CYBERSECURITY RESEARCH PAPER

IT 104

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on http://oai.gmu.edu/the-mason-honor-code-2/ and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site."

Heading 1: Introduction

Cybersecurity and Hacking, Cybersecurity is the process whereby all internetworking-capable devices are secured and the act of preventing unauthorized users from accessing the devices, both physically and from the internet. Hacking is the inverse of cybersecurity where an unauthorized user gains access to a unit or system. Cybersecurity as a profession is currently experiencing a massive boom in population, offered programs, and in importance. The National Security Agency has even called for an increase in the amount of Cybersecurity professionals in the industry, citing a shortage of capable professionals and a growing need for them. (Smith, 2012) Hacking has also experienced a similar boom in the number and types of hacking methods have increased dramatically in the past 3 decades. As the internet becomes bigger and bigger, and as more and more types of device become connected to the internet, the importance of Cybersecurity becomes greater exponentially. This paper will discuss the social, ethical, and legal ramifications of the act of Cybersecurity using evidence from real life sources when discussing how cyber security has developed. This paper will also use the hypothetical explorations of science fiction to discuss theoretical convergences of different fields of IT as they relate to cybersecurity in the future.

Heading 2: Background

The history of Hacking and Cybersecurity is an intertwined history with one giving rise to the other. In a sense, Cybersecurity rose as a counter-phenomenon to Hacking. In the 1960's, "the term hacker was accepted as a positive label slapped onto computer gurus who could push computer systems beyond the defined limits." (Spyd3r, 2002) Although, as time went on and the medium of computer science became more and more sophisticated and widespread, the term hacker became known as a negative term on the same order as criminal, or delinquent. "In the 1970s, 'Captain Crunch' devised a way to make free long distance calls and groups of phone hackers, later dubbed 'phreakers' emerged." (Spyd3r, 2002) The Captain Crunch incident is the most well-known of early uses of H/P culture becoming closely tied to negative and even criminal actions. It is also the most well-known of the early uses of exploiting a glitch. "During the 1980s, hacking was not known amongst the masses as it is presently. To be a hacker was to be a part of a very exclusive and secluded group. The infamous hacker groups the "Legion of Doom," based in the USA and the "Chaos Computer Club," based in Germany, were founded and are still two of the most widely recognized and respected hacker groups ever founded." (Spyd3r, 2002) "During the 1990s, Kevin Mitnick is arrested after being tracked down by Tsutomu Shimomura. The trials of Kevin Mitnick were of the most publicized hacker trials in hacker history. As hackers and time progressed, hackers found ways to exploit holes in operating systems of local and remote machines." (Spyd3r, 2002)

During the 1970's and 1980's the internet experienced a population boom as more and more people were using it as a means of conducting business, recordkeeping, and communication. It wasn't until the 1989 and the 1990's with the invention of dedicated internet access lines, i.e. Ethernet, and the .com revolution that the internet's device population entered a stage of unprecedented expansion that continues to this day. The need for security has always been needed since personal or confidential data was uploaded to the internet. With the invention of social media, blogs, YouTube, Skype, Online Banking, E-stores, and other countless web-dependent functions that handle personal data; the need for protection has become quite obvious.

Heading 3: Potential Benefits

The potential benefits from cyber security to are numerous and obvious. The benefits range from peace of mind and to ease of access, to the secure communication of people from across the world. The potential benefits of Cybersecurity also steadily increased as more and more internet capable devices increases. As Cybersecurity make sure that these devices are secure and unable to be used against their owners by unauthorized users.

