User Centric Machine Learning Frame Work For Cyber Security Operations Center

SHAIK SHARUK[1], VADDI SRIVALLIDEVI[2]

[1]MCA Student, B V Raju College, Kovvada, Andhra Pradesh, India.

[2]Assistant Professor, B V Raju College, Kovvada, Andhra Pradesh, India.

ABSTRACT:

As the digital era matures, cyber security evolves and software vulnerabilities diminish, people however, as individuals, are more exposed today than ever before. Presently, one of the most practiced and effective penetration attacks are social rather than technical, so efficient in fact, that these exploits play a crucial role to support the greatest majority of cyber assaults. Social Engineering is the art of exploiting the human flaws to achieve a malicious objective. In the context of information security, practitioners breach defences to access sensitive data preying particularly upon the human tendency towards trust. Cyber criminals induce their victims to break security protocol forfeiting confidential information propitious for a more targeted attack. Disastrously, in many cases, targets are manipulated to involuntarily infect and sabotage the system themselves. This paper examines recurrent social engineering techniques used by attackers, as well as revealing a basic complementary technical methodology to conduct effective exploits.

Keywords: Social Engineering, security, efficiency.

1. INTRODUCTION:

Social engineering in the information security perspective refers to a collection of fraudulent activities on the network with the aim of getting confidential information from people. The attacker psychologically manipulate users' intelligence as a trick of getting sensitive data. The kind of data sought by attackers using this trick varies, the common sensitive data targeted are bank details, security credentials, password and secret PIN. Nowadays, attackers realised that social engineering attacker is easier than other technological ways of hacking the security systems. In other word, it is easier to fool people to give their security credentials than technically hacking for them. In a nutshell,

the weakest security breach channel in the security systems is human error. Consequently, social engineering attack is a serious problem to the information security professionals because no matter how secured a system is, this renders its vulnerable to attacks. Social engineering attack undermines the technical expertise of professionals in protecting software systems by getting unauthorized access to protected data. The success achieved by information security researchers in defending applications and software systems is defeated by social engineering attacks.

DEFINING SOCIAL ENGINEERING

Engebretson defines social engineering as one of the simplest methods to gather information about a target through the process of exploiting human weakness that is inherit to every organization. In essence, social engineering refers to the design and application of deceitful techniques to deliberately manipulate human targets. In a cyber security context, it is primarily used to induce victims towards disclosing confidential data, or to perform actions that breach security protocols, unknowingly infecting systems or releasing classified information. The basis of a social engineering attack is to avoid cyber security systems through deceit, exploiting the weakest link, the people involved. Throughout the interaction, victims are unaware of the destructive nature of their actions. The social engineer exploits innocent instincts, not criminal. Explicit methods such as threats or bribery do not fall within the scope of social engineering. A talented practitioner of this discipline understands and perceives social interaction patterns to manipulate the psychological aspects of the human mind. With this resolution, the attacker is capable of executing an efficient and cheap security compromise, without the need to invest in breaking technical security measures. Nevertheless, an educated social engineer on computer science may also complement technological means to the attack in order to accomplish the malicious intentions.

2. LITERATURE SURVEY

A survey conducted by [1] discovered that social engineering attacks rendered e-government systems vulnerable to numerous security violations. E-government is the use of information and communication technology (ICT) for delivery of public

services to citizens, businesses and collaboration with other government organs. E-government facilitates transparent involvement of citizens in governance. However, despite the numerous benefits of e-government adoption, security challenges such as security threats to the e-government network, issues of identification violations, the trade-off between security and usability, and access control to sensitive information are some of the barriers to its implementations. A study by [2] identified infrastructure, human and government factors as the key success factors that increases the chances of failure in e-government systems. According to the author, the adoption of e-government is more successful in the developed countries than the developing countries. Consequently, further research toward enhancing the success of e-government projects in developing countries is desired. The study focused on investigating the human factor in the e-government projects. Exploitation of software system by technical attacks has declined due to the success in the security mechanisms developed and used in modern software applications. It is difficult for attackers to identify vulnerable points in the systems. Consequently, hackers these days exploits people's trust and psychology for their malicious activities instead of the technical vulnerabilities of the systems. The most common attack to information security nowadays is social engineering attacks ([3, 4]). According to [3], social engineering attacks deserves the same attention with its technological counterparts. [4] identified E-mails, social media networks, advertisements and mobile phones as the most common medium of social engineering attacks. The use of deception for malicious activities is not new. However, the popularity of the internet and World Wide Web for public service provision has increase the spread and success of online social engineering attacks. [5] defined online social engineering attacks as the use of internet facilities such as World Wide Web applications as a means of manipulating users' behaviour to exploit the systems resources. The evolution of internet based communications simplifies information sharing using many social networks such as Emails, Facebook, Twitter, WhatsApp, and Web Services. This platforms enables decentralized, timely, cheap and easy interaction among people. However, it makes it easy for social engineering attackers get

