INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

NETWORK SECURITY AND THREATS IN MODERN ERA-REVIEW

MR. NIKHIL E. KARALE

ME, CSE, PRMIT, Maharashtra, India

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: One of the most difficult challenges in computer network is the computer network security .This paper presents the various network security and different threats, which causes to computer system. Almost all organizations and sectors are currently faced with the problem of insider threats to vital computer assets. Internal incidents can cause more than just financial losses. The three primary goals of network security which are confidentiality, integrity and availability are achieved by setting the security goal. The complexity of these functions can cause significant delays in the processing of packets, resulting in degraded performance, traffic, bottlenecks, and by violating Quality of Service constraintke.

Keywords: Network security, Confidentiality, Integrity, Availability.

Corresponding Author: MR. NIKHIL E. KARALE

Access Online On:

www.ijpret.com

How to Cite This Article:

Nikhil E. Karale, IJPRET, 2015; Volume 3 (9): 890-900

PAPER-QR CODE

INTRODUCTION

Part 1 - Evolution of Network Security and Prevention Techniques

The past few years have seen a radical evolution in the nature and requirements of network security. There are many factors contributing to these changes, the most important of which is the shift in focus from so-called 'network-level' threats, such as connection-oriented intrusions and Denial of Service (DOS) attacks, to dynamic. When the laptops are brought back into the office, the entire network is at risk since the user entered the network "behind the firewall". This is one of many reasons that an emerging "best practices" in secure network design is to segment the network into separate "security zones" such that attacks can be contained in the event of an outbreak, content-based threats such as Viruses, Worms, Trojans, Spyware and Phishing that can spread quickly and indiscriminately, and require sophisticated levels of intelligence to detect. There are several major drivers that are shaping the new security landscape:

1 - Increasing complexity in networks

Where a network 10 years ago might have consisted of a LAN connected to the Internet through a WAN connection, and maybe a few remote accesses or site-to- site VPN tunnels, the reality today is much more complex.

In addition, the workforce is becoming more mobile. From telecommuters who work from a home office to mobile workers who are never in a particular location for more than a day, this growing "distributed" model adds a significant amount of risk to the network. To help mitigate these risks, the IT manager must ensure that all remote locations and remote clients are protected with the same level of security as is present in the corporate network.

2 - Increasing sophistication of applications and attacks

Applications are growing in complexity. Where Windows NT launched with 5 million lines of code in 1994, Windows Vista has over 50 million… more than 1,000% growth! With this increased complexity comes increased vulnerability, particularly in server systems, which must be patched on a regular system.

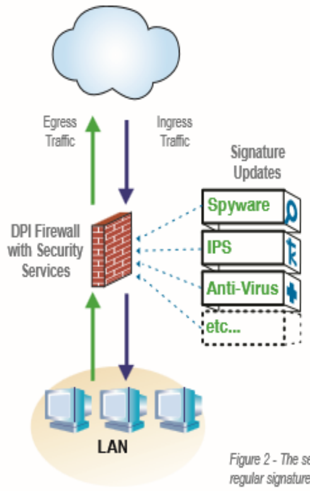
While applications are becoming more sophisticated, so are the attacks. A "serious" attack in the early 2000's might have consisted of a simple indiscriminate DOS attack aimed at restricting or temporarily disrupting network access. Today's serious attacks target applications themselves, and in many cases have goals of significant criminal intent, as is demonstrated by the Sasser worm described below.

Intrusion Attacks, Worms and Trojans:

The grand-daddy of them all, the universe of Intrusion attacks is wide and deep. Intrusion attacks are modern threats that target applications and application layer protocols (e.g. using the SMTP protocol to exploit a buffer overflow on an Outlook Exchange server), rather than the networks they are transported on (e.g. DOS attacks that utilize ICMP echo and TCP SYN floods). The security appliance is now a dynamic threat prevention system that requires constant, real-time updates to its attack signature libraries, URL lists, virus definition files, etc. to ensure the network.

Viruses:

Viruses (and Worms) are a class of attack whereby an infected attachment or download causes damage to a host system or network. The damage can range from minor (client DOS attack) to catastrophic (full-blown corruption of critical stored information or system registries).



A major impact of IPS (and the other DPI-oriented technologies described below) is that the security appliance is no longer a static element that sits in the network.

The security appliance is now a dynamic threat prevention system that requires constant, real-time updates to its attack signature libraries, URL lists, virus definition files, etc. to ensure the network is protected against threats that are present this hour... as well as those of last week, last month and last year.

