Host-based Intrusion Prevention Systems and their Place in Securing the Enterprise

By Brian O'Higgins

A TOUGH CHALLENGE

Information security has never been a tougher challenge. At the same time that organizations are providing deeper access to their networks to employees, partners and customers enabling flexible work environments and more efficient business relationships—organizations are faced with an increasingly hostile threat environment as well as rising complexity associated with corporate and regulatory compliance.

Internet-based attacks against enterprise networks are unrelenting, more sophisticated and, because today's attackers are motivated by profit, more dangerous to the data those networks hold. Not only has the frequency and likelihood of an attack increased, so has the nature of attacks. Compared to a few years ago, there have been significant changes with respect to where attacks are originating and what attackers are exploiting. Today, a greater percentage of attacks are occurring over the network and software vulnerabilities have become the primary point of attack (FIGURE 1). (Sources: zone-h.org and Secunia.com Feb 2005)

The rising threat environment is not the only thing driving the increased security risks. The consequences of a security breach are also fueling this escalation. The costs can be very significant, in direct costs as well indirect costs including lost productivity, erosion of brand equity as well as consequences associated with regulatory issues.

In today's environment, lawmakers and regulatory agencies have made it clear that confidential data must be protected. Individuals and organizations have no alternative. The penalties for failure are severe and not strictly financial, as they may also include criminal, class action and civil legal actions against the organization and its directors.

There are many regulations that impact your organization depending on your business. These include the Health Insurance Portability and Accountability Act (HIPAA) that requires protection of medical information, the Gramm-Leach-Bliley Act (GLBA) requiring banks to protect consumer information, California Senate Bill 1386 that requires disclosure of any breach of personal information, and Sarbanes-Oxley (SOX), that obliges companies trading on U.S. exchanges to attest that internal controls relating to financial systems are in place to ensure accurate reporting. U.S. federal departments and agencies are required by the Federal Information Security Management Act (FISMA) to implement "risk-based, cost-effective approaches to secure their information and systems, identify and resolve current IT security weaknesses and risks, as well as protect against future vulnerabilities and threats."

FIGURE 1: ORIGIN AND TYPES OF ATTACK

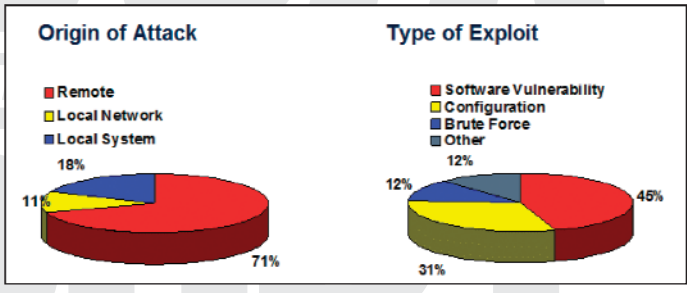


TABLE 1: FIVE TOP SECURITY SOLUTIONS BY COMPANY SIZE

Ranking	Small business	Midsize business	Large business
1	New firewalls	Firewall upgrades	Firewall replacements
2	Antivirus renewals	Intrusion detection	Intrusion detection
3	Security event monitoring, auditing and reporting	Security event monitoring, auditing, and reporting	Security event monitoring, auditing and reporting
4	Intrusion prevention	Antivirus renewals and upgrades	Antivirus upgrades and replacements
5	Antispyware and VPNs	Intrusion prevention	Intrusion prevention

Source: Aberdeen*Group*, March 2005

Of all the external regulatory pressures facing large and midsized companies in the U.S., SOX is the most pressing. This year most of these organizations will undergo testing of internal controls that are required by SOX. Small business and offshore firms that trade on U.S. based exchanges have been given another year to comply.

Regulatory compliance is not an absolute, rather it is a negotiation with the auditors and the company to demonstrate that adequate controls are in place. Limiting and segmenting access to sensitive corporate and customer data are at the heart of the IT security solutions that are the most relevant security controls. Accordingly, sensitive data on servers undergoes close scrutiny. Network security infrastructure and tools are among priorities for IT executives for the next year. Table 1 shows the priority list ordered by company size, according to research done by the Aberdeen Group.