confidential or unauthorized information from unsuspecting people, which renders the system vulnerable to cyberattacks. Therefore, it is high time governments and organizations invest on ways of detecting as well as preventing social engineering attacks. An effort to conceptually analyse empirical studies conducted on SEAs, [6] proposed theoretical framework for SEA research to social engineering research by evaluating features of SEA-based on extant theories in the cognitive science. While [7] investigated phishing detection among participant in autism and discovered that social disorder may not necessarily influence SEAs. Similarly, [8] studied cases of cryptocurrency violations in the community by evaluation of ontological cases of SEA to enhance the security awareness among Blockchain users. Relating human factors to specific aspect of SEAs risks and threats, [9] proposed solution to address SEA in cloud environment.

CLASSIFICATION OF CYBERCRIME BASED ON THE TARGET:

DATA CRIME:

Data interception:

To collect information, an intruder tracks data streams from or to the target. This assault can be carried out to gather evidence in favour of a latter attack or the details gathered may be the ultimate purpose of the attack. This assault normally includes sniffing the traffic of the network but can also require the detection of other data stream forms, for example radio. The attacker is passive and merely controls normal contact with most variations of this attack. In other variants, though the attacker may try to trigger a data stream or alter the essence of the transmitted data. In all versions of this attack, though the intruder is not the expected beneficiary of the results, separating it from other methods of data collection. The intruder monitors clear data sources (e.g. network traffic) as compared as certain other attacks on data leakage and read the information. This is distinct from attacks that produce more quality knowledge, including the frequency of traffic, which is not directly conveyed through the data source.

Data modification:

Communication secrecy is necessary if data cannot be changed or accessed in transit. The distributed environments cause a malicious

third member to perpetrate a machine crim by modifying data when travelling between sites. An unauthorised individual on the network intercepts data in transit during a data manipulation assault and alters part of the data before transmitting it. An example is a change from $100 to $10,000 in dollars for a financial transaction. A whole sequence of valid details is interjected into the network repeatedly in a replay assault. For eg, a legitimate $100 bank transfer transaction should be replicated, one thousand times (CAPEC, 2010).

Data theft

Word used to define how material is copied unlawfully or obtained from an organisation or another individual. Users' records, such as codes, social security numbers, payment card information, personal information, or other private business information, is widely used. As this information is accessed illegly, it would certainly be punished to the utmost degree if the person who stole this information is apprehended.

NETWORK CRIME

Network interferences and sabotage

Network impairment by input, transmission, harm, erase, deteriorate, change or suppress a computer network data network. Network interruption by Network sabotage or inept administrators that attempt to do network roles naturally. It could be just that or a mix of things. Although if Verizon utilises assist children to block the first line of respondents, they may use network concerns as an apology to get the federal government to participate in the public interest.

If these workers are obviously pressured by the Federal Government to come to work as unions and protest anyway (DSL Notes 2011).

ACCESS CRIME

Unauthorized access

Unlicensed entry is an insider's perception of the hidden machine cracker. The shooting was carried out in the United States, the Netherlands and Germany. 'Unauthorized entry' sees the characters beyond electronic displays and tries to distinguish the mainstream hysteria from the truth of the 'outlaw intruder' (Virus Glossary 2006).

Virus dissemination

Malicious programming that interacts with other programming such as malware, bugs, a trojan horse, time bomb, logic bomb, rabbits and bacteria is an example of malicious software that destructs the victim's machine (Virus Glossary 2006).

3. METHODOLOGY

Besides the usage of antivirus, firewall and portal programmes, solid passwords, stable Wi-Fi, training for internet users, etc. there are several other activities that discourage security attacks from happening on the data and network. Adaptation of digital signatures to verify the completeness of documents, cryptography defence against unwanted access to sensitive information, routine compliance assessments to track and update data security activities, creation of domestic and international cyber forensics to help cyber crime investigations, and other technical and management instruments.

DIGITAL SIGNATURE

A digital signature is a methodology through which user data can be protected in a way which verifies the originator of the information and the authenticity of the data. Authentication is often called this method to guarantee the sources and completeness of knowledge. The presence or lack of an authorised handwritten signature is determining the genuineness of many legal, financial, and other documents. Hand-written signatures would be supplemented with automated signatures for a computerised message system to substitute physical paper and ink delivery. Only a technology to be used with various verification implementations is a digital signature. For an E record, the usual handwritten signatures are very close in their function. Through using specialised crypto-software the consumer itself may create key pairs. IE and Netscape from Microsoft permit users to build their own main pair. Anyone may file a request for a Digital Signature Certificate to the Certifying Authority.

