Process Solutions

Honeywell

White Paper

Application Whitelisting

Executive Summary

The increasing complexity and volume of applications, and the issues stemming from threats to these applications, is resulting in the requirement for new or improved security tools.

As the security threat landscape continues to evolve so too must our response to security tools and best in class products and support of your infrastructure. One of the more recent developments in security protection is the concept of Application Whitelisting.

Application Whitelisting is an effective tool for enhancing your “Defense in Depth” security strategy. With increasing numbers of attempted intrusions, cautionary tales of security breaches and the potential for resulting damages at your site, Application Whitelisting can be an important addition to your security arsenal.

Table of Contents

Application Whitelisting in Control Systems

Defense in Depth is a fundamental building block for providing a more secure infrastructure and is the most widely accepted approach recommended for today's control systems. When ubiquitous flash drives can become precision guided munitions, we quickly conclude that the more in-depth the defense mechanisms, the better. Understanding the various tools that can enhance your security strategy is key to successful implementation.

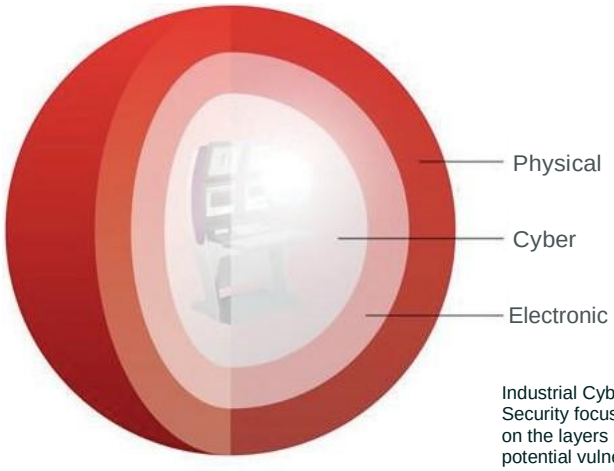

Figure 1: Defense in Depth

Application whitelisting is an approach to combating viruses and malware, allowing software considered safe to run and blocking all others. This approach is in contrast to the blacklisting approach used by anti-virus software, which is a standard signature-based approach that blocks or removes known harmful software. There are positive attributes to both approaches, and they are not mutually exclusive.

One of the major characteristics of the blacklisting (anti-virus) approach is that it blocks ***known*** bad actors—leaving a time gap between the detection of a new piece of malware and the inclusion of its signature in the latest update from the anti-virus vendor. During that time gap, there is a window of exploitation where your system may be vulnerable to the new malicious code.

The blacklist is growing at a rapid rate. Malware examples, such as the Storm[i] and Conficker[ii] worms, utilize signature-morphing methods that can quickly outpace our ability to adapt.

In Q1, 2012, McAfee reports that "…this period shows the largest number of malware detected per quarter in the last four years!" [iii] and goes on to suggest the total number of pieces of malware in their database should exceed 100 million by the end of this year. Because malware has become such a growth industry, an additional defense approach is needed—whitelisting. Application whitelisting permits only applications and executable files which are on the "approved list" and blocks everything else. The onus, then, is on the administrator of the whitelisting system to determine what is safe, and to ensure that critical applications are not omitted from the approved list.

While both blacklisting and whitelisting approaches are being employed in many industries, perhaps none is as cautious as the control systems industry. Exploitations may range from the annoying, merely irritating to financially harmful in traditional information systems, and even approach levels of national security. For control systems, these exploitations can have safety issues, with potential loss of life or damage to the environment.

Application Whitelisting 101

The basic concept behind application whitelisting is to permit only good known files to execute, rather than attempting to block malicious code and activity. Application whitelisting accomplishes its objectives by creating a list of approved hashes and allowing only files with approved hashes to execute.

The general concept is quite simple, but the application of the concept can be complex. In general implementation, conflicts can arise in today's open creative workplace. Control systems are less tolerant of the limitations that can result from an application whitelisting implementation.

Why white list? Perhaps your first introduction to the "white list" approach was for email management—specifically, for eliminating spam and allowing messages you want to receive. We see it today as a way to prohibit unapproved software/applications from running on the protected system. "Good" software makes its way onto the white list, while unauthorized software is prohibited from executing. Whitelisting is a good defense against certain types of "zero day" intrusions, but cannot protect against all zero day defects.

