Implications of Traffic Analysis to Homeland Security

Bob Duhainy Ph.D.

Bob.Duhainy@waldenu.edu

Walden University
100 Washington Avenue South
Suite 900
Minneapolis, MN 55401

Abstract - One of the biggest challenges currently faced by the Department of Homeland Security is guaranteeing cybersecurity. Each and every day some type of cybercrime occurs. Such crimes have the potential to affect the country's national security. This paper investigates the significance of internet traffic and analysis to Homeland Security. It will look at the importance of internet traffic and analysis to Homeland Security as well as encrypted traffic and its implications to cyber-security. The manner in which the U.S. has handled cybersecurity over the past twenty years and the methods that the government has used in this time period will be discussed. Encrypted mobile messaging applications will also be discussed. At the end of the discussions, solutions are recommended and a conclusion given.

Categories and Subject Descriptors

K.5.2 [Cybercrime]: National Security – Implications

General Terms

Internet Traffic Analysis, Homeland Security

Keywords

Cybercrime, Cyber Security, NSA, FBI, Terrorism, Encryption Education, Messaging Applications, Internet Traffic

1. INTRODUCTION

In the recent past, the DHS (Department of Homeland Security) and the DoD (Department of Defense) signed an agreement to enhance the cooperation between the two, with regards to improving United States' cyber-security capabilities. The agreement is aimed at specifically enhancing cyber-security cooperation on capabilities development, mission activities and strategic planning. The agreement also outlined the specific individual and joint goals and responsibilities for both departments. The most crucial element in the agreement is personnel swap, which the Department of Defense expects to improve the different lines of communication between DHS and DoD. Under the cooperation agreement, the Department of Homeland Security will appoint an individual for the position of Director of Cyber-Security collaboration who will work in the NSA (National Security Agency) and serve as the Department's liaison to the United States Cyber Command. In addition, the agreement specifies that the DHS will supply more staffs from its office to the National Security Agency, including officers from its Office of the General Counsel, Office for Civil Rights and Civil Liberties and Privacy Office (Bobby, 2010). The DoD was to, in return, send a group of experts from its Cryptologic Services Group, to the Department of Homeland security's NCCIC (National Cyber-security and Communications Integration Center) with the aim of supporting Homeland Security's cyber-security efforts and coordinating those efforts with the operations of the DoD. In spite of the significant support that both departments will be offering each other, the agreement in no way interferes with the DHS and the DoD authorities, oversight mandates, command relationships or civil and privacy liberties. One of the most important strengths of the agreement is that Homeland Security will have more access to the Department of Defense, particularly its National Security Agency and its expertise and resources.

2. BACKGROUND

The fact that cyberspace threats are borderless in nature calls for increased collaborations between countries so as to combat the threats. International collaboration is a key component of DHS's cyber mandate of safeguarding and securing the US's cyberspace. The Department, through the NPPD (National Protection and Programs Directorate), has created several functions to boost its international cooperation programs with other nations and organizations. The functions are carried out under the Office of Cyber-security and Communications in NPPD. Several parties have, however, insisted that for the NPPD to succeed in its international collaborations program, it should streamline its functions and operations so that it can consolidate its recourses and use them to better facilitate foreign relations (DHS Can Strengthen Its International Cybersecurity Programs, 2012). The United States Computer Emergency Readiness Team also needs to improve its information-sharing with related agencies so that it can better coordinate incident response.

Cyber-security entails all operations and activities aimed to protect and secure a cyberspace and computer infrastructure, in addition to the measures aimed at restoring ICT (Information and Communication Technology) systems and the information contained in such systems. To best protect a cyberspace, there is the need to form security policies, best practices, collect tools, form guidelines, approaches, train staff, and have the technologies. Additionally, cyber-security also involves reduction of threat / vulnerabilities, incident response and deterrence of attacks, international cooperation and recovery measures. Due to the fact that cyber-attacks are borderless in nature, there is a need for governments and international organizations to act in concert so as to develop the cyber-security policies, procedures and plans, with the objective of enhancing cooperation, incident response and deterrence operations.

