# Using Host Intrusion Prevention in a Distributed Control System

Ernest A. Rakacsky, Al Soares
Invensys Operations Management
Quebec, Canada
{ernest.rakaczky, al.soares}@ips.invensys.com

**Abstract:** Security is often discussed in terms of layers of protection. One of the challenges is to decide what is appropriate in terms of implementing specific countermeasures at specific layers. This paper discusses the appropriateness of implementing Host Intrusion Prevention (HIP) at the workstation and server levels within a distributed control system (DCS). Because of its potential overhead in terms of installation, configuration and runtime load, this type of protection has been done at the boundary of the DCS with the "outside" world, including other networks within an organization. However, the technology has been advancing along with the capacities of computing platforms such that it has become viable, as well as desirable, to deploy HIP in a DCS.

In addition to providing the conceptual background and reasons for employing HIP in a DCS, information will be shared about the practical aspects and challenges experienced during a project where this was done for an actual commercially available DCS.

**Keywords:** Host Intrusion Protection System, HIPS, Anomaly Detection, Security Management

## 1 Introduction

A strongly recommended approach to site networks and control system security is based on the following principles:

- View security from both management and technical perspectives
- Ensure security is addressed from both an IT and control system perspective
- Design and develop multiple layers of network, system and application security
- Ensure industry, regulatory and international standards are taken into account
- Prevention is critical in plant control systems and is supported by detection

The first stage in building a solid defense against unwanted intrusion into business network and process control systems is to develop a security policy statement and then define the requirements to implement a secure process environment. Once security goals are clear, a detailed plan can be developed to address current needs.

Developing a prevention approach to plant control systems will require a new approach to network security between the plant network layer and business / external systems. This paper focuses on one key piece within the overall network architecture – Host Intrusion Prevention (HIP). This document provides an overview on how and why HIP is a viable and strongly recommended layer of protection within a Distributed Control System (DCS).

When reviewing this technology, some of the key elements taken into consideration were the current requirements to manage the ability to both apply required security patches and update antivirus signature files while knowing that a particular host device could be the overall connection point from the control network to the next layer or plant network, see Figure 1, or a host device serving various business layers with required process data.

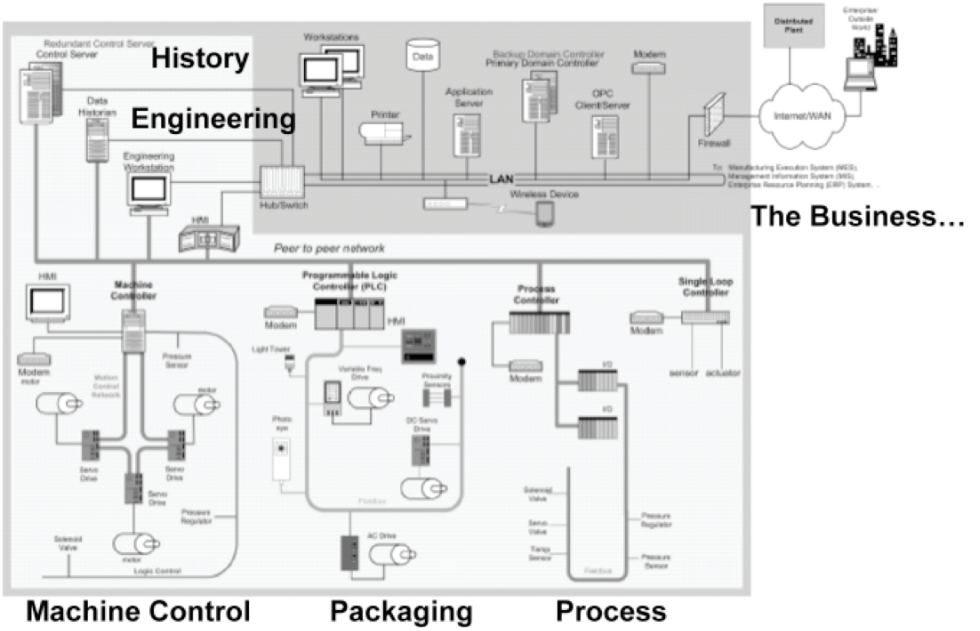


*Figure 1 – Typical DCS Network Topology*

One of the key concerns in addressing cyber security requirements for a process control system is providing measures and layers of protection that in the end, have a focus on the possible impact of a zero day exploit.