Application whitelisting can be applied in a monitor only mode, and is used in this manner typically by organizations that cannot lock down systems—due to operational issues. When used in this manner the whitelisting system can provide visibility as to the executables running on a system and can be used to detect, confirm and respond to attacks.

Whitelisting does put in place a capability to enable better change management, protecting against unauthorized changes to the system configuration—an approach that might have provided some defense against Stuxnet. Some asset owners are now implementing whitelisting in response to NERC-CIP requirements.

Forward-thinking whitelisting advocates are looking at advancements in whitelisting as a way to quarantine unauthorized software upon discovery, quarantine after blocking, enhance whitelist management, and as a way to produce a file system inventory that can accelerate verification of software on a hardware platform.

Application whitelisting is designed to prevent unauthorized applications from running, and should:

- Enforce a list of approved applications,
- Include an administration tool that allows for adjustment to the whitelist, and
- Monitor and report attempts to violate the policy.

For control systems, whitelisting solutions must undergo the same level of scrutiny that was used on anti-virus solutions over the past several years. Much of the experience with security tools has been at the Business Information Technology (IT) level. When it comes to security, the focus of Business IT is ***different*** from industrial control systems. This point of discussion has been documented in many publications, including the National Cyber Security Division of the Department of Homeland Security.

Figure 2: Level of Importance

The simple way of stating the differences is C**IA**—Confidentiality, Integrity, and Availability—and the level of importance associated with each area. According to the referenced report[iv], Business IT ranks Confidentiality and Integrity with high importance, and Availability with lower importance.

You might guess that industrial control systems have a different view, with Availability at the very high importance level, Integrity at medium importance, and Confidentiality ranked as low importance. More easily stated, industrial control systems rank the importance of these three elements in reverse order from Business IT's ranking.

As you might expect, whitelisting was designed and architected for the enterprise environment (Business IT). Industrial control systems provide some unique challenges for whitelisting products, including:

- Availability and access for downloading the latest updates,
- Processing requirements that prohibit rebooting except at specific times,
- Legacy systems that have limited resources available,
- High importance of stability,
- Importance of meeting Critical Infrastructure Protection (CIP) standards set forth by NERC for the electricity industry and similar standards in other industries.

This list of challenges applies not only to whitelisting, but to most mechanisms that are deployed for industrial control systems. That is why Honeywell tests any and all new technologies extensively on its core control systems. We understand the essential need for availability in process control environments.

Managing the Whitelist

One of the major considerations when implementing an application whitelisting solution is how to manage the whitelist. Available whitelisting solutions provide a variety of management options.

Most application whitelisting products will include one or more of the following management methods.

- **The Gold Image**—This option is a good solution for situations where software is relatively static and not subject to a lot of change. The idea is that a standard workstation image is hashed and becomes the *gold image*. For user workstations, this gold image is only the starting point and changes often in most organizations. After building the workstations to the first whitelist, keeping it up to date becomes a challenge.
- **Digital Certificates**—This option is one of the most effective techniques because it can recognize certain publishers of software, since most software vendors digitally sign their applications. The digital signature can then be used by the whitelisting software to approve software automatically from a trusted vendor list. This approach can be of great help in a Microsoft environment on *patch Tuesday*, where updates from Microsoft with the trusted digital signature will automatically be accepted. This approach can be very helpful in enabling organizations to create general policies to trust certain software publishers while still blocking malicious code.
- **Trusted Update Methods**—This method is based on a set of pre-defined accounts, processes or network locations that are trusted automatically. For instance, a key process that needs to be trusted is patch management. Rather than go through a time-consuming process of recalculating hashes against a known good image, most organizations will opt to trust updates from their patch management systems. Other options in the method include trusted network shares and trusted user accounts, where installation files may be placed for approved programs, and the associated file hashes are added automatically to the whitelist.
- **Manually approve updates to the system**—This method carries the most overhead, but has lower risk if implemented properly, with adequate checks of all files added to the system before approving them.

Hence, we can conclude that administration of the whitelisting system is a key function that must be understood and planned.

