IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 6, Ver. I (Nov - Dec 2018), PP 86-88
www.iosrjournals.org

Information Security

Somnath Saha
Assistant Professor, department of Computer science,Cooch Behar College, Booch Behar
Email: somnath325@gmail.com

Abstract:
Organizations rely heavily on the use of information technology (IT) products and services to run their day-to-day activities. Ensuring the security of these products and services is of the utmost importance for the success of the organization. The main reason is that security is expensive to set up and a nuisance to run, so people judge from experience how little of it they can get away with. Since there's been little damage, people decide that they don't need much security. In a distributed system with no central management like the Internet, security requires a clear story about who is trusted for each step in establishing it, and why. The basic tool for telling this story is the "speaks for" relation between principals that describes how authority is delegated, that is, who trusts whom. The idea is simple, and it explains what's going on in any system I know. The many different ways of encoding this relation often make it hard to see the underlying or
Therefore, protecting corporations' information becomes more important, and information security is essential to maintain. Information security is defined as protecting the information, the system, and the hardware that use, store and transmit the information, to ensure integrity, confidentiality and availability of data and operation procedures are protected. Therefore, protecting companies information becomes more important, and information security is essential to maintain. Information security is defined as protecting theinformation, the system, and the hardware that use, store and transmit the information, to ensure integrity, confidentiality and availability of data and operation procedures are protected.

Keywords: *Information, Cyber Crime, Network Security, Internet of Things, Attacks*

I. Introduction

People have been working on computer system security for at least 30 years. During this time there have been many intellectual successes. Notable among them are the subject/object access matrix model , access control lists , multilevel security using information flow and the star-property, public key cryptography, and cryptographic protocols. In spite of these successes, it seems fair to say that in an absolute sense, the security of the hundreds of millions of deployed computer systems is terrible: a determined and competent attacker could destroy most of the information on almost any of these systems, or steal it from any system that is connected to a network. Even worse, the attacker could do this to millions of systems at once. The Internet has made computer security much more difficult than it used to be. In the good old days, a computer system had a few dozen users at most, all members of the same organization. It ran programs written in-house or by a few vendors. Information was moved from one computer to another by carrying tapes or disks. All these problems cause two kinds of bad results. One is vandalism, motivated by personal entertainment or statusseeking: people write worms and viruses that infect many machines, either by exploiting buffer overrun bugs that allow arbitrary code to run, or by tricking users into running hostile code from e-mail attachments or web pages. These can disrupt servers that businesses depend on, or if they infect many enduser machines they can generate enough network traffic to overload either individual web servers or large parts of the Internet itself. The other bad result is that it's much easier to mount an attack on a specific target (usually an organization), either to steal information or to corrupt data.

Due to the rapid increase of using technologies, that provide some comfort to the user, such as saving time and effort. The Internet of Things (IoT) is considered the best technology, with its applications that facilitate our work and live by providing features (i.e. connectivity, active engagement) that help us to achieve improvement, increase evolution and knowledge exchange. IoT is definedas a group of people and devices interconnected with each other. In addition, it allows devices to communicate with each otherwithout involvement of human, it includes interconnected sensors of real world, devices of electronics and systems to the Internet.The main support of the IoT is the Internet. So that, any security threats that target the Internet can affect the IoT.

What is security?

What do we want from secure computer systems? Here is a reasonable goal: Computers are as secure as real world systems, and people believe it. Most real world systems are not very secure by the absolute standard suggested above. It’s easy to break into someone’s house The technological components of information security are relatively well understood. Firewalls monitor, block and filter traffic on networks. Antivirus, anti-spyware and anti-malware software scans programmes and data for mal-icious content. Strong encryption secures data, data transferand communications against eavesdropping and accidentalleaks. Access management, version management and auditlogs help maintain the integrity of information systems. These components are the high walls, locks, security gates and the barred windows of information security, interrupt- ing the free flow of information in order to ensure its con- trol. But it is a mistake to think of information security as a matter or erecting fences, barricading entrances and choos- ing the most secure locks. Security is not something that is *applied* to information systems and processes after the fact, it is something that must be built in from the beginning.

. As a result, people use them only for things that are seldom needed and either expensive or hard to replace. Practical security balances the cost of protection and the risk of loss, which is the cost of recovering from a loss times its probability. Usually the probability is fairly small (because the risk of punishment is high enough), and therefore the risk of loss is also small. When the risk is less than the cost of recovering, it’s better to accept it as a cost of doing business (or a cost of daily living) than to pay for better security. People and credit card companies make these decisions every day. With computers, on the other hand, security is only a matter of software, which is cheap to manufacture, never wears out, and can’t be attacked with drills or explosives. This makes it easy to drift into thinking that computer security can be perfect, or nearly so. Information security is a matter of understanding and managing risk, and not eliminating threats. When every functional computing device is also a networked computingdevice, there is no such thing as an absolutely secure infor-mation system. Just as important as maintaining the con- fidentiality of information is maintaining the fitness for purpose of both information and the processes into whichit is slotted, and this inevitable involves risk. People behave in ways that they shouldn’t and that theyknow they shouldn’t because often it is more convenient, more polite or just normal practice. They use simple or predictable passwords, they use the same passwords on multiple systems, they write down their passwords, they share their log in details with colleagues, they respond helpfully to inquiries, they leave systems logged-in, they take home files on memory sticks and they use the same email for personal and professional purposes. We all knowthese things are a problem. Yet, we all almost certainly indulge in some of these bad information security habitsat some point. So ubiquitous are they that it becomes almost irresponsible to ignore them.