To address this concern the authors believe it is necessary to incorporate technology that is not addressed in antivirus signature updates and patch management processes. These layers of protection fall short and somewhat always will. Even if both the latest antivirus signature and the latest security patches are in hand, there is always going to be a high probability they will not be able to be installed due to the operational risk they

may induce. All actions like updating antivirus signatures or applying patches will have to be well-prepared, very deliberate and in sync with ongoing operational requirements.

Also when reviewing basic network protection within this control environment, such as firewalls, network intrusion detection or protection, adding HIP creates a "Last Line of Defense". If all else DCS security measures fail, HIP can provide a final layer of protection. The goal of HIP is to protect against known attacks, unknown attacks and denial of service attacks as shown in Figure 2.

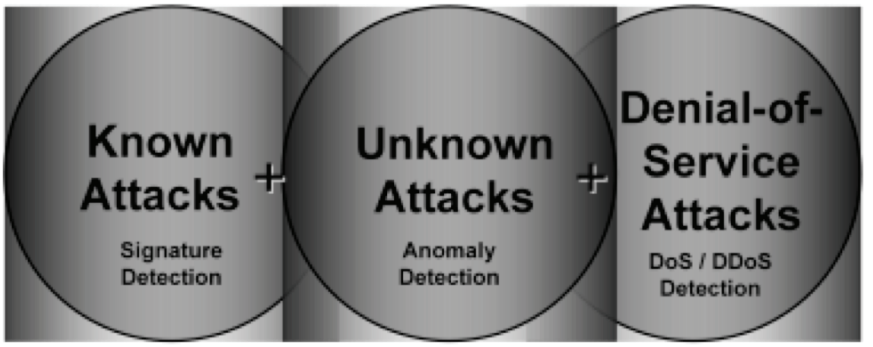


*Figure 2 – Attack Categories and Detection Methods*

## 2 What is Host Intrusion Prevention?

HIP is the discovery of, and response to, unauthorized action undertaken with the intent of hindering, damaging, incapacitating, or breaching the security of a host system. A Host Intrusion Prevention System (HIPS) is a software package that loads and runs on the host system it is protecting. HIPS attempts to detect and respond to attempted intrusions into a host server or workstation system. HIPS complement firewalls or antivirus software by thoroughly inspecting the contents of network packets arriving at the host as well as the behavior of the host application software and operating system.

When malicious activity is detected, the HIPS provides a variety of custom responses based on the attack and the HIPS configuration; these actions range from logging the event and sending an alert to blocking an application or operating system function from executing.

Each HIPS agent ships with default policy templates for protection out of the box. Agents also contain powerful customization features that allow security professionals to create and tune policies for their unique environments to reduce false positives. The agent examines specific system calls and API calls, both of which are used by all applications to request services from the operating system. It quickly and efficiently compares its behavioral rules and known attack signatures against a range of information about each call, e.g. the process making the call, the security context in which the process runs, or the resource being accessed. The HIPS agent then blocks all calls from

malicious behavior or malware. Agents automatically retrieve encrypted and authenticated updates from the management system, ensuring that each agent has the latest policies and new attack signatures.

# 3 What to Look for in Host Intrusion Prevention

How can an organization make informed decisions when choosing HIPS products? Here are some technology best practices for HIPS based on the authors experience in a recent project.

Any organization that intends to protect itself by using intrusion prevention technology should consider a number of factors when evaluating products that address the organization's defined security requirements. Care should be taken to choose solutions that meet corporate security, manageability, and flexibility requirements, lest the solution be a partial one, or worse, introduce a significant management burden that overshadows the security benefits.

