Vulnerability-Focused Threat Detection: Protect Against the Unknown

Vulnerabilities and threats are being discovered at a pace that traditional exploit-based attack detection technology cannot meet. Vulnerability-focused detection technologies provide the solution to this problem with broader threat detection, fewer signatures, and day-zero detection capabilities. This paper describes the difference between exploit-focused and vulnerability-focused detection and how Cisco® intrusion prevention systems (IPSs) use vulnerability-focused detection to provide comprehensive threat protection.

Introduction

This paper is intended for IT security staff and security managers considering deploying or expanding the deployment of intrusion detection systems (IDSs) or IPSs in their organization; analysts and researchers looking for information on detection technology; and security consultants and other security professionals who desire a deeper insight into the advantages of Cisco IPS technology.

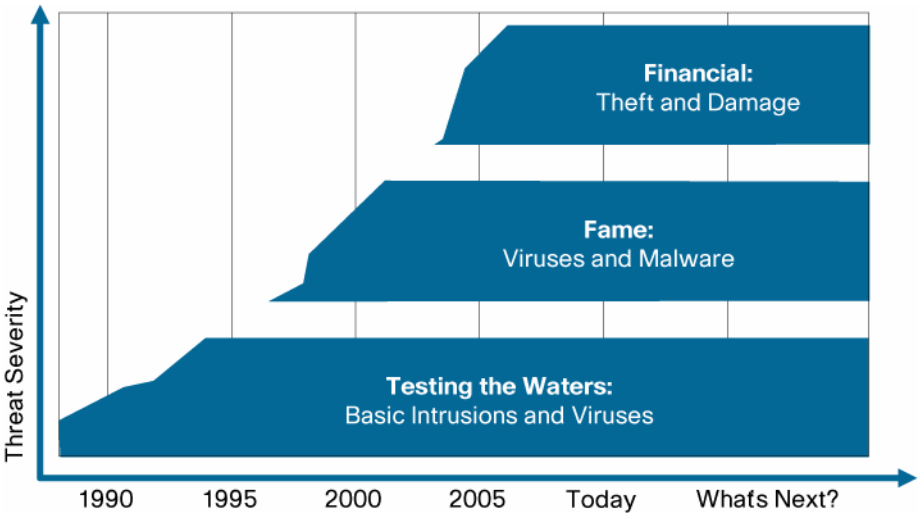
The main points made in this paper are:

- Vulnerability-focused signatures detect a wide range of day-zero threats, obfuscated attacks, and exploit variants without frequent intrusive updates or large signature counts.
- Exploit-focused systems detect known exploits but require a large number of signatures to remain up-to-date; ultimately, these systems provide inferior protection as they still miss new and altered attacks.
- Cisco has more than 10 years of IDS and IPS development experience, with a seasoned team of signature developers writing effective vulnerability-focused signatures that block even the most determined attacker.

The Evolution of Intent in Network Hacking

In the past, network attacks were aimed at creating disruption and inconvenience, for “settling scores,” or providing notoriety for hackers. Now, professional hackers, intelligence groups, and criminal organizations create attacks designed to exploit programming errors (bugs), design flaws, or insufficient protections in network applications to provide unlimited access to network devices or computers for purposes of financial gain through data theft, identity theft, spam distribution, intelligence-gathering, DDoS attacks, and numerous other potential criminal uses. Figure 1 shows this transition.

Figure 1. The Evolution of Intent: From Hobbyists to Professionals



Exploit-Focused Detection: The First Generation

Vulnerability: A weakness or flaw in a computer application, operating system, or protocol that can be exploited to cause the application to operate in a manner unintended by its designers. A single vulnerability can be targeted by hundreds or thousands of different exploits.

Exploit: An attack program used by malicious hackers to exploit a vulnerability, usually for the purpose of running arbitrary code on a target system. Exploits comprise a large range of potential attacks, from HTTP commands designed to extract data from or imbed malware on Web servers, to buffer overflow attacks that can cause target systems to run arbitrary software.

IDS solutions were initially designed to look for suspicious behavior such as scanning activity, multiple login attempts, and anomalous traffic behavior. This approach still works well when there is a highly skilled operator with the time, knowledge, and tools to analyze the data and discover patterns of potential abuse.

However, hacking tactics have shifted toward more active exploitation of application vulnerabilities for the purpose of compromising hosts. To meet this challenge, IDS solutions added a new defense: exploit-focused signatures. Exploit-focused signatures are static (unchanging) pattern matching signatures that identify well-known exploit code as they cross the wire.

IPS operators use these capabilities to stop well-known attacks and old, fast-moving worms such as Slammer, a simple, 404-byte UDP packet or Nachi, a simple ICMP Echo Request worm consisting of a few dozen bytes of repeated data in an ICMP packet. In fact, one of the reasons that there have been so few outbreaks in the last few years[1] is that the exploit-focused approach has been effective in stopping unsophisticated worm attacks. However, as the nature of attacks has shifted from fame to profit, the attacks become more sophisticated and the limitations with an exploit-focused approach became increasingly apparent.