Theway to address information security is to understand how information slots into the work processes within an orga- nization, and where the vulnerabilities lie.

Real security

The end result should not be surprising. We don’t have “real” security that guarantees to stop bad things from happening, and the main reason is that people don’t buy it. They don’t buy it because the danger is small, and because security is a pain. • Since the danger is small, people prefer to buy features. A secure system has fewer features because it has to be implemented correctly. This means that it takes more time to build, so naturally it lacks the latest features. A secondary reason we don’t have “real” security is that systems are complicated, and therefore both the code and the setup have bugs that an attacker can exploit. This is the reason that gets all the attention, but it is not the heart of the problem. Will things get better? Certainly when security flaws cause serious damage, buyers change their priorities and systems become more secure, but unless there’s a catastrophe, these changes are slow.

Basic Security Concepts

Three basic security concepts important to information on the internet are confidentiality, integrity, and availability. Concepts relating to the people who use that information are authentication, authorization, and nonrepudiation. When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality. For some types of information, confidentiality is a very important attribute. Examples include research data, medical and insurance records, new product specifications, and corporate investment strategies. This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting. Information can be erased or become inaccessible, resulting in loss of availability. This means that people who are authorized to get information cannot get what they need. Availability is often the most important attribute in service-oriented businesses that depend on information (for example, airline schedules and online inventory systems). 1 Availability of the network itself is important to anyone whose business or education relies on a network connection. When users cannot access the network or specific services provided on the network, they experience a denial of service. To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. Authentication is proving that a user is the person he or she claims to be. That proof may involve something the user knows (such as a password), something the user has (such as a “smartcard”), or something about the user that proves the person’s identity (such as a fingerprint). Authorization is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted—the user cannot later deny that he or she performed the activity. This is known as nonrepudiation. These concepts of information security also apply to the term information security; that is, internet users want to be assured that In addition, information assurance extends to systems of all kinds, including large-scale distributed systems, control systems, and embedded systems, and it encompasses systems with hardware, software, and human components. The technologies of information assurance address system intrusions and compromises to information.

Network Securiy

For network security attacks, auth categorized some basic class of network attacks in three categories, in addition, they suggest to perform some procedures to avoid security gaps, including regularly updating the operatingsystem, having an updated antivirus program, and limiting the access to any network user.

In order to investigate attacks on different systems, authors in [9] made a security analysis of the network communication betweenthe components of SCADA systems namely, Programmable Logic Controllers (PLCs) and the engineering stations, they showedthat this communication can be compromised by successfully conducting three network security attacks, replay attack, Man-In-The-Middle attack (MITM), and Stealth command modification attack, these attacks allow to interfere with the PLC-Process ControlSystem 7 (PLC-PCS7) communication and send commands to the PLC that control and reprogram it, this leads to serious SCADAsystem insecurity

II. Conclusion:

The key information security issues and respective research contributions. The information security contributions were analyzed from the viewpoints of a meta-model for IS, the research approaches employed, and the reference disciplines utilized. The analysis showed that information security research has focused primarily on technical issues.. While the issues of access to IS and secure communications have been widely recognized, there is a great need for empirical studies on the development of secure IS and security management (using empirical theory-creating and testing, and utilizing qualitative and quantitative studies) based on appropriate reference theories.

References

[1]. Abrams, M. D. and Moffett, J. T. (1995). “A Higher Level of Computer Security Through Active Policies,” Computer & Security, Vol. 14, No. 2, pp. 147-157.

[2]. Abrams, M. D. and Podell, H. J. (1995). “Evaluation Issues,” in Abrams, M.D., Jajodia, S. and Podell, H.J. (Eds.), Information Security - An Integrated Collection of Essays, Los Alamitos, CA: IEEE Computer Society Press. Ajzen, I. (1991). “The Theory of Planned Behavior,” Organizational Behavior and Human Decision Processes, Vol. 50, pp. 179-211.

[3]. BBC (2015) Talk talk cyber attack, BBC. Available at: http:// www.bbc.co.uk/news/uk-34611857 (accessed 10 May 2016).

[4]. Computer Security Act of 1987, Public Law 100-235, 101 Stat 1724 https://www.gpo.gov/fdsys/pkg/STATUTE-101/pdf/STATUTE-101- Pg1724.pdf.

[5]. E-Government Act of 2002, Public Law 107-347, 116 Stat 2899. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW107publ347.pdf.

[6]. U.S. Department of Commerce. Secure Hash Standard (SHS), Federal Information Processing Standards (FIPS) Publication 180-4, August 2015, 36pp. https://doi.org/10.6028/NIST.FIPS.180-4.