Cisco highlights malware, phishing, man-in-the-middle attack, denial-of-service attack, SQL (Structured Query Language) injection, and zero-day exploit as the most common attacks. Malware, phishing, man-in-the-middle attack, SQL injection, and zero-day exploit can potential access data which attacker should not have access to. Malicious software, malware, breaches a network and can covertly transmit data. Phishing can steal sensitive information through fraudulent communications. Information is compromised by a man-in-the-middle attack because attackers insert themselves between a two-party transaction. SQL injection is an attack where attackers insert malicious code to a server using SQL and can access information, they should not have access to. During zero-day exploit attackers emphasize on an announced exploit that has not been patched and so if the exploit allows for access to data, data is sufficiently released.

Cisco highlights malware, phishing, man-in-the-middle attack, denial-of-service attack, SQL injection, and zero-day exploit as the most common attacks. These attacks compromise sensitive information or give attackers unauthorized access to information. Early detection or anticipation of an attack minimizes damages and secures the information of people/organizations.

The world is becoming perpetually connected. IoT, the Internet of Things where every device is becoming connected to the internet, is a growing concern. We understand cyber security is become more important by the day. Therefore, exploring current technologies and how they are growing is essential for growing in cyber defense. Improving cyber security is important because threats are always evolving. My aim is to understand how big data is being used in cyber defense.

New and old technology often lack security features because of oversight. These technologies range from IoT devices to network based instruments that did not anticipate the need for security. Exploring how Big Data is being employed can lead to advances in security.

North Korea has been systematically improving their cyber warfare capabilities since the 1990s. Most of their cyber attacks are well-coordinated attack that require 3 to 7 months of preparation. These attacks are carried out in neighboring countries and target financial, press, or government institutions. South Korea’s deals with North Korean Cyber attacks by minimizing the damage caused by these attacks. Since these attacks can be sector specific and sometimes not completely traceable to north Korea, than analysis of the attacks is limited and restricts learning about the attacks. A countermeasure system where sharing the information and subject of an attack is initially proposed for sharing malicious code, origin of attack, and hacking info. Lee explains developed countries in surveillance have set up cross established surveillance systems. Currently big data analysis in cyber security is large-scale log analysis, abnormal transactions/actions, and detection of malicious code. Lee proposes real-time information sharing based on a standardized format. With vast amounts of information collected in real time, lee proposes the use of analysis methodologies such as machine learning and cluster analysis to detect changes in cyber-attacks. The infrastructures would prevent more North Korea cyber-attacks because resources can be concentrated on predicted points.

North Korea has systematically improved their cyber capabilities since the 1990s and can carry out well-coordinated attacks from within a neighboring country in 3 to 7 months. Current defense strategies focus on minimizing damages. Sector specific attacks and limited analysis of attacks leads to minimal learning about an attack. Lee proposes a countermeasure system where information like subject of attack, malicious code, origin of attack, and hacking info are shared in real-time. Increasing information available on attacks would increase overall understanding of attack structures and themes. Currently big data analysis for security focuses on large-scale log analysis, abnormal transactions/actions, and detection of malicious code. Real-time information sharing using a standard format would increase understanding because information could be processed with machine learning or cluster analysis to detect changes and uncover patterns.

Attacks on nuclear power plants are a serious concern because they can lead to real threats or terror. Well-known attacks on a nuclear plant are mitigated by “signature-based detection methods or vaccines”. These signature-based methods have patterns they match and block to similar patterns in networks or URLs containing. Signature-based methods struggle identifying emerging threats, therefore analyzing logs improves the security measures. The volume of raw logs has increased and become segmented and coupled with increasing network flow data volume and number of full-packet logs/atypical logs allows for the categorizing of security threats. SIEM is a next gen log analyzing method since it applies self-established rules to store, analyze, and delete logs. With current SIEM methods a detection scenario is needed. Therefore in developing the security scenario, hacking codes are statically and dynamically analyzed in security events to create signatures by observing status of internal information leaks. A set of base rules for analyzing are complemented by a set of threat rules that create a detection. Signatures are iteratively applied to security equipment in the scenario with broadening rules until the threat is detected. Events that caused misdetections are excluded and events that lead to a positive threats lead to the creation of scenarios based on level of threat. Using the system assets and system status hypotheses and theories are used for security scenarios where a security breach will be detected.

Attacks on nuclear power plants are a serious concern. Currently, attacks are mitigated through “signature-based detection methods or vaccines”. Current methods struggle identifying emerging threats. Logs help identify threats, but raw logs have become more voluminous and are more segmented. Analyzing raw logs with increased network traffic and atypical logs leads to possible categorization of security threats. SIEM is a log analyzing method that applies self-established rules to store, analyze, and delete logs. SIEM requires a detection scenario, therefore malicious code is analyzed in specified security events to create signatures that observe internal information leaks. A set of base rules is complemented by a set of threat rules are used to create detections of a threat. Signatures are applied iteratively to equipment until threats are detected; misdetections are excluded, and positive threats lead to a scenario with an attached threat level. System assets and system statues are used for hypotheses and theories which are applied to security scenarios for breach detection.