# Cryptography, Network Exploitation, Crime & Policy Impact

James Campbell

December 4, 2016

Saint Leo University

# Cryptography, Network Exploitation, Crime & Policy Impact

Telecommunications, computer networks, and information systems continue to develop at momentous rates. Seemingly with every blink of an eye there are brilliant innovations and advances in technology which discover new ways to connect our lives to our devices. However, with every new advancement are new vulnerabilities and endless amounts of data to be exploited by hackers for a myriad of nefarious reasons. As cyber-security professionals, software engineers, analysts, etc., the industry and consumers rely on the workforce to drive the markets and technologies forward in order to deliver cyber security products and solutions to match current and future demands. In order to properly defend against cyber-attacks, we need to understand cyber criminals, assess our networks, take appropriate measures, and establish clear, specific information assurance policy.

State actors, non-state actors, and cyber-criminals who wish to carry out attacks on a network generally plan their attacks by scanning or probing a network for exploitable flaws or vulnerabilities within their operating systems, applications, network security, etc. Theoretically, analyzing darknet traffic could provide cybersecurity professionals with critical information about potential intruders, allowing companies to get ahead of malware trends. Through monitoring attacks packets, cyber security professionals could build a security monitoring and response model based upon traffic analysis of malicious attack patterns (Choi, Song, Kim, & Kim, 2014).

According to the World Economic Forum, the theft of information and malicious attacks against networks or information systems are among the top concerns for modern businesses. Hackers and cybercriminals conduct reconnaissance prior to attacks and are well versed in network flaws and vulnerabilities. It is crucial that a company does a proper risk assessment,

understands its network vulnerabilities, and takes calculated risks in order to find a cost-effective means to protect against hackers. Likewise, companies must also detect and respond to security incidents after conducting computer forensics by taking the appropriate measures: discover, qualify, mitigate, and recover (Brewer, 2015).

In response to the rising trend in cybercrime, the Cabinet Office of the United Kingdom has launched the Cyber Security Information Sharing Partnership, building upon a government cyber security strategy which focused on the promotion of information sharing between government and civilian entities. British intelligence analysts from GCHQ and the Security Service (MI5) will collaborate with industry experts to form a fusion cell focused on detecting exploitable flaws in software as well as monitoring threats and attacks across finance, defense, energy, telecommunications, and healthcare systems which are at risk (Elsevier ltd., 2013).

It is essential that network administrators must be able to detect network intrusion in order protect information systems and data against network attacks. Failure to recognize a network attack could lead to devastating financial losses and irreparable damage to a company's assets and reputation. Network attack recognition models have been constructed in order to clearly identify and recognize the process of a network attack including analysis of hostile agents, exploitation of vulnerabilities, observations of failed actions, and hackers' concurrent goals. Understanding the exploitation process as well as being familiar with network vulnerabilities will allow network administrators to be aware of temporal constraints which limit hackers and allow cyber security experts to predict their next actions for alert correlation and effective planning (Liu & Gu, 2013).

Attack graph has been the industry standard tool which alerts of potential network attacks. This tool assesses risk analysis through provided static information about attack paths and is able

to tip off system administrators to the threat of an attack by providing the probability of vulnerability exploitation. Accuracy of intrusion detection and network attack forecasting has much room for improvement though, as attack graph's algorithm fails to take in significant parameters such as intrusion alerts, service dependencies, or active responses. Updating intrusion detection and attack response algorithms will help redefine the approach to network security and reduce the risk of future attacks (Ghasemigol, Ghaemi-Bafghi, & Takabi, 2016).

Complex network configurations, such as Advanced Metering Infrastructure (AMI), share vast amounts of consumer data regarding consumption, outages, rates, reliability, and efficiency between interconnected smart devices over mesh networks. These complex networks, though sophisticated, are also difficult to safeguard and offer opportunities to cybercriminals to compromise and steal data, interfere with services, and exploit information. In a puppet attack, a network intruder uses any normal node as a puppet and flood the puppet node with attack packets, causing the puppet node to drop connection and reconnect with neighboring nodes, thus infecting them with the attack packets and ultimately causing targeted Denial of Service (DoS) on the network (Yi, Zhu, Zhang, Wu, & Pan, 2016).

Password-Based Encryption is a cryptographic implementation which derives an encryption key to protect and store local files and data by the means of a user-defined password. Some examples of a Password-Based Encryption API (application program interface) are the Java Cryptography Extension (JCE) and Bouncy Castle (for both Java and C#). The downside to Password-Based Security is that it makes the encryption less random and less effective due to the bit value. Keys should be randomly generated, opposed to based-upon dictionary terms or memorable dates or predictable values. Password values can be detected by free tools, such as john the ripper, that are easily and readily available to hackers. The average password length for

user accounts is eight characters. A truly random password of eight characters has a maximum entropy of 56 bits. Using an eight-character password containing dictionary words, repeating characters, or more predictable values is even less secure. Even with longer passwords, hackers can use dictionary attacks to some levels of success against user-defined passwords. Users can protect passwords against dictionary and exhaustive brute-force attacks by "salting" passwords with a randomly generated character string represented by the value *k*. MD5 is no longer considered to be secure and there is an active search for better, stronger hash functions (Boklan, 2009).

Telecommunications in a post 9/11 world have focused heavily on the debates of data privacy, freedom of information, and the use of cryptography. With the expansion of telecommunications into Voice over Internet Protocol (VoIP) Law Enforcement are seeking to expand the 1994 Communications Assistance for Law Enforcement Act with the justification that it will aide officers in carrying out their duties to keep communities safe. Legal efforts are also being put forth which could require Internet Service Providers (ISPs) to retain their data and logs for several years to share with the government at their request (Whitfield, 2007).

