A Review, Challenges and Mitigations of Cyber Attacks

RAJESH RAO K[1], Dr.G.N.K.SURESH BABU[2]
[1] Assistant Professor, Acharya Institute of Technology, Bangalore – 90,
Mail Id : rajeshrao@acharya.ac.in
[2] Associate Professor, Acharya Institute of Technology, Bangalore – 90
Mail Id : gnksureshbabu@gmail.com

Abstract - The objective of this paper is how to protect data from the cyper attacks and provides cyber security to on line users (ICT-Information and Communication Technology). Now a day's all the organizations completely depends on line data and huge volume of transactions done through on line only. For example, Net Banking (money transfer from one account to another), Ticket Booking and on line purchasing through E-Commerce portals. Since the volume of transactions done through online is increasing day by day we have to protect our data and customer data safer from the attackers. This paper is to throw light on factors that implementation of cyber security. Cyber security is a set of people, process and technical practices aimed at protecting critical infrastructures, digital business and sensitive information from internal and external threats or negligence. This paper investigates practical solutions to the implementation of cyber security.

Keywords : Security, Cyber attack, Encryption, Decryption

I INTRODUCTION

Over the past several years, experts and policymakers have expressed increasing concerns about protecting ICT systems from *cyber attacks*—deliberate attempts by unauthorized persons to access ICT systems, usually with the goal of theft, disruption, damage, or other unlawful actions. Many experts expect the number and severity of cyber attacks to increase over the next several years. The biggest discussion of today is a fundamental question about the reliability and security of the Internet and perhaps technology as a whole. "Cyber security" refers to the protection of everything that is potentially exposed to the Internet. In this paper the author reviews encryption algorithms and suggests solutions for cyber challenges.

II CYBER ATTACKS

The act of protecting ICT systems and their contents has come to be known as cyber security. The risks associated with any attack depend on three factors: threats (who is attacking), vulnerabilities (the weaknesses they are attacking), and impacts (what the attack does). The management of risk to information systems is considered fundamental to effective cyber security.

Threats - People who actually or potentially perform cyber attacks are widely cited as falling into one or more of five categories: *criminals* intent on monetary gain from crimes such as theft or extortion; *spies* intent on stealing classified or proprietary information used by government or private entities; *nation-state warriors* who develop capabilities and undertake cyber attacks in support of a country's strategic objectives; "*hacktivists*" who perform cyber attacks for nonmonetary reasons; and *terrorists* who engage in cyber attacks as a form of non-state or state-sponsored warfare.

Vulnerabilities - Cyber security is in many ways an arms race between attackers and defenders. ICT systems are very complex, and attackers are constantly probing for weaknesses, which can occur at many points. Defenders can often protect against weaknesses, but three are particularly challenging: inadvertent or intentional acts by *insiders* with access to a system; *supply chain* vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition process; and previously unknown, or *zero-day*, vulnerabilities with no established fix. Even for vulnerabilities where remedies are known, they may not be implemented in many cases because of budgetary or operational constraints.

Denial of Service (DoS) - A denial-of-service (DoS) attack is an attempt to make an online resource – often a website – unavailable to its legitimate users.

DoS attacks work by "flooding" the resource with a large number of requests. This overwhelms the server, which is no longer capable of responding to all the requests. Regular users trying to use the resource are thus not able to get access. A DoS attack originating from one source computer would be easy to block. Therefore most DoS attacks are distributed denial-of-service (DDoS) attacks. This simply means that the attack originates from more than one source, i.e. a large number of computers sending requests to the same server. DDoS attacks can be conducted by having computer users voluntarily join forces to participate in the attack. More commonly, DDoS attacks are orchestrated using botnets – networks of compromised computers whose users are not even aware that their machines are involved in an attack. Malicious software (malware) installed on the computer allows a third-party – the actual attacker – to take control of the machine and turn it into a bot (short for robot) participating in the DDoS attack. It is important to understand that DDoS attacks are at the lowest end of the spectrum when it comes to cyber attacks. They cause no lasting damage, are comparatively easy to protect against, and are trivial to orchestrate if one has either enough money to rent a botnet or enough supporters who are willing to contribute their resources to the attack. As Jose Nazario of Arbor Networks pointed out, a DDoS attack requires "just a lot of people getting together and running the same tools on their home computers". Even more importantly, a DDoS attack just means that the attacked resource, for instance a website, is temporarily unavailable. A DDoS attack alone does not mean that the attackers got access to any of the data on the targeted machine or were able to do any other harm.

