Ozone – Host Intrusion Prevention System

White Paper
May 2004

Author: Eugene Tsyrklevich, Chief Technical Officer

SYNOPSIS

This White Paper examines why current security products, such as anti-viruses, firewalls and Intrusion Detection Systems (IDS), are failing to protect organisations from the new breed of computer attacks.

It also provides an in-depth look at Host Intrusion Prevention Systems, a new security technology that is able to effectively combat the ever-growing number of new security threats.

The paper consists of two parts:

Part I

A round up of current security technologies, how they work and how they fail to protect modern day organisations.

Part II

An examination of Host Intrusion Prevention Systems (HIPS), including detailed information on Security Architects' new software product, Ozone.

PART I: WHY CURRENT DEFENCES ARE INADEQUATE

Over the past few years, there has been a sharp rise in the number of reported vulnerabilities and worms. According to Microsoft, the computer worm Blaster was single-handedly responsible for successfully infecting over 8 million computers around the world.

To combat these security threats, the majority of organisations utilise existing reactive security products such as firewalls, Intrusion Detection Systems and anti-viruses. Yet, these solutions have proved to be ineffective and have left many organisations at the mercy of malicious computer attacks.

The main reason existing security technologies fail to protect organisations from emerging security threats, is that they rely on incomplete or inaccurate information. Some rely on analysing network traffic, others use signatures of known attacks, whilst some combine both. But, none of these technologies can effectively protect organisations from the new breeds of computer worms and other malicious attacks.

Anti-Viruses

Anti-viruses are undoubtedly one of the oldest and most ubiquitous security technologies on the market. Anti-viruses work by scanning computer files for signatures of known viruses and other malware.

As multiple new viruses are released every day, virus signatures constantly need to be updated.

Apart from looking for signatures of known viruses, anti-viruses can do little else to protect computer systems from a myriad of other security threats (e.g. buffer overflows or application specific attacks).

Overall, anti-viruses can be used to protect desktop computers against known virus threats, but they are unable to protect client and server computers from more sophisticated attacks.

Firewalls and Perimeter Security

The next most widely used security tool is a firewall.

The majority of organisations protect their networks and computer systems by focusing on hardening their perimeter security. Unfortunately, internal computer systems are left completely unprotected.

More often than not, an organisation's perimeter security consists of a firewall that blocks all incoming network connections and allows all outgoing connections. These configurations protect an organisation's internal systems against attacks originating from the Internet. Some perimeter security configurations might also include a second firewall (the so called DMZ deployment) that provides an extra security layer to protect server farms.

Of course, attackers know that a firewall is not the weakest link in the security chain. It is far easier to attack an organisation by sending an employee an email with a trojaned attachment, by exploiting a client application (such as Internet Explorer) or simply by finding another way into the network (e.g. through a dial-up or a VPN link) that bypasses the firewall altogether.

These threats were highlighted by recent worms such as Sasser and Blaster that were able to infect internal computer systems protected by firewalls. These worms bypassed the firewalls altogether and entered corporate networks through other entry points such as VPN links and unsecured mobile devices (e.g. laptops).

Overall, firewalls are useful security tools, but they cannot be solely relied upon to protect organisations against all security threats.

Intrusion Detection Systems (IDS)

In addition to putting their trust in firewalls and perimeter security, some organisations also rely on Intrusion Detection Systems (IDS).

Network based IDS systems operate by scanning network traffic for signatures of existing attacks. This approach, however, suffers from several serious flaws.

Firstly, Intrusion Detection Systems are only able to detect those attacks they have signatures for. Thus, whenever a new vulnerability or a new worm is released, the IDS needs to be updated with a new signature.

Secondly, Intrusion Detection Systems rely on network traffic as their only source of information. Therefore, maliciously crafted network packets, encrypted traffic or event large amounts of network data can all potentially bypass security inspection.

Finally, even if an Intrusion Detection System detects an attack, it cannot *prevent* it. This was well illustrated by the recent Witty worm that exploited a buffer overflow in ISS's Intrusion Detection System product line. The worm attacked and corrupted the very same security system that was supposed to protect other computers.