The United States Office of Personnel Management (OPM) failed to properly encrypt the data of 21.5 million federal employees in national security positions, leading to a major data breach in a hack likely originated in China. Notably, the OPM data breach resulted in the theft of 5.6 million fingerprints, biometric data, social security numbers, and other personally identifiable information. Cybersecurity experts believe that the biometric data, including the fingerprint data, could be used to spoof biometric readers to gain unauthorized access into information systems or facilities (Elsevier, 2016).

Over the past few years, the network security of our organizations and infrastructure has struggled to keep up with the threats that surround them. This not only threatens the infrastructure of our networks, but our corporate infrastructure, our individual employment, and even the freedoms afforded to us as citizens. In December 2014, Sony Pictures Entertainment was subjected to an alleged state sponsored attack sponsored by the North Korean government for Sony's holiday release of the R-rated comedy "The Interview", which controversially depicted the assassination of North Korea's head of state, Kim Jong Un. Despite Sony Pictures Entertainment's large security budget, Sony fell subject of an embarrassing attack which led to the cancellation of a blockbuster film's release, the resignation of several senior-level executives, and large financial losses. While Sony is an example of why the industry needs to make further advancements in Information Security, additional research suggests that 80% of attackers exploit well-known security flaws and gain access due to insufficient action of the security team (Jan Hof Affiliation: Forescout Technologies, 2015).

With so much at stake, organizations can no longer afford to stand by passively waiting for network intrusions and attacks. Instead corporations, government agencies, and organizations should take a proactive lean-forward approach to cybersecurity. Proactive cybersecurity practices can include more orthodox security standards such as real-time analytics and cybersecurity audits promoting resilience, but can also include more controversial methods such as hack back, honeypots, and information sharing. The 2014 National Institute for Standards and Technology (NIST) Cybersecurity Framework aims to improve private sector security through voluntary standards developed in coordination with the industry. It is also important to understand the laws that are in place to protect our information systems. The 1986 U.S. Computer Fraud and Abuse Act (CFAA), as amended in 2008, remains one of the more relevant

laws to proactive cybersecurity, prohibiting and penalizing the unauthorized access of a computer or unauthorized transmission of malware, as well as damaging a protected computer network, obtaining and trafficking private information, and affecting the use of a computer (Craig, Shackelford, & Hiller, 2015).

Generally speaking, the majority of users on a network or information system have a very limited if not poor understanding of how it integrates, or conflicts, with their daily lives, opening the door to abuse by those who wish to exploit network vulnerabilities. Technology has evolved much more quickly than our technology education, laws, and social conventions. While in the 1970's a computer operator was a highly educated specialist, in the Present, even our children can operate a computer, connect to a network, and communicate with other network nodes around the globe. While information security is improving, the exploits of today are far more sophisticated and the security gap continues to widen. CISOs, cybersecurity analysts, computer scientists, and network engineers need to work together to innovate cutting edge cybersecurity methods. The industry cannot sit idly by as we teeter at the edge of total cyber warfare (Singer & Friedman, 2014).

Information assurance laws and public policy, proactive cybersecurity, and public education of information systems is vital to ensuring the future success of our economy, infrastructure, and our liberties. We need to further understand cyber criminals, assess our own network flaws, and take appropriate measures to close the cybersecurity gap which is exploited by cyber criminals who wish to take advantage of and harm others. It is important that public policy addresses cyber security in a way that is clear and is not so broad that they could potentially stifle the very freedoms that they intend to protect. In order to achieve these results, we need subject matter experts who are willing to dedicate themselves to lawmaking and public policy.

# Works Cited

Boklan, K. D. (2009). Large Key Sizes and the Security of Pasword Based Encryption. *International Journal of Information Security and Privacy*, 65-72.

Brewer, R. (2015). Cyber threats: reducing the time to detection and response. *Network Security*, 5-8.

Choi, S.-S., Song, J., Kim, S., & Kim, S. (2014). A model of analyzing cyber threats trend and tracing potential attackers based on darknet traffic. *Security and Communications Network*, 1612-1621.

Craig, A. N., Shackelford, S. J., & Hiller, J. S. (2015). Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis. *American Business Law Journal*, 721-787.

Elsevier ltd. (2013). UK shares information to combat cyber-threats. *Computer Fraud & Security*, 1, 3.

Elsevier, B. (2016). OPM hack now stands at 5.6m fingerprints. *Biometric Journal Today*, 1-2.

Ghasemigol, M., Ghaemi-Bafghi, A., & Takabi, H. (2016). A comprehensive approach for network attack forecasting. *Computers and Security, v58*, 83-105.

Jan Hof Affiliation: Forescout Technologies. (2015, October 1). Addressing new demands on network security. *Network Security*, pp. 5-7.

Liu, Y., & Gu, W.-X. (2013). An effective recognition method for network attack. *Optik - International Journal for Light and Electron Optics*, 4823-4826.

Singer, P., & Friedman, A. (2014). Cyber Security and Cyberwar. *Network Security*, 4.

Whitfield, D. (2007). *Privacy on the Line: The Politics of Wiretapping and Encryption.* Cambridge: MIT Press.

Yi, P., Zhu, T., Zhang, Q., Wu, Y., & Pan, L. (2016). Puppet Attack: A denial of service attack in advanced metering infrastructure network. *Journal of network and computer applications, 59*, 325-332.