Network Security-Proposals

A. Swetha, Y. Madhavi Latha

Abstract: ***The explosion of the public Internet and e-commerce, private computers, and computer networks, if not adequately secured, are increasingly vulnerable to damaging attacks. Hackers, viruses, vindictive employees and even human error all represent clear and present dangers to networks. Loss of irreplaceable data is a very real threat for any business owner whose network connects to the outside world. Remote access for employees and connection to the Internet may improve communication in ways you've hardly imagined. Access to the Internet can open the world to communicating with customers and vendors, and is an immense source of information. But these same opportunities open a local area network (LAN) to the possibility of attack by thieves and vandals.***

Keywords- LAN.

I. INTRODUCTION

"SECURITY" in this contemporary scenarios has become a more sensible issue either it may be in the "REAL WORLD" or in the "CYBER WORLD". In the real world as opposed to the cyber world an attack is often preceded by information gathering. Movie gangsters "case the joint"; soldiers "scout the area". This is also true in the cyber world. Here the "bad guys" are referred to as intruders, eavesdroppers, hackers, hijackers, etc. The intruders would first have a panoramic view of the victim's network and then start digging the holes. Today the illicit activities of the hackers are growing by leaps and bounds, viz., "THE RECENT ATTACK ON THE DNS SERVERS HAS CAUSED A LOT OF HULLABALOO ALL OVER THE WORLD". However, fortunately, the antagonists reacted promptly and resurrected the Internet world from the brink of prostration. Newton's law says "Every action has got an equal but opposite reaction". So is the case with this. Nevertheless the security breaches and eavesdroppers, the technological prowess has been stupendously developed to defy against each of the assaults.

Various antidotes that are in fact inextricable with security issues are – Cryptography, Authentication, Integrity and Non Repudiation, Key Distribution and certification, Access control by implementing Firewalls etc. The Internet has undoubtedly become the largest public data network, enabling and facilitating both personal and business communications worldwide. More and more communication is taking place through e-mail; mobile workers, telecommuters, and branch offices are using the Internet to remotely connect to their corporate networks; and commercial transactions completed over the Internet, via the World Wide Web, now account for large portions of corporate revenue.

Manuscript received on May, 2013.

Y. Madhavi Latha, Asst. Professor, Dept of Electronics & Computer Engineering, K.L. University, Guntur (A.P.), India

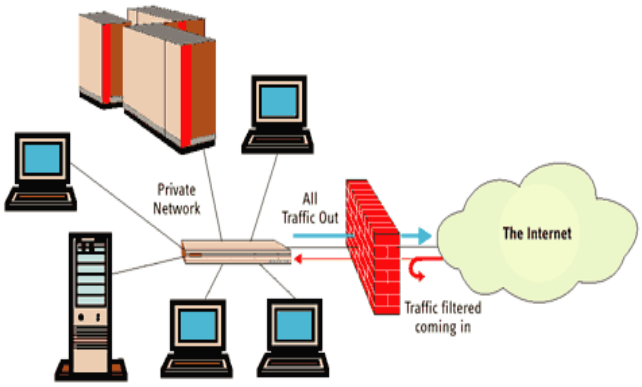
A. Swetha, Dept of Electronics & Computer Engineering, K.L. University, Guntur (A.P.), India

The Internet, intranets, and extranets enable fast and effective communication between employees and partners. However, such communication and efficiency can of course be impeded by the effects of a network attack. An attack may directly cause several hours of downtime for employees, and networks must be taken down in order for damage to be repaired or data to be restored. Securing and operating today's complex systems is challenging and demanding.

We discuss about the **security tools** i.e. providing security using the tools such as **firewalls, Cryptography**, **Intrusion detection and Honey pots**

(i) FIREWALLS

A firewall is a system that enforces an access control policy between two networks—such as your private LAN and the unsafe, public Internet. The firewall determines which inside services can be accessed from the outside, and vice versa. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one to block traffic, and one to permit traffic. A firewall is more than the locked front door to your network—you're your security guard as well.



Different types of Firewalls:

1. Packet filtering firewalls.
2. Circuit level gateways.
3. Application level gate ways.
4. Stateful multi layer inspection.

(ii) CRYPTOGRAPHY :(DES Vs AES)

Does increased security provide comfort to paranoid people? Or does security provide some very basic protections that we are naive to believe that we don't need? During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with.

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography. But it is important to note that while cryptography is necessary for secure communications, it is not by itself sufficient. The search for a replacement to DES started in

January 1997 when NIST announced that it was looking for an Advanced Encryption Standard (AES)**.**

II. PURPOSE OF CRYPTOGRAPHY

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Within the context of any application-to-application communication, there are some specific security requirements, including:

- ***Authentication****:* The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- ***Privacy/confidentiality****:* Ensuring that no one can read the message except the intended receiver.
- ***Integrity****:* Assuring the receiver that the received message has not been altered in any way from the original.
- ***Non-repudiation****:* A mechanism to prove that the sender really sent this message.