As Intrusion Detection Systems are unable to stop attacks, they need to be monitored 24/7. This requires trained personnel to scan IDS logs for any signs of attack. But, the monitoring process is both time consuming and costly. In addition, it also has to take into account inevitable episodes of human error.

Taking all of the above into consideration, Intrusion Detection Systems cannot be relied upon to protect modern enterprises. They can still be used to monitor network traffic for signs of known attacks, but they cannot be expected to keep up and protect against the emerging threats.

Network Intrusion Prevention Systems (NIPS)

To compensate for some of the flaws associated with Intrusion Detection Systems, vendors have started to offer hybrid systems labelled Network Intrusion Prevention Systems. The emphasis has shifted from detection to prevention, but the underlying technology has remained the same.

Network Intrusion Prevention Systems act as an in-line IDS, through which all perimeter network traffic must first pass and be inspected. Alternatively, Network Intrusion Prevention Systems can look for network traffic anomalies and try to reset or throttle abnormal network connections.

Whilst NIPS technology differs from that of Intrusion Detection Systems, the underlying flaws are similar.

Firstly, NIPS systems designed to prevent host attacks still rely on signatures. Thus, whenever a new vulnerability or a new worm is released, the NIPS needs to be updated with a new signature.

Secondly, Network Intrusion Prevention Systems rely on network traffic as their only source of information. Therefore, maliciously crafted network packets, encrypted traffic or event large amounts of network data can all potentially bypass security inspection.

Finally, NIPS systems might be bypassed altogether, by using other communication channels such as dial-up or VPN links. In addition, unprotected mobile devices such as laptops can also be used to circumvent NIPS perimeter based protection.

Network Intrusion Prevention Systems try to address the flaws created by Intrusion Detection Systems. Unfortunately, the technology continues to suffer from the same serious flaws as the IDS technology. Therefore, Network Intrusion Prevention Systems can be used to filter incoming Internet network traffic for signs of known attacks, but they cannot be expected to keep up and protect against all emerging threats.

Patching

Whilst not a security technology as such, patching still plays an integral part of an organisation's security lifecycle. Patching involves downloading a security fix (patch) from a software vendor and installing it on all vulnerable systems. Whilst simple in theory, patching involves a number of complex practical issues that need to be addressed.

Firstly, patches might take a long time to be released from the moment a vulnerability becomes public. It is not unheard of for a vendor to take up to 6 months to produce a patch. This means that millions of computer systems around the world remain vulnerable until a patch is released.

Secondly, once a patch becomes available, it needs to undergo further testing in the environment where it is going to be deployed. Without proper testing, networks and computer systems can be rendered unusable due to unforeseen interactions. The need for further testing increases the length of time computer systems remain vulnerable.

Finally, once a patch is released and tested, it needs to be installed on all vulnerable computer systems. This in itself presents a huge task, considering that many organisations have thousands of computers requiring protection.

Microsoft alone published 45 separate security bulletins in 2003 which amounted to almost one every week. As the patching process needs to be repeated for every single security patch that becomes available, patching cannot be solely relied upon to protect organisations.

PART II: THE WAY FORWARD

Host Intrusion Prevention Systems (HIPS)

The bad news is that even if an organisation has firewalls, Intrusion Detection Systems, anti-viruses and all the latest patches installed, it is still not protected from 0-day (i.e. previously unknown) exploits.

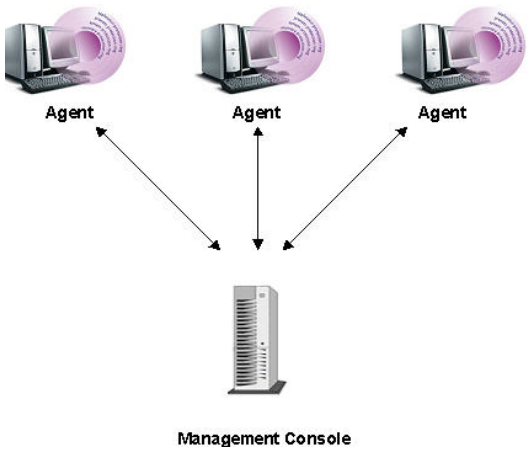
It might only be a matter of time before a malicious 0-day worm is released. A 0-day worm will propagate through computer networks like wildfire, as existing security technologies will not be able to prevent it. If such a worm also happens to carry a malicious payload, it will be able to destroy data on millions of computers and could disrupt parts of the global economy.