Virtually all organizations deploy network defenses to establish a security perimeter or multiple security zones. Generally this includes firewall, anti-virus and network intrusion detection capabilities. Unfortunately due to the nature of modern networks and the sophistication of attackers, perimeter security defenses are easily circumvented and no longer adequate. As soon as one hole is patched, another one shows up.

To this point, the last few months have shown a trend for attacks that target vulnerabilities in web applications. These applications encompass the class of technologies that deliver information from backend application servers, up through web servers, and to the end user through a browser interface. As a result, web services greatly expand the number of potential attack points within the enterprise. According to the most recent Symantec Internet Security Threat Report, approximately half of the total vulnerabilities disclosed in the last 6 months of 2004 affected web applications.

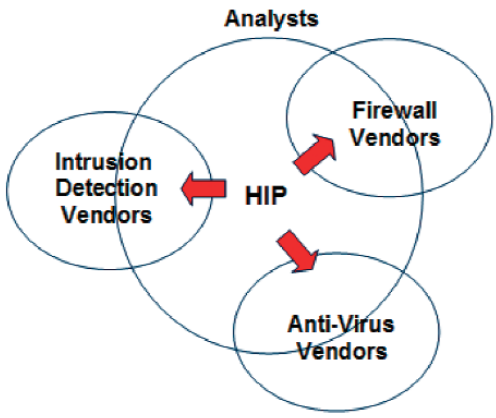
Application level threats range from generic worms that impact a wide set of systems, to more targeted and sophisticated attacks such as SQL command injection attacks. Firewalls and virus scanners cannot detect or prevent these and similar attacks. The malicious code appears to be normal port 80 web traffic that goes through to the web server. Even more worrisome, these attacks can also go through encrypted VPN tunnels and authentication infrastructures, and enjoy a protected ride right through to the vulnerability in the application. Similarly, firewalls by necessity have open ports to allow email, ftp, or perhaps other applications. In each case, attack traffic can reach the end server easily.

To address these deficiencies, organizations have turned to patching as quickly as possible as a means of eliminating vulnerabilities—unfortunately this is a race that attackers regularly win. More and more vulnerabilities are being published, enabling attackers to create more malicious code in a shorter period of time, often before software vendors create and release patches. With the proliferation of new and easy-to-use hacking tools, the skills necessary to launch attacks is decreasing. Complex servers are difficult to patch on a timely basis and the interval between a patch being announced and malicious code appearing is becoming extremely short. In fact, the average duration between notification of a vulnerability and the arrival of exploit code is now less than 10 days. In the case of the Santy worm in 2004, it was 1 day.

Patching entails risk—IT administrators need to properly test and schedule patches to minimize disruption. The fear that a hastily deployed patch could cause a major business disruption is very real and dictates a minimum amount of effort and time to ensure the cure isn't worse than the problem.

Additionally, patching cannot protect organizations against vulnerabilities they are not aware of. Often referred to as unknown vulnerabilities—the risk is the result of an attacker becoming aware of a vulnerability and launching an exploit before either the application vendor knows of the problem or has created a patch and notified all the potential targets. Exploits taking advantage of unknown vulnerabilities represent a significant percentage of successful attacks and it is clear that organizations need to turn to compensating controls other than patching for protection. An important compensation control is to deploy Host-based Intrusion Prevention systems (HIP).

FIGURE 2: COMPETING DEFINITIONS OF HIP



INTRUSION PREVENTION AND DEFENSE-IN-DEPTH STRATEGY

Given the ways that the traditional network perimeter can be breached, today's security best practices implement a defense-in-depth strategy. The last line of defense can be considered to be HIP solutions on the servers themselves.