Heading 4: Legal issues

There has been a lot of discussion of Cybersecurity and Hacking in terms of legality, especially in the last 20 to 25 years. The discussion of legality about Cybersecurity can be narrowed into a single category in regards to what they've been about: The legality of data ownership. On the subject of the first category, the subject of data ownership definitely has its origins in copyright and copyrighted content. The most prominent piece of legislature that relates to both entertainment and cybersecurity is the Digital Millennium Copyright Act of 1998 (DMCA). The DMCA defines the ownership of digital content, whether it's distributed online or

in a physical data storage medium. Numerous political and court rulings involving copyrighted content have been made with the DMCA as a base, including the most recent Viacom vs YouTube, Google case. In this case, Viacom Incorporated accused YouTube and its parent company, Google, of engaging in a massive copyright infringement in the form of YouTube videos being allowed to be uploaded online. They also alleged that the copyright infringements costed about 1.65 billion dollars in damages. (Broache, 2007) The case was eventually settled using the DMCA's "safe harbor" provisions which shields content owners and parent companies from suits regarding content ownership.

There are even more proposed laws in the House and the Senate that involve Cybersecurity. They are as follow: The Cyber Intelligence Sharing and Protection Act of 2012 or CISPA (H.R. 3523), Cybersecurity Act of 2012 (S. 2105), The SECURE IT Act (S. 3342), and The Obama Administration Proposal. CISPA would grant the director of national intelligence the ability to set up channels of information sharing with the Private Sector. CISPA also would prevent any information provided by companies to be shared with any unwanted federal agencies. It would also protect any information shared with the agencies from being used for commercial benefit. (CYBERSECURITY LEGISLATION: THE FINAL FOUR., 2012)

Then there is the Cybersecurity Act of 2012 (S. 2105), which would be another measure for protection of shared data from companies with the federal government. It would also call for the Department of Homeland Security to develop specific standards for exchanging information about cybersecurity threat and vulnerabilities with companies in the private sector.

"The SECURE IT Act, S. 3342, would establish cybersecurity intelligence sharing between the private sector and multiple centers throughout the federal government These centers must follow standards set by the secretaries of Commerce and Homeland Security to protect personal and trade information, and those providing information would be protected from legal reprisal or public disclosure of shared content. Additional control is provided to the private sector, as those sharing information must provide consent before data may be shared with government. Any shared knowledge may only be used for cybersecurity, national security, or law enforcement purposes." (CYBERSECURITY LEGISLATION: THE FINAL FOUR., 2012)

"This plan seeks to strike a compromise between the two competing Senate bills. It assigns DHS the responsibility of carrying out cybersecurity information sharing. Private-sector information used by the government must be related to cyber threats to federal networks or critical infrastructure, personal information must be protected from unauthorized access or disclosure, and those using federal networks must be notified that their traffic may be monitored. Shared information may also be used for law enforcement purposes with the approval of the attorney general. Cooperation with the federal government is protected from public disclosure." (CYBERSECURITY LEGISLATION: THE FINAL FOUR., 2012)

Heading 5: Social Issues

The social issues with cyber security are most commonly associated with people stealing information or accessing data they are not allowed to access. This unauthorized access of personal data is a serious issue in the Cybersecurity industry and it in general. There is also the issue of people stealing credit card numbers and other financial information along with personal information with the intention of committing identity and market fraud under a victim's name and with a victims financials.

Heading 6: Security Concerns

There are a number of currently pressing security concerns that currently exist in the field of Cybersecurity. The most immediate of these concerns is the security problems facing the fields of medical technology, automotive technology, and that of the industrial networks.