[1] IronPort: 2008 Internet Security Trends

The Problem with Exploit-Focused Detection

Although the limited exploit-focused approach can be useful for basic “traffic sanitization,” it has several basic flaws; most importantly, its inability to detect attacks with variations in their structure at the network or protocol level. By making even small changes in the payload or headers of the attack, an attacker can completely bypass the detection capabilities of an exploit-focused signature and gain unlimited access to sensitive servers.

Another popular way for attackers to evade exploit-focused systems is by using one or more encoding techniques that cause the attack to appear differently on the wire but decode the same way at the client. This technique is easily demonstrated with a brief discussion of Unicode, a common HTTP encoding construct used by Web servers to represent non-English characters. To illustrate the point, we can examine a number of Unicode byte encoding variations. For example, consider the letter “c.” Three basic forms exist to represent “c” (using hexadecimal notation).

```
Single-byte encoding:   %63
Double-byte encoding:   %c1%a3
Triple-byte encoding:   %e0%81%a3
```

In addition, older versions of Microsoft IIS allow base 36 encoding, an encoding error where the Microsoft UTF8 decoder accepts 36 characters (A–Z and 0–9) as valid hexadecimal characters in the UTF8 encoding instead of the normal 16 characters (A–F and 0–9). In the following example, the (normally) illegal character “0xJ” is interpreted as a hexadecimal “0x13.” A “Z” is interpreted as a “0x23,” which is used in the second example. The third line demonstrates the use of triple-byte encoding plus base 36 encoding to create a further obfuscated example.

```
Microsoft 36: %5J   %5 + J (0x13)   %63
              %4z   %4 + z (0x23)   %63
              or %cw%o1%q3
```

Some versions of IIS can also accept double encodings, meaning that the individual characters used to describe the encodings can themselves be encoded. For example:

```
Starting with %63
              % can be encoded 48 different ways
              6 can be encoded 48 different ways
              3 can be encoded 64 different ways
%63 has 147,456 different ways to be represented
```

Microsoft also has an additional way to represent UTF characters called “%u encoding” for encoding wide Unicode streams. Again, to represent the letter “c”:

```
Single-byte encoding: %63     %u0063
Double-byte encoding: %c1%a3  %uc1a3
```

In combination, these encodings can create literally millions of variations for the same set of characters. An exploit-focused detection technology cannot provide protection for this. Even

simple encoding variations make it impossible for an exploit-focused detection system to discover encoded attacks. The only choice of action for an exploit-focused system in this situation is to choose to cover certain known exploits and those generated using specific test tools. At best, this provides some protection against unsophisticated attackers and acceptable results in test tool-based evaluations. In reality, this provides a false sense of security and places your network at high risk from attack.

Exploit-focused detection methods also suffer from a need for frequent updates. Since new signatures must be created for every new exploit that is discovered, frequent updates are a necessity to maintain up-to-date protection, a process that creates additional overhead and disruption for users. This also increases the signature count, creating additional space and processing requirements on the IPS itself.

Vulnerability-Focused Detection: The New Generation of IPS Technology

Rather than focusing on the unbounded problem of discovering, cataloging and writing signatures for new exploits, vulnerability-focused detection systems focus on protecting the vulnerabilities that criminals are attempting to exploit (see definitions sidebar). This approach is much more complex and requires detection techniques that can look for indications that a transaction may actually be attempting to exploit a known (or potentially unknown) vulnerability.

Although the vulnerability-focused approach is more difficult to implement, it provides vastly better protection than exploit-based methods. The greatest advantage is that since a vulnerability-focused signature is designed to look for exploitation of a specific vulnerability, any potential exploit or exploit variant will trigger the signature, be it a test tool, known attack, obfuscated exploit, or entirely new (day-zero) attack.

Vulnerability-focused signatures not only detect day-zero attacks, but can also catch day-zero vulnerabilities in some instances. An example of this is a signature 5477.2 for Cisco IPS. This single signature detects 38 different exploits and vulnerabilities accessible through Microsoft Internet Explorer, including a large number of ActiveX vulnerabilities and associated exploits. As another example, signature 5813 for the Microsoft Internet Explorer VML vulnerability protects against 19 different verified exploits.

Table 1 shows the exploits and vulnerabilities that a single vulnerability-focused signature can cover.