## 3.1 Host Based Protection

As more companies adopt technologies like high-speed networks, switching, and end-to-end encryption, providing desired security at the network level becomes a major challenge. The data that should be analyzed is much greater due to bandwidth increases; the data may not be easily accessible by the sensor or detection engine due to the topology design; and the data may be encrypted that, while protecting the confidentiality, prevents any analysis to identify attacks.

The best place to enforce security is increasingly found at the workstations and servers where the actual work is performed and where the potential for damage is greatest.

A HIPS may also compensate for less than perfect anti-virus signature updates or security patch deployment. Consider the value of only a HIPS solution that prevents new malware or a zero day attack where updates to prevent these attacks have not yet been developed or deployed. This is of considerable value in the control environment where one of the key challenges is the deployment of security vulnerability patches in a timely manner. It is common for control systems to remain unpatched for a month or more even with a patching program due to testing requirements.

## 3.2 Real Time Prevention Systems

To ensure the highest levels of security and minimize the ability to bypass the security policy on a host, application calls must be intercepted at the kernel level, where the HIPS determines their adherence to a defined policy. Solutions implemented outside the kernel can easily be bypassed by replacing shared libraries or analyzing system audit logs. An effective intrusion prevention strategy includes preventing violations in real-time, rather than noting attacks or system changes after the fact.

## 3.3 Defense in Depth

To completely enforce a company's security policy, HIPS must intercept all major points of communication between applications and the underlying system.

Network controls must limit client/server communications at the port and protocol level, as well as hosts for permitted communications. File system controls must allow or deny read and write access to folders and files on an individual and group basis. Registry controls must prevent the overwriting of important registry keys that control how the system and other applications operate. And COM controls should restrict inter-process communication to allowable access.

Attacks have multiple phases: exploiting network and application-level weaknesses, replicating and distributing themselves, and making unauthorized changes to the system. A complete intrusion prevention strategy must protect systems from all these phases, so if a new class of attack releases, it will be thwarted at one or more of the stages.

## 3.4 Real Time Correlation

Correlation deployed at the HIPS agent provides a level of accuracy on prevention decisions that does not exist with signature matching approaches. Correlating sequences of events within the context of an application's behavior significantly reduces the potential for false positives.

Correlation at the enterprise level enables security to be adaptive. By correlating the events on distributed agents, you can dynamically update HIPS policies to prevent propagation of malicious code, thus preventing widespread damage to numerous resources.

## 3.5 Behavioral Approach

The intrusion prevention approach must enforce appropriate system and application behavior to ensure the security implemented is proactive, not reactive. Solutions that rely on signatures only provide security to the release of the most recent signature update.

## 3.6 Flexibility

Virtually every control system has some degree of uniqueness in configuration and how it manages the details of the operating system and applications. Intrusion prevention solutions must permit the policy customization and creation to accommodate unique applications and implementations. The solution must support automated policy creation to ease the management burden of creating policies by hand.

## 3.7 Ease of Deployment

A HIPS strategy should minimize the personnel overhead associated with agent deployments. Solutions must provide out-of-the-box functionality to allow for rapid deployment of the desired security policies, and must allow for the roll out of new and custom policies as needed without additional intervention at the host level. The solution

must allow for easy integration with standard corporate software distribution mechanisms.

### 3.8 Centralized Event Management

All events the HIPS agents generate must roll up into a centralized repository from which alerts and reports may be generated. Solutions must support standard alerting interfaces, such as SNMP, paging, e-mail and flat files. They should also allow for custom interfaces to the alerting system to easily integrate with corporate systems.

### 3.9 Platform Coverage

HIPS solutions must provide coverage for the key operating systems the organization wants to protect. In light of attacks like Nimda, which target multiple hosts, the same management and enforcement paradigm must apply to workstation and server-based systems.

### 3.10 Administration

To ease HIPS policy management, policies must be definable centrally and automatically distributed to HIPS agents on a configurable interval. They must also be exportable for replication and archive purposes.