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use.

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption

Secret key cryptography algorithms that are in use today include:

Data Encryption Standard (DES): The most common SKC scheme used today, DES was designed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS) [now the National Institute for Standards and Technology (NIST)] in 1977 for commercial and unclassified government applications. DES is a block-cipher employing a 56-bit key that operates on 64-bit blocks.

IBM also proposed a 112-bit key for DES, which was rejected at the time by the government; the use of 112-bit keys was considered in the 1990s, however, conversion was never seriously considered. The DEA, often called DES, has been extensively studied since its publication and is the best known and widely used symmetric algorithm in the world.

Advanced Encryption Standard (AES)*:* In 1997, NIST initiated a very public, 4-1/2 year process to develop a new secure cryptosystem for U.S. government applications. The result, the Advanced Encryption Standard, became the official successor to DES in December 2001.

AES uses an SKC scheme called Rijndael, a block cipher designed by Belgian cryptographers Joan Daemen and Vincent Rijmen. FIPS PUB 197 describes a 128-bit block cipher employing a 128-, 192-, or *CAST-128/256:* CAST-128, described in Request for Comments (RFC) 2144, is a DES-like substitution-permutation crypto algorithm, employing a 128-bit key operating on a 64-bit block.

CAST-256 (RFC 2612) is an extension of CAST-128, using a 128-bit block size and a variable length (128, 160, 192, 224, or 256 bit) key. CAST is named for its developers, Carlisle Adams and Stafford Tavares and is available internationally. CAST-256 was one of the Round 1 algorithms in the AES process 256-bit key.

(iii) INTRUSION DETECTION

It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called **Intrusion Detection.**

The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The recent denial of service attacks on major Internet sites have shown us, no open computer network is immune from intrusions. The wireless ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense.

The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective. Many intrusion detection techniques have been developed on fixed wired networks but have been turned to be inapplicable in this new environment. We need to search for new architecture and mechanisms to protect wireless networks and mobile computing application.

We examine the vulnerabilities of wireless networks and say that we must include intrusion detection in the security architecture for mobile computing environment. We have showed such architecture and evaluated key mechanisms in this architecture such as applying mobile agents to intrusion detection, anomaly detection and misuse detection for mobile ad-hoc networks.

III. NEED FOR INTRUSION DETECTION

A computer system should provide *confidentiality*, *integrity* and *assurance* against denial of service. However, due to increased connectivity (especially on the Internet), and the vast spectrum of financial possibilities that are opening up, more and more systems are subject to attack by intruders. These subversion attempts try to exploit flaws in the operating system as well as in application programs and have resulted in spectacular incidents like the Internet Worm incident of 1988.

There are two ways to handle subversion attempts. One way is to prevent subversion itself by building a completely secure system. We could, for example, *require* all users to identify and authenticate themselves; we could protect data by various cryptographic methods and very tight access control mechanisms. However this is not really feasible because:

(1) In practice, it is not possible to build a completely secure system. Miller gives a compelling report on bugs in popular programs and operating systems that seems to indicate that (a) bug free software is still a dream and (b) no-one seems to want to make the effort to try to develop such software. Apart from the fact that we do not seem to be getting our money's worth when we buy software, there are also security implications when our E-mail software, for example, can be attacked. Designing and implementing a totally secure system is thus an extremely difficult task.

(2) The vast installed base of systems worldwide guarantees that any transition to a secure system, (if it is ever developed) will be long in coming.

(3) Cryptographic methods have their own problems. Passwords can be cracked, users can lose their passwords, and entire crypto-systems can be broken.
(4) Even a truly secure system is vulnerable to abuse by insiders who abuse their privileges.
(5) It has been seen that that the relationship between the level of access control and user efficiency is an inverse one, which means that the stricter the mechanisms, the lower the efficiency becomes.

The history of security research has taught us a valuable lesson – no matter how many intrusion prevention measures are inserted in a network, there are always some weak links that one could exploit to break in. We thus see that we are stuck with systems that have vulnerabilities for a while to come.

If there are attacks on a system, we would like to detect them as soon as possible (preferably in real-time) and take appropriate action. This is essentially what an Intrusion Detection System (IDS) does. An IDS does not usually take preventive measures when an attack is detected; it is a reactive rather than pro-active agent. It plays the role of an informant rather than a police officer.

