Cybersecurity in the Age of Global Mistrust

Esfandiar Haghverdi

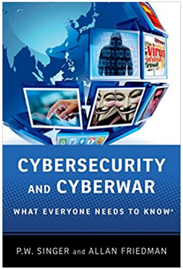
Luddy School of Informatics, Computing, and Engineering
Indiana University
Bloomington, Indiana

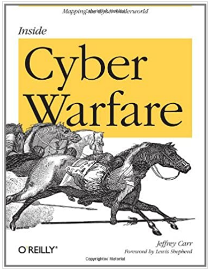
December 3, 2022

Outline

- Central Problems of Security
- Malicious Software
- Verizon DBIR
- AI and Cybersecurity
- Cybersecurity Programs at IUB

Books


CYBERSECURITY AND CYBERWAR
WHAT EVERYONE NEEDS TO KNOW
P.W. SINGER and ALLAN FRIEDMAN


Inside
Cyber Warfare
O'REILLY
Jeffrey Carr
Foreword by Lewis Shepherd
Copyrighted Material

Central problems of security

- What assets need protection?
- How are these assets threatened?
- How to counter these threats?

- *Computer Security:* Measures and control that ensure confidentiality, integrity and availability of information system assets including hardware, software, firmware, and information being processed, stored and communicated.
    - Confidentiality: Data confidentiality, Privacy
    - Integrity: Data integrity, System integrity
    - Availability
- The CIA triad
- Authenticity: Users can be verified, input source can be trusted.
- Accountability: Actions of an entity can be traced uniquely to that entity.

Levels of Impact

- Low: E.g., Directory information of faculty (C)
- High: E.g, Patient allergy information (I)
- Moderate: E.g., University website (A)

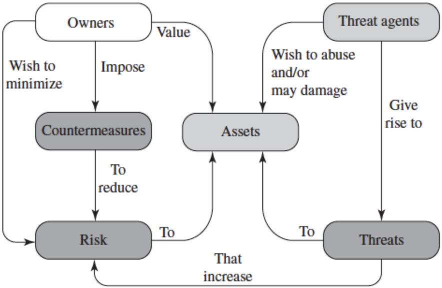


Figure 1.1 **Security Concepts and Relationships**

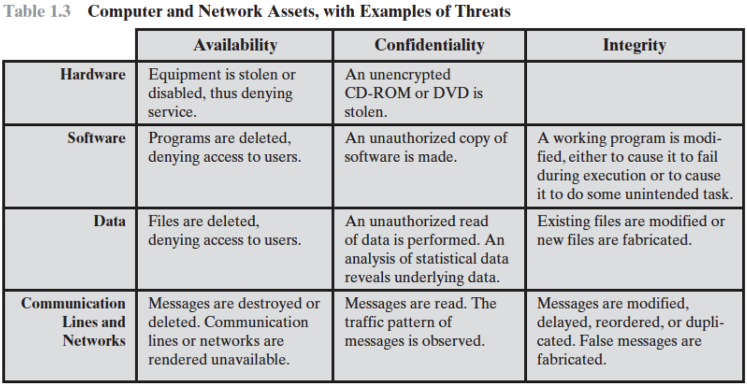


Table 1.3 **Computer and Network Assets, with Examples of Threats**

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Strategy

- Specification/policy: What is the security scheme supposed to do?
- Implementation/mechanisms: How does it do it?
- Correctness/assurance: Does it really work?

Specification

- Value of the assets
- The vulnerabilities of the system
- Potential threats and likelihood of attacks
- Trade-offs: Ease of use vs security, and Cost of security vs cost of failure and recovery

Implementation

- Prevention
- Detection
- Response
- Recovery

Correctness

- Assurance
- Evaluation

Malicious Software

- *Malware*: a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim.

Propagation Mechanisms

- Infection of existing executable or interpreted content by viruses that is subsequently spread to other systems
- Exploit of software vulnerabilities either locally or over a network by worms or drive-by-downloads to allow the malware to replicate
- Social engineering attacks that convince users to bypass security mechanisms to install Trojans, or to respond to phishing attacks.

