International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol. 1, Issue 2, December 2014

Analysis of Security Techniques for Computer Networks

[1]Ritu Makani,[2]Yogesh Chaba
[1]Assistant Professor,CSE, G J U S& T Hisar (Haryana)
[2]Professor,CSE, G J U S& T Hisar (Haryana)
[1]ritu_nagpal22@yahoo.co.in,[2] yogeshchaba@yahoo.com

Abstract: **The security requirements of an enterprise vary depending on how important its tasks are. If they are financial dealers they need to be aware of insiders, outsiders and close-ins(social engineering). The kind of attacks or malicious activities the enterprise encounters within its security perimeter decides its security infrastructure. Four kinds of measures can be taken to provide security: pattern matching using signature based schemes, Statistical and Correlation Analysis for latest trends in malware, manual examination of event and system logs and monitoring for unusual data exfiltration attempts. The security may be required at various levels and layers resulting into multilayered security model. The system files, data files, program files all require to be protected from intruders who wish to gain unauthorized access to these resources by infiltrating into the associated network. The threats posed to a network or host change as the adversary acquires better programming skills for malware creation. The Advanced Persistent Threats (APTs) tend to creep into the network with authenticated credentials and use GET to export as much data as required. Contextual security is required to prevent exploitation of such threats. Signcryption scheme may be required to prevent such kind of advanced malware-style attacks such as Stuxnet in cyberwar. So present paper gives a brief overview of the background knowledge of the type of attack various security mechanisms and their analysis on merits and the current development in network security.**

KEY WORDS :Security, IDS , Pattern Matching, Contextual Security, Signcryption, APT

I. INTRODUCTION

A large number of people of varied fields ranging from business people to defense personnel and banks to business organizations to researchers are using the internet. There is a huge amount of commercial, military and personal information is on networking infrastructures worldwide. Security of this precious information is of utmost concern. There are basically two different types of networks, a) Data networks b) Synchronous network comprised of switches. Synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. Security is emphasized in data networks, such as the internet, and other networks that link to the internet. Internet is considered a data network and consists of computer-based routers. Viruses like, trojan horses, can be inserted in the routers to have access to the information.[1] The vast topic of network security is analyzed by researching the following:

1. Flashback of security in networks
2. Architecture of internet and study of vulnerabilities for its security.
3. Different types of attacks and methods to counter them.
4. Security for networks with internet access
5. Developments in network security hardware and softwareNetwork design and development follows the rule of open systems interface (OSI) model which inherits modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development [1].

A hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.[1]

In data security we transform client's data to unintelligible data for transmission. For intercepting, a key is needed to decode the message. This method of security is effective to a certain extent. Strong cryptography in the past can be easily broken today. Cryptographic methods have to continue to advance due to the advancement of the hackers as well. A secure network is helpful in transferring cipher text over a network. This will protect the cipher text so that it is less likely for many people to even attempt to break the code. A secure network will also not allow, inserting unauthorized messages into the network. Therefore, hard ciphers are needed as well as attack-hard networks [2].

Application writers know that the cryptography occurs at the application layer . The user can possibly choose different

methods of data security. Whereas network security is mostly contained within the physical layer. Layers above the physical layer are also used to accomplish the network security required [2]. Authentication is performed on a layer above the physical layer. Network security in the physical layer requires failure detection, attack detection mechanisms, and intelligent countermeasure strategies [2].

An attack can be successful attempt if it exploits a threat or vulnerability in system file, data, program, configuration file, protocol, application software, network, Host, networking components or any other resource.[3]

The main categorization of attacks is

1. Active and passive attacks,
2. Reactive and proactive attacks

The **Passive Attacks** include scanning or monitoring traffic in its unencrypted form with an intention to reuse it in causing other forms of attack. The **Active Attacks** attempt to create, modify or delete traffic in the line. These attacks attempt to break into secure systems by any malicious means by unauthorized users through viruses, worms ,stealth, DoS. [3]

II. DIFFERENT NETWORKS SCENARIOS AND SECURITY ISSUES:

The security may be required at various levels and layers resulting into multilayered security model [3]. IDS deployment can give us a good example of this. IDS can be classified into different categories depending on their deployment.[4]

Host-based Monitoring

A host-based IDS is deployed on devices that have other primary functions such as Web servers, database servers and other host devices.

Network-based Monitoring

Network-based IDS is deployed to monitor the traffic of that network. This ensures that the IDS can observe all communication between a network attacker and the victim system, resolving many of the problems associated with log monitoring. Typical Network-based IDS are Microsoft Network Monitor, Cisco Secure IDS (formerly Net Ranger), Snort etc.

Target-based Monitoring

Target- based ID systems typically use scanning techniques to form an image of what systems exist in the protected network, including such details as host operating system, active services, and possible vulnerabilities. Formulating effective rule sets is a fundamental portion of the Contextual approach to network security. For example APTs(Advanced Persistent Threats) has a specific objective and is executed by skilled and well funded operators. Asset awareness is first step to defending against APTs. The businesses today use combinations of firewalls, encryption, and authentication mechanisms to create “intranets” that are connected to the internet but protected from it at the same time. Intranet is a private computer network that uses internet protocols. Intranets differ from "Extranets" in that the former are generally restricted to employees of the organization while extranets can generally be accessed by customers, suppliers, or other approved parties[5].

