Defending Against Cyber Attacks with Session-Level Network Security

May 2010
**Executive Summary**

Threat actors are determinedly focused on the theft / exfiltration of protected or sensitive information including digital assets and/or identity information, and are continually evolving their attack methods to bypass organizations security countermeasures. Traditional network security tools based on packet inspection and/or signatures have struggled to address custom attacks, attacks above the protocol layer, and attacks that take advantage of user behavior.

Because of this, threat actors are using more custom “zero day” attacks, moving the attack technology further up the architecture to the application layer, and often targeting users’ activity through both technical and social mechanisms. These evolved threats, often from talented and persistent adversaries, have made it challenging for traditional threat mitigation measures (e.g., firewall, IDS/IPS, A/V) to mitigate risks, and require a new approach to counter these advanced cyber attacks.

Fidelis XPS™ provides an important layer of defense to the network security infrastructure by providing real-time session-level visibility and control for outbound and optionally bi-directional communications, to protect sensitive information from breach, whether to leakage, theft or exfiltration. As the threat has evolved to target applications and end users, deep packet inspection technology have failed to keep up.

The Fidelis XPS Deep Session Inspection™ technology platform provides visibility and control from the protocol through enterprise content to ensure protected and sensitive information is protected. Fidelis XPS controls include port-independent inspection covering all 65,535 ports on multi-gigabit speed networks; content inspection for protected / sensitive information; content inspection for malicious traffic and payloads; port-hopping / tunneling detection; data flows to unexpected countries; and rogue encryption at both the network and file level.

These robust controls enhance the network security architecture enabling pro-active prevention of cyber attacks and more efficient incident response, resulting in more comprehensive protection of protected and sensitive information from cyber attacks.

**Threats have Evolved Past Packet and Signature Approaches**

The threat landscape has changed. Motivations have gone from fame to profit and espionage. Threat actors have evolved from individuals to sophisticated organizations including nation states, terrorist groups, and organized crime. Targets, and therefore the associated attacks, have moved from being broad in scope to being incredibly focused on a single organization or type of information. Goals have moved from embarrassment and denial of service to exfiltration or theft of high-value information. Technical means have moved from virus and worms to customized malware, phishing, application layer, and social attacks.

Despite this incredible evolution in the threat, many organizations still rely on dated firewall, intrusion prevention system (IPS), and signature anti-virus controls which are insufficient to mitigate the risk today. A new approach to these problems is needed.

**Custom & “Zero Day” Attacks**

As the targets have become more focused, so have the attacks. Traditional viruses and worms were designed to infect as many people as possible, and were often very “loud” about their actions by sending e-mails, taking down services, and other very visible activities. These “loud” attacks enabled a reactive security industry whose success was measured by how fast they could react with a new signature when a new threat appeared, typically in an anti-virus or IDS/IPS...
solution. The resulting signature was based on having an index case or primary case, for which to base the signature on. While this approach may help contain these loud, broad risks, it has failed to address the threat evolution that has ensued.

As threat actor motivations have changed, so has their attacks. Sophisticated threat actors realized years ago that the majority of enterprise security defenses required the attack to have been seen “in the wild” in order for a signature to exist. This has formed an entire new domain of research and development inside of malicious actors including nation states and organized crime, as well as a new industry available for outsourced malware creation. This research has resulted in many new names for malware—designer malware, customer malware, rootkits, Trojans, polymorphic malware, and others. However, they all of one key attribute it common—the ability to evade signature detection, which can be accomplished by a variety of methods ranging from running at levels of the systems where it cannot be detected, changing attributes to avoid signature detection, or true custom malcode that has never been seen before and therefore would never have a signature. These attacks have become common place. Cyveillance’s 1H 2009 Cyber Intelligence Report reveals that traditional antivirus (AV) vendors fail to address these new threats, with testing showing that more than half of active malware threats on the Internet continue to go undetected and an average detection rate of 29 percent for malware attacks. Additionally, the AV-Comparatives most recent retrospective/proactive test showed results ranging from 32-74% effectiveness. We need to look beyond signatures for a solution.

Application Layer Attacks

Another key trend in the attack landscape has been the movement of the attacks up the architecture to the application layer. According to SANS research, “during the last few years, the number of vulnerabilities being discovered in applications is far greater than the number of vulnerabilities discovered in operating systems.” This is particularly troublesome as the attacks have moved to focus on theft or exfiltration of information, the application is a natural layer to conduct those operations. In particular, these exploits have focused on common applications including browsers, Microsoft Office®, and other common components like Adobe PDF and Flash.

