IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Issue-12 E-ISSN: 2347-2693

Security Technology

Adil Jamil Zaru

adiljamilzaru@gmail.com

Available online at: www.ijcseonline.org

Received: 21/Nov/2016 Revised: 02/Dec/2016 Accepted: 20/Dec/2016 Published: 31/Dec/2016

Abstract- All input is evil until proven otherwise!‖"so security technology come into play.With the rapid growth of interest in the Internet, network security has become a major concern to companies throughout the world. The fact that the information and tools needed to penetrate the security of corporate networks are widely available has increased that concern. Because of this increased focus on network security, network administrators often spend more effort protecting their networks than on actual network setup and administration. Tools that probe for system vulnerabilities, such as the Security Administrator Tool for Analyzing Networks (SATAN), and some of the newly available scanning and intrusion detection packages and appliances, assist in these efforts, but these tools only point out areas of weakness and may not provide a means to protect networks from all possible attacks. Thus, as a network administrator, you must constantly try to keep abreast of the large number of security issues confronting you in today's world. This paper describes many of the security issues that arise when connecting a private network. Understand the types of attacks that may be used by hackers to undermine network security. For decades, technology has transformed almost every aspect of business, from the shop floor to the shop door. While technology was a fundamental enabler, it was often driven from an operational or cost advantage and seen as separate from business itself. The new reality is that technology doesn't support the business—technology powers the business. IT risks are now business risks and IT opportunities are now business opportunities.

***Keywords*:** Security, Fires, IP networks, Internet, Filtering

Introduction

Security is the process of protecting data (in any form the data may take: electronic, print, or other forms) from unauthorized access, use, disclosure, destruction, modification, or disruption so as not to compromise the confidentiality, integrity, and availability of the information for use by the Enterprise or SMB organization throughout the Security Lifecycle.

Today, information security is a fundamental enabler for business. As business technology provides the ability for enterprises to automate, adapt and accelerate

their business strategy, information security is now essential for safeguarding business continuity. Whether enabling sharing and collaboration with partners, preventing or detecting insider attacks, or defending against vandalism by unseen and random network attackers – information security is a key element in any IT infrastructure.

Security Threats When Connecting to the Internet:

When you connect your private network to the Internet, you are physically connecting your network to more than 50,000 unknown networks and all their users. Although such connections open the door to many useful applications and provide great opportunities for information sharing, most private networks contain some information that should not be shared with outside users on the Internet. In addition, not all Internet users are involved in lawful activities. These two statements foreshadow the key questions behind in lawful activities. These two statements foreshadow the key questions behind most security issues on the internet.

Common types of attacks

Virus

A virus is a program that propagates itself by infecting other programs on the same computer. Viruses can do serious damage, such as erasing your files or your whole disk, or they may just do silly/annoying things like pop up a window that says "Ha ha you are infected!" True viruses cannot spread to a new computer without human assistance, such as if you trade files with a friend and give him an infected file (such as on a floppy or by an email attachment).

Worm

Like a virus, a worm is also a program that propagates itself. Unlike a virus, however, a worm can spread itself automatically over the network from one computer to the next. Worms are not clever or evil, they just take advantage of automatic file sending and receiving features found on many computers.

Trojan horse

This is a very general term, referring to programs that appear desirable, but actually contain something harmful. The harmful contents could be something simple, for example you may download what looks like a free game, but when you run it, it erases every file in that directory. The trojan's contents could also be a virus or worm, which then spread the damage.

Protecting Confidential Information

Confidential information can reside in two states on a network. It can reside on physical storage media, such as a hard drive or memory, or it can reside in transit across the physical network wire in the form of packets. These two information states present multiple opportunities for attacks from users on your internal network, as well as those users on the Internet. We are primarily concerned with the second state, which involves network security issues. The following are five common methods of attack that present opportunities to compromise the information on your network:

When protecting your information from these attacks, your concern is to prevent the theft, destruction, corruption, and introduction of information that can cause irreparable damage to sensitive and confidential data.

