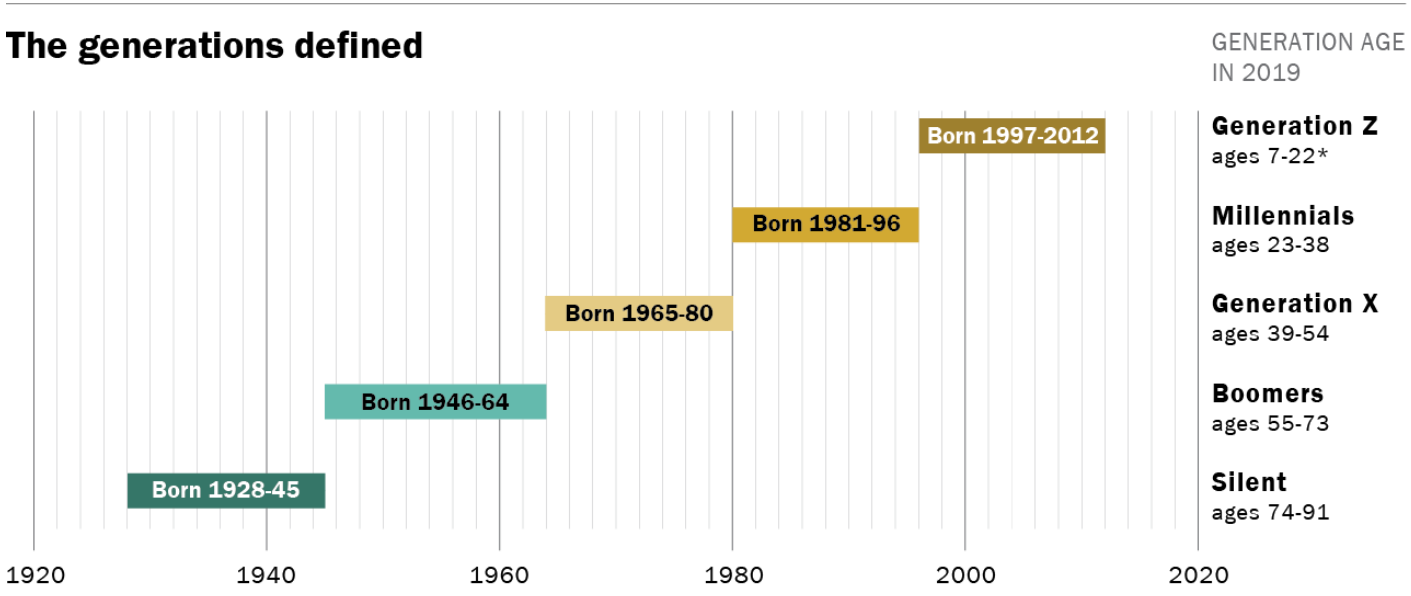
- As companies rushed to adapt to pandemic-inspired changes in work and business models, many seem to have left security behind
- Half or more of the CISOs and CIOs say they haven't fully mitigated the risks associated with remote work (50%), digitization (53%) or cloud adoption (54%).
- Securing remote work is still in progress
- 70% of organizations relied on a password-centric authentication approach as of March 2020
  - even with advances in biometrics, multi-factor authentication (MFA) and tokenization.
- Employees — especially those of the millennial generation (51%) and generation Z (45%) admit to using applications and programs on their work devices that their employer has expressly prohibited
- Remote work has pushed the edge of the organization to common home devices that are not hardened to the same degree as corporate networks.

https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/2021-digital-trust-insights/cyber-threat-landscape.html

The Threat Landscape

innovate achieve lead

Key Industry Trends



https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/2021-digital-trust-insights/cyber-threat-landscape.html

The Threat Landscape

innovate achieve lead

Key Industry Trends (as of mid 2021)

