HURWITZGROUP

A Primer on Preventing Attacks at the Host

— OKENA, Inc.

▶ Hurwitz Report

HURWITZGROUP

A Primer on Preventing Attacks at the Host

— OKENA, Inc.

A Hurwitz Group white paper written for:

OKENA, Inc.
71 Second Avenue
Waltham, MA 02451
Tel: 781 209 3200
Fax: 781 209 3199
www.okena.com

Published by:
Hurwitz Group, Inc.
111 Speen Street, Framingham, MA 01701 ▶ Telephone: 508 872 3344 ▶ Fax: 508 872 3355
Email: info@hurwitz.com ▶ Web: www.hurwitz.com

February 2002

Executive Summary

In the security profession, we often spend our days reacting to the latest intrusion attempts or viruses that have been identified. Current security solutions seek to identify attacks through signatures, by analyzing and characterizing specific traits and behaviors. That approach has a number of problems with timing and latency.

OKENA provides security without signatures. It protects both desktops and servers using preventive means. By monitoring how an application acts and comparing it to a set of rules, OKENA ensures that known and unknown attacks are prevented.

Introduction

A Day in the Life of the Security Officer

Sometimes the day begins quietly, with thoughts about securing the new CRM solution or supply chain software. Perhaps today will be a good day to get started on that long-lingering network security review. Other times, you know that before you get in the plans and strategies will be put on the backburner again due to the latest virus or attack. In either case, the plans go out the window because it's time to react again.

FDPC (Fire Department, Personal Computers)

React mode is a common state in security. Often, security doesn't get its due when all is calm and systems are running smoothly. The planning and proactive work that does somehow get done amidst the backdrop of "putting out fires" is often force-fed to system and network administrators with their own competing priorities.

Competing Priorities

Even within the security function, priorities abound and must be evaluated based on risk and return and the impact on defined budgetary guidelines. A security officer must split his or her time determining the security implications of many different technology platforms — email, browser, server, and enterprise apps — that are often integrated to perform some business function. There has to be a better approach.

Complexity Drives Vulnerabilities

What does client-server plus load balancing plus Internet access plus enterprise application integration equal? It equals complexity — complexity of software solutions and the resulting complexity of the security to protect them. Nowadays, it isn't just the operating system that gets broken into, but the application servers, web servers, database servers, and other pieces of a solution that are vulnerable. With all of the different pieces to an application, hackers can choose which components to attack. This increased complexity leads to increased vulnerabilities and many different opportunities to exploit a system. It is crucial to protect the foundational systems from all of these attacks through proactive, preventive security measures.

A Better Approach

The better approach is here, and it is obvious. The better approach is prevention, with its ability to protect against a problem rather than react to it.

This white paper discusses some traditional ways to protect desktops and servers along with their drawbacks. It introduces the new class of security from OKENA — security without signatures that prevents malicious or inappropriate activity.

Problems with the Traditional Approach

The primary method of addressing attacks today, both antivirus and intrusion detection, is to create signature files of any particular attack and update the detection software. This approach, though time tested, comes with some basic problems.

Sacrificial Lamb

The clock begins. To identify a new attack or virus, a "sacrificial lamb" needs to get infected for the good of the masses. This "lamb" becomes the first casualty in an attack. In the lucky event that an "on the ball" administrator recognizes the infection and realizes that existing antivirus and/or intrusion detection software did not catch anything, the administrator must submit it for review by the vendor. Then comes signature creation.

Signature/Patch Creation Latency

The clock is ticking. The vendor receives a sample of the attack and immediately begins parsing it and evaluating its payload. How does it propagate? What destructive action does it take? What vulnerability is exploited? The virus or worm needs to be analyzed and questions need to be answered in order to derive the appropriate detection signature or create a patch. After a signature or patch is created, it gets distributed to subscribers. From this point, the question of speed becomes mired in the complexities of the computing environment that is being protected.

Signature/Patch Deployment Latency

Once the signature update is received, the enterprise administrator must make a difficult decision — how much testing is required before the update can be deployed throughout the enterprise? This often depends on the severity and type (client or server) of the threat and the nature of the update. In the case of signature files, enterprises normally accept the risk and begin distributing the update almost immediately. Patches follow a different route in testing, and may need some "leap of faith" trust that, for example, a web server won't fail when updated. In cases like this, there are no easy answers. And still the clock ticks.

The distribution itself can be very time-consuming. In the case of a signature file update for client antivirus software, there are many ways to get the file updated, but the most oft-used one is a "brute force" approach to notify users to update their files. Even the best situation, where the signature file is automatically updated from a particular source, creates a finger-crossing moment that remote employees will somehow connect and have their systems upgraded. Even under the very best of circumstances, nothing is "automatic" in this process.

Difficulty with Variations

Although the update process is complete, the question of coverage still remains. Ideally the signature of the attack should be specific enough to stop that attack and broad enough to identify new variations, even when some of the payload or distribution mechanisms are modified slightly. Even more insidious is the ability to compress or encrypt the payload or delivery mechanism to create a new virus or worm.

Bottom Line: Reactive Approaches Are Inefficient

There is a bottom line to all of this — although a company's approach was the best it had in the past, it is constantly being hit with new attacks at an even faster rate than ever before. Reactive approaches are costly and inefficient, and do not provide timely coverage. The result is a struggle to get the patch updated quickly, along with the need to recover and rebuild those systems that get hit prior to the time when effective protection is deployed.

Clearly, a more proactive approach is a necessity; an approach that involves intrusion prevention ends up being more efficient and ultimately more effective.