The following describes the common methods of attack and provides examples of how information can be compromised.

Various Security Technologies

PGP

Pretty Good Privacy is a computer program that provides cryptographic privacy and authentication. It was originally created by Philip Zimmermann in 1991.

PGP and other similar products follow the Open PGP standard (RFC 4880) for encrypting and decrypting data.

How PGP encryption works

PGP encryption uses public-key cryptography and includes a system which binds the public keys to a user name. The first version of this system was generally known as a web of trust to contrast with the X.509 system which uses a hierarchical approach based on certificate authority and which was added to PGP implementations later. Current versions of PGP encryption include both alternatives through an automated key management server.

Security quality

The cryptographic security of PGP encryption depends on the assumption that the algorithms used are unbreakable by direct cryptanalysis with current equipment and techniques. For instance, in the original version, the RSA algorithm was used to encrypt session keys; RSA's security depends upon the one-way function nature of mathematical integer factoring. New, now unknown, integer factorization techniques might, therefore, make breaking RSA easier than now, or perhaps even trivially easy. However, it is generally presumed by informed observers that this is an intractable problem, and likely to remain so. Likewise, the secret key algorithm used in PGP version 2 was IDEA, which might, at some future time, be found to have a previously unsuspected cryptanalytic flaw. Specific instances of current PGP, or IDEA, insecurities –— if they exist -— are not publicly known. As current versions of PGP have added additional encryption algorithms, the degree of their cryptographic vulnerability varies with the algorithm used. In practice, each of the algorithms in current use is not publicly known to have cryptanalytic weaknesses.

Any agency wanting to read PGP messages would probably use easier means than cryptanalysis, eg. Rubber-hose cryptanalysis, or by installing some form of trojan horse or keystroke logging software/hardware on the target computer to capture encrypted keyrings and their passwords. The FBI have already used this attack against PGP in their investigations. However, it is important to note that any such vulnerabilities apply not just to PGP, but to all encryption software

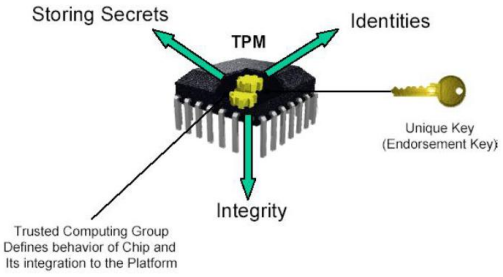
Trusted Platform Module

In computing, Trusted Platform Module (TPM) is both the name of a published specification detailing a secure cryptoprocessor that can store secured information, as well as the general name of implementations of that specification, often called "TPM chip", "Fritz chip" or "TPM Security Device" (Dell). The TPM specification is the work of the Trusted Computing Group.

Overview

A Trusted Platform Module offers facilities for secure generation of cryptographic keys, the ability to limit the use of cryptographic keys, as well as a hardware random number generator. It also includes capabilities such as remote attestation and sealed storage. Remote attestation creates an nearly unforgeable hash key-summary of the hardware and software. To what extent the software is being summarized is decided by the software that is encrypting the data . This allows a third party to verify that the software has not been changed. Sealing encrypts data in such a way that it may be decrypted only if the TPM release the right decryption key, which it only does if the exact same software is present as when it encrypted the data. Binding encrypts data using the TPM's endorsement key, a unique RSA key burned into the chip during its production, or another trusted key.

Platform Security technology



VMM

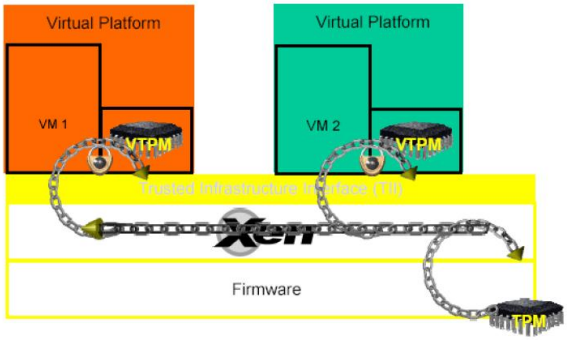
Virtual Machine Manager redirects here. For the virtual machine monitoring application from MicrosoftIn computer science, A virtual machine (VM) is a software implementation of a machine (computer) that executes programs like a real machine.