This focus has led to a significant struggle for traditional security infrastructures. First, many signature vendors struggle to have the visibility, knowledge, and/or integration required to act at higher levels of the architecture. The wide variety of potential configurations and versions alone plays well to the attacker, not the defender. When operating at the packet and signature level, trying to manage state, decompression and complex analysis is often not even possible, and the limited cases where it can be done becomes highly computationally expensive, which is difficult to address as network bandwidth continually increases. Beyond the challenges of the security tools themselves, most organizations also struggle greatly with patching applications. The above SANS report also states that “application patching is much slower than operating system patching, given the attacker a longer time to exploit the vulnerability.”

Attacking the User: Social Engineering

Another disturbing trend in attacks has been the focus on attacking the end user directly. Years ago, attacks were focused at the system level and tried to avoid any interaction with the user. However, many attacks today focus on the end user directly, taking advantage of end user behavior which can allow for a very effective attack without any security flaws in the underlying infrastructure—making traditional signature and infrastructure security highly ineffective. Historically social engineering was an offline activity, but over the past few years it has become a
key element of many attacks. Phishing, and its derivates including targeted spear-phishing, whaling, and pharming, exploit users to visit false sites and share sensitive information which could be valuable itself, but also often collects passwords and other knowledge useful in expanding the attack. Phishing is just one form of the social engineering attacks being carried out today by advanced threat actors. Social networking sites are filled with fake profiles waiting for users to connect and trust the malicious actor behind the profile. Many applications in the new “app economy” evolving on social networking platforms and consumer devices are being used to harvest sensitive information, often via innocuous quizzes. Traditional social engineering still exists too.

Value of Session-Level Network Security

Traditional network security controls like firewall, IPS, and gateway anti-virus are widely deployed and adequate to keep historic threats at bay, but are insufficient to mitigate the risk today. These legacy controls are often the key line in defense against these evolved threat actors, many of whom have access to sophisticated R&D resources. Antivirus and the associated dependence on security signatures date back to reactions from the Brain virus in 1986. With the launch of the firewall in 1988 packet inspection came to life. Intrusion Detection Systems (IDS) delivered deep packet inspection commercially in 1997, though government research dates back to the 1980s. The first IPS which brought control to deep packet inspection was delivered in 1998. While the adversary innovates, the majority of security infrastructures continue to use very dated technology as their primary defense.

Rather than continuing to focus on the packet, regardless of how deep, a solution that provides insight beyond the packet is needed to protect information and defend against new methods used to evade traditional security technologies. On the network, the new requirement is session-level security—the required functionality to have the visibility to applications and content necessary to prevent attacks.

By operating at the session-level, an entirely new level of visibility and control is available. At this level, more robust knowledge of the application is available, payload in attachments and compressed files can be analyzed and the full enterprise human-readable content can be inspected. This provides completely new context to the security decision making process, opening new avenues for defending computer networks. This value can be seen in four key areas:

Content Protection

With robust access to the full enterprise human-readable content, organizations can now make decisions about the true content of the session, not just its attributes or metadata. As mentioned before, today’s attacks are about the information itself, so knowledge of its use is a critical control to protect it. Data breaches have become a daily news item, ranging from loss of personal identity information to valuable digital assets and intellectually property. Regardless of the source of the breach, from inadvertent or accidental data leakage to malicious theft or exfiltration of information, knowledge of the information transferred provides a critical component of the context required to protect our valuable information.

Application Activity Control

As attacks have moved up the application layer, understanding details about not only what the application is, but also the context of how it’s used is critical to computer network defense. The session level presents unique visibility beyond the protocol into the application (many applications
share common protocols lower in the stack), the user, and the context of its use. This knowledge of channels and applications running on the network and their attributes gives an organization the ability to control particular features of applications (e.g., no file transfers in IM, no chats in social networking), as well as block high risk applications from the network, even if they masquerade as other services (e.g., Skype, p2p). This helps mitigate the risks presented to sensitive information by these applications.

**Encryption Policy Enforcement**

While encryption is often thought of as a key method in data protection, it unfortunately can also be used for nefarious activities too. Generally, most network security technologies cannot decrypt network traffic in real-time for all traffic. Some solutions do exist to inspect “official” encryption at the web or mail gateways, but they only see a subset of the actual encrypted traffic on the network. However, just because encrypted traffic cannot be completely inspected, it doesn’t mean that it should be ignored. At the session-level of the network, there are key attributes available to help determine what encryption is being used to protect information from rogue encryption used to subvert security controls. These include key attributes like cipher type, key strength, sender, recipient, application/protocol/port, and session attributes, which are available both for session level encryption (e.g., SSL, SSH) and file encryption (e.g., ZIP, Office, PGP). These attributes can be used by a session-level network security solution to identify and prevent rogue encryption to subvert security controls.