The invention of the self-driving car has brought about both a stunning new innovation in the field of automotive engineering and a stunning conundrum in the field of Cybersecurity. The automotive industry has not been very responsive to the need for a strong security system for their cars as Senator Edward Mackey's report title" Tracking & Hacking: Security & Privacy Gaps Put American Driver's at Risk" has pointed out. "The encryption and security measures (response group 1) are not systems that can detect intrusion events. Automobile security experts consulted by Senator Markey's staff have noted that the ECU monitoring (response 2) described simply monitors the normal functioning of an ECU, the firewall/watchdog systems (response 3) would only protect against random outside influences like electromagnetic frequency interference and not malicious intrusions, the seed-key system (response 4) can be defeated by hackers, and the remote keyless entry systems (response 5) will only protect against people getting into the car to steal it but will do nothing to prevent or respond to remote hacking. Also, only 1 of the systems, the seed-key system, is capable of alerting the manufacturer in real-time." (Markey, 2015) However, this negligence is compounded in a relatively recent article in a recent article published by Allyson Versprille in the National Defense Magazine revealed that it's entirely possible that a hacker could penetrate into the control software for a self-driving car and cause it to crash or otherwise take control of the vehicle. This security flaw could prove to be extremely dangerous or even fatal if used by an attacker. They could exploit this access ability to potential kill or kidnap specific targets with their own vehicle.

Infrastructure networks are some of the most vulnerable networks that could have some of the most devastating consequences if hacked by an attacker. Most industrial company networks are airgapped, which means the network has no physical connections to unsecure networks. However, in the case of Industrial Networks, the real threat lies in physical security, in other words, an attacker could just walk into a plant and access the local control software and take control via a self-contained physical package and be able to control and monitor an entire facility from remote. Most industrial networks are relatively unsecured once you get past the airgap. This represents a very serious problem as the physical locations are sometimes entirely unprotected, or their protections are easily bypassed.

With the new innovation of the Stent Electrode or "Stentrode" for short. This brand new technology has the greatest potential for disabled patients who wish to regain functionality of their limbs in the form of artificial and articulate prostheses that respond to commands from the brain, as if they were their own organic limbs. (Oxley, et al., 2016) This technology has the potential to further the field of robotic prostheses greatly; while also providing a very serious and concerning potential threat to the personal security of those who use it. It's entirely feasible that someone could hack these devices, both the stentrodes and the prostheses themselves, and potentially use them to bring harm or to blackmail a user of these technologies. Alexandra Ossola of Popular Science wrote about a similar example of hacking of pacemaker and the use of ransomware to force people to give a ransom to a hacker in exchange for not shutting down their medical implant. (Ossola, 2015)

Heading 7: Further required research

There's a lot of research to be done in a few fields of Cybersecurity, such as strengthening encryption methods and developing protective measures for burgeoning, new technologies such as the brand new Quantum Computing field. Given the state of the field at present, however, it is highly unlikely that cybersecurity will reach this field in the foreseeable future, given that complex creations have yet to be engineered on the principles of Quantum Computing.

Heading 8: Conclusion

Overall, there is much to be had in the field of cybersecurity and much exists already in the field. The field itself presents solutions to a number of possible security issues with information technology. It also presents a number of problems in the field, most notably in emerging technologies such as self-driving cars and areas of industry that are very high risk and to intrusion and vulnerable to cyber-attacks.

References

Broache, A. (2007, March 17). *Viacom sues Google over YouTube clips*. Retrieved from CNET: http://www.cnet.com/news/viacom-sues-google-over-youtube-clips/

>This citation is a website article documenting the developments in the Viacom v. Google lawsuit. The article includes highly-detailed information about the lawsuit. In addition to the details on the case, the article contains some useful commentary on said case. The source appears to be quite authoritative and is very relevant. I'm using this source as an example of copyright law and as an example of legal concerns for cyber-security.

CYBERSECURITY LEGISLATION: THE FINAL FOUR. (2012). *National Defense, 97*(705), p. 35. Retrieved from http://search.proquest.com/docview/1033362123?accountid=14541

>This citation is from the National Defense publication by an anonymous author. This publication is the main news distributor for the federal services. The authority of this publication would entirely depend on how trusting you are of government publications. However, given the correctness of this publication, it provides an invaluable insight into current legislation being proposed in the house and the senate. It also provides an insight into the attitude of the current administration toward cybersecurity.

Markey, E. (2015). *Tracking & Hacking: Security & Privacy Gaps Put American Driver at Risk.* Massachusetts.

