A Review of Information Security for Data Transmission

Eliakim Ombati Akama

Lecturer, Department of Mathematics & Computer Science, University of Eldoret, Kenya

Abstract:- **As our society becomes more dependent on the network to aid smooth communication and increased output, preserving confidentiality, integrity and the authenticity of data while it is being stored, transferred and even when it is being processed must be taken into consideration with greater weight. It is very important to note that, sensitive information in transmission, especially the electrical commission's application, if not well secured it can result in a compromise. Advancement in technology not only in the area of cryptosystem but also in parallelism technology can be of great effect to our data during trans Progression in computing powers and parallelism technology is creating an environment that can be suitable for a secured end to end communication.**

Keywords:-**Data privacy, encryption, internet-of-things (IoT), Identity theft, MIT.**

I. INTRODUCTION

As our society becomes more dependent on the network to aid smooth communication and increased output, preserving confidentiality, integrity, and authenticity of data while it's being stored, transferred and even when it's being processed must be taken into consideration with greater weight. One of the greatest security challenges emerging in unguided communication can be related to the privacy and security of sensitive information. This is as a result of open windows that give interceptors from unauthorized people a chance to modify data in a wireless transmission when it is on the air via radio waves.

Radio waves are still one that uses a medium for data transmission but an organization using this kind of media should understand its downfalls: it is so easy for information to be accessed by unauthorized people since its not bound to a specific boundary. So it is very hard to keep the signals within a restricted boundary. The best way to handle depends on users' accessibility. There are secured access points that use the transmission protocols to access the network securely. Obtaining secured transmission is determined by these access points which are secured.

The existing protocols are the wired equivalent privacy protocol (WEP) and the wireless fidelity (Wi-Fi) Protected Access Protocols (WPA or WPA2)

However, the protocols still require the use of radio waves as a transmission medium and as such data can be intercepted and used by unauthorized persons. There is also increased use of Hotspots and Wi-Fi areas mostly in which are densely populated like institutions, financial organizations mean that other alternative security arrangements need to be made. The core principles of data security include:

1. Confidentiality where sensitive data or information belonging to an organization or government should not be accessed by or disclosed to unauthorized people.
2. Integrity, data should not be modified without the owner's authority. Data integrity is violated when a person accidentally or with malicious intent, erases or modifies important files such as payroll or a customer's bank account file.
3. Availability, The information must be available on demand. This means that any information system and communication link used to access it must be efficient and functional. An information system may be unavailable due to power outages, hardware failures, unplanned upgrades or repairs.

II. DATA PRIVACY

Privacy on the Internet is an issue that is of significant interest. The lack of knowledge among people and organizations is the greatest threats to data security (Mitnick & Simon 2002). There are different kinds of information being transmitted on the network for example in the military work. All the data need a greater level of confidentiality. There are two fundamental issues:

- Privacy of data during transmission;
- Privacy of stored data.

The first issue, privacy during network transmission, has been studied widely in the Internet area and addressed by the Secure Socket Layer protocol (SSL) (Freier, Karlton, & Kocher Nov 1996) and Transport Layer Security (TSL) protocol (Dierks & Allen Nov 1997). The second issue, the privacy of stored data in relational databases is less studied and of greater relevance to the database as a service model. If the database as a service is to be successful, and customer data is to reside on the site of the database service provider, then the service provider needs to find a way to preserve the privacy of the user data. There is a need to have a secured measure in place so that even if the data is stolen, the thief cannot make sense of it.

Like now in Kenya, the issue of 'Huduma number' is one of the technologies discovered recently to circle all the individual information in Kenya. Huduma number is a unique account that creates and manages a central master population register which is termed to be an authentic source of truth of the identity of all people residing in Kenya. The intention for the Kenyan government might be for positive effect but we can't rule out the issue of information theft as well as identify theft. And so there is a need to secure this information.

III. IDENTITY THEFT

We can describe this animal as "knowingly transferring or using" without lawful authority, a means of identification of another person with the intent to commit or to aid or abet, any unlawful activity that constitutes a violation of federal law.

In Nairobi Kenya may 3 2017, it was published in capitalism that "identity theft is one of the leading scheme bank fraudsters are using to steal money from banks or customers after the adoption of EMV enabled ATMs in 2013".

We can also talk about "medical identity theft (MIT)". MIT occurs when a patient's name or medical insurance information is used without the patient's knowledge or consent, to steal their insurance cover or creation of fictitious medical records to circumvent statutory requirements like Immigration or employment regulations.

The cost of identity theft can range from a small to an astronomical amount. No matter the amount was stolen, there are more other issues such as time and cost for recovery which occurs from identity theft and even death in the case of MIT.

Most organizations eyes on the technical defenses such as encryption, access control, firewalls and intrusion detection that is associated with information protection (Ande,1972 & sand, 1996) however there its little study on how companies should: prepare for facing security incidents by selecting appropriate security measures, measure the degree of vulnerability of a company to security incidents, asses the damages of past security incidents, train security personnel in law enforcement agencies to better prepare for dealing with security incidents and to reduce the cost of happening.