- The past 18 months have been the perfect conditions for cybercrime to thrive
- Cybercriminals are still not short of sophisticated and malicious ways to achieve their goals
- Core attack methodologies being utilized by threat actors today
  - Phishing attempts
  - Denial of Service (DoS) and Distributed Denial of Service (DdoS) attacks
  - Ransomware and access brokers
  - Business email compromise (BEC)
  - Data breaches
  - Supply chain attacks
  - Cryptojacking

https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/the-threat-landscape-in-2021-so-far/

The Threat Landscape

innovate achieve lead

Some Perspectives of Security

- Let's understand some perspectives of security
  - Technology is the cause of attack
  - Risk-Reward Ratio and Ease of stealing
  - Cyber crime Vs. Physical crime
  - Information is an asset to both criminals and organizations
  - Personal Computing Assets (Remote Working due to COVID-19)
  - The Digital Divide
  - The Growing Internet of Things
  - Increasing use of Social Media

The Threat Landscape

Technology is the cause of attack

- In today's world the growth and prominence of technologies and data are showing no signs of slowing down
- The technology changes in unimaginable ways
  - We can be attacked both physically and virtually
- For today's organizations that rely heavily on technology (particularly the Internet) for doing their business
  - Virtual attacks are far more threatening
- For every vulnerability fixed, another pops up, ripe for exploitation
- When a vulnerability is identified, a tool that can exploit it is often developed and used within hours
  - This is faster than the time it normally takes for the vendor to release a patch, and certainly quicker than the time many organizations take to install that patch
- The adoption of new innovations creates an environment where threat landscapes can change quickly

The Threat Landscape

innovate achieve lead

Risk-Reward Ratio & Ease of Stealing

- The technology gives attackers a huge advantage over the defenders
  - They attack anyone, anywhere, from the comfort of their home
  - They often have automated tools to identify their victims – and their vulnerabilities
- From an attacker's perspective, there is often a very good risk-to-reward ratio:
  - For the victim, it can be hard enough to detect that the attack happened at all, never mind trace who was behind it
- It is the very nature of the digital information that we are trying to protect that is easy to copy
- In fact, stealing the information does not require removing it from its original location at all
  - meaning that the owner of that information may never realize that the theft happened

The Threat Landscape

Cyber crime Vs. Physical crime

- Committing crimes over the Internet can also be very lucrative
- Physical pickpocketing compared with digitally targeting someone
  - Stealing cash and credit cards can only be beneficial for short term
  - Stealing a person's identity can get credit cards issued in the victim's name
- Upscale that to targeting businesses
  - A criminal might get access to thousands or even millions of credit card details and personal information
  - They can use the information for themselves or sell it on the dark web
    - where you can buy virtually anything, from drugs and organs to hacking software and stolen credentials
- The profits are certainly far greater compared to a physical crime conducted in the same timescale and with the same manpower

The Threat Landscape

innovate achieve lead

Information is asset to both criminals and organizations

- Information 'assets' – by definition, someone else wants to get hold of them
- Individuals normally go through the proper channels – but not everyone will take the legal route
- Everyone is a target because virtually every organization (even a small business) holds valuable information (often in huge quantities)
- Being the most important asset, organizations cannot do business if they lose access to that information
- The fact that criminals can extract significant value from this information means that it is an asset to them too

The Threat Landscape

Personal Computing Assets (Remote Working)

- Threat landscapes commonly prioritize corporate and governmental networks assets as high priorities
  - Personal networks and resources are treated as lower-level threats
- Covid-19 pandemic resulted in over 40% of people working from home
  - This requires a reassessment of prioritization levels
- This change enabled bad actors with more opportunities to prey on remote workers
  - This forces reassessment of the risk level of home networks
- Today's threat landscape must also include personal computing assets as high-risk and high-value targets
  - This is because often-sensitive data being accessed outside of the protected corporate networks

https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in-todays-cybersecurity