The good news is that a new type of security system called **Host Intrusion Prevention System (HIPS)** is quickly establishing itself as a technology that can effectively prevent unknown worm outbreaks and many other security threats.

Unlike firewalls and Intrusion Detection Systems, that only have access to the network traffic, Host Intrusion Prevention Systems are deployed by installing software agents on all computers requiring protection. By placing security back where it belongs – on the end hosts – HIPS systems cannot be blinded with large amounts of malicious network traffic, encrypted data or bypassed using communication channels such as VPN links.

Ozone

Ozone is an advanced Host Intrusion Prevention System developed by Security Architects. It consists of software agents that run on all computers requiring protection. A central management console is used to administer the software agents.



Ozone Approach

Unlike reactive security products, such as anti-viruses and Intrusion Detection Systems (IDS), Ozone does not rely on constantly updating thousands of signatures in order to keep up with the latest security threats. This means that Ozone can detect and prevent not just known, but more importantly also unknown attacks. (i.e. 0-day exploits).

Instead of looking for signs of ‘bad behaviour’ (i.e. known attack signatures), Ozone enforces good behaviour. Unlike bad behaviour, which can exhibit itself in thousands of different ways, the good behaviour set is limited.

For example, a web server is supposed to serve web pages. Therefore, its good behaviour set includes actions such as listening on port 80 and reading web files.

However, the bad behaviour set for a web server includes all types of undesirable actions such as deleting files, connecting to arbitrary Internet hosts, redirecting traffic and so on.

Enforcing ‘good behaviour’ is a much easier problem to solve than trying to describe all types of ‘bad behaviours’. Thus, Ozone is able to provide a much better security guarantee.

Ozone Agent Technology

Ozone agent technology incorporates multiple security rings that closely integrate with each other. Each ring is designed to address specific attack vectors ranging from low-level buffer overflow attacks to high-level application specific attacks.

Memory Protection Ring

The memory protection ring is designed to protect computers from various memory corruption attacks such as stack based buffer overflows, heap based buffer overflows and format bugs. These types of security bugs were responsible for the spate of recent worms such as Sasser and Witty.

With Ozone, all applications continue to function as normal, but are transparently protected from memory corruption attacks.

System Protection Ring

The next security ring, also known as the system protection ring, is responsible for protecting the underlying operating system from various low-level attacks. It disallows all users, including Administrators, to load kernel modules into memory, overwrite system files on disk or corrupt any running applications. As Ozone is loaded before all other applications, it is able to guarantee system integrity.

The system protection ring is also designed to protect all running system and user applications against unauthorized tampering.

Without Ozone, high-privileged users, such as Administrators, would be allowed to tamper with running processes. For example, it would be possible for an Administrator to inject code into a security system process (LSASS) and steal all password hashes. Or, malicious programs could inject code into the Internet Explorer process in order to bypass personal firewalls.

The system protection ring protects against these attacks and plays an important role in guaranteeing operating system security and integrity.

Process Protection Ring

Besides protecting the operating system, Ozone also protects all running programs. Ozone achieves this by executing all processes inside a virtual 'sandbox' from which they cannot escape and cause damage. The process protection ring enforces the 'Least Privilege' security principle, which states that a user or a computer program should be given the least amount of privileges necessary to perform its job.

For example, Internet Explorer will be allowed to browse web pages, but it will not be allowed to overwrite system files, execute untrusted programs or do anything else it is not explicitly allowed to.

Besides protecting popular applications such as Internet Explorer and IIS, Ozone can also be configured to run any 3rd party or in-house built applications inside a 'sandbox'.

Application Protection Ring

The application protection ring is responsible for protecting programs from application specific attacks. The ring protects from attacks that do not modify the normal behaviour of a victim application, but are nevertheless harmful.

For example, SQL injection attacks do not cause database servers to perform any actions outside of their 'good behaviour' set, but are nevertheless dangerous and would be need to be addressed further.

The application protection ring consists of application specific modules that are designed to address specific high-level attack vectors such as SQL injection.

Ozone Advanced Features

Besides protecting the operating system and various applications, Ozone is also designed to allow organisations to control the behaviour of their users.