There does not necessarily have to be any access from the organization's internal network to the Internet itself. When such access is provided it is usually through a gateway with a firewall, along with user authentication, encryption of messages, and often makes use of virtual private networks (VPNs)[5,6,7].For broader data sharing, it might be better to keep the networks open, with these safeguards:

- Firewalls that detect and report intrusion attempts
- Sophisticated virus checking at the firewall
- Enforced rules for employee opening of e- mail attachments
- Encryption for all connections and data transfers
- Authentication by synchronized, timed passwords or security certificates

III. CURRENT DEVELOPMENTS IN NETWORK SECURITY

Biometrics provides a better method of authentication than passwords. This might greatly reduce the unauthorized access of secure systems. New technology such as the smart card is surfacing in research on network security. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented[8]. The research being performed assists in understanding current development and projecting the future developments of the field.

A. Hardware Developments

Biometric systems and smart cards are the new hardware technologies that are widely impacting security. The most obvious use of biometrics for network security is for secure workstation logons for a workstation connected to a network. The main use of Biometric network security will be to replace the current password system. Maintaining password security can be a major task for even a small organization. Passwords have to be changed every few months and people forget their password. Voice biometric package can be a costly affair but may be able to manage the secure log-in of up to 5000 machines[8] Hardware device such as computer mice with built in thumbprint readers would be the next step up. The advantage of voice recognition software is that it can be centralized, thus reducing the cost of implementation per machine.

Smart cards are usually a credit-card-sized digital electronic media. The card itself is designed to store encryption keys and other information used in authentication and other identification processes. The main idea behind smart cards is to provide undeniable proof of a user’s identity. Smart cards can be used for everything from logging in to the network to providing secure Web communications and secure e-mail transactions. But the interesting thing is what happens when the user inputs the PIN. The PIN is verified from inside the smart card. Because the PIN is never transmitted across the network, there’s absolutely no danger of it being intercepted. The main benefit, though, is that the PIN is useless without the smart card, and the smart card is useless

without the PIN. There are other security issues of the smart card. The smart card is cost-effective but not as secure as the biometric identification devices.

B. Software Developments

The software aspect of network security is very dynamic. Basically security paradigm is working on the following lines these days :Pattern matching using signature based schemes, Statistical and Correlation Analysis for latest trends in malware, Manual examination of event and system logs and monitoring for unusual data ex filtration attempts.Improvements in the design and implementation of firewalls, cryptographic techniques with authentication mechanisms and antivirus softwares is a continuous process. Development of intrusion detection and prevention systems is another upcoming area of concern [9,10].Egress filtering is monitoring and restricting the flow of information outbound from one network to another. It helps ensure malicious traffic never leaves the internal network. Continuous study of everyday changing attack methods is also the key to device guard against them. Many small and complex devices can be connected to the internet. Most of the current security algorithms are computational intensive and require substantial processing power. Therefore, there is a need for designing light-weight security algorithms. Research in this area is currently being performed.

IV. FUTURE TRENDS IN SECURITY

Vulnerability scanners, Monitoring techniques, Egress filtering, SSL decryption and inspection are some of the latest software development areas on which work is being done. What is going to drive the network security is the set of these kind of applications more than anything else. The future will possibly be that the security is similar to an immune system. As the immune system guards our body from diseases similarly network security fights off attacks and builds itself to fight tougher enemies. Many security developments that are taking place are within the same set of security technology that is being used today with some minor adjustments.

V. CONCLUSION

With the expansion of internet, network security field is increasingly gaining attention. The security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software based, but many common hardware devices are used. The current development in network security is very impressive but going at a slow rate as compared to new threats being faced. The embedded security of the new internet protocol IPv6 may provide many benefits to internet users. Although some security issues were observed, the IPv6 internet protocol seems to evade many of the current popular attacks. Combined use of IPv6 and security tools such as firewalls, intrusion detection, and authentication mechanisms and the latest software developments discussed here will be effective in guarding almost all the varied areas of the network security field.

REFERENCES

[1] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," *Computer*, vol.31, no.9, pp.24- 28, Sep 1998

[2] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," *Communications, 2008. ICC '08. IEEE International Conference on*, pp.1469-1473, 19-23 May 2008

[3] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*,vol., no., pp.77- 82, 13- 15 May 2008

[4] Marin, G.A., "Network security basics," *Security & Privacy, IEEE* , vol.3, no.6, pp. 68- 72, Nov.- Dec. 2005

[5] "Intranet." *Wikipedia, The Free Encyclopedia*. 23 Jun 2008, 10:43 UTC. Wikimedia Foundation, Inc. 2 Jul2008

[6] "Virtual private network." *Wikipedia, The Free Encyclopedia*. 30 Jun 2008, 19:32 UTC. Wikimedia Foundation, Inc. 2 Jul 2008

[7] Bhavya Daya"Network Security: History, Importance and Future"Univ.of Florida

[8] Al- Salqan, Y.Y., "Future trends in Internet security," *Distributed Computing Systems, 1997., Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of* , vol., no., pp.216- 217, 29- 31 Oct 1997

[9] Serpanos, D.N.; Voyiatzis, A.G., "Secure network design: A layered approach," *Autonomous Decentralized System, 2002. The 2nd International Workshop on*, vol., no., pp. 95- 100, 6- 7 Nov. 2002

[10] C. Warrender, S. Forrest, B.A. Pearlmutter, "*Detecting intrusions using system calls: Alternative data models"*, In IEEE Symposium on Security and Privacy, pages 133-145, 1999