Malware Classification

- Need host program (viruses) vs self-contained programs (worms, Trojans, and bots)
- Malware that does not replicate (Trojans and spam e-mail) vs malware that does (viruses and worms)

Payload Actions

- Corruption of system or data files
- Theft of service in order to make the system a zombie agent of attack as part of a botnet
- Theft of information from the system, especially of logins, passwords, or other personal details by keylogging or spyware programs
- Hiding; where the malware hides its presence on the system from attempts to detect and block it.

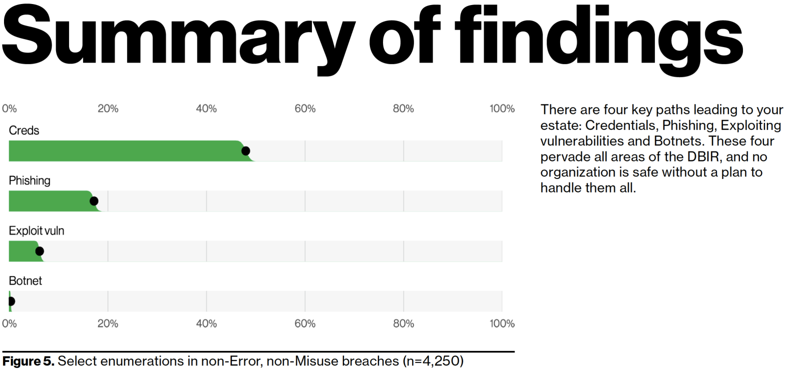
Crimeware

- The Zeus crimeware toolkit is a prominent, recent, example of an attack kit.
- APTs differ from other types of attack by their careful target selection, and persistent, often stealthy, intrusion efforts over extended periods. A number of high profile attacks, including Aurora, RSA, APT1, and Stuxnet, are often cited as examples.

Verizon DBIR 2022

- **Incident:** A security event that compromises the integrity, confidentiality or availability of an information asset.
- **Breach:** An incident that results in the confirmed disclosure–not just potential exposure–of data to an unauthorized party.

Verizon DBIR 2022



Summary of findings

There are four key paths leading to your estate: Credentials, Phishing, Exploiting vulnerabilities and Botnets. These four pervade all areas of the DBIR, and no organization is safe without a plan to handle them all.

Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

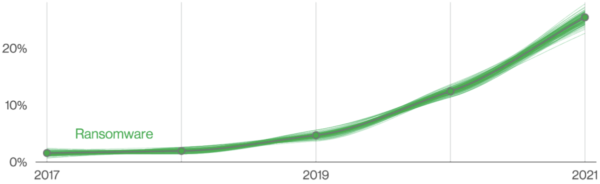


Figure 6. Ransomware over time in breaches

This year Ransomware has continued its upward trend with an almost 13% increase–a rise as big as the last five years combined (for a total of 25% this year). It's important to remember, Ransomware by itself is really just a model of monetizing an organization's access. Blocking the four key paths mentioned above helps to block the most common routes Ransomware uses to invade your network.

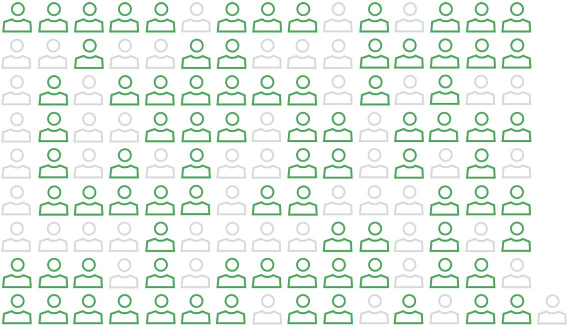


Figure 7. Partner vector in System Intrusion incidents (n=3,403)
Each glyph represents 25 incidents.

2021 illustrated how one key supply chain breach can lead to wide ranging consequences. Supply chain was responsible for 62% of System Intrusion incidents this year. Unlike a Financially motivated actor, Nation-state threat actors may skip the breach and keep the access.