The Threat Landscape

innovate achieve lead

The Digital Divide

- The changing threat landscape has made a large segment of society to use technology insecurely
- People who may lack skills needed to protect themselves from security attacks now use their computers for education, work, and play
- In many situations, multiple family members utilize the same electronic device, greatly increasing the chance for exposure to malware
- Educational institutions are now required to quickly transition to online learning without implementing necessary training and cybersecurity protocols
  - These training and protocols are part of traditional online models
- Educators who may have not previously utilized technology are now sharing files as part of their daily online classroom interactions
  - This could introduce malware onto their devices

https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in-todays-cybersecurity

The Threat Landscape

innovate achieve lead

Growing Internet of Things

- Connected appliances
- Smart home security systems
- Autonomous farming equipment
- Wearable health monitors
- Smart factory equipment
- Wireless inventory trackers
- Ultra-high speed wireless internet
- Biometric cybersecurity scanners
- Shipping container and logistics tracking

- Connected Cars
- Connected Homes
- Connected Agriculture
- Connected Retail
- Connected Hospitality
- Connected Health
- Connected Manufacturing
- Connected Cities

https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in-todays-cybersecurity

The Threat Landscape

innovate achieve lead

Growing Internet of Things

- A growing Internet of Things (IoT) has exposed devices to cyberattacks
  - A few years ago these would never have been included in most threat landscape models
- More healthcare and fitness apps for people to manage their health
  - This increases scope for attack surfaces
  - An attack on such apps, exposes large amounts of personal data and puts personal lives at risk
- Large number of payment apps such as GooglePay & PayTM
  - Such apps expose the possibility of stealing credit card and bank account information
- Modern agriculture equipment incorporates large amounts of technology
  - including data centers, networks, satellites and even artificial intelligence (AI)
  - a successful large-scale attack by either a lone individual or an organized group could potentially damage our food supply

https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in-todays-cybersecurity

The Threat Landscape

innovate achieve lead

Increasing use of Social Media

- Greater numbers of individuals use social media as a news source
  - More than half of Americans receive their news by social media (Forbes)
- The manipulation of video using techniques such as deepfake make it increasingly difficult to recognize altered videos in social media
  - https://youtu.be/EfREntgxmDs
  - https://www.youtube.com/watch?v=bt5ZZq926VA
  - https://www.youtube.com/watch?v=C8FO0P2a3dA
  - https://www.youtube.com/watch?v=pkF3m5wVUYI
  - https://edition.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/
- Conspiracy theories are often shared online as facts, introducing yet more confusion in actual messaging to users looking for current news
- The risk of wireless technology remains constant
  - In addition, widespread use of 5G has introduces additional vulnerabilities

https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in-todays-cybersecurity

The Threat Landscape

innovate achieve lead

Wireless Technology

- Previous mobile network topology provided for fewer pieces of hardware at which point traffic could be monitored
- The decentralized nature of 5G requires implementation of monitoring and security solutions at an exponentially greater number of devices
- The increased bandwidth and ability to add large numbers of IoT devices will require security solutions that are scalable and able to respond rapidly in order to provide a secure computing environment
- Understanding today's threat landscape is critical to developing strategies and solutions to establish a strong cybersecurity framework
- It is critical for both organizations and individuals to not become complacent and remain vigilant, regularly defending their threat landscape

https://www.securitymagazine.com/articles/93367-the-changing-threat-landscape-in-todays-cybersecurity

The Threat Landscape

innovate achieve lead

Some Facts

Fact	Source
95% of cybersecurity breaches are caused by human error	Cybint
The worldwide information security market is forecast to reach $170.4 billion in 2022	Gartner
88% of organizations worldwide experienced spear phishing attempts in 2019	Proofpoint
68% of business leaders feel their cybersecurity risks are increasing	Accenture
On average, only 5% of companies' folders are properly protected	Varonis
Data breaches exposed 36 billion records in the first half of 2020	RiskBased
86% of breaches were financially motivated and 10% were motivated by espionage	Verizon
45% of breaches featured hacking, 17% involved malware and 22% involved phishing	Verizon
Between January 1, 2005, and May 31, 2020, there have been 11,762 recorded breaches	ID Theft Resource Center
The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%	Symantec
An estimated 300 billion passwords are used by humans and machines worldwide	Cybersecurity Media