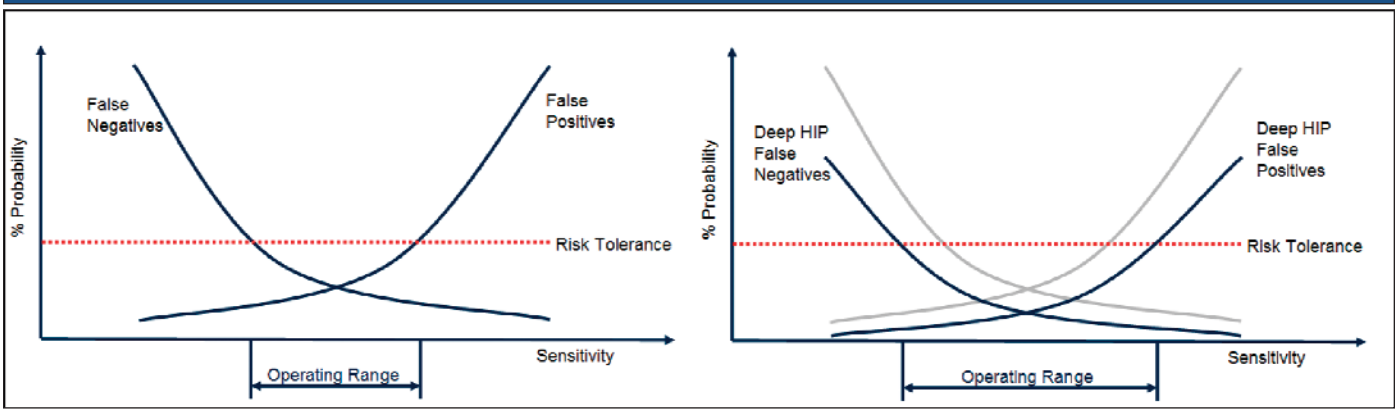
Defense-in-depth assumes that no single component, policy or process can assure security. The modern computing environment is too complex and diverse. Attackers have access to the same vulnerability bulletins as everyone else, and a growing range of automated tools with which to exploit them. The potential risk of failure and regulatory penalties requires security managers not just to arm themselves against a minimum standard of documented threats but to anticipate the unknown: in effect, to 'prove a negative,' and show they are not insecure.

While providing many of the same proven security technologies used in perimeter security, such as firewall and anti-virus scanning, HIP solutions also protect applications by means of application data input validation and application behavior control to provide comprehensive host protection. While HIP solutions are relevant to basically anything with an IP address, they are particularly effective in environments subject to high threats, such as the DMZ where probes and attacks are frequent, or high value hosts, or other hard to patch environments that remain vulnerable longer until they are finally patched.

While the need to provide a last layer of defense at the host itself is easily understood, there is currently confusion over what constitutes a HIP product. Security vendors and analysts have all jumped into the fray, each positioning a slightly different view of what constitutes HIP technology, including existing technology such as firewalls, Intrusion Detection Systems (IDS) and anti-virus signature based approaches (FIGURE 2).

Even among analysts there are varying definitions of HIP that focus on different attributes, for example some identify technology such as heuristic-based systems that learn a normal behavior, and trigger on anomalies.

FIGURE 3: ADVANTAGES OF IMPROVED ACCURACY



A broad definition of HIP is simply security capabilities deployed at the host to effectively keep it running, free from viruses, worms or other malware. This broad definition provides a lot of leeway in what would be considered HIP technology. The key, however, is overall effectiveness. Accordingly, HIP solutions need to embody the following characteristics:

- Comprehensive Protection
- High Performance
- Robust Security
- Low Cost of Ownership

COMPREHENSIVE PROTECTION

While many first generation approaches suffered from being too specific in terms of supported platforms or the types of threats and vulnerabilities they protect against, an effective HIP solution must be comprehensive. This includes host coverage with two dimensions, a wide range of platforms as well as a wide range of target applications.

With new vulnerabilities and corresponding exploits being created all the time, breadth of attack coverage is critical not just for providing adequate protection for today's attacks, but also to protect against future attacks.

A key consideration that organizations should take into account when looking at attack coverage is level of risk. Any two attacks or classes of attack are not necessarily equal in terms of the risk they pose to a host, and should not be considered equal when evaluating HIP products. For instance, many attacks need a certain sequence of events to occur in order to succeed. In host environments, the sequence of events for one type of attack may already be prevented by other protection mechanisms or the probability of them occurring may be extremely low.

Remote versus local attacks are a classic example of this challenge. In many cases a local attack, although potentially originating remotely, requires a specific action to occur at the host before the attack is successful, such as running a particular service or surfing to a specific web site. Organizations may have existing controls in place for their servers such as physical security, operator training or configuration management that greatly reduces the risk in these cases. Most remote attacks, on the other hand, are not prevented by such measures and pose a greater risk to server environments. HIP products need to be particularly effective for the range of remote attacks.

