

## AUTHOR PROFILE:

**KEVIN PRINCE,**  
CHIEF TECHNOLOGY OFFICER

Named Chief Technology Officer of Perimeter in 2009, Kevin Prince spearheads the company's technology strategy and leads the technical team in working closely with its customers to manage all of the complexity and compliance requirements of securing information across the enterprise.

With more than 19 years of expertise in Information Technology and 11 years focused on Internet security, Mr. Prince is an evangelist on Internet security topics, including network security threats, fraud, identity theft, cyber terrorism and data breaches. Through regular speaking engagements, webinars, whitepapers and blog postings, Mr. Prince is dedicated to educating organizations on how to manage information complexity, meet increasingly stringent compliance and security requirements, and mitigate risk. Mr. Prince has trained federal examiners for several years.

# SECURING CRITICAL SYSTEMS WITH HOST-BASED INTRUSION PREVENTION

When I first started explaining to people how HIPS can improve their overall information security posture, they looked at me kind of strange. I soon realized that in their minds some of them thought about belly dancers, others Elvis and his famous hip gyrations, and still others thinking of the more recent Shakira and her "Hips Don't Lie" mainstream hit.

HIPS is the acronym for Host-Based Intrusion Prevention System. When people refer to it that way, they focus on the "Intrusion Prevention" portion and not on the "Host-Based" part. In other words, people hear "Intrusion Prevention" and say, "Oh, I already have that." HIPS is very different from Intrusion Detection and Prevention Systems, which are typically network-based. Network-Based IDS/IPS systems (often called NIDS or NIPS) usually attempt to detect attacks across an entire network or network segment. In-line IDS devices monitor traffic as it passes through them and IPS devices can even block or stop malicious traffic. Passive IDS devices listen to all the traffic on a given network or network segment and can send alerts when malicious packets are detected.

HIPS is software that is loaded onto mission critical systems that can protect those systems much better than network-based technology solutions. This is important because many people still have the mind set that because they have a firewall and Network-Based IDS, they are safe from hackers.

Most companies use security devices such as firewalls and Network IDS/IPS devices to protect their networks and systems. These security solutions are necessary for a strong security posture. However, some of the latest and most advanced attacks by cyber criminals can literally bypass and subvert these systems. Hackers use a variety of techniques to accomplish this, all of which can be grouped into two different categories:

1. Criminals use simple techniques to get users to compromise their own systems.
2. A series of very sophisticated inbound attacks that are difficult to detect through traditional network-based security solutions.

## SELF COMPROMISE TECHNIQUES

There are several methods criminals use to get individuals to compromise themselves. This includes home computers, work computers, laptops, and even smartphones. Here are a few of the most popular methods:

- **Phishing** attacks use "lures" which can include emails, IMs, SMS texts, social network sites, or a host of other methods to send a message that includes a file or link that when clicked can install malicious software, giving the hacker full control of the system.
- **Pharming** is a technique where the hackers compromise systems that can redirect your computer when trying to access a resource. For example, they may change the DNS (domain name server) address for www.mybank.com and redirect you to a site that looks like your bank, but the site captures your credentials and/or installs malicious software on your system.

# SECURING CRITICAL SYSTEMS WITH HOST-BASED INTRUSION PREVENTION

- **SEO Poisoning** is a method whereby criminals alter the results that Google, Bing, Yahoo, or other search engines may present to you and when clicked may redirect and/or compromise your system.
- **Drive by downloads** are popular for criminals as well. This is where you access a legitimate web site that has been compromised by hackers. The hackers have injected malware that is triggered simply by viewing the web site, completely compromising your system.

Some Network-Based IDS/IPS systems are designed to look for attacks after the system has been compromised. These would be signatures that attempt to match on the outbound traffic rather than the inbound traffic. Cyber criminals usually use encryption protocols to disguise their outbound connections while using standard firewall ports to remain under the radar. As a result, IDS/IPS systems that rely on outbound traffic signature match are less effective than a few years ago.

