ASEE's 123rd Annual • Conference & Exposition • New Orleans, LA • June 26-29, 2016

New Orleans JAZZED about Engineering Education

Paper ID #17379

Helping the Human Element: Educating in Social Engineering

Samuel Moses, Brigham Young University

Samuel Moses is a Security Analyst at Brigham Young University Office of Information Technology. He earned his Bachelors in Information Technology August 2015, emphasizing in the fields of System Administration and Cyber Security. Currently Samuel Moses is working on his Masters in Technology emphasis in Cyber Security.

Mr. Nathaniel Scott Baker

Nate is a recent addition to the BYU Cyber Security Research Lab. After graduating from high school at the age of 16, he attended junior college at Sierra college for a year before transferring to BYU. Nate has taken a wide variety of courses, ranging from chemistry to business to computer engineering, and plans on graduating with a degree in Information Technology in 2016. He has recently discovered an interest in cyber security, and started working as a research assistant in the CSRL in order to begin developing his skills. In his free time, Nate enjoys playing guitar, snowboarding, and theater.

Dr. Dale C. Rowe, Brigham Young University

Dr. Rowe has worked for nearly two decades in security and network architecture with a variety of industries in international companies. He has provided secure enterprise architecture on both military and commercial satellite communications systems. He has also advised and trained both national and international governments on cyber-security. Since joining Brigham Young University in 2010, he has designed a variety of courses on Information Assurance, Cyber Security, Penetration Testing, Cyber Forensics and Systems Administration and published over a dozen papers in cyber-security.

Helping the Human Element: Educating in Social Engineering

Abstract

Cybersecurity professionals seek to stop hackers and other malicious parties from gaining access to their systems by shoring up all possible gaps in their technology, but often overlook the weakest point in their system: the human element. Because people are often one of the first things a malicious party will attempt to manipulate during an intrusion, Social Engineering must be protected against alongside other forms of exploitation, in order to best protect information. However, much of the industry information regarding Social Engineering are anecdotal, making it difficult to teach industry professionals proper defense mechanisms and policies. If the cybersecurity industry is going to protect against Social Engineering attacks, proper in-depth education on the subject needs to be available to those within the field.

In this paper, the writers explore and discuss the field of cybersecurity known as social engineering. After a review of the field as it currently stands, the writers will outline a graduate-level curriculum for social engineering education, which can be used to teach aspiring offensive cybersecurity analysts the best methods to test the security of an organization's human element, as well as teach aspiring security professionals about best practices and policies that they can use to protect the resources they are responsible for.

Introduction

Modern cybersecurity is seeing a spike in attention. Recent vulnerabilities and exploits have prompted industry professionals to spend a greater amount on cybersecurity measures, from powerful and comprehensive authentication systems to the most thorough and comprehensive firewall and anti-virus systems. However, there is a simple fact that cannot be negated by any amount of money or technological security measures: people seek to please one another, help those that help them, and quickly appease those who approach them in order to maintain their personal space. Where hackers have found themselves stymied upon being faced with an overly aggressive firewall or unbreakable authentication system, an exploitation of the human element has been key in obtaining the desired information or resource.

The path of human history is covered in examples of Social Engineering; from the Trojan horse to the first Ponzi scheme, people have been manipulating the trust of others to achieve their goals since the beginning of time. However, it is with the rise of computing and its integration into businesses that Social Engineering has become a key concern for a significantly large portion of the population. Recent Social Engineers such as Kevin Mitnick and the Badir Brothers have shown the world what determined people with the right social skills can accomplish, and now more than ever companies need to train their employees to handle situations where someone is attempting to exploit them[1]. With the advent of the digital age, malicious parties have also taken to the Internet, using fraudulent measures such as phishing to gain access to victim accounts, and these attacks have only gotten more sophisticated as the years have gone by[2]. In 2016, a company that fails to train its employees to recognize Social Engineering attacks is failing to properly secure itself.