Website Attack - A website attack is an attack on a website that changes the content of that website. Often the new content reflects the motivation of the attacker , ridicules the target, or both. One of the most common methods for website defacements is a technique known as SQL injection. In an SQL injection attack, the attacker is able to pass commands to a database by entering malicious data in a web form. In theory, SQL injections are easy to protect against, since they are only possible due to programming errors in the website. However, in practice many websites are vulnerable to them due to lax security practices.

A more serious issue are break-ins into computers other than mere web servers (or break-ins into web servers if these machines are used to store data other than just the public website). Such break-ins can be perpetrated using techniques similar to the ones used for website defacement, such as SQL injection. The difficulty of a break-in depends on the IT security level of the target system. Once an attacker has gained access to a machine, they may be able to access other computers on the same network, steal confidential data, install malware to turn machines into zombies for a botnet, or cause other damage. It is impossible to make generalised statements about computer break-ins, except to say that a break-in itself does not constitute an act of war. However, the results of the break-in might – in the very unlikely case that the attacker was able to, say, cause significant physical damage by manipulating an Industrial Control System.

III Challenges of Cyber Attacks

The main cyber security risks arise from the extensive and growing dependence on ICT infrastructure and e-services by the Estonian state, the economy and the population. Therefore, the key fields on which the Cyber Security Strategy focuses are ensuring vital services, combating cybercrime more effectively and advancing national defence capabilities. Additional supporting activities will include: shaping the legal framework, promoting international cooperation and communication, raising awareness, and ensuring specialist education as well as the development of technical solutions. All vital services and their dependencies must be mapped, alternatives must be developed and operational readiness to implement them must be achieved. The preservation of data and information systems that are essential to the functioning of society must be ensured in both the public and private sectors. The timely detection of and response to cyber threats threatening the state, society and the individual must be ensured. **Cybercrime** undermines the functioning of the economic space, reduces trust in digital services, and, in a worst-case scenario, could lead to incidents causing loss of life. Competent personnel and modern technical tools are needed in order to ensure prevention, detection and prosecuting of cybercrime. Operational information exchange between countries is becoming increasingly important in the fight against cybercrime. In order to prevent and deter **future security** threats, it is necessary to constantly develop cyber security related know-how and to invest in technology. Implementing forward-looking procurement procedures is necessary to ensure production of reliable and competitive solutions and will support their export as well, whereas the knowledge and resources obtained in that process must be re-invested into innovative solutions. As a **supporting activity**, a modern legal framework must be ensured to provide complete solutions to the above-listed challenges. At the international level, the preservation of a free and secure cyberspace as well as Estonia's central role in guiding and developing international cyber security policy in international organizations as well as like-minded communities must be ensured.

IV Encryption Algorithms

The author reviews some important algorithms which is used for implementing cyber security. Encryption is the process of scrambling a message so that only the intended recipient can read it. Encryption can provide a means of securing information. As more and more information is stored on computers or communicated via computers, the need to insure that this information is invulnerable to snooping and/or tampering becomes more relevant. With the fast progression of digital data exchange in electronic way, Information Security is becoming much more important in data storage and transmission. Information Confidentiality has a prominent significance in the study of ethics, law and most recently in Information Systems. With the evolution of human intelligence, the art of cryptography has become more complex in order to make information more secure.

Symmetric key encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption.

Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys – one a public key and one a private key. It is also known as public-key encryption.

A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together. Asymmetric encryption techniques are about 1000 times slower than Symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use a stronger key than symmetric encryption technique.

The generation, modification and transportation of keys have been done by the encryption algorithm. It is also named as cryptographic algorithm. There are many cryptographic algorithms available in the market to encrypt the data. The strength of encryption algorithm heavily relies on the computer system used for the generation of keys. Some important encryption algorithms are discussed here:

Rivest-Shamir-Adleman (RSA) - RSA is designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. It is one of the best known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data. RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption and decryption purpose.