Figure 2 - The security appliance is now a dynamic system that requires regular signature updates

There is also a new class of virus-related attack called a 'blended threat'. A blended threat is a 'perfect attack' whereby a virus is accompanied by a number of other attack and intrusion techniques to maximize penetration and damage. A good illustration of this type of attack is the So Big virus detailed below.

3 - Financial rewards for hackers with the advent of Spyware and Phishing:

The Internet has evolved from being a general information source to a critical enabler of international commerce. Because of the sensitive type of information that now flows freely over the Internet, a new breed of threat aims at obtaining this information… sometimes honestly and sometimes with malicious intent. Because the information obtained in these types of attacks has value, hackers are being financially compensated for their work, often by major public corporations; sometimes by organized crime. **Spyware:**

Spyware (and Adware) is one of the most misunderstood of the new generation of application-layer threats because there is no consensus on what defines a threat (or more appropriately, what the difference is between 'annoying' Adware and a true threat).

There are three general classes of Spyware:

Harmless-but-annoying:-Generally consists of actions such as changing the default home page of your browser, or unsolicited/untargeted pop-up ads.

Information-collecting:-Cookies are the most common type of information collecting mechanism, but simple keystroke and activity loggers are becoming more common. This class of Spyware is generally interested in collecting basic information about you, the sites you visit, and other preferences so that a 3rd party can send you targeted ads or promotions. There is generally not malicious intent, but many would call this an invasion of privacy.

Malicious:-Collecting private information with the intent of sending the information to a collection server. The information is collected, and sold to 3rd parties who have varying interests. Even today, this type of Spyware can be downloaded instantly on a Client device simply by visiting a URL… no further clicking necessary. This type of Spyware is illegal and critical for an organization to detect and stop. To further add to the complexity, there are three major Spyware delivery mechanisms:

Embedded Installs:- The most 'honest' of the three mechanisms, embedded installs are typically Spyware/Adware elements that are embedded into programs or services that are downloaded from the web.

Drive-by Installs:-In this method, a banner ad or popup attempts to install software on a PC, usually through the ActiveX controls distributed within Windows and by default enabled in Internet Explorer. Depending on the security settings on the PC browser, the Spyware downloads silently or was downloaded when the user clicked 'Yes' in the installer dialogue box.

In many cases, Drive- by's also take advantage of browser exploits that can force an unsuspecting PC browser to automatically download and execute code that installs the Spyware.

Browser Exploit:- As described above, targets vulnerabilities in the web browser code to install Spyware. A classic example is the Internet Explorer iFrame vulnerability. Because IE is such a targeted browser, many IT departments are migrating to alternate browsers such as Mozilla's Firefox. Client and server based Anti-Spyware software will detect and try to prevent users from accessing known bad sites, and to a limited extent provide more advanced functionality to detect suspicious behaviour from actual downloads and ActiveX controls. The software will also inspect individual system memory, system registries, start-up files and other stored items to detect and remove Spyware. While necessary, client and server based Anti-Spyware software is not enough.

Since Spyware is carried by so many delivery mechanisms and is getting so sophisticated, an additional gateway-based Anti-Spyware element is required

4 - Governmental regulations compliance:

Another important trend affecting network security is the growing number of governmental regulations in the US and abroad. One popular example of recent US regulation is the Health Insurance Portability and Accountability Act (HIPAA), which regulates how and when sensitive medical patient data can be transmitted. This regulation mandates that health organizations have Intrusion Prevention and secure connectivity (e.g. VPN) technologies in place to ensure conformance. Another recent US regulation is the Children's Internet Protection Act (CIPA), which aims at protecting minors from pornography, obscenity and other material harmful to minors. CIPA conformance mandates that all publicly accessible Internet connections are protected by URL and Web Content Filtering, which ensures only "proper" sites are accessible from the PC.

5 - Security as a tool to increase workforce productivity

One of the most profound impacts of security is how it is utilized across all types of organizations to increase operational efficiencies through enhanced workforce productivity. There are two main technologies that are helping achieve this:

Web Security and Policy Enforcement It is no longer a secret that a good amount of an average employee's day can be spent online doing non-work-related activities. Web surfing, online shopping, online gambling, stock trading and even online dating are a few of the more common uses of company Internet resources. In addition to workforce productivity and liability protection, URL Filtering technology is also the first line of defence at preventing users from accessing Spyware sites. As noted in the previous section, however, Spyware is a much more complicated problem than URL filtering alone can handle.

SPAM

Spam has grown into a major problem for all companies and organizations. Spam is especially problematic for public email addresses (listed on a website, for instance), or for common email addresses (support@your_company.com). Spam is also the primary delivery mechanism for Phishing attacks, so its importance has grown over the years. In 2006, over 86% of all e-mail was classified as spam. Over 63% of this spam originates from new or unknown sources.