ENCRYPTION

The protection of confidential logs and communications in transit and in stock is among the most effective and critical measures for computer device protection. It's a long colourful past for cryptography. Historically, the humanities, military, diplomatic corps, diarists and lovers have been used and contributed by four

individuals. The army played the most delicate position and formed the ground. In the protection of a government, corporate safety and any individual who operates for his/her personal gain, knowledge and data security currently play a vital role. In order to encrypt the message or data recognised as a plaintext, a feature that is initialised by a KEY is transformed. Cypher text is then sent via the dangerous contact channel to create an encryption method known as cypher text. Cryptanalysis is the method of cracking cyphers. Cyptology is collectively regarded as cryptology, the practise of constructing and cracking cyphers (cryptography). It is achieved by utilising algorithms, which are few – Hidden Key Algorithm, Data Encryption (DES, Public Key Algorithm, RSA Algorithm, etc.).

SECURITY AUDIT

A safety audit regularly assesses the safety of an information system of an organisation by assessing the degree to which it conforms to a series of standards. The vulnerabilities posed by a company with their IT architecture need to be recognised. The protection of the physical setup and setting, applications, knowledge processing, and usage practises usually is measured in a comprehensive audit.

CYBER FORENSICS

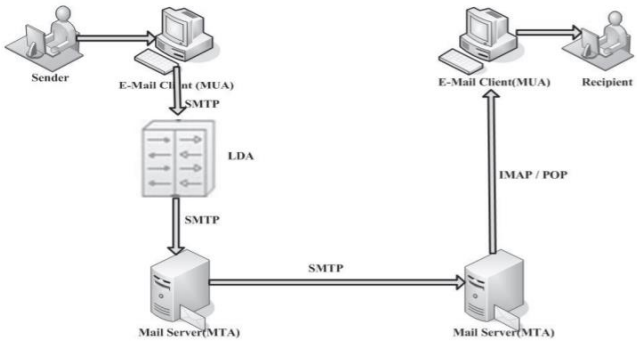
In solving computer crime, cyber forensics is a very necessary ingredient. Cyber forensics are the identification, examination and restoration of data obtained from every information device feature that allows prosecutors to resolve a criminal offence. Computer forensics questions are primarily regarding imaging media for retrieval, retrieval of missing images, slack and free space quest and lawsuit conservation of the data gathered. The other thing is network forensics, and cyber forensics is a more theoretically complicated question. It collects knowledge that is transmitted across broad and complicated networks in digital electronic) shape. Kerala has founded a national cyber-forensic laboratory. E-discovery study encompasses fields of cash theft, corruption, financial manipulation, cybercrimes, serious fraud and prosecution of white collar criminals. E-discovery systems are currently in early childhood in India, and this is the explanation that many corporate and cyber-crimes cases remain unreported. Organizations must be equipped for what is

unexpected, in order to resist unintended cyber misfortunes and strong impacts. Increased enforcement costs for addressing the upward rise in the regulatory standards and the continual advancements in technology against a context in underinvestment of defence departments will both mix cybercrime with the spike in online triggers (hacktivism) to contribute to a perfect threat environment. Organizations which decide the company's key reliance would be in a position to measure the business case for investing in resilience, minimising the impact of unexpected cyber misfortune.

EMAIL SECURITY

Electronic mails are a common medium of structured and commercial correspondence around the globe. The sum of e-mails collected and the quantity of spam e-mails is rising slowly. Spam mails are classified as electronic communications that are normally posted for commercial or benefit to thousands of recipients. Any of the spam emails transform into phishing emails that search for sensitive details of users and enter their bank accounts with financial fraud intentions. A consumer may submit an email or another website to a phishing site. Some emails which often include spam and phishing text-based attachments, such that the spam philtres are tricked that normally searches for content alone in the document. In addition, in order to fool the predominant spam philtre schemes, the material (e-mail bodies) alone can even be vulnerable to a term deconfusion technique. Originally the e-mails were developed and used to exchange knowledge inside ARPANET network study groups (Gary Canon 1998). A series of protocols was created to connect computational resources transparently in various geographical locations. The DARPA (Defense Advanced Research Projects Agency) research project ARPANET was the Internet precursor. In 1965 the Massachusetts Institute of Technology produced a Mailbox model, which established and deployed the first SENDMSG email application to connect with ARPANET users. E-mail is the most significant application in its growth and gave exposure to the masses and raised the need for security protocols considerably. The table below describes different email protection protocols for email transport such as SMTP, POP and IMAP. Many tech developers have created their own MPIs, which are used by the Microsoft Exchange Server, and which

have expanded proprietary and closed features, such as the Message Software Development Kit (SDK).