https://www.varonis.com/blog/cybersecurity-statistics/

The Threat Landscape

innovate achieve lead

Some Facts

Fact
There is a hacker attack every 39 seconds
43% of cyber attacks target small business
The global average cost of a data breach is $3.9 million across SMBs
9.7 Million Records healthcare records were compromised in September 2020 alone
Approximately $6 trillion is expected to be spent globally on cybersecurity by 2021
Connected IoT devices will reach 75 billion by 2025
Unfilled cybersecurity jobs worldwide is already over 4 million
More than 77% of organizations do not have a Cyber Security Incident Response plan
Most companies take nearly 6 months to detect a data breach, even major ones
Share prices fall 7.27% on average after a breach
Total cost for cybercrime committed globally will reach $6 trillion by 2021

https://www.cybintsolutions.com/cyber-security-facts-stats/

The Threat Landscape

innovate achieve lead

References

- The Cyber Security Handbook – Prepare for, respond to and recover from cyber attacks by Alan Calder *Published by IT Governance Publishing, 2020*
- UK Department for Digital, Culture, Media & Sport, "Cyber Security Breaches Survey 2020", March 2020, https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020.

Understanding Vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Overview

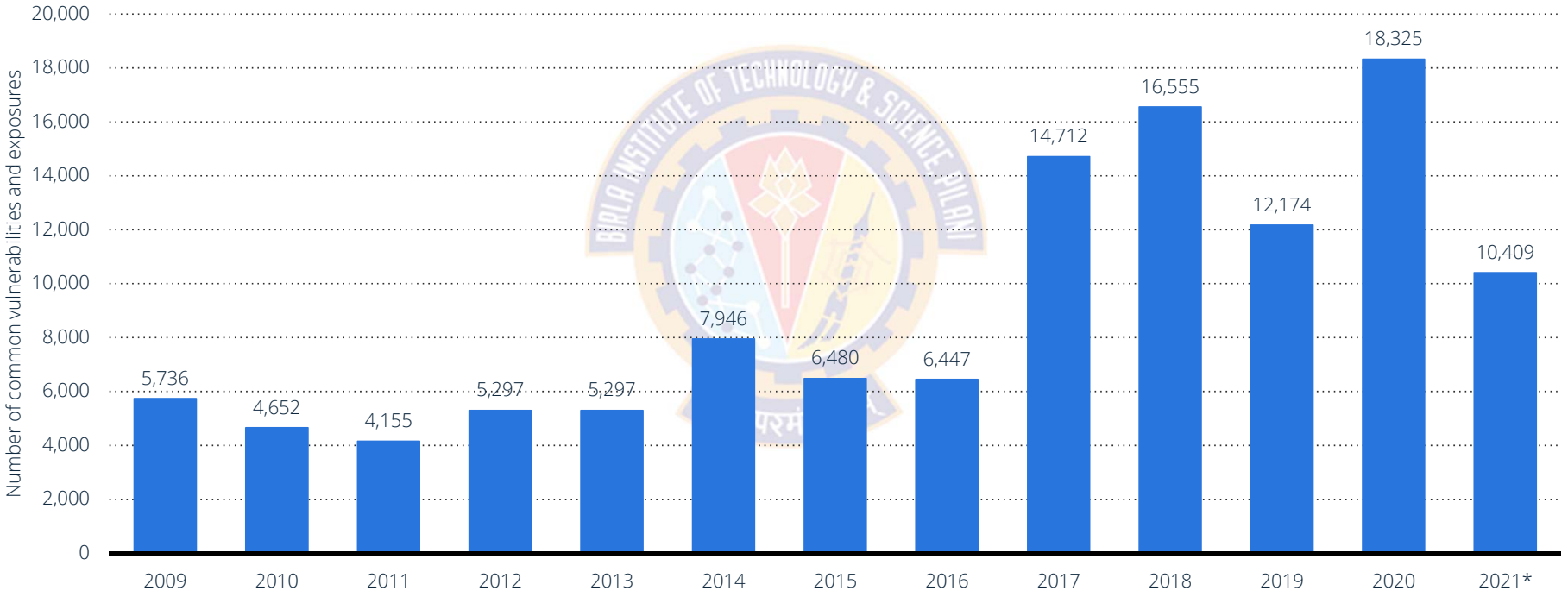
- A vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack
- Attackers will look to exploit any of them, often combining one or more, to achieve their end goal
- To exploit an existing vulnerability, an attacker needs to have at least one tool that connects to a system weakness:
  - The vulnerability then becomes what is known as the "attack surface".

