

THE EMERGENCE OF THE VULNERABILITY SHIELD

A Spire Research Report – April 2003

By Pete Lindstrom, Research Director



Spire Security, LLC
P.O. Box 152, Malvern, PA 19355
www.spiresecurity.com

Executive Summary

Security professionals are constantly looking for the “holy grail” of security products. They have bought firewalls, vulnerability assessment tools, and intrusion detection systems (IDS), hoping to find the ultimate security tool. The truth is much more difficult – security is an ongoing process that involves multiple layers of protection.

Individual security tools on their own each play an important role in securing the enterprise. But there is more value to be had with a solution that can link the solutions together and share the various types of information available. This means that the vulnerability assessment tool can identify the exposures in a computing environment; an IDS solution can limit its coverage to attacks against only those vulnerabilities; and a firewall can block attacks as they occur.

This white paper discusses the strengths and weaknesses of individual security solutions, then addresses ways to leverage the strengths of each into a cohesive whole known as a **vulnerability shield**. Finally, it discusses the characteristics of ipANGEL, Lucid Security’s vulnerability shield solution.

About Spire Security

Spire Security, LLC conducts market research and analysis of information security issues and requirements. Spire provides clarity and practical security advice based on its “Four Disciplines of Security Management,” an operational security model that encompasses identity management, trust management, threat management, and vulnerability management. Spire’s objective is to help define and refine enterprise security strategies by determining the best way to deploy policies, people, process, and platforms in support of an enterprise security management solution.

This white paper was sponsored by Lucid Security. Spire Security maintains its independence regarding the content and assertions that is the product of years of security audit, design, and consulting work.



The Emergence of the Vulnerability Shield

Table of Contents

State of Security Affairs.....	1
Tools of the Trade	1
Vulnerability Assessment Tools – Probing for Weaknesses	2
Firewalls – Protecting the Perimeter	2
Intrusion Detection Systems – Sniffing the Traffic	2
Leveraging Security Investments	3
From point products to security solutions.....	3
VA becomes useful	3
IDS becomes smarter	4
Firewalls become more effective	4
Introducing the Vulnerability Shield.....	4
The Lucid Security Approach	5
Introduction	5
The Four Steps to a Vulnerability Shield.....	5
Spire ViewPoint	6



State of Security Affairs

It is no secret that an “unprepared” host (i.e. one without strong security measures) connecting to the Internet will be potentially attacked within hours. We expect that. But these attacks are not always planned – they are random reconnaissance scans, programmed to constantly monitor the Internet and identify new targets. Attackers often focus on targets of opportunity; it doesn’t matter whether a site is “important” or not, if it is vulnerable, it provides another notch on the hacker’s belt and can be enlisted into the zombie army for some future denial-of-service attack against another unsuspecting site.

Through the years, information security has generally evolved to meet the needs of enterprise computing infrastructures. As client-server and network computing became popular, vulnerability assessment solutions provided a way to evaluate the various configurations of the multiplying hosts and servers across the network. Basic Internet connectivity brought with it the need to protect the trusted network from the public Internet, and thus firewalls became common. As more and more services are offered across the Internet, intrusion detection systems are gaining a place inside networks to monitor the residual flow of traffic.

We are at a point where the “tools of the trade” are useful but not complete. We are always looking for bigger budgets and more resources in pursuit of complete security. Another option is to leverage the existing security investments. On their own, each of these investments is functional but deficient in some way. Together, they can be leveraged to create some new synergies.

Tools of the Trade

The three primary tools for protecting servers from attack mentioned earlier – vulnerability assessment tools provide proactive security evaluations; firewalls form the foundation of perimeter defense; and intrusion detection systems constantly monitor systems and seek out malicious activities – are obvious candidates for evolution as they are combined in new effective ways. Each of these tools must be reviewed in further detail to fully understand their strengths and weaknesses.



Vulnerability Assessment Tools – Probing for Weaknesses

Vulnerability assessment (VA) solutions identify weaknesses and exposures in a computing environment. They scan systems looking for two basic classes of problems: configuration problems that can be exploited to gain information or control over a system and missing patches that fix known security bugs in software programs. Each violation of specific problems or risk to “best practices” is added to a laundry list of vulnerabilities for evaluation and remediation.