Table 1. Single Vulnerability-Focused Signature Covers 38 Verified Exploits and Vulnerabilities

Cisco IPS Signature 5477-2: Possible Heap Payload Construction		
Vulnerabilities	**Public Exploits**	**Non-Public Exploits and Tools**
Microsoft Internet Explorer window Arbitrary Code Execution Vulnerability	[Metasploit] mozilla_compareto v1.3	[Non-Public] IE MS06-42 Patch Exploit
CVE-2006-1359 MS April—Cumulative Security Update for Internet Explorer	[Metasploit 2.5] mozilla_compareto 1.3	[Non-Public] MS Internet Explorer 6/7 (XML Core Services) Remote Code Exec Exploit 3
MS06-071—Microsoft XML Core Service XMLHTTP ActiveX Control Remote Code Execution Vulnerability	[Metasploit] Mozilla Firefox Memory corruption via QueryInterface on Location, Navigator objects	[Non-Public] IE XML HTTP Exploit
CVE-2007-0024 [MS07-004] Vulnerability in Vector Markup Language Could Allow Remote Code Execution	[Metasploit] ie_createtextrange v1.4	[Non-Public]: Firefox and Mozilla compareTo

Cisco IPS Signature 5477-2: Possible Heap Payload Construction		
Vulnerabilities	**Public Exploits**	**Non-Public Exploits and Tools**
CVE-2007-3040 [KB938827] Vulnerability in Agent could allow Remote Code Execution	[Metasploit] Multiple Mozilla Products Memory Corruption/Code Injection/Access Restriction Bypass Vulnerabilities firefox_queryi	[Non-Public] MS Windows (.ANI) GDI Remote Elevation of Privilege Exploit (MS07-017)
CVE-2007-3902 [KB942615] Cumulative Security Update for Internet Explorer	[Milw0rm] IE COM Object Heap Overflow DirectAnimation.PathControl	[Milw0rm] Yahoo Messenger Web Cam Exploits
CVE-2007-5344 [KB942615] Cumulative Security Update for Internet Explorer	[Milw0rm] MS Internet Explorer (VML) Remote Buffer Overflow Exploit (SP2) (pl)	[Non-Public] Microsoft Speech API ActiveX control Exploit
CVE-2007-3903 [KB942615] Cumulative Security Update for Internet Explorer	[Milw0rm] MS Internet Explorer WebViewFolderIcon setSlice() Exploit (pl)	[Non_Public] McAfee Subscription Manager ActiveX Exploit
	[Milw0rm] MS Internet Explorer WebViewFolderIcon setSlice() Exploit (c)	[Non-Public]: IE createTextRange() exploit v1.3
	[Milw0rm] Yahoo! Widget < 4.0.5 GetComponentVersion() Remote Overflow Exploit	[Non-Public]Yahoo Messenger YVerInfo.dll ActiveX Multiple Remote Buffer Overflow Vulnerabilities
	[Milw0rm] McAfee ePolicy Orchestrator ActiveX Exploit	[Non-Public] Mozilla Firefox InstallVersion.compareTo() Overflow
	[Milw0rm] MS Internet Explorer 6/7 (XML Core Services) Remote Code Exec Exploit 2	[Non-Public] Microsoft Internet Explorer window() exploit 1.6
	[Milw0rm] MS Internet Explorer VML Remote Buffer Overflow Exploit (MS07-004)	[Non-Public] IE VML buffer overflow exploit update 1.6
	[Milw0rm] Yahoo! Music Jukebox Remote exploits (3)	[Non-Public] Media Player PNG header overflow exploit
		[Non-Public] Microsoft Agent MS07-051 Exploit Update
		[Non-Public] AskJeeves Toolbar 4.0.2.53 activex Remote Buffer Overflow Exploit

Vulnerability-focused signatures have additional advantages over traditional exploit-focused IPSs, including fewer signatures and less frequent updates. Signatures only need to be updated when new vulnerabilities are discovered; updates are not needed as frequently, reducing the disruption and testing overhead created by systems with more frequent updates. This is in sharp contrast to exploit-focused systems that can sometimes require daily updates to stay current.

Vulnerability-focused detection technology does have disadvantages. The signature may not be able to identify the exact exploit being used. For example, a buffer overflow attempt may not be positively identified as a specific attack. For analysts that desire additional insight into the specific attack tools being used, the vulnerability-focused approach supports adding additional exploit-specific signatures to identify known attacks. This can aid analysts in identifying new day-zero attacks.

Vulnerability-focused signatures are also much more difficult to create than exploit-focused signatures. A large and experienced team of security analysts is needed to discover, validate, and analyze new vulnerabilities and create new signatures to effectively detect exploitation. Cisco has more than 10 years of experience developing IDS and IPS solutions and a large, global team of security analysts working 24x7 to discover new vulnerabilities, understand the evolving threat landscape and create sophisticated detection technologies.

Conclusion

Vulnerability-focused detection systems are markedly superior to earlier exploit-focused detection systems. The ability of exploit-focused IPSs to process packets quickly is more than outweighed by the inability of those systems to detect and block new attacks, their excessive signature counts, and their need for overly frequent signature updates. Vulnerability-focused IPSs detect multiple exploit variants, obfuscated attacks, and day-zero attacks, providing truly comprehensive, superior protection from the threats of today and tomorrow.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-470178-00 05/08