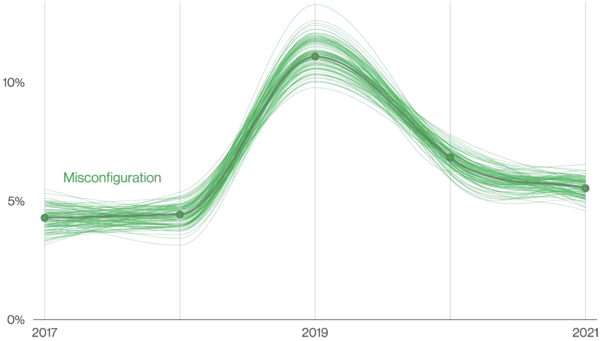


Figure 8. Misconfiguration over time in breaches

Error continues to be a dominant trend and is responsible for 13% of breaches. This finding is heavily influenced by misconfigured cloud storage. While this is the second year in a row that we have seen a slight leveling out for this pattern, the fallibility of employees should not be discounted.

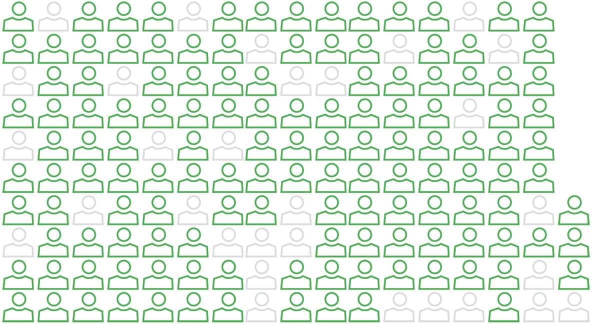


Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

The human element continues to drive breaches. This year 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse, or simply an Error, people continue to play a very large role in incidents and breaches alike.

AI and Cybersecurity

- One of the most notorious pieces of contemporary malware - the Emotet Trojan - is a prime example of a prototype-AI attack.
- Emotet's main distribution mechanism is spam-phishing, usually via invoice scams that trick users into clicking on malicious email attachments.
- The Emotet authors later added another module to their Trojan, stealing email data from infected victims. Sending out contextualized phishing emails at scale.

- Can automatically insert itself into pre-existing email threads, which gives the phishing email more context, thereby making it appear more legitimate.
- The methodology could easily leverage AI to supercharge this attack.
- An AI-powered Emotet Trojan could create and insert entirely customized, more believable phishing emails.

Offensive AI: a paradigm shift in cyberattacks

- Impersonation of trusted users: AI attacks will be highly tailored yet operate at scale.
- Blending into the background: AI will also be able to learn the dominant communication channels and the best ports and protocols to use to move around a system, discretely blending in with routine activity.
- Faster attacks with more effective consequences: Sophisticated attacks require skilled technicians to conduct research on their target and identify individuals of interest, understand their social network and observe over time how they interact with digital platforms. An offensive AI achieves the same level of sophistication in a fraction of the time, and at many times the scale.

Defensive AI

- AI can discover new and sophisticated changes in attack flexibility: Conventional technology is focused on the past and relies heavily on known attackers and attacks, leaving room for blind spots when detecting unusual events in new attacks.
- AI can handle the volume of data: AI can enhance network security by developing autonomous security systems to detect attacks and respond to breaches.
- An AI security system can learn over time to respond better to threats: AI helps detect threats based on application behavior and a whole network's activity.

Drawbacks and Limitations of Using AI

- Data sets: Creating an AI system demands a considerable number of input samples, and obtaining and processing the samples can take a long time and a lot of resources.
- Resource requirements: Building and maintaining the fundamental system needs an immense amount of resources, including memory, data, and computing power.
- False alarms: Frequent false alarms are an issue for end-users, disrupting business by potentially delaying any necessary response and generally affecting efficiency. The process of fine-tuning is a trade-off between reducing false alarms and maintaining the security level.

- Attacks on the AI-based system: Attackers can use various attack techniques that target AI systems, such as adversarial inputs, data poisoning, and model stealing. Adversarial attacks are hard to detect, prevent, and counter against.
- Majority of approaches proposed today are model-free methods. These models require a large quantity of training data, which are hard to obtain in real cybersecurity practice.
- AI can help protect the system against cyber-threats but can also facilitate dangerous attacks; i.e., AI-based attacks. Malicious actors can leverage AI to make attacks flexible and more sophisticated to bypass detection methods to penetrate computer systems or networks.