Many organisations have building and personnel security policies that control who is allowed to enter and use various facilities. The very same organisations also have computer security policies in place that describe what computer users are and are not allowed to do. The difference between physical and computer security policies is that organisations have the guards and locks to enforce the former, but lack the tools to effectively enforce the latter.

Ozone bridges this existing gap and provides organisations with a “tool” that allows the enforcement of an organisation’s computer security policies.

For example, using Ozone, a security manager can specify that user John Smith using computer #2 is allowed to access a corporate database, but is not allowed to connect to the Internet. Similarly, user Jane Brown using computer #13 is allowed to browse the Internet, but is not allowed to install any new applications or copy data onto USB removable drives.

Ozone agents are also designed to protect data from unauthorized removal. Ozone can disallow data to be copied over the network or onto removable media such as USB drives.

Ozone Layers

The default Ozone layers are designed to cover most organisations' needs. Ozone comes with 5 pre-configured layers: Desktop, Web Server, Database Server, Mail Server and Terminal Server.

These layers are designed to protect most of the applications being used by modern day organisations.

In other words, the Desktop Layer would come pre-configured with security policies for popular client applications such as Internet Explorer, Outlook, Real Player, etc. Similarly, the Web Server layer would come pre-configured with security policies for web servers such as Microsoft IIS and Apache.

As every organisation's needs differ, Ozone has been designed to be flexible. Besides protecting common applications, Ozone can also protect any 3rd party and in-house built applications. The process involves building a security policy for each application requiring protection and is quite painless, as Ozone automatically learns and creates the required security policy.

Desktop Layer

Desktop computers are generally placed behind corporate firewalls completely unprotected. Whilst firewalls prevent direct connections to these machines, this approach is flawed as demonstrated by the recent outbreaks of computer worms, such as Sasser and Blaster, inside corporate networks.

Although these recent worms were unable to directly attack client computers hidden behind firewalls, they still managed to infect them. They achieved this by completely bypassing firewalls and entering networks through other unprotected communication channels such as Virtual Private Networks (VPN). Other worms infected client computers by sending their malicious payloads by email.

Yet another type of worm attacked desktop machines by exploiting zero day vulnerabilities (i.e. previously unknown vulnerabilities) in client applications such as Internet Explorer.

All this amounted to enormous loses in terms of money and time spent on cleaning up the damage, as well as costs relating to any proprietary information that was stolen.

Ozone Desktop Layer protects client applications such as Internet Explorer and Outlook from various attacks such as buffer overflows and unauthorized code execution.

The process protection ring protects desktops by running client applications in virtual ‘sandboxes’ from which they cannot escape and cause damage.

This ring protects against Internet Explorer vulnerabilities such as the recent ‘ITS Protocol Handler’ vulnerability (CERT Technical Cyber Security Alert TA04-099A) that allowed attackers to trick Internet Explorer into running malicious programs.

It also protects against Outlook vulnerabilities such as the ‘Outlook URL Handling Vulnerability’ (CERT Technical Cyber Security Alert TA04-070A) that allowed attackers to trick Outlook into running malicious programs.

Besides protecting the popular Internet Explorer and Outlook applications, Ozone Desktop Layer can also protect other Internet enabled applications such as web browsers (Netscape, Opera), media players (Microsoft Media Player, Real Player) as well as Instant Messaging and Peer 2 Peer applications.

Ozone Desktop Layer is also designed to protect organisations from insider attacks. Ozone can protect proprietary information by disallowing data to be copied over the network or onto removable media such as USB drives.

Web Server Layer

Web servers have evolved from being simple programs that send static HTML pages, to becoming multi-threaded enterprise supporting applications that drive the digital economy.

The constant drive for better performance and more features has caused web servers to become increasingly complex. Today, modern web servers such as Microsoft IIS consist of multiple and complex processes that work closely together. Yet very few people understand this complexity and it has led to a myriad of security bugs being found in various web servers and applications.

Most recently, all major web servers including Microsoft IIS and Apache have had at least one remotely exploitable vulnerability that allowed security worms to penetrate tens of thousands of vulnerable web servers around the world.