Definitions

A virtual machine was originally defined by Popek and Goldberg as an efficient, isolated duplicate of a real machine. Current use includes virtual machines which have no direct correspondence to any real hardware.[1]

Virtual machines are separated in two major categories, based on their use and degree of correspondence to any real machine. A system virtual machine provides a complete system platform which supports the execution of a complete operating system (OS). In contrast, a process virtual machine is designed to run a single program, which means that it supports a single process. An essential characteristic of a virtual machine is that the software running inside is limited to the resources and abstractions provided by the virtual machine -- it cannot break out of its virtual world.

VMM technology to build secure systems



Applications of The Security Technologies

In defence field various security technologies are used.In the missile Technology we are using the security technologies

IN THE INTERNET SECURITY

The security technologies used in the internet security are:

TPM applications :

Microsoft's new desktop operating system Windows 7 Windows 8 uses this technology as part of the feature BitLocker Drive Encryption. Available only in the Ultimate and Enterprise editions of Windows. BitLocker encrypts the computer's boot volume and provides integrity authentication for a trusted boot pathway (i.e. BIOS, boot sector, etc.) Other volumes can be encrypted using built-in command-line tools (although not via the GUI currently). Future Windows versions are expected to have increased TPM and BitLocker support for additional cryptographic features and expanded volume encryption. BitLocker requires two NTFS-formatted drive volumes, one for Windows boot code and BitLocker operational code, and the other containing the boot volume (i.e. the volume where the operating system is stored). It should also be noted that contrary to its official name of Full Volume Encryption

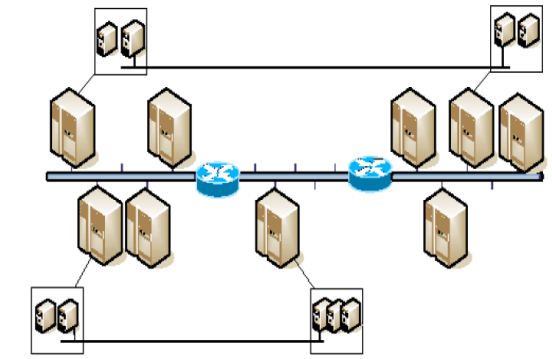
(FVE), BitLocker only encrypts logical volumes which may or may not be an entire drive.

The main advantages of system VMs are:

Multiple OS environments can co-exist on the same computer, in strong isolation from each other;

the virtual machine can provide an instruction set architecture (ISA) that is somewhat different from that of the real machine.

VMM network to build secure system



Multiple VMs each running their own operating system (called guest operating system) are frequently used in server consolidation, where different services that used to run on individual machines in order to avoid interference, are instead run in separate VMs on the same physical machine. This use is frequently called quality-of-service isolation (QoS isolation).

The desire to run multiple operating systems was the original motivation for virtual machines, as it allowed to time-share a single computer between several single-tasking OSes.

Used in Web applications:

- Server secures communications using SSL/TLS with a X.509 server certificate
- Server authenticates clients using data in client X.509 certificate, if required
- Certificate authority issues a certificate for which the server holds a root certificate
- Used in distributed applications
- Application uses SSL/TLS communication channel
- Client and server applications authenticate using certificates

Protecting Your Network:

Maintaining Internal Network System Integrity

Although protecting your information may be your highest priority, protecting the integrity of your network is critical in your ability to protect the information it contains. A breach in the integrity of your network can be extremely costly in time and effort, and it can open multiple avenues for continued attacks. This section covers the five methods of attack that are commonly used to compromise the integrity of your network:

When considering what to protect within your network, you are concerned with maintaining the integrity of the physical network, your network software, any other network resources, and your reputation. This integrity involves the verifiable identity of computers and users, proper operation of the services that your network provides, and optimal network performance; all these concerns are important in maintaining a productive network environment.