IV. SECURITY CHALLENGES

There is a great swift of technology from the old error of manual work to an advanced even more advanced technology where almost everything is done through the internet. We got something we call the Internet of Things that is a trending technology in the communication of data through the internet. Internet of Things (IoT), is a system of interrelated computing devices, mechanical and digital machines, objects, or even people that are provided with a unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. The IoT depends on a host of technologies such as application programming interfaces (APIs) that connect devices to the internet. With this advancement in technology, there are several challenges that may exist as follows:

1) Data Privacy: Some manufacturers of smart TVs collect data about their customers to analyze their viewing habits so the data collected by the smart TVs may have a challenge for data privacy during transmission.

2) Data Security: Data security is also a great challenge. While transmitting data seamlessly, it is important to hide from observing devices on the internet.

3) Insurance Concerns: The insurance companies installing IoT devices on vehicles collect data about health and driving status to take decisions about insurance.

4) Lack of Common Standard: Since there are many standards for IoT devices and IoT manufacturing industries. Therefore, it is a big challenge to distinguish between permitted and non-permitted devices connected to the internet.

5) Technical Concerns: Due to the increased usage of IoT devices, the traffic generated by these devices is also increasing. Hence there is a need to increase network capacity, therefore, it is also a challenge to store the huge amount of data for analysis and further final storage.

6) Security Attacks and System Vulnerabilities: There has been a lot of work done in the scenario of IoT security up till now. The related work can be divided into system security, application security, and network security.

a) System Security: System security mainly focuses on the overall IoT system to identify different security challenges, to design different security frameworks and to provide proper security guidelines to maintain the security of a network.

b) Application security: Application Security works for IoT application to handle security issues according to scenario requirements.

c) Network security: Network security deals with securing the IoT communication network for communication of different IoT devices.

V. ANALYSIS OF DIFFERENT TYPES OF ATTACKS

The IoT is facing various types of attacks including active attacks and passive attacks that may easily disturb the functionality and abolish the benefits of its services. In a passive attack, an intruder just senses the node or may steal the information but it never attacks physically. However, the active attacks disturb the performance physically. These active attacks are classified into two further categories that are internal attacks and external attacks. Such vulnerable attacks can prevent the devices to communicate smartly. Hence the security constraints must be applied to prevent devices from malicious attacks, Different types of attack, nature/behavior of attack and threat level of attacks are discussed in this section. Different levels of attacks are categorized into four types according to their behavior and propose possible solutions to threats/attacks.

1) *Low-level attack:* If an attacker tries to attack a network and his attack is not successful.

2) *Medium-level attack:* If an attacker/intruder or an eavesdropper is just listening to the medium but don't alter the integrity of data.
3) *High-level attack:* If an attack is carried on a network and it alters the integrity of data or modifies the data
4) *Extremely High-level attack:* If an intruder/attacker attacks on a network by gaining unauthorized access and performing an illegal operation, making the network unavailable, sending bulk messages, or jamming network.

VI. CONCLUSION

Data is now the most critical element in every organization and has become part of every organization's mission to formulate policies that can safely guide the honey in this endangered element. In the recent past, most companies used encryption as a sure means of data protection but now as technology increases, attackers too haven't been stuck rather they are advancing every day. And so the security of data transmission cannot be achieved by encryption alone. Completely securing the baseline infrastructure in an unobtrusive and unconstrained manner will pave the way for delivering and protecting all forms of data as well as educating people on security awareness in-order to know how to handle security threats.

Data transmission lines cannot be physically secured as they were during the day of dedicated physical links. Logical security methods must be implemented to ensure the same levels of security without the physical attributes that can be afforded by hard-wired links.

At a minimum, the following four criteria must be given greater consideration:

1. World-class cryptography and key management.
2. Protection of encrypted data as it moves through the infrastructure
3. Consistency in performance, regardless of frame size and data classification methods.
   And then, Regional information Society should encourage the business community, governmental and private organizations to depend more and more on carrying out their day to day data transmission and communication using the information technology infrastructure if the privacy and integrity of their data are protected and secured.

REFERENCES

[1]. Butler Shawn, Fischbeck Paul, Multi-Attribute Risk Assessment. Technical Report CMU-CS-01-169, December 2001

[2]. A. Freier, P. Karlton, and P. Kocher. The SSL Protocol Version 3.0 Internet-Draft. November 1996.

[3]. T. Dierks and C. Allen. The TLS Protocol Version 1.0 Internet-Draft. November 1997

[4]. Anderson J. (1972) "Computer Security Technology Planning Study," U.S. Air Force Electronic Systems Division Tech. Rep.

[5]. Sandhu, R. S.(1996) Coyne, E., J., Youman, C. E., 1996, "Role-based Administration of Rules," ACM Transactions of Information Systems.

[6]. D. E. Denning. Cryptography and Data Security. Addison-Wesley Publishing Company, Inc, 1982.

[7]. N. R. Adam and J. C. Wortmann. Security control methods for statistical databases: a comparative study. ACM Computing Surveys, 21(4):515-556, 1989.