The primary areas of utilizing AI for cybersecurity

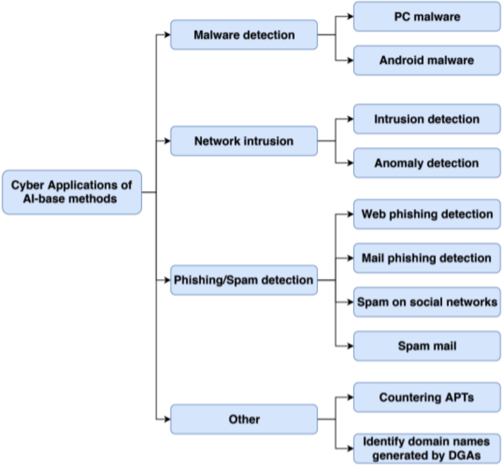


Figure 1. Main branches of cybersecurity applications adopting AI techniques.

Leveraging AI for malicious activities.

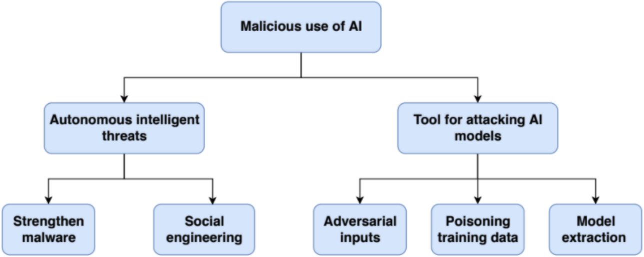


Figure 2. The use of AI for malicious activities in cybersecurity.

IBM's DeepLocker

- One of the best examples of using AI to empower malware.
- Target class concealment
- Target instance concealment
- Malicious intent concealment
- Facial recognition of the target activates the malware unlocking mechanism.
- Would not be possible without the use of AI.

Cybersecurity Programs at IU

- BS in Cybersecurity and Global Policy (Luddy + HLS)
- Security specialization, BS in CS (Luddy)
- Security Informatics Cognate and Minor, BS in Informatics (Luddy)

Cybersecurity Programs at IU

- BS in Cybersecurity and Global Policy (Luddy + HLS)
- Security specialization, BS in CS (Luddy)
- Security Informatics Cognate and Minor, BS in Informatics (Luddy)
- MS in Secure Computing (Luddy)
- MS in Cybersecurity Risk Management (Luddy + Kelley + Maurer)
- Enterprise Security concentration in MSIS (Kelley)

Cybersecurity Programs at IU

- BS in Cybersecurity and Global Policy (Luddy + HLS)
- Security specialization, BS in CS (Luddy)
- Security Informatics Cognate and Minor, BS in Informatics (Luddy)
- MS in Secure Computing (Luddy)
- MS in Cybersecurity Risk Management (Luddy + Kelley + Maurer)
- Enterprise Security concentration in MSIS (Kelley)
- 4 graduate certificates (Luddy, Maurer, Kelley)

Cybersecurity and Global Policy Program

- Bachelor of Science in Cybersecurity and Global Policy
    - Technical Foundations (16 cr)
    - Policy Foundations (12 cr)
    - Cybersecurity Core (15 cr)
    - Global Policy Core (12 cr)

Extra and Co-curricular Activities

- Hacking for Defense (H4D): Course as part of NSIN partnership
- CyberForce: A DoE Cybersecurity Workforce Development Program
- HackIN: A Capture the Flag event revolving around hardware/firmware reverse engineering and analysis
- NCCDC: The largest college-level cyber defense competition in the USA

Student Activities

- Women in Cybersecurity (WiCyS) IU Student Chapter
- CTF Team
- CTF Club
- Cybersecurity Club
- Cyber Camps: One camp in 2021, two camps planned for 2022
- CyberCorps SFS: Our newest scholarship program (through NSF)
- IoT House & Hacking Nights: Activities at the research house

Outreach

- K-12 CTF: Online CTF as a continuation of a DoD CAE CySP capacity building grant. Boys & Girls Club, summer 2021.
- K-12: Capture the Flag Challenges for area middle and high schools, simultaneous teacher PD
- K-12: Online teacher PD for Cybersecurity, multiple online curriculum modules and activities
- Teach-IT: Teaching the community partners
- Serve-IT: Cybersecurity team to help non-profits in local community

Jobs

- Job Analysis