OVER COME METHODS:

Over the last number of seasons, spam emails and phishing have been rising at a high pace. For enterprise customers, network operators and even regular users this has become a big threat. E-mail is a communication system that transfers data stored on the machine through telecommunications. The e-mails are sent to multiple persons and people. Even though the email helps move details, spam or junk messages create significant problems. Spam letter, obtained by the citizens who cause annoyance and are flooded in the inbox, is unsolicited correspondence. It irritates consumers of email by wasted time and contribute to problems with bandwidth in ISP. So it is more essential to identify and distinguish incoming e-mails into spam and ham. Therefore this segment discusses prior email identification and classification strategies. This segment discusses several of the recent works in the field of classification of emails. Amandeep Singh et al (2013) examine the relevance of email and spam problems. This spam emails generate a lot of pressure when sharing details such as anonymity and handling of post. The paper proposes therefore that spam mails develop more problems such that more safe contact can be controlled. The CIA circles around many things contemporary information security. The lack of secrecy, honesty and availability of one or more of these components can have significant consequences for the protection of the company. Two main elements are confidentiality: verification and authorisation. Authentication defines the users and verifies the users. Approval defines access privileges through authorising or refusing access to services. Integrity guarantees trust (or legitimacy) in details. It guarantees the accuracy and non-modification of all the information or the resources accessed. For instance, attackers who hacked an ISP mail server might substitute a malicious content

with an original email address, and the naïve consumer would not realise that it has been updated. Finally, the provision of details affects the end user's availability if appropriate.

CONCLUSION

The Information Age is maturing, complemented by an extremely increased usage of the Internet; humanity evolves rapidly as the growth of public accessible knowledge has been greatly nurtured and facilitated. Consequently, an unmistakable dependence on the World Wide Web has been established in civilization. The digital realm, as a propitious infrastructure for a grand variety of criminal offenses, has grown with the society needs to become an increasingly protected environment. Cyber security develops to grow in sophistication but individuals however, are currently more exposed than ever before. At present, cybercrime is practiced by threat actors that do not necessarily possess a very substantial technical knowledge on information systems, they exploit the human vulnerabilities. Recent studies have shown that people are at the core of the infection chain in the greatest majority of cyber attacks. Social engineering is increasing both in sophistication and ruthless efficiency, because people, make the best exploits. As such, facts point to the conclusion that in the foreseeable future, social engineering will be the most predominant attack vector within cyber security, and thus deserve to be studied further as it evolves in order to advise good practices and measures for individuals and organizations.

REFERANCES

[1] Wenke Lee, Bo Rotoloni, “Emerging cyber threats, trends and technologies”, Technical report, Institute for Information Security and Privacy, 2016.
[2] “Internet organized crime threat assessment”, Technical report, Europol, 2016.
[3] James Comey, “Worldwide threats to the homeland: ISIS and the new wave of terror, statement before the house committee on homeland security”, FBI, July 2016.
[4] “Internet security threat report”, Technical report, vol. 21, Symantec, April 2016.
[5] Nahal Sarbjit, Ma Beijia, Tran Felix, “Global cybersecurity primer”, Technical report, Bank of America Merrill Lynch, 2015.
[6] Nabie Y Conteh, Paul J Schmick, “Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks”, International Journal of Advanced Computer Research, Vol.6 pp.23-31, 2016.
[7] “State of cyber security implications for 2016”, Technical report, ISACA and RSA, 2016.
[8] “The human factor”, Technical report, Proofpoint, 2016.
[9] Kevin D Mitnick, William L Simon, “The art of deception: Controlling the human element of security”, John Wiley & Sons, 2011.

[10] “Hacking the human operating system: The role of social engineering within cybersecurity”, Technical report, Intel Security, 2015.
[11] Prashant Kumar Dey, “Prashant's algorithm for password management system”, International Journal of Engineering Science, pp.2424, 2016.
[12] Seppo Heikkinen, “Social engineering in the world of emerging communication technologies”, Proceedings of Wireless World Research Forum, pp. 1-10, 2006.
[13] Rahul Singh Patel, “Kali Linux Social Engineering”, Packt Publishing Ltd, 2013.
[14] Joseph Muniz, “Web Penetration Testing with Kali Linux”, Packt Publishing Ltd, 2013.
[15] Andrea Cullen, Lorna Armitage, “The social engineering attack spiral (seas). In Cyber Security And Protection Of Digital Services (Cyber Security)”, 2016 International Conference On, pp.1-6, IEEE, 2016.