In many modern attacks, the key reason Social Engineering prevails is simply due to lack of education. One of the greatest hacks of 2015 against the director of the CIA started as a simple Social Engineering attack against a Verizon employee[3]. While many academic institutions are making a push for great cybersecurity education, those same institutions focus strongly on technological cybersecurity education[4], and proper attention is rarely given to policy creation and implementation. In order to meet the cybersecurity needs of the coming years, an institution will need to teach the interpersonal alongside the technical if they seek to provide a comprehensive cybersecurity education.

As a solution to this need, the authors propose a graduate-level course in Social Engineering. The course will have a lecture-based component focusing on the different psychological aspects of Social Engineering, as well as a lab-based component where students learn what common implemented Social Engineering exploits look like in practice. Through assignments, students will also learn how to write effective policy that can be implemented in an organization to help employees recognize and protect against Social Engineering attacks. What follows is the author's definition of the practice of Social Engineering, a review of potential texts that the authors will reference and could serve as reference for students, and what the authors believe would be the best course of study in the topic of Social Engineering.

What is Social Engineering?

While Social Engineering has existed for many years, the world has yet to settle on a concrete, concise definition for what it is. Several authors have produced papers on Social Engineering for The SANS Institute, and each have defined Social Engineering in a way that best suits their arguments; Aaron Dolan states "Social Engineering is essentially using human relationships to attain a goal,"[5] while Radha Gulati further elaborates that "Social Engineering is the 'art' of utilizing human behavior to breach security without the participant (or victim) even realizing that they have been manipulated."[6] A military Joint Task Force publication, The Wire, defines Social Engineering as "art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques."[7] Malcom Allen, another SANS writer, pulls definitions from a variety of sources for their paper, ranging from Wikipedia to an actual Guide for Social Engineering[8]. The U.S. Department of Homeland Security, offering tips for protection from Social Engineering, defines it as "a tactic which involves approaching an individual, either online or in person, and manipulating them into providing personal information that can be used to break into a computer network or assume someone's identity."[9]

For the purpose of creating a graduate-level course, the authors have crafted their own definition of the discipline: Social Engineering is the use of persuasive techniques that target human nature to convince people to conform to one's own desires. The authors' definition focuses on the more theoretical and scholastic nature of the Social Engineering discipline. It also highlights the purely social nature of the discipline; any technological interaction beyond a Social Engineering attempt begins to fall under hacking categories. The course that will be outlined must thoroughly educate students regarding the many methods used to perform Social Engineering, as well as how to create policies that can undermine such attacks.

Book Review

Planning readings for the field of Social Engineering requires a proper balance between several aspects. A proper Social Engineering text must be anecdotal in nature, since so many exploits occur on a specific basis and students need to see what the discipline is like in action. However, if a text focuses too heavily on anecdotes, without explaining the psychology behind the exploit, then a student cannot learn how to repeat that success in a slightly different scenario. The authors obtained the following books on the field of cybersecurity and Social Engineering; the coming sections will discuss the merits and faults of each selected text for the purpose of teaching a course on the subject.

The Art of Intrusion

The first book examines for use in this course was *The Art of Intrusion* by Kevin Mitnick. The book was an interesting and insightful read, but was more of a story book rather than informative and instructing. *Intrusion* emphasized layman stories and case studies rather than the technical instruction that would be best for a formal course. However, *Intrusion* would be helpful for someone as preparatory reading for the class; reading the different stories can help students develop more of the attacking mindset and learn from what past hackers have done, and generate excitement regarding the topic of study. The book was well written and can help develop precursory knowledge for the class, but did not have the contents needed in a textbook for graduate-level education.

The Art of Deception

Intrusion was followed by *The Art of Deception*, also by Kevin Mitnick. Unlike *Intrusion*, *Deception* focuses solely on Social Engineering, making it a much better candidate for the course textbook. Each chapter details a different type of Social Engineering exploit, explored thoroughly in a lengthy anecdote. Following each story, the author performs a small analysis of the story, and ends each chapter by making some minor notes about preventing that type of exploit. While *Deception* outperforms Intrusion in terms of focus on the topic of Social Engineering, the book still reads as overly conversational in nature, and its heavy-handed focus on stories again makes it difficult for students to replicate that same success in their own Social Engineering. While *Deception* will be very useful in helping students begin to understand policy and prevention, it cannot serve as a stand-alone textbook for this course.