The Intrusion Prevention Approach

Intrusion prevention eliminates traditional signatures and adds a proactive spin to the typical detection process. Its primary benefits are:

- **Monitor application behavior.** Intrusion prevention works by monitoring and analyzing the behavior of an application. Every application interacts with the operating system and potentially other applications. The first step in prevention is understanding what an application is normally allowed to do.
- **Create application rules.** Once an application's behavior is understood, a set of rules, must be created for an application. These rules mirror the information that was collected during the application analysis phase and provide the preventive measures that enforce policy.
- **Alert on violations.** A straight-forward need for any security solution is to provide alerting capabilities so that any compromise or attempted intrusions that are prevented will be identified and recorded. (Enterprises have many different ways to provide these alerts, making flexibility and options key to providing the alert in a timely manner.)
- **Correlate with other events.** It is becoming more clear now than ever that security professionals can be more effective through the correlation of information from

multiple devices or sensors. The ability to understand when an attack is under way, prevent it, and notify other devices provides the chain mail armor across the enterprise.

- **Protect desktop and server.** Intrusion prevention software provides coverage for any application. It is installed on the host and monitors the activity for that host, regardless of whether it is a client PC or a server. This contrasts with the common use of antivirus and personal firewall software on the client, and intrusion detection software either on the network or server. In this case, intrusion prevention solutions provide the same benefits to any type of host, reducing costs associated with a multiple product/multiple vendor solution.

Intrusion Prevention ROI

How do you get a return on investment for a security solution? As you move from a solution that is detective in nature to one that is preventive, the answer is clear — increased efficiency and effectiveness. These concepts are described below:

- **Reduce recurring hot fixes.** Hot fixes are a balancing act — they exist solely to plug a hole in a dyke that is already leaking. The ability to reduce the need for hot fixes, and wait for a regular patch or periodic update, reduces the amount of administration time on the host and also reduces the risk that a hot fix will result in system downtime or create other problems.
- **Lower recovery costs.** If an attack is prevented, the compromise can't take place. Therefore, there will be a significantly reduced requirement for system recovery. Lower recovery costs can be substantial in a complex dynamic network environment with high-volume and sensitive activity.
- **Reduce incident response costs.** Rather than wait for an alert and then respond, intrusion prevention solutions deny the ability to compromise a system. The monitoring and deployment of incident response teams is all but eliminated with a proactive approach.
- **Eliminate system downtime.** A final element of ROI is the limitation of system downtime. Since the host is not compromised, it remains in operation. When the function is financial or of other significant value, downtime costs are measured in minutes. A preventive approach eliminates system downtime.

OKENA's StormSystem

There's a StormSystem on the horizon, and it's coming from OKENA. OKENA has created a comprehensive, non-signature approach to intrusion prevention. Its core elements are as follows:

- **StormFront.** Adds to OKENA's out-of-the-box policies for common applications and extends prevention to new and custom applications in an enterprise. StormFront is responsible for monitoring an application's behavior and creating a set of rules, or policy, out of it. It is this solution that evaluates read/write activities and determines what file access, network settings, and registry settings may be allowed as appropriate.
- **StormWatch.** Provides the agent technology to monitor activity and prevent it from occurring. Leveraging OKENA's INCORE architecture (see Figure 1), the agent intercepts calls to the kernel or file access or some other process, allows or denies the access based on policy, and then notifies the central management server.
- **StormTrack.** Audits the existing security configuration of a host and determines what operating system and applications are running and compares this to the existing policies to determine what security measures are missing, yet should be in place. StormTrack then interfaces with StormWatch to create the missing security policies .By evaluating the security posture of the host, StormTrack bridges the gap between unsecured and secure systems.

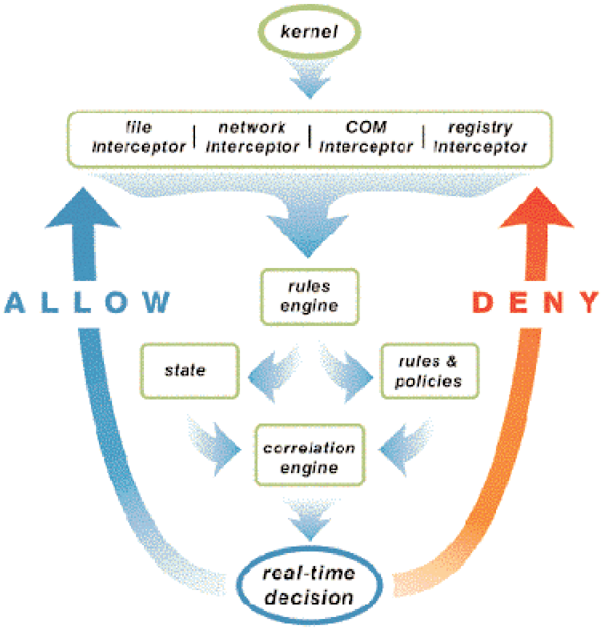

Figure 1. OKENA'S INCORE architecture.

Conclusion

OKENA's StormSystem provides a comprehensive new approach to protecting desktops and servers. With OKENA's solutions, enterprises are no longer reliant on the need for timely system patches and signature file updates, which are created only after an attack has been identified. An approach that is preventive reduces costs and is more efficient than solutions that are reactive or detective in nature.

About Hurwitz Group

Hurwitz Group, an analyst, research, and consulting firm, is a recognized leader in identifying and articulating the business value of technology. Known for its real-world experience, consultative style, and pragmatic approach, Hurwitz Group provides strategic guidance to its clients by delivering analysis, market research, custom content, and consulting services. Clients include Global 2000, software, services, systems, and investment companies.

111 Speen Street   Framingham, MA 01701   **T** 508 872 3344   **F** 508 872 3355   www.hurwitz.com