In the present day world, many aspects of our day-to-day lives have been moved to computers and online systems, for instance, education (we have online research, report cards, and virtual classrooms), healthcare (computer-based equipment and medical forms), finance (online bank transactions, bank accounts, electronic paychecks and loans), governments (online filing of birth records, death records, tax records and social security), transportation (aircraft navigation, car engine systems, and traffic control signals) and communications (texting, cell phones and email). Think of how much of your own personal data is stored on your own computer or in someone else's system. Is your computer or the system fully secure? This is where cyber-security comes in – it involves all the protective measures aimed at deterring cyber-attacks, and securing our computer systems (Cyber security Awareness, 2012). The growing volume and increasingly sophisticated nature of attacks targeting data theft, phishing scams and other vulnerabilities require that we stay vigilant in protecting our computers and ICT systems. The chart below shows the most common types of cyber attacks witnessed nowadays. (Cyber Crime Statistics and Trends [Infographic]

Attack Types	**%**
Viruses, malware, worms, trojans	50%
Criminal insider	33%
Theft of data-bearing devices	28%
SQL injection	28%
Phishing	22%
Web-based attacks	17%
Social engineering	17%
Other	11%

Figure 1: Internet Attack types

The internet has empowered people like never before. Even adolescents with the right skills can effectively disable traffic control systems, manipulate stock trading and steal personal information from online databases. What such individuals can easily do on their own, criminals groups can also do. In fact, organized crime groups have been involved in cybercrime for quite some time now. Cyber-security experts, scholars, law enforcement agencies and governments contend that traditional criminal groups are becoming more and more involved in electronic crimes. However, available data shows that cyber criminals are more likely to be loosely linked to online networks rather than be strong members of criminal organizations. In the past few years, extremist organizations have also been found to use cybercrime to finance their activities. For instance, Imam Samudra, the mastermind of the 2002 Indonesia bombings, is reported to have called on his followers to use credit card fraud to finance their militant activities.

Other important things to look at include:

Data Breach by Industry (Cyber Crime Statistics and Trends [Infographic]

Industry	**%**
Medical / Healthcare	38.9
Business	35.1
Educational	10.7
Government / Military	9.9
Banking / Credit / Financial	5.3

Figure 2: Cybercrime statistics and trends

3. IMPORTANCE OF INTERNET TRAFFIC AND ANALYSIS / IMPLICATIONS / MOBILE MESSAGING

Traffic analysis is defined as the process of intercepting and looking at online communications with the aim of making inferences from the patterns of communications. Such an analysis can be done even when the online communications / messages cannot be decrypted (Kiran and Anish, 2015). This type of analysis best works with large volumes of messages, in that the higher the number of messages intercepted, the more that can be deduced from that information. Traffic analysis can be done by agencies for counter intelligence or military intelligence. It can also be used by criminal organizations, making it a concern to cyber-security experts. Knowing who is communicating with whom, at what time and for what duration, can give clues to an attacker about information that one might rather that he or she should not know.

The size of the packets being exchanged amidst two hosts could also be important data for an attacker, even though they are not able to see the traffic contents. Observing a short bout of single-byte payload packets having regular pauses between every packet may signify an interactive session amidst two hosts, whereby every packet signifies a keystroke (Kiran and Anish, 2015). Huge packets maintained over time have a tendency of signifying transfer of files amidst hosts, also showing the host that is sending and the one that is the recipient of the file. On its own, this data may not be very detrimental to the network's security; however, a creative attacker shall be capable of combining this data with other data to evade intended security procedures (Northcutt, 2015). An article on a mechanism founded on traffic behavior, which assists in the identification of P2P users, and even goes further to differentiate the kind of P2P application being utilized was run by Focus. IP/TCP lends itself to traffic analysis to the point that "fingerprinting" of systems is possible. Fyodor's NMAP site has a tutorial, which intensively elaborates this; however, NMAP functions through sending packets to stimulate the host. Also, it is possible to passively fingerprint; Tenable's Passive Vulnerability Scanner and Source Fire's RNA are examples of commercial devices to passively fingerprint. A powerful free device known as P0f is also available. In accordance to Honeynet project, the following areas are vital in OS fingerprinting. Mobile devices intents or identities cannot be verified. Hence, nodes need to cooperate for the integrity of the network's operation. Nodes might, however, decline to cooperate through not forwarding packets for others, so as not to wear out its resources (Northcutt, 2015). Other certain aspects that make the job of secure communication in informal wireless networks challenging, are a promiscuous operation mode, mobility of nodes, restricted processing power, and restricted availability of resources, like bandwidth, memory and battery power.