Spam is best dealt with at the security gateway. The reason for this is simple once Spam emails are inside the network; they are already consuming precious network resources (such as storage, bandwidth and mail server CPU cycles).

Part 2 - Issues with Current Security Solutions

Whether dealing with Intrusion attempts through application buffer overflows, Spyware through drive-by installs, Phishing through deceiving emails or any of the other threats described in this paper, there is one capability the security appliance requires above all else: Deep Packet Inspection (DPI) intelligence.

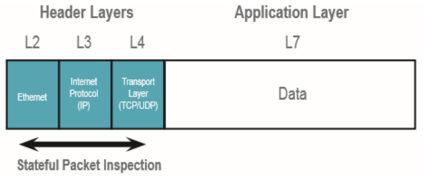


Figure 7 - Ethernet frame and how Stateful Packet Inspection (SPI) views it

As shown in the Ethernet frame above, Stateful Packet Inspection (SPI) essentially has access to Layers 3 and 4 of the OSI stack (sometimes Layer 2, as well). SPI firewalls perform the 'classic 5-tuple lookup'… that is, they scan and make allow/deny decisions based on:

1. Source transport layer address (typically TCP or UDP)

2. Destination transport layer address (typically TCP or UDP)

3. Source IP address

4. Destination IP address

5. Service type (e.g. FTP, HTTP, SMTP, and POP3)

What does this really mean? Using a Post Office analogy, the SPI firewall essentially looks at the to and from addresses on a package, as well as the package type (tube, box, letter, etc), and makes a decision about whether to mail the package based on pre-defined rules. There is no knowledge of what is inside the package.

The figure below shows the same Ethernet frame, but this time with application-layer information.

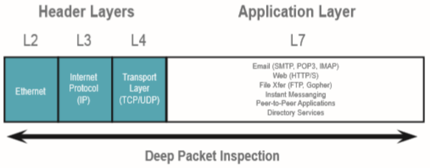


Figure 8 - Ethernet frame and how Deep Packet Inspection (DPI) views it

In addition to the classic 5-tuple lookup, DPI firewalls have "application awareness". Application awareness is a very broad term, but in general it means that the security appliance understands L7 protocols such as HTTP, SMTP, POP3, IMAP and FTP, and also understands the actual applications that rely on those protocols. For instance, Microsoft Outlook Exchange Server relies heavily on the SMTP protocol; Microsoft Explorer and Mozilla Firefox rely on the HTTP protocol, etc. In addition, there are custom protocols for applications such as Instant Messaging, Microsoft SQL Server, Oracle Server, Siebel, etc.

Part 3 - Current Network Security Alternatives

To protect against modern network threats, there are essentially two deployment architectures that are available to the IT manager:

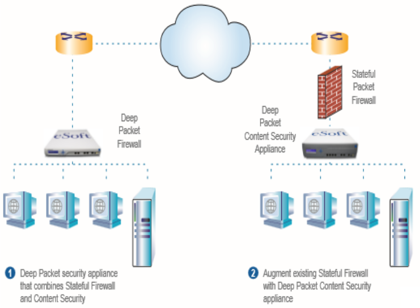

Stateful Packet Firewall
Deep Packet Firewall
Deep Packet Content Security Appliance
eSoft
eSoft
1 Deep Packet security appliance that combines Stateful Firewall and Content Security
2 Augment existing Stateful Firewall with Deep Packet Content Security appliance

Figure 9 - Modem alternatives for Deep Packet security

Part 4 - The eSoft Solution

Soft offers a complete line of next-generation Deep Packet Inspection security appliances that fit into either deployment scenario described above.

InstaGate Integrated Security Gateway

The InstaGate line Integrated Security Gateways provides state-of-the art Firewall and IPSec VPN functionality, in addition to DPI services such as Anti-Virus, Intrusion Prevention, Anti-Spyware and Anti-Spam. In addition, for the IT manager who wants FULL integration, many of the InstaGate products can be configured with optional office server elements such as Internet server, Email server, Webmail server and File/FTP and Print servers. InstaGate gateways currently integrate Deeper Packet security services than any other vendor on the market

ThreatWall Content Security Appliances

The ThreatWall is an award-winning platform that performs ultra-high-performance Deep Packet Inspection services such as Anti-Virus, Anti-Spam, Web URL Filtering as well as Intrusion Prevention, Anti-Phishing and Anti-Spyware. ThreatWall is tailored for networks with an existing Firewall/VPN system, and can be deployed either in-line in Transparent mode, or in an off-line proxy mode, making it exceptionally versatile for diverse network environments.