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Common IT vulnerabilities and exposures worldwide 2009-2019



Note(s): Worldwide; 2009 to 2021
Source(s): Website (cvedetails.com); ID 500755

statista

Understanding Vulnerabilities

innovate achieve lead

Vulnerability Categories

- Virtually, there can be 1000s of vulnerabilities
- However, they can be broadly grouped into following categories
  - Server and Host Vulnerabilities
  - Network Vulnerabilities
  - Virtualization Vulnerabilities
  - Web Application Vulnerabilities
  - Internet of Things Vulnerabilities
  - Database Vulnerabilities

Source: CompTIA CySA+ (CS0-001): Complete Course and Practice Exam
Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

About MITRE

- The MITRE Corporation is an American not-for-profit organization based in Bedford, Massachusetts, and McLean, Virginia
  - Note: MITRE is not an acronym
- It manages federally funded R&D centers (FFRDCs) supporting several U.S. government agencies
- MITRE maintains the Common Vulnerabilities and Exposures (CVE) system and the Common Weakness Enumeration (CWE) project
- Since 1999, the MITRE Corporation has been functioning as editor and primary numbering authority of the CVEs
- CVE is now the industry standard for vulnerability and exposure names
- It provides reference points for data exchange so that information security products and services can interoperate with each other

Source: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/

Understanding Vulnerabilities

innovate achieve lead

CWE Top 25 - 2021

- The Common Weakness Enumeration (CWE) identified the Top 25 Most Dangerous Software Errors (CWE Top 25)
- The CWE Top 25 provides insight into the most severe and current security weaknesses
- This is a demonstrative list of the most common and impactful issues experienced over the previous two calendar years
- While the list remains comprehensive, there are many other threats that leave software vulnerable to attack
- These weaknesses are dangerous because they are often easy to find, exploit, and can allow adversaries to completely take over a system, steal data, or prevent an application from working
- The CWE Top 25 is a valuable community resource that can help developers, testers, project managers, security researchers, and educators provide insight into the most severe and current security weaknesses.

https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html

Understanding Vulnerabilities

innovate achieve lead

Common Computer Security Vulnerabilities

Vulnerability	Score	Vulnerability	Score
Out-of-bounds Write	65.93	Use After Free	16.83
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.84	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.69
Out-of-bounds Read	24.9	Cross-Site Request Forgery (CSRF)	14.46
Improper Input Validation	20.47	Unrestricted Upload of File with Dangerous Type	8.45
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19.55	Missing Authentication for Critical Function	7.93
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19.54	Integer Overflow or Wraparound	7.12

2021 CWE Top 25 Most Dangerous Software Weaknesses

https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Understanding Vulnerabilities

Common Computer Security Vulnerabilities

Vulnerability	Score	Vulnerability	Score
Deserialization of Untrusted Data	6.71	Exposure of Sensitive Information to an Unauthorized Actor	4.74
Improper Authentication	6.58	Insufficiently Protected Credentials	4.21
NULL Pointer Dereference	6.54	Incorrect Permission Assignment for Critical Resource	4.20
Use of Hard-coded Credentials	6.27	Improper Restriction of XML External Entity Reference	4.02
Improper Restriction of Operations within the Bounds of a Memory Buffer	5.84	Server-Side Request Forgery (SSRF)	3.78
Missing Authorization	5.47	Improper Neutralization of Special Elements used in a Command ('Command Injection')	3.58
Incorrect Default Permissions	5.09		