Social Engineering: The Art of Human Hacking

The final book that was considered for the course's main text was *Social Engineering: The Art of Human Hacking*, by Christopher Hadnagy. The book follows a similar approach to *Intrusion* and *Deception*, but instead of focusing primarily on stories, *Human Hacking* moves quickly through its anecdotes before moving quickly on to the psychology behind the exploits discussed. The text presents a psychological principle, and for each topic it discusses, goes over specific skills a security professional can hone in order to master that subset of Social Engineering. The book also details a set of software and other tools that can aid the interpersonal element of Social Engineering, creating a perfect merging of the psychological and the technical.

The above attributes indicate that *Social Engineering: The Art of Human Hacking* is the best option as a textbook for a graduate course in Social Engineering. Using the psychological foundations of each section, a course can be created, and students can gain an appreciation for successful stories while still learning the interpersonal techniques in play. The curriculum that follows is based greatly off of Hadnagy's work, and students will need to read through the entire text as a part of their course requirements.

Curriculum

This course is to be taught in a traditional classroom lecture setting, with additional lab time to help reinforce the lessons taught in the classroom. Before class starts the students are required to complete reading material or other prerequisite studying to help facilitate interaction and discussion in the classroom.

Student Screening

As a graduate level course, students of Social Engineering will need to be working towards a Master's or Doctorate degree in a technology-related field, or be an approved undergraduate senior with plans to complete graduate-level education in a technology-related field. Additionally, due to the morally volatile topics the course will cover, each student will need to have prior approval by a faculty member to take this course. As criteria for approval, faculty should consider their prior interactions with the student, as well as the student's trustworthiness as proven in other academic cybersecurity involvement. For students that are relatively unknown to the faculty, a one-on-one interview with the student may be appropriate. All students wishing to take this course must also submit an Ethics Agreement to reinforce the ethics expected of a cybersecurity professional. An example of a cybersecurity course Ethics Agreement can be found in Appendix A.

Learning Outcomes

The Social Engineering course learning outcomes include the following:

1. Explain the various techniques that can be used to complete Social Engineering exploits.

2. Develop an understanding of the psychology of human interaction and how it can be exploited for gain.
3. Learn what technical controls, trainings, and processes can be used to help defend and establish security in-depth to protect against Social Engineering.
4. Overcome uncomfortable feelings such as trepidation when interacting under the pretext of lying or taking on a role.
5. Help establish a desire for lifelong learning and how it is essential to continually improve and learn as a cybersecurity professional.

Lecture Topics

The classroom's curriculum was designed around the textbook chosen for the class, *Social Engineering: The Art of Human Hacking*. Other topics in the class have been included after reviewing more Social Engineering books and consulting with cybersecurity professionals to learn what skills are valuable.

1. Intro
    a. What is Social Engineering?
    b. Overview of the Course
    c. Sign Ethics Agreement
2. Influence
    a. The Five Fundamentals of Influence and Persuasion
    b. Discuss ethical implication of Social Engineering
3. Develop Your Tools
    a. What tools can be used in Social Engineering?
    b. How to be resourceful?
    c. Baiting
4. Open Source Intelligence (OSINT)
    a. Gathering information
    b. Sources of available information
5. Becoming Another Person
    a. What is pretexting?
    b. Researching your target
    c. Plan and prepare
6. Know Your Enemy
    a. System Scanning and Surveillance (Antivirus, OS version, etc)
    b. Phone calls, surveys, phishing, scrapers
    c. Practice Makes Perfect
7. Mind Tricks
    a. Basic Building Blocks of Social Engineering
    b. Microexpressions, and how to use them
8. Elicitation
    a. Subtly extract information during normal and "innocent" conversations

    b. Using Intelligent Questions

9. Non-Tech Hacking
    a. Shoulder surfing
    b. Dumpster diving
    c. Moving past reliance on technology
10. The Lying Lockpicker
    a. Methods of lockpicking
    b. Types of locks
    c. The psychology of lying
    d. Reacting to Body Language
11. Getting Past Physical Systems
    a. Be aware of your surroundings
    b. Know ways to get past physical security
12. Reverse Social Engineering
    a. Use pretexting to establish a link and connection with targets
    b. Exploit vulnerabilities as you become relied upon

Assignments

As part of the work for this class, students will complete two assignments. This will promote critical thinking and help students develop a deeper understanding of Social Engineering.