Figure 10 - InstaGate Integrated Security Gateways

SoftPaks and the SoftPak Director At the core of both the InstaGate and Threat Wall appliances is eSoft's patented (U.S. Patent No. 6,961,773 B2) and industry-renowned SoftPak and SoftPak Director (SPD) architecture for enforcing and managing Deep Packet Inspection services. As shown in Figure 12 below, SPD is the mechanism by which:

- Software services are added to the InstaGate and ThreatWall products
- Signature updates are automatically scheduled and downloaded to each device
- Subscription maintenance and billing is performed

ThreatPaks

Network ThreatPak

Modern network threats such as Spyware, Worms and Trojans were built to bypass traditional firewalls. Worse yet, technologies such as Instant Messaging (IM) and Peer to Peer networking have opened up serious holes in the security fabric that are incredibly hard to detect and prevent. The Network ThreatPak combines many of eSoft's proven security technologies to provide the network and its user's protection from the dynamic threats that cause network outages, Virus infections, Spyware installs and loss of intellectual property.

Features:

- Real-time Spyware Protection
- Active Intrusion Prevention
- Gateway Anti-Virus for Web and FTP
- Instant Messaging and P2P Application Control
- Myspace and Social Networking Application Control
- eSoft Distributed Intelligence Architecture Integration
- Detailed Reporting and Statistics

Web ThreatPak

Assure maximum workforce security and productivity by monitoring and enforcing the use of organizational Internet resources. Web ThreatPak also protects against legal liability brought on by inappropriate/illegal use of Internet resources. A database containing millions of global URLs is continually updated with web sites in 30 categories. Policy based control allows selection of which categories should be blocked at different times of day, and which users are affected.

SoftPaks

Desktop Anti-Virus / Anti-Spyware

This easy-to-deploy SoftPak, which combines full Anti-Virus and Anti-Spyware protection into a single, easy-to-manage client, is a key tool in protecting the organization from costly network outages caused by Viruses, Worms, Trojans and Spyware. Automatic signature updates an 'invisible' deployment ensure that users are always protected at the maximum level. The use may not uninstall the software.

Gateway Anti-Spyware

Gateway Anti-Spyware combines signature matching, intrusion prevention and web filtering techniques to detect and prevent Spyware from infecting the network, whether delivered by web, email or other delivery mechanisms. Infected computers on the internal network are also detected and blocked from sending private data to Internet collection sites. Proactive security at the gateway stops new Spyware infections, prevents confidential data from leaving the network and eliminates resource drains that result from reactive measures of constantly scanning and cleaning each computer on the network.

SiteFilter

Filters Internet content according to your organization's security policies and user guidelines. It allows you to manage Internet access ranging from simple access restrictions to complete blocking of any site. SiteFilter includes a base access control list of more than four million URLs covering 12 languages, all categorized into 40 different content groups, ten of which you can define and customize. In combination with Threat Wise Technology, SiteFilter enables implementation of highly customized and detailed access restrictions-by category, user, day, and time-for improved business productivity and liability control.

CONCLUSION

The evolution of network and application-layer security threats has significantly altered the requirements for modern network security architecture. Just a few years ago, a simple Stateful Packet Inspection (SPI) Firewall was sufficient to stop basic attacks such as port scans and DOS attacks. To detect and prevent these threats, a completely new kind of security system is required. This system still performs all of the classic functions of the firewall, but much more. This system is based on Deep Packet Inspection (DPI) technology, where the appliance has the brains - and the horsepower- to inspect every bite of every packet… even across multiple thousands of streams of packets.

ACKNOWLEDGMENT

The work has been guided by Prof. Gupta sir, ME cse, PRMIT, Maharashtra India. The Authors would like to thank all the concerned people.

REFERENCE

1. C. Chen, P. Maniatis, A. Perrig, A. Vasudevan, and V. Sekar, “Towards verifiable resource accounting for outsourced com- putation,” in Proc. of ACM VEE, 2013

2. Z. Wang, C. Wu, M. Grace, and X. Jiang, “Isolating commodity hosted hypervisors with hyperlock,” in Proc. of EuroSys 2012.

3. G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T. Shimeall, and L. Flynn, “Common sense guide to mitigating insider threats, 4th edition,” Software Engineering Institute, Carnegie Mellon University, Tech. Rep. CMU/SEI-2012-TR-012, 2012.

4. M. Salem, S. Hershkop, and S. Stolfo, “A survey of insider attack detection research,” Insider Attack and Cyber Security, pp. 69–90, 2008.

5. B. Lampson, “A note on the confinement problem,” Communications of the ACM, vol. 16, no. 10, pp. 613–615, 1973.