Ozone’s multi-ring technology protects various web servers, such as Microsoft IIS and Apache, from a number of attacks. These range from low-level attacks such as buffer overflows, to high-level attacks such as HTTP specific attacks.

The process protection ring protects web servers by running web processes in virtual ‘sandboxes’ from which they cannot escape and cause damage.

In addition, the application protection ring deeply integrates with web servers to guard against HTTP specific attacks.

Database Server Layer

Over recent years, many database servers such as Oracle and Microsoft SQL Server have been exposed to at least one remotely exploitable vulnerability that allowed attackers to completely take over the database server.

Some database servers were even targeted by computer worms such as SQL Slammer, which in the US alone caused millions of dollars worth of damage and brought down vital infrastructure such as 911 emergency systems and various ATM machines.

Ozone protects a variety of database servers including Oracle, Microsoft SQL Server, and MySQL. Ozone's multi-ring technology protects database servers from a variety of attacks, ranging from low-level attacks such as buffer overflows to high-level attacks such as SQL injection.

The process protection ring protects database servers by running database processes in virtual 'sandboxes' from which they cannot escape and cause damage.

In addition, the application protection ring deeply integrates with database servers to provide protection against database specific attacks such as SQL injection.

Mail Server Layer

Modern businesses heavily rely on digital communication channels such as email and any incurred downtime can negatively affect a company's image and revenues.

Unfortunately, the number of email related attacks is on the increase and Email servers themselves are vulnerable. This was clearly illustrated by the recent Microsoft Exchange buffer overflow vulnerability.

But, due to the huge importance of email, no business can afford to be without an email server and this places them in a Catch-22 situation.

Ozone's multi-ring technology protects various mail servers, such as Microsoft Exchange and other SMTP, POP3 and IMAP servers, from a variety of attacks such as buffer overflows.

The process protection ring protects email servers by running system processes in virtual 'sandboxes' from which they cannot escape and cause damage.

In addition, the application protection ring deeply integrates with email servers to guard against SMTP specific attacks.

Terminal Server Layer

Today's business community operates 24 hours a day, 365 days a year. This is why remote access to digital information is essential for any business.

While Terminal Servers provide a fast and easy way to access corporate information remotely, they also expose businesses to a myriad of security threats such as unauthorized data and application access. In addition, Terminal Servers themselves often come under attack.

Ozone's multi-ring technology protects the Microsoft Terminal Server from a variety of attacks ranging from buffer overflows to unauthorized application execution.

The process protection ring protects the Terminal Server by running user processes in virtual 'sandboxes' from which they cannot escape and cause damage.

In addition, Ozone Terminal Server Layer strictly limits what applications users are allowed to use, as even published applications can be tricked into running other programs. The Terminal Server Layer protects against this and many other attacks.

Conclusion

The number of reported vulnerabilities and worms continues to steadily increase.

Yet existing security technologies such as firewalls, Intrusion Detection Systems and anti-viruses fail to keep up with the emerging threats.

The good news is that a new type of security system called Host Intrusion Preventions System (HIPS) is quickly establishing itself as a technology that can effectively prevent worm outbreaks and many other security threats.

Unlike firewalls and Intrusion Detection Systems, that only have access to the network traffic, Host Intrusion Prevention Systems are deployed by installing software agents on all computers requiring protection. By placing security back where it belongs – on the end hosts – HIPS systems can provide unprecedented levels of security.

Ozone is a Host Intrusion Prevention System developed by Security Architects.

Unlike reactive security products, Ozone does not rely on constantly updating thousands of signatures in order to keep up with the latest security threats. This allows Ozone to detect and prevent not just known, but more importantly also unknown attacks.

Ozone's approach signifies a paradigm shift in the security arena. Ozone puts security managers back in control of their networks and computer systems instead of trying to play catch-up with the latest security threats.

About Security Architects

Security Architects offers advanced security solutions to organisations and individuals needing to secure their networks and systems.

Its main product, Ozone, is an Intrusion Prevention System that protects server and client machines from both known and unknown computer attacks.

Security Architects also provides professional services, ranging from penetration testing and code auditing to tailor-made security courses.

Secarch Ltd.
Universal House
88-94 Wentworth Street
London
E1 7SA
UK

T/F: +44 (0) 207 375 1006

www.securityarchitects.com