2021 CWE Top 25 Most Dangerous Software Weaknesses

https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Understanding Vulnerabilities

innovate achieve lead

Causes of Vulnerabilities

- They can occur through:
  - Flaws
  - Features
  - User error
  - Zero-day vulnerabilities

Source: CompTIA CySA+ (CS0-001): Complete Course and Practice Exam
Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Causes of Vulnerabilities

- Flaws
  - A flaw is an unintended functionality
  - This may either be a result of poor design or through mistakes made during implementation (coding)
  - Flaws may go undetected for a significant period of time
  - The majority of common attacks we see today exploit these types of vulnerabilities
  - Between 2014 and 2015, nearly 8,000 unique and verified software vulnerabilities were disclosed in the US National Vulnerability Database (NVD)
  - Vulnerabilities are actively pursued and exploited by the full range of attackers
  - Consequently, a market has grown in software flaws, with 'zero-day' vulnerabilities fetching hundreds of thousands of dollars

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Causes of Vulnerabilities

- Features
  - A feature is intended functionality which can be misused by an attacker to breach a system
  - Features may improve the user's experience, help diagnose problems or improve management, but they can also be exploited by an attacker
  - Example:
    - Microsoft introduced macros into their Office suite in the late 1990s. They soon became the vulnerability of choice. E.g., Melissa virus in March, 1999
      - It was a mass-mailing macro virus. It targeted Microsoft Word and Outlook-based systems, and created considerable network traffic
      - The virus would infect computers via Email, the email being titled "Important Message From", followed by the current username
      - Upon clicking the message, the body would read: "Here's that document you asked for. Don't show anyone else ;)." Attached was a Word document titled list.doc containing a list of pornographic sites and accompanying logins for each
      - It would then mass mail itself to the first 50 people in the user's contact list and then disable multiple safeguard features on Microsoft Word and Microsoft Outlook

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Causes of Vulnerabilities

- Features
  - Macros are still exploited today
    - The Dridex banking Trojan that was spreading in late 2014 relies on spam to deliver Microsoft Word documents containing malicious macro code, which then downloads Dridex onto the affected system.
  - JavaScript, widely used in dynamic web content, continues to be used by attackers
    - E.g., Diverting the user's browser to a malicious website and silently downloading malware, and hiding malicious code to pass through basic web filtering.

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Causes of Vulnerabilities

- User Error
  - Users can be a significant source of vulnerabilities
  - They make mistakes, such as choosing a common or easily guessed password, or leaving their laptop or mobile phone unattended
  - Even the most cyber aware users can be fooled into giving away their password, installing malware, or divulging confidential information
  - These details would allow an attacker to target and time an attack appropriately
  - A carefully designed and implemented computer system can minimize vulnerabilities
  - Such efforts can be easily undone
    - E.g., an inexperienced system administrator who enables vulnerable features, fails to fix a known flaw, or leaves default passwords unchanged

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Causes of Vulnerabilities

- Zero-day vulnerabilities
  - The term "zero-day" refers to a newly discovered software vulnerability
  - Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn't been released
  - So, "zero-day" refers to the fact that the developers have "zero days" to fix the problem that has just been exposed — and perhaps already exploited by hackers
  - Once the vulnerability becomes publicly known, the vendor has to work quickly to fix the issue to protect its users.
  - But the software vendor may fail to release a patch before hackers manage to exploit the security hole
  - That's known as a zero-day attack.

Source: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html

Understanding Vulnerabilities

innovate achieve lead

Causes of Vulnerabilities

- Vulnerabilities are not just software-based
- Vulnerabilities can be found on hardware, network, even the users — impacting all assets across an organization
- Vulnerabilities can come from many sources, complexity, misconfiguration, connectivity, software bugs, etc.
- The most common source of vulnerabilities is the human user
  - Which poses a significant risk for organizations and their security posture.