High ranked U.S. officials and lawmakers have intensified worries regarding the growing threat of jihad-driven terror attacks against the U.S. Tweets made by one of the two gunmen seemed to connect him to radical Islamic terror groups ('Terrorism has gone viral': US officials, lawmakers warn of growing jihad-inspired attacks, 2015). James Comey, FBI director, stated that the attack, whereby a security officer was shot in the leg, features the difficulties experienced by the FBI. Also, the group is increasingly guiding followers into meetings, which permit encrypted data, making it more difficult for law enforcement officers to access. Additionally, the Islamic State has been persuading followers to join the caliphate at Syria. According to the Obama administration, last week's attack at Dallas was a "lone wolf" attempt.

Even though portable tools might increase productivity, they also expose the Department to new security risks, like unintentionally exposing sensitive data or even download of viruses. Also; portable devices are in short of certain security features, which could be found on desktop computers. Some of the security threats to portable devices are theft, electronic eavesdropping, electronic user tracking, and illegal access to information / data (*DHS Needs to Address Portable Device Security Risks, 2012*). In addition, iOS- and Android-based smartphones lack the security features and functionality required to be centrally controlled in a government or enterprise surrounding. Moreover, the iOS- and Android-based tablet computers are not structured to utilize the Federal Information Processing Standard (FIPS) 201-compliant Personal Identity Verification card to determine two-factor authentication for the access of Federal information systems without any attachment / accessory. To enhance its workforce's mobility, DJS together with its components, are assessing the possibility of incorporating these consumer oriented portable devices in their networks. For instance, the USGC (United States Coast Guard) has started to deploy iOS- and Android-based smartphones to its personnel. The USCIS (United States Citizenship and Immigration Service) is also exploring Blackberry Playbooks and iPads as possible platforms for its high ranked officials. Given that every element has a special mission, their needs and requirements for utilizing and protecting the devices differ.

4. RESOLUTION

The Department of Homeland Security (DHS), Office of Cyber-security and Communications (CS&C) continues to enhance its ability to protect federal civilian Executive Branch agency networks from cyber threats. Just like EINSTEIN 1 and EINSTEIN2, DHS shall set up EINSTEIN3 Accelerated (E3A) to improve cyber-security study, security response, and situational awareness (*Privacy Impact Assessment for EINSTEIN 3 - Accelerated (E3A), 2013*). E3A shall allow DHS to identify malicious traffic targeting federal government networks and also stopping malicious traffic from destroying those networks. This shall be achieved via conveying invasion prevention abilities as a Managed Security Service offered by Internet Service Providers (ISP).

In response to developing cyber-security mission requirements from the Administration and Congress back in 2008, The National Cyber-Security Protection System (NCPS) was created to secure the federal civilian Executive Branch government network and stop suspected cyber threats. Network Security Deployment (NSD) functions as the NCPS program Office and heads the development and application of the NCPS that offers cyber-security technologies to constantly oppose surfacing cyber threats and implement effective risk reduction strategies to identify and discourage these threats (*Privacy Impact Assessment for EINSTEIN 3 - Accelerated (E3A), 2013*). NSD collaborates with all of the CS&C branches to make sure that NCPS abilities deployed by NSD encourage and enhance the mission capabilities of those branches. The NCPS entails an invasion prevention capability referred to as E3A. E3A permits DHS to better identify, respond to, and effectively counteract, suspected cyber threats detected in the federal network traffic it monitors. E3A keeps an eye on select Internet traffic, either originating from, or destined to, federal civilian Executive Branch agencies and departments. CS&C presents E3A invasion prevention capabilities as a Managed Security Service offered by Internet Service Providers (ISP). Managed Security Service is simply a model via which the government conveys requirements, which address the levels of service and objectives anticipated for their constituencies.