1. Ethical Paper
    a. Develop your own personal code of ethics specifically related to Social Engineering situations. Think about different sources you could pull inspiration from: great leaders, church, clubs or organizations like Boy Scouts or Girl Scouts, and develop your own code or guideline.
2. Paper - Research a Social Engineering Topic of Your Choice
    a. Produce a research paper on a Social Engineering topic of interest to gain more knowledge and experience in a Social Engineering domain. Include real life examples or case studies.

Projects

As part of the class students will complete a project and have the option to complete a second project to replace one lab.

1. Dropbox
    a. Students will create a discrete host that can be used as a work-around when a firewall has interrupted a security assessment. Students will learn about reverse SSH tunneling and other methods of circumnavigating a firewall, as well as what policies might fend off an attempt to place a dropbox within their own organization.

2. Build Your Own Lab
    a. This is a chance for students to develop their skills in an area of their choice by designing a lab which they think would be of value to their own studies and the course. Student are allowed to work in teams of 2 or 3. Approval for the lab needed from the professor beforehand.

Technical Labs

A series of labs has been created for the practical application of the instruction in the classroom, allowing the students to gain real world experience. Some of the labs guide the students, allowing them to gain an understanding of the principles, while the rest of the labs are more open-ended, giving the students guidance while providing them with the opportunity to find their own answers and be resourceful and creative. Each of these labs has two parts. The first part is completing a Social Engineering exploit, the second is report writing. In order to perfect this skill, students will write up the attack they accomplished and will complete a one page policy that would serve to counteract the exploits they've learned within a work environment. A good cybersecurity professional doesn't just break something and say how. A good cybersecurity professional helps a client understand the problem and how to best resolve it.

The following labs are designed to be used in the course:

1. Build Your Kali VM
    a. Each student prepares a Kali VM to use throughout the semester for labs.
2. Footprint Your Target
    a. Students will be randomly assigned another student in class. They are to investigate and build a profile on the person. This allows students real experience on trying to find open source information while the target learns what information about them can be found online.
3. Chameleon
    a. Pick a famous person. Learn as much as you can find out about the person, and impersonate them for the class. The target must be approved by the instructor.
4. Developing Your Tools
    a. Develop a Windows Scraper tool: A tool that will run without administrator access and can pull the OS version and as much host information as possible.
    b. Create a macro-enabled malicious Word document that opens a Meterpreter session on the attacker's machine.
    c. Create a script on a flash drive that can run Mimikatz in under a minute.
5. Plan Your Approach
    a. Design 10 exploits you could use realistically to manipulate people and obtain information (at least 1 exploit from each type of influence taught in item 3 of section 4.2).
6. Complete Your Approach

a. Perform 3 of the 10 exploits you designed from lab 5. Document how the interaction went, and what information you were able to find.

7. No Tech Scavenger Hunt
    a. In teams of two, complete 4 of the following tasks, and present your favorite one.
        i. Photograph an unlocked, unattended terminal.
        ii. Shoulder surf and get a legible photo of a screen in use.
        iii. Go dumpster diving to obtain a photo of sensitive and/or potentially valuable information.
        iv. Get a photo of an ID badge that is good enough to make a duplicate.
        v. Take a picture of sensitive or potentially valuable information left in someone’s car.
8. Become a Lock-picker
    a. Use lock picks to unlock a set of locks up to level 4. Prove it by doing it in front of the Instructor or the Teacher’s Assistant.
9. Case the Joint
    a. Photo document the security cameras in the building and establish a route through the building that could be completed without being recorded.
10. Make the Target Come to You
    a. Create a phishing email with a link to a mock website. Design it for use in Reverse Social Engineering to establish trust and create a new point of contact.