The below are the some examples of the attacks described previously and explains how they can be used to compromise your network's integrity.

IP Spoofing

IP spoofing can yield access to user accounts and passwords, and it can also be used in other ways. For example, an attacker can emulate one of your internal users in ways that prove embarrassing for your organization; the attacker could send e-mail messages to business partners that appear to have originated from someone within your organization. Such attacks are easier when an attacker has a user account and password, but they are possible by combining simple spoofing attacks with knowledge of messaging protocols. For example, Telnetting directly to the SMTP port on a system allows the attacker to insert bogus sender information.

Establishing a Security Perimeter

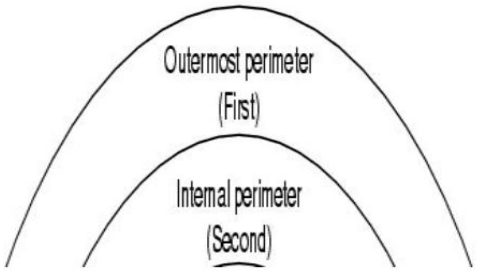
When you define a network security policy, you must define procedures to safeguard your network and its contents and users against loss and damage. From this perspective, a network security policy plays a role in enforcing the overall security policy defined by an organization.

A network security policy focuses on controlling the network traffic and usage. It identifies a network's resources and threats, defines network use and responsibilities, and details action plans for when the security policy is violated. When you deploy a network security policy, you want it to be strategically enforced at defensible boundaries within your network. These strategic boundaries are called perimeter networks.

Perimeter Networks

To establish your collection of perimeter networks, you must designate the networks of computers that you wish to protect and define the network security mechanisms that protect them. To have a successful network security perimeter, the firewall server must be the gateway for all communications between trusted networks and untrusted and unknown networks.

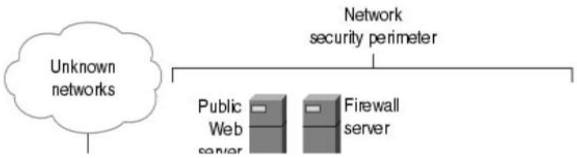
Three Types of Perimeter Networks Exist: Outermost, Internal, and Innermost



The outermost perimeter network identifies the separation point between the assets that you control and the assets that you do not control—usually, this point is the router that you use to separate your network from your ISP's network. Internal perimeter networks represent additional boundaries where you have other security mechanisms in place, such as intranet firewalls and filtering routers.

Figure depicts two perimeter networks (an outermost perimeter network and an internal perimeter network) defined by the placement of the internal and external routers and the firewall server.

The Diagram Is an Example of a Two-Perimeter Network Security Design



The outermost perimeter network is the most insecure area of your network infrastructure. Normally, this area is reserved for routers, firewall servers, and public Internet servers, such as HTTP, FTP, and Gopher servers. This area of the network is the easiest area to gain access to and, therefore, is the most frequently attacked, usually in an attempt to gain access to the internal networks. Sensitive company information that is for internal use only should not be placed on the outermost perimeter network. Following this precaution helps avoid having your sensitive information stolen or damaged.

Developing Your Security Design

The design of the perimeter network and security policies require the following subjects to be addressed.

Identify Any Assumptions

Every security system has underlying assumptions. For example, you might assume that your network is not tapped, that attackers know less than you do, that they are using standard software, or that a locked room is safe. Be sure to examine and justify your assumptions. Any hidden assumption is a potential security hole.

Understand Your Environment

Understanding how your system normally functions, knowing what is expected and what is unexpected, and being familiar with how devices are usually used will help you detect security problems. Noticing unusual events can help you catch intruders before they can damage the system. Auditing tools can help you detect those unusual events.