DHS shares the cyber threat data it obtains via E3A steady with its existent procedures and policies, with the inclusion of sharing and working together with any affected or involved federal departments and agencies, together with other federal cyber-security mission partners. The involved agencies and departments shall enter into a Memorandum of Agreement (MOA) with DHS to approve the implementation of intrusion prevention capabilities by DHS. The MOA particularly determines the parameters of agency in the NCPS program and approves the inspection as well as modification of agency traffic and other dealings with agency information systems in relation with the implementation of such intrusion prevention capabilities (*Privacy Impact Assessment for EINSTEIN 3 - Accelerated (E3A), 2013*). DHS expects that ISPs shall also obtain a letter of agency or a similar agreement from the agencies and departments taking part, informing ISPs of their agreement to take part in the NCPS program with DHS. The ISPs shall offer the services obtained through its agreement with DHS to those involved agencies and departments, which utilize the contacted ISP(s) as their service provider. The source of data assessed by the ISPs shall be the federal network traffic transiting to or from the involved agencies.

In the coming generation of wireless communication systems, there shall be a need for a quick deployment of independent mobile users. Such network scenarios cannot depend on organized or centralized connectivity, and could be visualized as applications of Mobile Ad Hoc Networks. A MANET is simply an independent collection of mobile users, which communicate over considerably bandwidth-limited wireless connections. Given that the nodes are portable, the network topology might quickly and suddenly change over time. The network is decentralized, where all the network activity like conveying messages must be executed by nodes, that is, routing functionality shall be included into the mobile nodes. A MANET is some kind of ad hoc network that could alter locations and organize itself on the fly. Since MANETs are portable, they utilize wireless connections to link with particular networks. This could be a standard Wi-Fi connection, or another medium, like a satellite or cellular transmission. Various MANETs are limited to a local region of wireless devices, whereas others might be linked to the internet (Kiran and Anish, 2015). For instance, a VANET or perhaps a "Vehicular Ad Hoc Network" is a kind of MANET, which permits automobiles to connect with devices on the roadside. Although the vehicles might not hold an Internet connection; however, the wireless pavement apparatus might be linked on the internet, permitting information from the vehicles to be conveyed over the internet. The information from the vehicle might be used to gauge the traffic conditions, among many other uses. Mobile devices intents or identities cannot be verified or even predetermined. Hence, nodes need to work together for the integrity of the network's operation. Nodes might, however, decline to cooperate through not forwarding packets for others so as not to wear out its resources. Other certain aspects that make the job of secure communication in informal wireless networks challenging are a promiscuous operation mode, mobility of nodes, restricted processing power, and restricted availability of resources like bandwidth, memory and battery power.

5. CONCLUSION

The Obama administration released its Cyberspace Policy Review in May 2009: Guaranteeing a Trusted and Resilient Information and Communications Infrastructure that it anticipated would lay the foundation for a new national cyber-security approach. The most important (the Cyber-Security Act of 2009) suggested major alterations in present federal government advances. The common starting point of each of these reform attempts is that present federal organization and present national cyber-security policy is insufficient for the job of protecting cyberspace (Harknett and Stever, 2015). Whereas most of the current cyber-security argument leans toward radical reforming, we recommend an incremental strategy to reorganization, which builds on the hard work of the previous decade accompanied with a re-conceptualization of the solution set. The rod to cyber-security is designed to be long, challenging, and tortuous. No really significant federal policy reform could be achieved without taking into consideration the intergovernmental policy dimensions, accompanied with the general threat perception fueling those reforms. Success shall stay obscure if the general public stays inactive in its contribution to national cyber-security (Harknett and Stever, 2015).