Future Work

Cybersecurity is an ever-changing discipline. With every advancement in technology and every new vulnerability discovered, the dynamic of cybersecurity changes. Due to this, the training and instruction of cybersecurity professionals needs to evolve with these changes. Courses constantly need to be updated and improved upon to keep up with the advancements in technology and cybersecurity. Beyond the pure maintenance of keeping the course up to date, there is other work that can be completed.

Gathering Results

Feedback from the students is important. Classes have student ratings surveys that help rate the overall learning experience of a course. In the design of a new course, regular feedback from students becomes essential. Once a week, a survey will be sent to the students for feedback on the lectures, labs, and assignments. This will help us be able to evaluate which labs the students enjoyed the most, and which one they found the most helpful with their learning. Some of the questions will be on a scale range of 1 to 5 to give objective indicators of the students’ experience. To enable a better experience during re-teachings of the course, some questions will be open-ended to allow more subjective feedback to be weighed and considered for further improvements. The data will be collected, analyzed, and allow the authors to report back on the most successful parts of the class, as well as where further improvement and course development are necessary.

Inter-Scholastic Collaboration

The new challenges facing the world of cybersecurity are diverse and require many different frames of mind to overcome. Collaboration and curriculum-sharing between universities is key in order to meet the demands of the industry; the NSA places significance on this collaboration for all its Centers of Academic Excellence. While the authors have geared this course of study towards students working on their graduate degrees, the framework presented above could be easily used to create a scaled-down course for undergraduate or even high school students.

Social Engineering Forensics

With a basic understanding of Social Engineering and some experience writing policy against it, students should become very aware of how likely it is that someone they know will fall victim to a Social Engineering attack. There are some in the industry who even think that it would be impossible for a person to go through life without falling victim to at least one attack of this nature (http://www.refinery29.com/2016/01/101964/amazon-social-engineering-security). With this in mind, it would be prudent for students to develop forensic skills related to Social Engineering as well as their offensive security knowledge. Using a similar course development method as the one outlined in this paper, the authors plan to create a course in forensics and recovery from Social Engineering related attacks; this course would act as a bridge for recovery from both technical and social manipulation.

Conclusion

The need for well-trained cybersecurity professionals is apparent. Industry needs well-rounded professionals who can handle the technical and policy needs to defend against the increasingly varied cybersecurity attacks. The graduate-level course described in this paper will better prepare students to test and defend against Social Engineering attacks by combining a lecture-based component, to teach the different psychological aspects of Social Engineering, and a lab-based component, to give the students practice performing the exploits. The lab reports and assignments have been designed to prepare the students for realistic report writing that would be necessary in industry. This course fulfills the present need to improve the training and preparation of cybersecurity professionals in the field of cybersecurity.

Appendix A: Cybersecurity Student Code of Ethics

LEGAL, POLICY AND REGULATORY

1. I will not knowingly engage in, or be party to unethical or unlawful acts of any type.
2. I will respect all scholastic regulations and local laws and customs, including but not limited to the departmental and organizational computer and network use policies, state and federal laws and international conventions. I understand it is my responsibility to become aware of these and that ignorance is not an acceptable excuse.

3. I understand the application of the industry ethics codes in the context of cyber-security and will uphold those ethical principles.
4. I agree that if I participate in, or perform any illegal acts, I take sole responsibility for the consequences. I will not hold any other party responsible for my actions including faculty, teaching assistants, or other agents of my academic institution.
5. I understand that if I violate this code of ethics, legal action may be taken against me in addition to disciplinary action from my academic institution, and/or expulsion from the security course and/or IT major.