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Common Vulnerability Scoring System (CVSS)

- While software bugs aren't inherently harmful (except for potential performance issues), many can be taken advantage of by "bad" actors
  - These are known as vulnerabilities.
- Vulnerabilities can be leveraged to force software to act in ways it's not intended to
  - E.g., gleaning information about the current security defenses in place.
- Once a bug is determined to be a vulnerability, it is registered by MITRE as a common vulnerability and exposure (CVE)
- The vulnerability is assigned a Common Vulnerability Scoring System (CVSS) score to reflect the potential risk it could introduce to the organization
- This central listing of CVEs serves as a reference point for vulnerability scanners

Source: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/

Understanding Vulnerabilities

Scanning Vulnerabilities

- A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses
- They are used to identify and detect vulnerabilities arising from misconfigurations or flawed programming within a network-based asset such as a firewall, router, web server, application server, etc.,
- A vulnerability scanner scans and compares an organization's environment against a vulnerability database, or a list of known vulnerabilities
- Once the vulnerabilities are detected, developers can use penetration testing as a means to see where the weaknesses are
- These problems can be fixed and future mistakes can be avoided
- Frequent and consistent scanning will enable us to see common threads between vulnerabilities and a better understanding of the system

Source: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/

Understanding Vulnerabilities

innovate achieve lead

Threat-Vulnerability-Risk

- Before we discuss identifying vulnerabilities, we need to understand threat and risk
- Threat
  - A potential for an attacker to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner
- Risk
  - The potential for loss computed as the combination of the *likelihood* that an attacker exploits some vulnerability to an asset, and the *magnitude* of harmful consequence that results to the asset's owner

Source: Computer and Security – Principles & Practice by William Stallings

Understanding Vulnerabilities

innovate achieve lead

Threat-Vulnerability-Risk

- Not all vulnerabilities are a security risk
- For example:
  - The risk of a vulnerability can depend on the potential impact that it could have on the business, in relation to which asset it impacts
- If the vulnerability is on a low-risk asset then it is much less likely of posing a significant risk
- The risk also depends on the time a vulnerability has existed
- A vulnerability which has been identified and quickly addressed poses much less risk than one that goes undetected for days, weeks, or even months

Source: https://www.ncsc.gov.uk/information/understanding-vulnerabilities

Understanding Vulnerabilities

innovate achieve lead

Threat-Vulnerability-Risk

- Identifying potentially significant risks to the assets requires answering the following questions for each asset:
  - Who or what could cause it harm?
    - This involves identifying potential threats to assets
  - How could this occur?
    - This involves identifying flaws or weaknesses in the organization's IT systems or processes that could be exploited by a threat source
- Mere existence of some vulnerability does not mean harm will be caused to an asset
  - There must also be a threat source for some threat that can exploit the vulnerability
- The combination of a *threat* and a *vulnerability* creates a risk to an asset

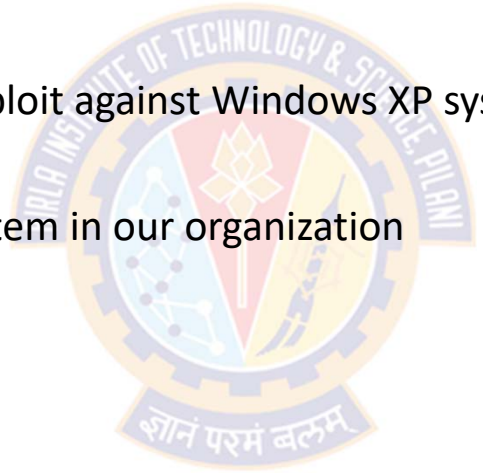
Source: Computer and Security – Principles & Practice by William Stallings