Then there are the more difficult-to-execute techniques, but these do not rely on a user making a mistake or waiting for someone else. A couple of these include:

- **Packet sequencing** - When one computer is communicating with another computer it sends the information in numbered packets. Numbers are used to put the packets back in their original order so it can be understood by the receiving computer. Many Network-Based IDS systems work based on "signature match", in other words they are looking for a specific data packet or sequence of packets. A hacker can use a process to scramble the packet sequence numbers so they are not sent in the normal order. This effectively tricks the IDS system because it cannot perform a match while the end system can simply look at the packet numbers and rebuild it in the proper order.
- **Encoding** - A method of changing elements of the packet in a way that do not change the message on the receiving side but are different enough to evade an IDS. For example, the Unicode equivalent of a space (when you press the space bar) is "%20". So all spaces can be replaced with a %20 in a message. If the IDS signature is not designed to "normalize" the traffic by replacing all %20s with a space, it may miss the attack.

Due to the sophistication and variety of methods hackers can now employ, we must move our security protection on to the systems that we are trying to keep safe. This is why the endpoint security market has exploded recently and why Host-Based Intrusion Detection and Prevention is so effective. Because HIPS is loaded directly on the computer you are trying to protect, sequencing, encoding, encryption and most other methods do not work.

HIPS agents work using either signature analysis, behavior based analysis, or both.

## SIGNATURE ANALYSIS

Signature analysis works similar to a Network-Based IDS in that it attempts to match specific requests to a database of known hacker exploits. When a match is made, alerts can be sent, mitigation techniques employed, or both.

# SECURING CRITICAL SYSTEMS WITH HOST-BASED INTRUSION PREVENTION

## BEYOND DETECTION

Most people today understand the difference between IDS and IPS. IDS simply detects and alerts while IPS can actively stop the attack. People often ask me why anyone would want IDS and not IPS. There are some good reasons why IDS should be employed in specific network environments where topology, bandwidth, or other considerations must be made. There was a time when IPS had a lot of “false positives”. In other words, the IPS would make a mistake and block something it wasn't supposed to. For a time, this made people shy away from using them. However, it has been several years since that was any kind of a major problem. So getting the benefit of real-time protection is of immense value.

HIPS will block malicious activity in real-time and because it is loaded on the system you are trying to protect, it has a much greater ability to stop the attack or malicious behavior.

## HIPS SYSTEMS

As I said before, HIPS should be loaded and used on specific systems, not on every system in your network. It should be loaded on “mission critical” systems which I define in this case as:

- Active Directory or other authentication systems where you user accounts are stored
- Internet facing systems such as email servers, web servers, FTP servers, or other systems that can be directly accessed from the Internet
- Systems that store customer or employee non-public information
- Other systems that you consider vital to the operation or integrity of your business

## MONITORING

Like other security solutions, it is important to have your system monitored 24x7 by properly trained information security specialists. Most organizations do not have this level of resource in-house, therefore outsourcing it to a qualified managed security service provider (MSSP) is critical. Without the management and monitoring, HIPS is just another piece of software that you load that has minimal value. In the hands of a proper security expert that can tune, manage, and monitor the system, you will get the highest level of protection you can get on an individual system.

## BREACHES

There are endless numbers of data breach incidents that would have been avoided if the company would have been using HIPS on the critical systems in their organizations. TJMaxx, Hannaford, Heartland, and many others could have avoided the class action lawsuits, loss in stock price, reduction in revenue, reputation loss, fines, fees, and everything else associated with a data security breach if they would have used HIPS.

Many hackers rely on malware getting installed on a system that allows them to remotely control, capture data, and secretly send it out of the company. A properly installed and monitored HIPS agent utilizing signature and behavior-based technologies can detect this type of behavior and stop it. When comparing the cost of a few HIPS agents loaded on key systems in your network to the cost and impact of a data breach, it becomes crystal clear that now is the time to use this technology.