## 4 HIPS Key Features and Benefits

### 4.1 Multi-Layered Protection

With the rapid growth of blended threats and profit-motivated cybercrime, organizations need layered protection to defend endpoints against known and unknown zero-day threats and to prevent loss of confidential data.

- Signature protection accurately identifies and blocks known attacks
- Behavioral protection secures endpoints against new, zero-day, threats
- Stateful firewall blocks unsolicited inbound traffic, controls outbound traffic, and applies policy rules based on traffic, ports, applications, and locations
- Application control helps create and enforce whitelists and blacklists to specify which applications can or cannot run
- Specialized server protection secures critical servers with customized protections to maintain system uptime and productivity

### 4.2 Reduced Security Patching Burden

A large percentage of exploits are released as little as three days after disclosure of vulnerabilities. Yet, on average, it takes organizations 32 days to deploy server patches. HIPS bridges this security gap while making the patching process easier and more efficient.

- Vulnerability shielding automatically updates with signatures to protect endpoints against attacks resulting from exploited vulnerabilities
- Out-of-the-box protection boasts a superior track record: Host IPS protected 97 percent[1] of all Microsoft vulnerabilities disclosed in 2007
- Signature updates are automatically and regularly downloaded in a similar manner to .DAT file updates for protection assurance.

## 4.3 Central Management

Companies struggle with the costs and effort required to manage separate security technologies deployed on their endpoints and network. By using a single, integrated security console, companies reduce the number of IT managers needed to manage endpoint security with multiple consoles by 44 percent.[2]

- Access centralized event monitoring, reports, dashboard and workflow through a single web-based, management console
- Deploy, manage and update agents and policies from one management platform

## 4.4 Eases Compliance Reporting

Maintaining and proving compliance can consume a huge amount of IT resources. HIPS helps organizations obtain greater visibility and control to simplify their compliance efforts and make reporting and audits less painstaking.

- Gather attack details such as type, vector, source, severity, timestamp and more—all in clear and easy-to-understand language—for prompt reporting, audit, investigation, and response
- Produce compliance reports for auditors and other stakeholders
- Customize dashboards for real-time compliance status

[1] McAfee Avert Labs
[2] Insight Express, 2007

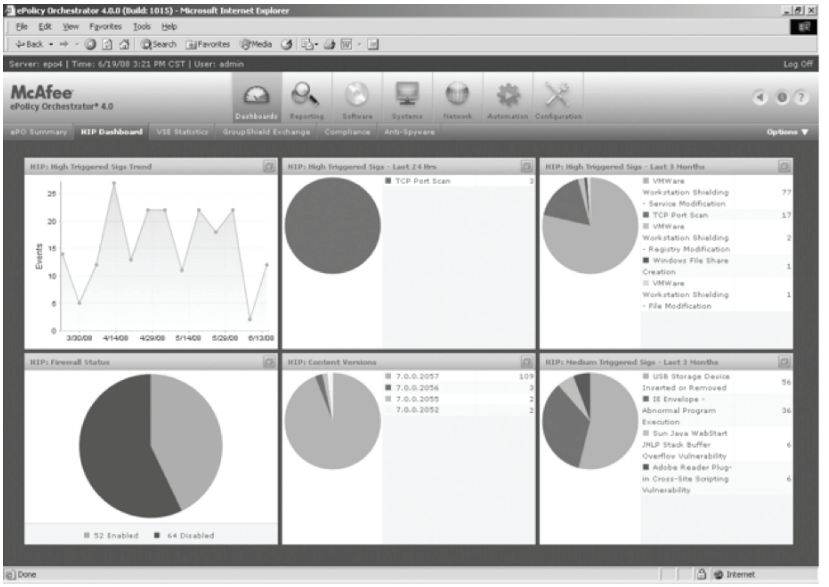


*Figure 3 – Sample Management Dashboard*

# 5 HIPS Integration Case in Review

The following is a high level summary of the process that was followed by the IOM Foxboro Development team in the implementation of the McAfee Host IPS suite with the Invensys Foxboro I/A DCS:

## 5.1 Background

As part of the security enhancements being offered with the latest release of the I/A Series platform Invensys decided to incorporate some security products from a third-party specializing in security rather than trying to reinvent similar technology in house. Previously, the McAfee VirusScan Enterprise product was incorporated in the OS images Invensys installs on the I/A Series workstations. However, it was decided to augment that with the McAfee Antispyware Enterprise product.