Understanding Vulnerabilities

innovate achieve lead

Threat-Vulnerability-Risk

- If you have a threat without a vulnerability, it isn't a risk
  - Threat
    - Hackers are using zero-day exploit against Windows XP systems
  - Vulnerability
    - We don't use Windows XP system in our organization
  - Risk
    - None



Source: CompTIA CySA+ (CS0-001): Complete Course and Practice Exam

Understanding Vulnerabilities

Threat-Vulnerability-Risk

- If you have a vulnerability without a threat, it isn't a risk
  - Vulnerability
    - Unpatched operating system software
  - Threat
    - Hackers haven't found any exploitable coding errors
  - Risk
    - None

Sources of Vulnerability Information

innovate achieve lead

Security Mailing Lists

- The following mailing lists contain interesting and useful discussion relating to current security vulnerabilities and issues
  - BugTraq (http://www.securityfocus.com/archive/1)
  - Full Disclosure (http://seclists.org/fulldisclosure/)
  - Pen-Test (http://www.securityfocus.com/archive/101)
  - Web Application Security (http://www.securityfocus.com/archive/107)
  - Honeypots (http://www.securityfocus.com/archive/119)
  - CVE Announce (http://archives.neohapsis.com/archives/cve/)
  - Nessus development (http://list.nessus.org)
  - Nmap-hackers (http://seclists.org/nmap-hackers/)
  - VulnWatch (http://www.vulnwatch.org)

Source: Network Security Assessment, 2nd Edition, by Chris McNab

Sources of Vulnerability Information

innovate achieve lead

Vulnerability Databases

- The following vulnerability databases and lists can be searched to enumerate vulnerabilities in specific technologies and products:
  - MITRE CVE (http://cve.mitre.org)
  - NIST NVD (http://nvd.nist.gov)
  - ISS X-Force (http://xforce.iss.net)
  - OSVDB (http://www.osvdb.org)
  - BugTraq (http://www.securityfocus.com/bid)
  - CERT vulnerability notes (http://www.kb.cert.org/vuls)
  - FrSIRT (http://www.frsirt.com)

Source: Network Security Assessment, 2nd Edition, by Chris McNab

Sources of Vulnerability Information

innovate achieve lead

Underground Web Sites

- The following underground web sites contain useful exploit scripts and tools that can be used during penetration tests:

- Milw0m (http://www.milw0rm.com)
- Raptor's labs (http://www.0xdeadbeef.info)
- H D Moore's pages (http://www.metasploit.com/users/hdm/)
- The Hacker's Choice (http://www.thc.org)
- Packet Storm (http://www.packetstormsecurity.org)
- Insecure.org (http://www.insecure.org)
- Top 100 Network Security Tools (http://sectools.org)
- IndianZ (http://www.indianz.ch)
- Zone-H (http://www.zone-h.org)
- Phenoelit (http://www.phenoelit.de)
- Uninformed (http://uninformed.org)
- Astalavista (http://astalavista.com)
- cqure.net (http://www.cqure.net)
- TESO (http://www.team-teso.net)
- ADM (http://adm.freelsd.net/adm/)
- Hack in the box (http://www.hackinthebox.org)
- cnhonker (http://www.cnhonker.com)
- Soft Project (http://www.s0ftpj.org)
- Phrack (http://www.phrack.org)
- LSD-PLaNET (http://www.lsd-pl.net)
- w00w00 (http://www.w00w00.org)
- Digital Offense (http://www.digitaloffense.net)

Source: Network Security Assessment, 2nd Edition, by Chris McNab

Sources of Vulnerability Information

innovate achieve lead

Vulnerability Databases

- https://cve.mitre.org/
  - Common Vulnerabilities and Exposures (CVE®) is a list of common identifiers for publicly known cybersecurity vulnerabilities
- https://nvd.nist.gov/
  - The National Vulnerability Database (NVD) is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP)
  - This data enables automation of vulnerability management, security measurement, and compliance
  - The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics.


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!