Make Security Pervasive

Almost any change that you make in your system may have security effects. This is especially true when new services are created. Administrators, programmers, and users should consider the security implications of every change they make. Understanding the security implications of a change takes practice; it requires lateral thinking and a willingness to explore every way that a service could potentially be manipulated.

References

[1]. "Using the Domain Name System for System Break-Ins" by Steve Bellovin, 1995

[2]. U.S. National Strategy to Secure Cyberspace, p. 30 February 2003

[3]. RIPE NCC DNSSEC Policy Department of Homeland and Security wants master key for DNS Heise News, 30 March 2007

[4]. Analysis: of Owning the keys to the Internet [UPI]], April 21, 2007

[5]. Shivlal Mewada, Umesh Kumar Singh and Pradeep Kumar Sharma, "Simulation Based Performance Evaluation of Routing Protocols for Mobile Ad-hoc Networks (MANET)", International Journal of Computer Science, Information Technology and Security, Vol. 2, No. 4, Aug 2012.

[6]. Dipali D. Punwatkar and Kapil N. Hande, "A Review of Malicious Node Detection in Mobile Ad-hoc Networks", International Journal of Computer Sciences and Engineering, Volume-02, Issue-02, Page No (65-69), Feb -2014, E-ISSN: 2347-2693

[7]. Shivlal Mewada and Umesh Kumar Singh, "Measurement Based Performance of Reactive and Proactive Routing Protocols in WMN", Int. Journal of advanced research in Computer Science and Software Engineering, Vol. 1, No. 1, pp(1-4), Dec.-2011.

[8]. M. Nachammai and N. Radha, "Survey on Black Hole and Gray Hole Attacks in MANET", International Journal of Computer Sciences and Engineering, Volume-04, Issue-05, Page No (66-70), May -2016, E-ISSN: 2347-2693

[9]. Leena Pal, Pradeep Sharma, Netram Kaurav and Shivlal Mewada, "Performance Analysis of Reactive and Proactive Routing Protocols for Mobile Ad-hoc Networks", International Journal of Scientific Research in Network Security and Communication, Vol-1, Issue-05, pp.(1-4), Dec 2013.ISSN 2321-3256,

[10]. Nisha Mannan and Shipra Khurana, "Comparative Analysis of Reactive Protocols in Mobile Ad-Hoc Networks", International Journal of Computer Sciences and Engineering, Volume-02, Issue-04, Page No (233-237), Apr -2014

[11]. M. Nagendra and B.Kondaiah, "A Comparison and Performance Evaluation of On-Demand Routing Protocols for Mobile Ad-hoc Networks", International Journal of Computer Sciences and Engineering, Volume-02, Issue-05, Page No (15-19), May -2014,

[12]. Ritika Kachal and Shrutika Suri, "Comparative Study and Analysis of DSR, DSDVAND ZRP in Mobile Ad-Hoc Networks", International Journal of Computer Sciences and Engineering, Volume-02, Issue-05, Page No (148-152), May -2014

[13]. Mayank Kumar and Tanya Singh, "A Survey on Security Issue in Mobile AD-HOC Network and Solutions", International Journal of Computer Sciences and Engineering, Volume-02, Issue-03, Page No (71-75), Mar -2014,

[14]. Umesh Kumar Singh, Shivlal Mewada, Lokesh Laddhani and Kamal Bunkar, "An Overview and Study of Security Issues & Challenges in Mobile Ad-hoc Networks (MANET)", International Journal of Computer Science and Information Security, Vol-9, No.4, pp.(106-111), April 2011.

[15]. Nand Kishore, Sukhvir Singh and Renu Dhir, "Energy Based Evaluation of Routing Protocol for MANETs", International Journal of Computer Sciences and Engineering, Volume-02, Issue-03, Page No (14-17), Mar -2014