IV. BACKGROUND ON INTRUSION DETECTION

In the last three years, the networking revolution has finally come of age. More than ever before, we see that the Internet is changing computing, as we know it. The possibilities and opportunities are limitless; unfortunately, so too are the risks and chances of malicious intrusions.

It is very important that the security mechanisms of a system are designed so as to *prevent* unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called **Intrusion Detection.** A simple firewall can no longer provide enough security as in the past. Today's corporations are drafting intricate security policies whose enforcement requires the use of multiple systems, both proactive and reactive (and often multi-layered and highly redundant).

The premise behind intrusion detection systems is simple: Deploy a set of agents to inspect network traffic and look for the "signatures" of known network attacks. However, the evolution of network computing and the awesome availability of the Internet have complicated this concept somewhat. With the advent of Distributed Denial of Service (DDOS) attacks, which are often launched from hundreds of separate sources, the traffic source no longer provides reliable temporal clues that an attack is in progress. Worse yet, the task of responding to such attacks is further complicated by the diversity of the source systems, and especially by the geographically distributed nature of most attacks.

Intrusion detection techniques while often regarded as grossly experimental, the field of intrusion detection has matured a great deal to the point where it has secured a space in the network defense landscape alongside firewalls and virus protection systems. While the actual implementations tend to be fairly complex, and often proprietary, the concept behind intrusion detection is a surprisingly simple one: Inspect all network activity (both inbound and outbound) and identify suspicious patterns that could be evidence of a network or system attack.

V. HONEY POTS

Advances in computer and communication technologies have resulted in highly distributed systems that allow users to access information and resources from all over the globe. This interconnectivity emphasizes the longstanding problem of providing security in a distributed computer system by introducing many more possible attacking points

Rapid increase in the number of reported intrusions, break-ins and computer thefts results in a growing need for effective computer security measures. Richard pointed out that, even with the most advanced protection, computer systems are still not **100**percent secure. In fact, most computer security experts agree that, given user-desired features such as network connectivity, we'll never achieve the goal of a completely secure system.

As a result, we must develop intrusion detection techniques and systems to discover and react to computer attacks. So as a positive protection technology IDS becomes the focus in the field of network security at present.

Definition of honey pot

A honey pot can be defined as Honey pot is a "decoy" system that has anon-hardened operating system or one that appears to have several vulnerabilities for easy access to its resources. The decoy system should be set up in a similar manner to those of the production servers in the corporation and should be loaded with numerous fake files, directories, and other information that may look real. By making the honey pot appear to be a legitimate machine with legitimate files, it leads the hacker to believe that they have gained access to important information.

Honeypots are a highly flexible security tool with different applications for security. **Honey pots** all share the same concept: a security resource that should not have any production or authorized activity. In other words, deployment of **honey pots** in a network should not affect critical network services and applications. A **honey pot** is a security resource who's value lies in being probed, attacked, or compromised.

An example of a **honey pot** is a system used to simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be used to break into the machine. This kind of **honey pot** can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

There are two general types of **honeypots:**

- **Production honeypots** are easy to use, capture only limited information, and are used primarily by companies or corporations;
- **Research honeypots** are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.

Honey pot can improve the characteristics of an IDS

We propose that IDS with honey pot as its component solves all the problems mentioned A honey pot is designed to be compromised, not to be used for production traffic. Any traffic entering or leaving the network is suspicious by definition. This concept of no production traffic greatly simplifies the data capture and analysis.

VI. CONCLUSION

The diligent management of network security is essential to the operation of networks, regardless of whether they have segments or not. It is important to note that absolute security is an abstract concept – it does not exist anywhere. All networks are vulnerable to insider or outsider attacks, and eavesdropping. No one wants to risk having the data exposed to the casual observer or open malicious mischief. Regardless of whether the networks are wired or wireless, steps can and should always be taken to preserve network security and integrity.

We have said that any secure network will have vulnerabilities that an adversary could exploit. This is especially true for wireless ad-hoc networks. Intrusion Detection can compliment intrusion prevention techniques (such as encryption, authentication, secure MAC, secure routing, etc.) to improve the network security. However new techniques must be developed to make intrusion detection work better for the wireless networks.

We have shown that an architecture for better intrusion detection in wireless networks should be distributed and cooperative by applying Mobile Agents to the network and given few of the implemented approaches for intrusion detection.

Currently, the research is taking place in developing new architecture for wireless networks for better security.

REFERENCES

1. Cryptography and Network Security by William Stallings-2nd Edition
2. Network Security Fundamentals by Gert Delaet, Gert Svhauwers
3. Cryptography and Network Security by Kahate
4. Cryptography and Network Security by P S Gill.
5. Cryptography and Network security by William Stallings-5th edition