VA tools are the main source of proactive security measures that can be taken to secure an environment. They provide the most strategic insight into exposures of the computing environment. Although identifying weaknesses, VA tools fall short in remediation and management. Such tools rely heavily on manual work effort to identify, prioritize and remediate vulnerabilities. Additionally, some weaknesses can not be mitigated or mitigated in a timely manner. In some cases a vulnerability must remain active, such as when services are mission critical and a patch is not ready or it must be tested prior to remediation.

Firewalls – Protecting the Perimeter

Firewalls provide the foundation level of perimeter defense. They monitor network traffic and act as a basic gatekeeper, letting in traffic that meets the screening rules, typically based on IP address and/or destination port, and blocking everything else. The firewall defines the perimeter between trusted and untrusted systems, providing a comfort zone within which more sensitive operations can be performed while limiting the exposure to the external network.

But the traditional firewall is designed to work at layer three and layer four, operating as a basic filter of network traffic. Because the firewall has long been a stalwart on the perimeter; attackers have learned to bypass it by preying on open ports like port 80 for the web or port 25 for email. Nowadays, they attack higher-layer protocols to infiltrate a system, and then use their “insider” status to further exploit systems and send back useful information. In order to remain effective, firewalls will eventually evolve to inspect these higher level protocols.

Intrusion Detection Systems – Sniffing the Traffic

Intrusion detection systems (IDS) are constantly monitoring network traffic, seeking malicious packets. They attempt to match

patterns against a packet or sequence of packets or identify protocol and traffic anomalies based on predefined rules and known behavior.

IDS solutions rely on performance and intelligence for success – they must be fast enough to evaluate packets flowing across today’s networks (and ready for tomorrow) and smart enough to be able to identify malicious activity, and the next attack, from that constant barrage of data. IDS solutions are myopic in one very specific sense – they only focus on attacks. Any attack that meets the criteria of an IDS gets the same treatment, regardless of its likelihood of success. For example, an attack exploiting an Apache vulnerability in a pure Microsoft environment receives the same treatment as an IIS attack. The result is a level of inefficiency that consumes valuable time and resources.

Leveraging Security Investments

The value of the security solutions immediately increases when they are tied together.

From point products to security solutions

Each of the tools described above – firewalls, intrusion detection, and vulnerability assessment – address specific needs and provides solid contributions to the strategic security solution. But each on their own requires time and management attention and does not provide the level of security that can be gained if they are combined into a cohesive whole. As the security world evolves, these tools can be combined in ways to maximize their effectiveness. We describe ways in which these solutions can be maximized.

VA becomes useful

Vulnerability assessment tools, as much as they are a strategic asset to a security program, stop at the point of providing a “to do” list for overworked IT personnel. When vulnerabilities are remediated, the VA tool has done its job. Now, even without remediation vulnerability assessment solutions can provide a significant contribution by providing the target information necessary to an IDS solution that can then identify attacks that will cause damage. This approach ignores those attacks that will not succeed because the vulnerability being exploited doesn’t exist – either it has been mitigated or never existed in the first place. The end result is a

significant reduction in false positives and a focus on the attacks that matter.

IDS becomes smarter

IDS solutions are constantly being challenged in two areas – performance and false positives. These two areas work with each other to magnify the problems of IDS. While network bandwidth continues to increase, attacks are becoming more complex. Taken together, these requirements create an insatiable appetite for more processing power.

False positives serve to add to the problems on the incident response side. The complexity of today's attacks signals a need for prudence in identifying potentially malicious traffic. This leads to false positives.

An IDS that can identify “shots fired” can sound the alarm, but also creates extra work. When combined with vulnerability information about specific targets, precision IDS ensures that the shots being identified are those that have the greatest likelihood of success. Leveraging vulnerability information allows IDS to focus its efforts and thereby eliminate extra work.

Firewalls become more effective

Firewalls act as static gatekeepers on a dynamic perimeter, allowing and denying packets based on basic rules. IDS solutions typically provide deeper packet analysis and evaluation. A link between an IDS and firewall creates the ability to have dynamic rulesets that are more precise and effective. This capability extends the usefulness of the firewall into a new paradigm that is evolutionary in nature. Still the foundation of perimeter security, it now can act and react in response to threat levels. It is clear that the firewall will benefit significantly from its continuing evolution into a more comprehensive security solution.