VULNERABILITY DISCOVERY

1. On discovering a vulnerability that does not fall into the scope of a designed classroom laboratory, I shall immediately, without delay and for no financial charge (unless a pre-existing agreement permits a charge) report said vulnerability to the system owner via the appropriate channels. I will not, without explicit written permission attempt to gain access to the system.
2. In the case that a suspected vulnerability is inadvertently discovered on a host for which I do not have permission to examine, I will immediately cease all activity and connections to this system and notify the faculty advisor immediately. Inasmuch as this code has not been broken or abused, and without accepting liability for any actions or their associated impacts and/or losses, the faculty advisor will attempt to mediate a mutually beneficial outcome for all involved parties.

PROFESSIONALISM AND INTEGRITY

1. I will conduct myself professionally.
2. I will act with discretion in disclosing information.
3. I will exercise prudence in sharing knowledge that may be used for malicious purposes.
4. I will not copy, share or make publically available in any form course materials and will respect all intellectual property.
5. I will not practice or employ any offensive skill, including but not limited to penetration testing, malware analysis and scanning on any system unless:
   a. I exclusively and wholly own said system and associated networks or
   b. I am engaging in an IT lab for which the activity is prescribed or
   c. I have written permission from someone in authority to grant such permission.
6. I agree to not exaggerate or lie about my technical knowledge, and that I will not mislead potential employers about my skill with these security technologies or techniques.

USE OF LABS

1. I will use labs responsibly and for the appropriate purpose.
2. I will abide by all posted lab rules at all times and agree that I am required to report any damage immediately to the Lab Manager or Instructor.
3. I will not share the lab passcode.

SUMMARY

In signing this code of conduct, I acknowledge that I have had it explained to me and all questions have been answered. I am confident that I completely understand all parts of this document and sign it of my own volition having been offered the opportunity to withdraw from the course rather than accept this code of ethics.

1. Diana, Alison. "Social Engineering Targets Weakest Security Link: Employees." EnterpriseTech. 19 May 2015. Web. 30 Jan. 2016. <http://www.enterprisetech.com/2015/05/19/social-engineering-targets-weakest-security-link-employees/>.
2. Pierrotti, Andy. "Sophisticated Phishing Attacks on the Rise, Experts Say." KVUE. 11 May 2015. Web. 30 Jan. 2016. <http://www.kvue.com/story/news/investigations/defenders/2015/05/11/sophisticated-phishing-attacks-on-the-rise-experts-say/27125919/>.
3. Leetaru, Kalev. "When Social Engineering Hacked The Director Of National Intelligence." Forbes. Forbes Magazine, 15 Jan. 2016. Web. 30 Jan. 2016. <http://www.forbes.com/sites/kalevleetaru/2016/01/15/when-social-engineering-hacked-the-director-of-national-intelligence/#2715e4857a0b3e494f7d617e>.
4. Walsh College. "Cybersecurity: Taking Charge of the Future." Detroit News. 11 Jan. 2016. Web. 30 Jan. 2016. <http://www.detroitnews.com/story/sponsor-story/walsh-college/2016/01/11/information-technology-computer-science-new-technology/78314178/>.
5. Dolan, Aaron. “Social Engineering.” The SANS Institute. 10 Feb. 2004. Web. 30 Jan. 2016. <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-1365>.
6. Gulati, Radha. “The Threat of Social Engineering and Your Defense Against It.” The SANS Institute. 2003. Web. 30 Jan. 2016. <https://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232>.
7. "OpSec Alert: What is social engineering?" The Wire: An award-winning JTF journal 12.42 (7 Oct. 2011): 3. Web. 30 Jan. 2016. <http://www.jtfgtmo.southcom.mil/wire/wire/WirePDF/v12/wire-vol12-issue42-06oct.pdf>.
8. Allen, Malcolm. “Social Engineering: A Means to Violate a Computer System.” The SANS Institute. June 2006. Web. 30 Jan. 2016. <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529>.
9. Stop. Think. Connect. "Homeland Security." Protect Yourself Against Social Engineering Attacks. 12 July 2011. Web. 30 Jan. 2016. <http://www.dhs.gov/blog/2011/07/12/protect-yourself-against-social-engineering-attacks>.