Increased education is another recommendation. Ever since the 1990s, academic programs in information security have been available. The DHS and NSA co-sponsor the Center of Academic Excellence in Information Assurance Education (CAEIAE) program, which recognized academic curriculum and institutional dedication to information security education at two-year, four-year, graduate, and research institution. However, at this particular instance, there exists no recognized academic certification agency or body for HS or even cyber-security programs.

Academia should apply new thinking ways, new understanding, as well as new approaches to the country's response to cyber-attacks (Kessler, 2012). Similar to the way cyber-security is concerned with procedure instead of technology, the reaction to cyber-related security difficulties of today are not only about technical solutions, but must also entail numerous related subjects like national defense, political science, history, diplomacy, and several other social sciences. According to the Homeland Security Act (2002), academia should take an active stand in homeland security education (Kessler, 2012). Thus far, the DHS Science and Technology (S&T) Directorate has been the major point-of-contact amidst DHS and the academic community. Presently, the S&T Directorate supports 12 Centers of Excellence (COE) via its Office of University Programs. These particular centers signify a broad network of universities that enhance basic as well as applied research in science, technology, engineering, and mathematics (STEM) programs. STEM-oriented cyber-security programs are majorly founded in the physical sciences and focus on programming, tool development, and application of security methods, instead of the managerial, evaluation, or policy elements of the applied cyber-security. On the contrary, the majority of the HS programs have a tendency of being broad filed, applied social programs, which develop the critical and analytical assessment abilities of middle managers. The incorporation of cyber-security policy together with management elements in an HS course would particularly handle the academic needs of DHS as well as other homeland security agencies for the future.

REFERENCES

[1] Bobby, M. (2010, November 10). Harvard National Security Journal. *Harvard National Security Journal – DoD-DHS Memorandum of Understanding Aims to Improve Cybersecurity Collaboration*. Retrieved January 27, 2016, from http://harvardnsj.org/2010/11/dod-dhs-memorandum-of-understanding-aims-to-improve-cybersecurity-collaboration/

[2] (2012). *DHS Can Strengthen Its International Cybersecurity Programs*. Retrieved January 27, 2016, from http://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-112_Aug12.pdf

[3] (2015, May 10). Fox News - Breaking News Updates | Latest News Headlines | Photos & News Videos. *'Terrorism has gone viral': US officials, lawmakers warn of growing jihad-inspired attacks* | Fox News. Retrieved January 27, 2016, from http://www.foxnews.com/politics/2015/05/10/mccaul-terrorism-has-gone-viral.html

[4] Harknett, R., & Stever, J. (2015). The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen. *Journal of Homeland Security and Emergency Management*, 6(1).

[5] (2013). Homeland Security. *Privacy Impact Assessment for EINSTEIN 3 - Accelerated (E3A)*. Retrieved January 27, 2016, from http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf

[6] KESSLER, G., & RAMSAY, J. (2012). Paradigms for Cybersecurity Education in a Homeland Security Program. *Journal of Homeland Security Education*, 2. Retrieved January 27, 2016, from http://www.journalhse.org/sft710/kesslerramsayjhsearticlefinal.pdf

[7] Kiran, & Anish. (2015). Secure Hidden Routing in Mobile Ad Hoc Networks. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(4). Retrieved January 27, 2016, from http://ijarcsse.com/docs/papers/Volume_5/4_April2015/V5I4-0510.pdf

[8] (2012). MOHS. *Cyber security Awareness*. Retrieved January 26, 2016, from http://www.homelandsecurity.ms.gov/Pages/cyber.aspx

[9] Northcutt, S. (2015). Cyber Security master's degree | Information Security Master's Degree. *Traffic Analysis*. Retrieved January 26, 2016, from http://www.sans.edu/research/security-laboratory/article/traffic-analysis

[10] (2012). OIG/DHS HomePage. *DHS Needs to Address Portable Device Security Risks*. Retrieved 27, 2016, from http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-88_Jun12.pdf

[11] (2013). Web Design Company - Dubai Website Design and Web Application Development Company. *Cyber Crime Statistics and Trends [Infographic]*. Retrieved February 4, 2016, from http://www.go-gulf.com/blog/cyber-crime/