>This citation is a report published by the staff of Senator Edward Markey (D-Mass) published very recently in 2015. It provides in insight into how the concept of cybersecurity is being handled (or rather mishandled) by the automotive industry. It talks about the integration computers and wireless functionalities into cars with emphasis on the need for security. The authority of this publication would entirely depend on how trusting you are of government publications or how much validity senator Markey's office and staff have. I'm using this document as a source for how current innovation trends are heading and how the need for cybersecurity is indicated for these fields.

Ossola, A. (2015, November 23). *HACKED MEDICAL DEVICES MAY BE THE BIGGEST CYBER SECURITY THREAT IN 2016*. Retrieved from Popular Science: http://www.popsci.com/hackers-could-soon-hold-your-life-ransom-by-hijacking-your-medical-devices

>This citation is an article posted online in Popular Science briefly highlighting grave security concern that was likely to rise in the then future of 2016. The article was published on November 23rd, 2015 by Alexandra Ossola. The article speculates that online-enabled medical implants such as pacemakers and insulin pumps may become targets for cyber-attacks. Specifically, in the act of installing ransomware within these medical implants. I use this article as a means for speculating the future need for security of medical devices.

Oxley, T. J., Opie, N. L., John, S. E., Rind, G. S., Ronayne, S. M., & al., e. (2016, March). Minimally invasive endovascular stent-electrode array for high-fidelity, chronic recordings of cortical neural activity. *Nature Biotechnology, 3*(34), pp. 320-327. doi:http://dx.doi.org/10.1038/nbt.3428

>This citation is a research article on that was published by a highly skilled team of researchers and technicians in the journal Nature Biotechnology in March 2016. This article discusses the brand new piece of neural interfacing device called a Stent-electrode, or Stentrode for short. This minimally invasive device represents an incredibly leap forward in neural monitoring technology. I use this article as a launching point for speculation on the future of biotechnology and robot prosthesis. It's a highly authoritative direct source in a well-respected scientific journal.

Smith, D. E. (2012). NSA: Looking for a few good cybersecurity pros. *Network World, 29*(20), 10-11. Retrieved from http://search.proquest.com/docview/1265769742?accountid=14541

>This citation is an interview of Lieutenants Matthew Greene and Maxwell Love about their experiences with the NSA and how it relates to cybersecurity. The interview consisted of questions relating to their view of cybersecurity philosophies and concepts. This citation provides insight for in how government agencies acknowledge the need for cybersecurity professionals. In terms of authority, this citation seems authoritative as both of these men served as interns for the NSA during the interview. The authority of this publication would entirely depend on how trusting you are of government publications.

Spyd3r. (2002, April 8). *The History of Hacking*. Retrieved from Help Net Security: https://www.helpnetsecurity.com/2002/04/08/the-history-of-hacking/

> This citation is a web article posted on a custom website by internet user, Spyd3r. This citation provides an invaluable insight into the early terminology and practices of the internet while it was still in the process of forming. While it was written some time ago, back in 2002, I still consider it to be an authoritative historical accounting of the early years of the internet. I use this source to provide background information on the history of cybersecurity and its origins. This source also provides much of the vocabulary used in the background section.

Versprille, A. (2015, May). *Researchers Hack Into Driverless Car System, Take Control of Vehicle*. Retrieved from National Defense Magazine: http://www.nationaldefensemagazine.org/archive/2015/May/Pages/ResearchersHackIntoDriverlessCarSystemTakeControlofVehicle.aspx

> This citation was retrieved from the online publication of the national defense magazine. It provides an insight into the how cybersecurity is being handled in developing fields of the automation, such as self-driving cars. The phenomenon of self-driving cars is a phenomenon that hasn't exactly been unforeseen in the realm of science fiction. However, it's an emerging technology in our reality. This source provides a launching point fro a possible direction of focus that cybersecurity will take in the future.