**Threat Mitigation**

The session-level also provides access to knowledge required to identify broad new threats. Talented actors, particularly ones funded by nation states, are well aware of the limitations of packet level inspection, and therefore have embedded attacks at the application level. Session-level network security provides the insight needed to detect attacks buried deeper inside of file formats, provides robust analysis of compressed files, and both binary and text analysis contents of varying file “containers.” Additionally, methods used to obfuscate and nest objects to bypass packet and signature technologies are available for policy application at the session level. Finally, as attacks target user behavior versus technical flaws, the content protection capabilities above become an important component of threat mitigation.

**Preventing Cyber Attacks with the Fidelis Extrusion Prevention System®**

The Fidelis Extrusion Prevention System, Fidelis XPS™, is the premier session-level network security solution providing visibility and control to prevent these evolved attacks.

Based on a patented Deep Session Inspection™ engine, Fidelis XPS provides comprehensive port-independent session and content visibility and control. With bi-directional inspection and prevention for all 65,535 ports, it enables organizations to prevent cyber attacks by protecting content, controlling application activity, enforcing encryption policy and mitigating threats.

These capabilities enable organizations to automate critical information protection and security processes in computer network defense, security operations centers and incident response teams.
Identifying Attacks

The first step to stopping attacks, even with automated prevention, is to identify the attack. Fidelis XPS provides the ability to identify (as well as prevent) attacks and compromised hosts based on:

- Content protection identifying transfers of sensitive or protected information;
- Application activity control and threat mitigation identifying non-normal or high-risk network traffic or files transferred.

In many cases, Fidelis XPS is able to be the primary source identifying the attack. However, the comprehensive network awareness at the session level provided by Fidelis XPS can also be externalized to event correlation engines. With highly customizable interfaces to share alert metadata via standard formats including syslog, CEF, SNMP, and SMTP, Fidelis can make security information and event management (SIEM) systems content and session aware, as well as provide important metadata to help identify the highest priority incidents to address.

Containing Attacks

Once an attack is identified, containing it so it doesn’t spread further or successfully exfiltrate data is critical. As Fidelis XPS has all-ports prevention capabilities, it provides a critical role in this area.

If the attack was identified by Fidelis XPS, but only in an alerting mode, Fidelis XPS can determine the cause of the breach and:

- Use application activity control and threat mitigation to analyze and, if desired, block rogue network communications;
- Use Fidelis XPS alerts to identify systems involved;
- Use content protection to identify the information transferred, and if desired, prevent further transfers of information.

Fidelis XPS also gives an organization additional value by containing attacks that may have been identified in other area. Forensics investigations may reveal information about attacks that cannot be addressed at the packet level on the network. Fidelis XPS capabilities in content protection, application activity control, encryption policy enforcement and threat mitigation provide the ability to bring to life threat intelligence derived in the forensics process on the network that wasn’t possible before session-level network security.

Eradicating Attackers

Finally, eradicating the attack and returning to non-deprecated operations is critical. While very similar to containing (above), it is important to put in safeguards to ensure the attack will not be successful again in the future. Fidelis XPS provides critical capabilities to eradicate the attack on the network by:

- Using content protection to prevent transfers of sensitive of protected information;
- Using application activity control and threat mitigation to block malicious communications (e.g., Command & Control, propagation);
- Using threat mitigation to block malicious payloads based on knowledge from the attack and/or compromised systems.
About Fidelis Security Systems

Fidelis Security Systems provides organizations with the power to leverage their sensitive information while protecting it from data leakage and cyber attacks. Built on a patented deep session inspection™ platform, the Fidelis Extrusion Prevention System® is the industry's only next-generation network security solution with the visibility and control necessary to stop data breaches by uniquely working at the session-level. Fidelis enables their government, military, and commercial enterprise customers around the globe to achieve comprehensive information protection in real time on multi-gigabit speed networks—allowing them to protect content, control application activity, enforce encryption policy, and mitigate threats. Learn more about Fidelis Security Systems by visiting www.FidelisSecurity.com.

FIDELIS SECURITY SYSTEMS, FIDELIS EXTRUSION PREVENTION SYSTEM, FIDELIS XPS, the FIDELIS SECURITY SYSTEMS logo, and/or other FIDELIS SECURITY SYSTEMS products referenced herein are trademarks of Fidelis Security Systems, Inc. Copying, use or distribution of any material contained herein is expressly prohibited. Copyright © 2010 Fidelis Security Systems, Inc. All rights reserved.