Data Encryption Standard (DES) - DES is one of the most widely accepted, publicly available cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard. The Data Encryption Standard (DES) is a block Cipher which is designed to encrypt and decrypt blocks of data consisting of 64 bits by using a 64-bit key. Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. The algorithm goes through 16 iterations that interlace blocks of plaintext with values obtained from the key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key are used for decryption. There are many attacks and methods recorded till now those exploit the weaknesses of DES, which made it an insecure block cipher. Despite the growing concerns about its vulnerability, DES is still widely used by financial services and other industries worldwide to protect sensitive on-line applications.

Triple DES (3DES) - 3DES or the Triple Data Encryption Algorithm (TDEA) was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Data Encryption Standard (DES) uses a 56-bit key and is not deemed sufficient to encrypt sensitive data. 3-DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys. The combined key size is thus 168 bits (3 times 56). TDEA involves using three 64-bit DEA keys (K1, K2, K3) in Encrypt-Decrypt- Encrypt (EDE) mode, that is, the plain text is encrypted with K1, then decrypted with K2, and then encrypted again with K3.

Advanced Encryption Standard (AES) - AES is the new encryption standard recommended by NIST to replace DES in 2001. AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. During encryption-decryption process, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text. AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For both encryption and decryption, the cipher begins with an AddRoundKey stage.

V Mitigations for Cyber attacks

The author suggests the following solutions for cyber attacks :

• To have better authentication mechanisms by which you can be 100% certain about who is connecting to a system.
• To be able to use secure applications over an insecure infrastructure. Acknowledging that PCs, tablets, phones and the Internet itself will never be secure, it is imperative to build secure applications on top of this insecurity.
• An increased role for biometrics, which could support authentication online, enabling new levels of security. This includes fingerprints, blood analysis, DNA sampling, heartbeat and other biomarkers.
• To have a self-learning security system: a system that could learn from day to day operation and which would automatically block all unusual movement in your systems.
• Auto classification of data, automatically finding which data is worth securing.
• To have a framework of security warnings and alerts that will help the user better understand the security risk and implications of certain actions. This could apply anywhere from an app store to certain actions inside a corporate system.
• A label to put on applications and certification for devices that would inform people of the level of security that is provided.
• The incident response plan must contain details on when and how to communicate to the public about security incidents. Depending on the severity of the incident, different types of messaging can be developed, but for any incident there should be a single and coherent message for both internal and external communications. The primary goal is to protect customers' interests and reduce their uncertainty. Communication has to be fast and effective and parties such as law enforcement authorities, regulatory agencies and partners must be informed when appropriate.
• Build a multi-functional response team: IT in collaboration with communications, legal, senior decision makers and other relevant business experts. This has been recommended practice for a while but still isn't done often enough.
• Test and practice the emergency response with the team, so they know each other and know the procedures. As one security consultant phrased it: "If there is an attack, do they know how to react, or otherwise know who to contact? Managing incidents should be simple and clear. If they need a manual, it will not work."

Security-by-design is one of the powerful approaches we have available to make everything more secure. Not using it is leaving a big opportunity on the table. With product vendors very aware of security risks, custom development is one of the most important places where vulnerabilities are introduced into your technology infrastructure. Putting security into every layer is the only way to be both resilient against attacks and be as future-proof as possible – for example being ready for new channels, new connections, new integrations, because the core system has security woven in throughout. In the software testing world and the privacy debate, we've learned that the earlier in the process you take certain requirements into account, the cheaper it is and the easier to implement. The same goes for security:
• Make security a part of the Enterprise Architecture discussion, with strong requirements about data, verification of authentication and by default not "trusting" other components or layers of your architecture. Establish an Enterprise Architecture process that is empowered and supportive in helping project teams make the right decisions.
• Create anti-patterns: negative use cases that describe the undesired behavior too, so that it's clear what should be built and tested along the way. For example when a genuine use case reads "An authenticated user can read his own latest five

transactions," you can turn that into the undesired situations of "A NON-authenticated user can read every latest five transactions" or "An authenticated user reads SOMEONE ELSE's latest five transactions." This helps to make clear what the underlying code should and should not allow, all the way to the data level. It establishes very early on in the design process where the restrictions should be built in.