Introducing the Vulnerability Shield

When the capabilities of individual point products are coordinated into a cohesive unit, the full solution becomes a vulnerability shield. This shield is not so much a new type of product as it is the logical evolution described above – the combination of vulnerability assessment, intrusion detection, and firewall products. With its specific task laid out for it – to identify and block attacks that will be successful if not stopped – vulnerability shields

become a powerful contributor to the enterprise security architecture.

The Lucid Security Approach

Introduction

Lucid Security was formed with evolution in mind. Its ipANGEL™ solution leverages the continually evolving capabilities of firewalls with intrusion detection systems and vulnerability assessment solutions to create a fully integrated vulnerability shield that monitors traffic destined for exposed systems. ipANGEL was designed specifically for Check Point Software Technologies Ltd's FireWall-1®.

The integration of ipANGEL with FireWall-1 is a multifaceted one. Other approaches are offered as solutions independent or nearly independent of the firewall. However, rather than duplicating processes of FireWall-1, the ipANGEL design takes into account the strengths of the firewall and focuses on what the firewall doesn't do.

The firewall, long the keystone of a secure perimeter, is continually evolving and has been charged with enforcing the state and integrity of the traffic which passes through it. IP attacks, including spoofing and fragmentation, Denial of Service (DoS) attacks including SYN flooding, and network probing such as port and service scanning, among many other types of information gathering and exploitation attempts are challenges FireWall-1 has risen to meet.

With the firewall defending protected networks against the aforementioned traffic, ipANGEL is able to utilize its full resources to identify and inhibit malicious activity directed towards applications it has determined are susceptible to exploit.

The Four Steps to a Vulnerability Shield

Functionally, ipANGEL uses the four basic steps below:

1. Build list of potential targets

First, ipANGEL performs a database query of FireWall-1 via the Check Point Management Interface and captures the rules identifying all systems and services that can be accessed from external sources. These are the potential attack points of an intruder or malicious program.

2. Scan for vulnerabilities in identified systems

With the explicit knowledge of systems and services being offered via the public Internet, ipANGEL performs a scan of the systems themselves to identify vulnerabilities. This second layer of intelligence augments the list of attack points with a list of specific vulnerabilities that are exposed.

At this point, the specific weaknesses in systems that may be targeted by outside sources are exposed. These are the “Achilles Heel” of an enterprise.

3. Create attack database

After gaining explicit knowledge of weaknesses, ipANGEL then builds its IDS signature database by identifying exploits against the known vulnerabilities in the enterprise being protected. With its database of targets available, the ipANGEL system shifts into “precision IDS” mode to identify attacks against these targets that exploit these vulnerabilities. As a side benefit, ipANGEL provides the enterprise with vulnerability data for patching and system hardening purposes, although ipANGEL protects the network until the vulnerability is mitigated.

4. Monitor and block activity

Operating passively, ipANGEL monitors for the specific attacks to which the network’s systems and services are vulnerable. When ipANGEL identifies an attack that is likely to succeed in exploiting a specific vulnerability on a system that is accessible from external sources, it leverages Check Point’s Suspicious Activity Monitor (SAM) API to drop traffic from the offending source IP address.

Before initiating the four-step process (usually daily), Lucid Security’s ipANGEL automatically updates its list of applicable tests and signatures for newly discovered vulnerabilities and attack exploits so that all information is up-to-date.

Spire ViewPoint

It is clear that today’s security tools are useful to the security professional. But it is also clear that the lines between the various capabilities of these tools are blurring. As attacks become more complex, it is crucial to identify the traffic that can harm an enterprise. The solution lies at the juxtaposition of firewalls, vulnerability assessment solutions, and intrusion detection systems – the vulnerability shield.

Lucid Security's ipANGEL is the glue that makes these tools work together. It is not a vulnerability assessment tool, but uses the information to its advantage, to distinguish between attacks against vulnerable systems and services and attacks against vulnerabilities that don't exist in the environment. It is not a firewall, yet it works with the firewall to block the traffic, making the firewall an integral part of its solution. And it is not an IDS solution, because it is only looking for specific attacks - those to which the environment is vulnerable. This solution is a vulnerability shield, the evolution of products into an intelligent security solution.

Contact Spire Security

To comment about this white paper or contact Spire Security, LLC about other security topics, please visit our website at www.spiresecurity.com.

This white paper was sponsored by Lucid Security. Spire Security maintains its independence regarding the content and assertions that is the product of years of security audit, design, and consulting work.