E/15/280

Premathilaka M.P.U

INTRODUCTION

One of the basic truths behind internet is that it is not secured for people. Therefore, in order to make it secure, many organizations, individuals, companies take necessary actions to protect their devices after connecting to the internet. This process is known as internet security. With the technological improvement the threat caused by the internet is also becomes advance. To prevent form being attacked by the internet high level security mechanisms should be used.

LITERATURE REVIEW

The history of internet security began with a research project. A man named Bob Thomas realized that it was possible for a computer program to move across a network, leaving a small trail wherever it went. The first computer virus was created in the early 1970s and was detected on ARPANET, the predecessor to the internet. According to Trend Micro's research paper, "Ransomware: Past, Present and Future" some of the earliest ransomware infections took place more than 10 years ago in 2005 and 2006. It states that most of the victims were initially found in Russia, and in one case the attacker has demanded $300 to access to victim's files and data.

When we look about modern threats, according to the internet security threat report published by Symantec in 2019, it states attack types as Formjacking, Cryptojacking, Ransomware, Living off the land and supply chain attacks, Targeted attacks and also Cloud and IoT are major victims of attacks. Also, as common attacks it can be stated Phishing, SQL Injection attack, Cross scripting and DOS.

METHODOLOGIES

Security must be applied to internet protocols to provide their service securely. The security that should provide to the protocol is depend on the structure of the protocol. Therefore, for different protocols different security mechanisms should be applied. But for most of the protocol common standard internet security mechanisms are applicable.

The security mechanism which should be implemented over the internet should be decided on some factors. Those are called decision factors and they are described below.

Threat Model: Threat modeling is a procedure for optimizing network security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. This is the most important factor when choosing a security mechanism. It should analyze what is expected to attack, what are the resources what will be attacking method. This will not be a major factor to concern if it is public website which provides information. But it is important to consider about threat model in a major backbone router or high-level Domain Name Server, should be protected by very strong mechanisms.

Granularity of Protection: When assessing the desired granularity of protection, protocol designers should take into account likely usage patterns, implementation layers and deploy ability. If a protocol is likely to be used with in a subnet, subnet granularity is appropriate.

Implementation Layer: The effectiveness of the security mechanism depends on the layer of implementation. Lower layer security mechanisms protect higher variety of threats rather than higher level security mechanisms. For example, link layer security protection applied to IP addresses as well as ARP packets.

In order to provide proper internet security, some standard security mechanisms are used according to IEFT (Internet Engineering Task Force)

1. **One-time password (OTP)**: This password is valid only for one-time login session or transaction on a computer system or digital system
2. **HMAC**: HMAC is a specific type of message authentication code involving a cryptographic hash function and a secret cryptographic key. It may be used to simultaneously verify both the data integrity and the authentication of a message, as with any MAC.

3. **IPsec**: IPsec is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

4. **TLS**: The primary goal of the TLS Protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol.

5. **SASL**: SASL (Simple Authentication and Security Layer) is a framework for negotiating an authentication and encryption mechanism to be used over a TCP stream. As such, its security properties are those of the negotiated mechanism

6. **GSS-API**: The Generic Security Service Application Program Interface is an application programming interface for programs to access security services

7. **DNSSEC**: DNS Security Extensions, commonly known as DNSSEC, provide a way to authenticate DNS response data. DNSSEC provides a level of additional security where the web browser can check to make sure the DNS information is correct and was not modified

8. **Security/ Multipart**: Security/ Multipart are the preferred mechanism for protecting email.

When implementing a computer network following Network Security Measures should be taken.

- A strong firewall and proxy to be used to keep unwanted people out.
- A strong Antivirus software package and Internet Security Software package should be installed.
- For authentication, use strong passwords and change it on a weekly/bi-weekly basis.
- When using a wireless connection, use a robust password.
- Employees should be cautious about physical security.
- Prepare a network analyzer or network monitor and use it when needed.
- Implementation of physical security measures like closed circuit television for entry areas and restricted zones.
- Security barriers to restrict the organization's perimeter.
- Fire asphyxiators can be used for fire-sensitive areas like server rooms and security rooms.

DISCUSSION:

The security threats are increasing day by day and making high speed network and internet services insecure and un-reliable. The above methodologies do not guarantee 100% security. There failure conditions in those mechanisms as well. Here are some examples, if your one-time password (OTP) device is ever stolen or lost, multiple login attacks by the hacker can permanently lock you out of your account. An unfortunate disadvantage of using HMAC for connection authentication is that the secret must be known in the clear by both parties, making this undesirable when keys are long-lived.

REFERENCES

1. https://blog.trendmicro.com/the-evolution-of-ransomware/
2. https://tools.ietf.org/html/rfc3631
3. https://resources.infosecinstitute.com/one-time-passwords-pros-and-cons/#gref
4. Internet security Threat Report Volume 4 | February 2019