In order to provide a configure a host-based configurable firewall, the McAfee HIPS was qualified for incorporation in the I/A Series system platform as well. Note: the Microsoft Windows XP firewall was considered inadequate to meet the requirements. In addition, it was decided to incorporate the McAfee Device Control product to allow customers to enable or disable access to devices such as floppy drives, CD drives and USB devices.

A natural decision was to incorporate McAfee's ePolicy Orchestrator product to provide a central console to install, configure and manage all of these McAfee products.

## 5.2 Experience

It quickly became evident that there was a steep learning curve for installing and configuring these products. There was considerable concern that this would not be palatable to our customers, whose main job is to control processes, not necessarily becoming experts on installing and configuring security products.

A project was undertaken to try to automate the installation and configuration of these products to make it easy for the customers. This undertaking turned out to be more ambitious than we initially anticipated. Because it was taking so much more time and energy to do this than was estimated, it was shelved for the time being. Instead, we decided to provide a comprehensive installation guide with step-by-step instructions and lots of screenshots to make it straightforward to install without needing to deal with the steep learning curve.

## 5.3 Results

While testing the firewall product, it became evident that it was nearly impossible to come up with a totally pre-configured set of firewall rules for all the possible applications that could run in this environment. Fortunately, the HIPS has an adaptive mode that allows it to learn what the system behavior is and to create firewall rules automatically. This is the same way it is employed in the IT world. Once the set of applications that are expected to be used is installed and running, the system is run for a while with adaptive mode turned on. After it is felt that the applications have been sufficiently exercised, the adaptive mode can be turned off. The HIPS will then block anything that does not have a rule created during the adaptive mode. If necessary, additional rules can be added without putting HIPS back in adaptive mode.

We found that these host-based security products could be used effectively on the Invensys DCS. They did not pose an obstacle to system performance while providing an extra layer of security protection. Having this initial suite of products will provide a foundation onto which enhancements can be incorporated as they evolve or other security products can be added as they are developed in the future.

It is important to put in place a process for customers to obtain updates and patches to these products. The world of security constantly changes in terms of types of threats and countermeasures. Consequently, the security vendors are continuously providing updates and working on enhancements.

# 6 Summary

With the incorporation of HIPS into an Invensys DCS system, it became clear there are elements that need to be considered and methodically approached when applying this technology in a control environment. We treated this application no different than when we first embedded host antivirus into our DCS components, all tuning elements must be well reviewed and understood equally. A very strong understanding of the actual control and process operations environments are critical for successful implementation. In others words, this is not an application you just load and let run. Some effort and fine-tuning is needed, customized signatures created, and the requirement of strong

management practices needs to be considered. However, in the end, HIPS can add a very strong level of protection and most importantly can be implemented into a process control environment.

---

**About the Authors** – Ernest Rakaczky is currently the Program Manager for Control System Cyber Security within the IOM Portfolio group. Mr. Rakaczky also participates in the efforts underway at ISA within SP99, Automation Federation, NIST-SMART GRID, within ICSJWG from DHS, MSMUG and plays an active role in the various Security initiatives with DOE, DHS, INL, NRC, NPRA, IAEA, and SANDIA. Most currently, Mr. Rakaczky, with the formation of the ISA Security Compliance Institute ISCI, was elected as the Marketing Chair of the initial Governing board.

Al Soares is a Consulting Engineer in the DCS Product Architecture group within the Invensys Operations Management (IOM) Division of Invensys Systems, Inc. He has been working on distributed control systems for about 25 years in various capacities ranging from human interface design and implementation to systems engineering and testing. Most recently, he has been engaged in designing and implementing security enhancements for the Invensys I/A Series Systems.