VI Conclusion and Suggestions for Cyber Attacks

Cyber security is a key risk that the broker-dealer industry faces today and that will likely grow in importance in the coming years. Firms should make the development and implementation of measures to address cyber security challenges one of the cornerstones of a sound business infrastructure. The principles and effective practices described in this report can help firms in that effort. A risk management-based approach to cyber security permits firms to tailor their approach to the individual circumstances and the changing threats each firm faces. The framework and standards discussed can inform firms' thinking at a programmatic as well as individual control level. Put enough time and budget into your projects to address all non-functional requirements right from the start: security, privacy, quality, usability, manageability, etc. There is no one-size-fits-all solution to address cyber threats. Much attention has been focused on advanced threats that firms face, and those certainly pose significant dangers. However, most successful attacks take advantage of fairly basic control weaknesses. While firms need to stay on guard, they can also take some comfort from this. To be sure, cyber security is challenging to address, but it is certainly not impossible. What is required is rigorous attention to detail and execution. Risk assessments can help firms identify and prioritize those steps that are most urgent to undertake. Information sharing can help firms understand the types of threats they may face and available mitigation measures. Digitalization has come to dominate all levels of society, ranging from individuals to large enterprises and states. The efficiency of digitalization has, however, also created security issues. Cyber attacks occur on a daily basis with or without actors knowing about it, and the number of attacks continues to rise. It has therefore become a core security issue in modern society. This motivated us to go further into depth with the puzzle of why it is difficult to implement effective exceptional measures in spite of the securitization of cyber threats, and has therefore been the focus of our research. Furthermore, as we see the issue of cyber security as highly important, we will also recommend further suggestions based on our findings.

Use and maintain a reputable antivirus software. Good antivirus software packages recognize and protect your computer against most known viruses. Once you have installed an antivirus package, you should use it to scan your entire computer periodically. Find a package that includes antispyware tools.

Keep antivirus software up to date. Install software patches and security updates for your antivirus software on a regular basis. They will help protect your computer against new threats as they are discovered. Many vendors and operating systems offer automatic updates. If this option is available, you should enable it.

Install or enable a firewall. Firewalls protect against outside attackers by shielding your computer or network from malicious or unnecessary Internet traffic. They are especially important for users who rely on "always on" connections such as cable or Digital Subscriber Line modems. Some operating systems include a firewall; if yours has one, you should make sure it is enabled. If not, consider purchasing a hardware- or software-based firewall.

VII References

[1] Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2012.

[2] Behrouz A Forouzan, "Data Communications and etworking", McGraw-Hill, 4th Edition.

[3] Domenici, H. and Bari, A. The Price of Cybersecurity: Big Investments, Small Improvements. A. Holmes, Ed., Bloomberg Government Survey (Jan. 31, 2012).

[4] Floyd, R. (2011), *Can securitization theory be used in normative analysis? Towards a just securitization theory*, Security Dialogue, August-October 2011; vol. 42, 4-5: pp. 427-439.

[5] Hansen, L., & Nissenbaum, H. (2009), *Digital Disaster, Cyber Security, and the Copenhagen School*, International Studies Quarterly (2009) 53, 1155–1175

[6] Moir, R. (October 2003) "Defining Malware: FAQ" Tech Net, Microsoft Corporation; URL: (http://technet.microsoft.com/en-us/library/dd632948.aspx), last accessed: June 10th, 2012

[7] Pram Gad, Ulrik & Lund Petersen, Karen (2011), *Concepts of politics in securitization studies*, Security Dialogue 42(4-5) 315–328

[8] Shashi Mehrotra Seth, Rajan ishra, "Comparative Analysis of Encryption Algorithms for Data Communication", International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, June 2011.

[9] William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson Education/Prentice Hall, 5th Edition.

[10] Xin Zhou and Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", the 6th International Forum on Strategic Technology, pp. 1118 – 1121, 2011.