There are a number of organizations providing valuable insight into classifying attacks and providing information to help organizations assess their risk. In particular, the Open Web Application Security Project (www.owasp.org) and the Web Application Security Consortium (www.webappsec.org) offer a starting point for evaluating product coverage.

HIP solutions need to be tuned for greater accuracy. This is usually measured by ability to prevent false negatives and false positives. False negatives occur when malicious traffic is not prevented by the control. False positives on the other hand, occur when the control prevents legitimate system execution or data traffic. These two error types trade off one another. As the sensitivity of a control is increased to lower the incidence of false negatives, the incidence of false positives increases. Conversely when control sensitivity is lowered in order to reduce the incidence of false positives, the incidence of false negatives increases.

Both from security and operational perspectives, neither false positives nor false negatives are desirable. While the security group may be naturally driven to dialing down false negatives, the operational group wants to dial down false positives. There will always be this natural tension, and policies will be specific to particular hosts, for example a web server in DMZ will have a different policy than a mail server. Both false positives and false negatives drive overall operational cost and effective HIP solutions should deliver superior accuracy in terms of zero, or near-zero, incidents of each as well as a broader operating range to reduce the need for continually tuning the system.

HIGH PERFORMANCE

While it is important to provide excellent protection at the host, if it comes at the cost of host performance it will either not be used or significantly add to overall cost as system architecture is modified to compensate.

To avoid this problem, HIP solutions must provide high throughput but only consume a small fraction of host resources and behave in a predictable way—allowing the operations group the confidence that the host will continue to operate as desired while at the same time ensuring they operate securely.

ROBUST SECURITY

The security guard is often the first to be attacked, and the same applies to security controls. Software based security in particular must be difficult to evade or disable.

An effective HIP solution eliminates threats and defeats attacks before they have had the chance to penetrate the host. This means solutions that provide in-line protection as close to the network layer as possible and eliminate both known and unknown attacks will be more secure. Some

implementations are signature based (similar to signature based anti-virus protection), and of course these only work if the signature has been published. These systems will be evaded by unknown attacks.

LOW COST OF OWNERSHIP

While security controls must reduce business risks to an acceptable level, organizations are concerned with both the cost of the risks being mitigated, and the cost of the control itself. HIP solutions must offer low cost of ownership in order to make sense in the overall risk equation.

Costs include acquisition and maintenance costs, as well as the overall operating impact. In many cases the operating impact has been large, especially for some first generation HIP solutions. Several operating characteristics that have a high impact on cost include:

- Accuracy—if a solution doesn't provide the needed accuracy, responding to false positives or negatives drives up costs.
- Performance—if the impact is significant it drives up additional expenditures.
- Operational Intrusiveness—if a solution directly impacts "normal operations" it can significantly drive up direct and indirect costs. Ideally operational impact is minimized. For example, a non-intrusive system does not hinder OS or other upgrades, is easily testable and reversible, and easily tunable as the threat environment changes. Conversely, HIP solutions should not require lengthy training periods or require a machine or service re-boot to take effect.

DEEP HIP

Much has been learned from first generation HIP approaches. Additionally there are a number of traditional security technologies, such as firewalls and signature based systems, that when deployed at host offer HIP. Individually, many of these technologies offer value but do not go far enough in solving the overall problem. However, taken together, they provide a very effective "Deep HIP" approach.

CONCLUSION

Today, attackers can analyze vulnerability and develop an exploit so quickly that traditional protection is inadequate. With no patch to plug the hole, or no signature to identify and block the malware, the enemy is within the gates before you know it. And the problem is becoming more critical. Even while security managers struggle to protect their networks, senior management is demanding greater openness through mobile computing, wireless networking, and Web applications to deliver closer online relationships with suppliers and customers.

With an organization's regulatory compliance, corporate reputation, brand and customer satisfaction at stake, it is imperative that HIP be considered a critical part of the overall information security strategy. Companies should evaluate potential solutions to ensure they are doing everything they can to mitigate the growing risk to their organizations.

NaSPA member Brian O'Higgins is a founding member of Third Brigade, a company focused on Host Intrusion Prevention.