Critical Functions

When considering application whitelisting software, keep in mind the critical functions that you expect that software to perform. A great deal of discussion in the marketplace has resulted in lists of these functions, and there are some variations in what some consider to be critical. However, there is a basic set of functions that should be present, including:

- **Accuracy/Effectiveness**
  The application whitelisting software should accurately identify and fingerprint applications and services on a given platform using one or more of the management methods discussed above.
- **Coverage**
  Coverage entails the breadth of file types covered by the solution. Whitelisting solutions can cover executable files, scripts, macro modules, and even write-protect any text or configuration file. Many whitelisting tools only cover executables (.exe files) and dynamic-link libraries (DLLs), not addressing code such as Java, ActiveX and specialty code such as drivers and kernel components. Most AWL solutions inspect the file header of all files on the system to determine which files are “of interest” based on the likelihood that they could be executed. AWL solutions do not typically rely on file extensions.
- **Administration**
  Administration addresses the level to which administrators can manage the system, the flexibility of the interface (allowing administrators to define trusted updaters, configuration in either audit or enforcement mode, etc.).
- **Reporting**
  Reporting can take on the added benefit as a prevention tool. The mechanisms that monitor and report on the actions of the tool within an environment vary, but it is important to understand what provisions are available with the tool, to determine if those provisions are adequate for your operation, and to evaluate how the tool will help in detecting, confirming and responding to attacks.
- **Value**
  While value may not be considered a critical function, the benefits upon which it is based entail certain functions that, if not present, devalue the solution. Value, then, is based on the cost of the tool measured against benefits to the operation. These benefits may vary by organization, but would include such measures as ease of integration, ease of deployment, and enhancement to the defense in depth strategy. An additional measure of value for certain industries is how whitelisting might fit into compliance strategies (such as NERC Critical Infrastructure Protection sections focused on change and configuration management; patching, malware prevention and privilege control; and incident handling and reporting).

Figure 3: Industrial Cyber Security Phases

Where Does Whitelisting Fit?

Industrial Cyber Security Solutions – Lifecycle Overview

Taking a logical approach to managing the Industrial Cyber Security lifecycle is key to securing your critical infrastructure. Each phase in the lifecycle is important, and the Assess phase is perhaps the most revealing. Assessing assets and vulnerabilities against industry standards and best practices provides a roadmap to eliminating or diminishing revealed areas of risk. During the assessment phase, the applicability, deployment strategy and proper selection of technologies like AWL will come to light. In future assessments the effectiveness and value of your AWL solution will be evaluated to ensure your solution evolves over time in line with security needs.

The Remediate phase begins by addressing vulnerabilities and misalignment with industry standard and best practices. A custom-designed security program is one of the deliverables from this phase. If you are just starting out with AWL and do not currently use it anywhere, this is the phase of the security lifecycle in which you will likely deploy AWL.

Once remediation has occurred, it is necessary to keep the network and security programs at their optimum level. This activity occurs in the Manage phase of the Industrial Cyber Security lifecycle. In this phase, ongoing management of systems and technology would include anti-virus and patch management services and network perimeter management.

The Assure phase requires the integration of multiple data sources along with the tools and functions that enable the ability to manage and to react to change. It is important that the design of an AWL technology be configured in such a way as to allow for visibility of data and easy access to reporting tools.

Conclusions

Cormac Herley, a principal researcher at Microsoft Research, argues that the existing data on the estimated losses from cyber attacks is wildly inaccurate to the point that analysts have no idea what the problem's economic impacts are.[v]

The discovery of the Stuxnet worm in 2010 brought the potential of cyber attacks to the attention of the industrial control system community like no other previous event. 2011 was the year that most organizations demonstrated their readiness to develop and deploy cyber tools.

Stuxnet was designed to carry out acts of sabotage. Other cyber weapons, used to destroy data at a given time, are likely to be more widely used. Programs such as kill switches, logic bombs, etc., can be developed on a regular basis and deployed systematically. The challenge for industrial control systems is one of preparation, vigilance, and agility.

Is Whitelisting a Silver Bullet?

Vendors of whitelisting products, who tend to be highly optimistic, are likely to say that whitelisting is indeed a silver bullet. Is it a replacement for AV software tools?

Honeywell's position is that whitelisting should be used as a "complementary" security defense. Whitelisting application control does detect attacks that AV and other Intrusion Prevention System technologies don't, but there are attacks like buffer overflows, SQL injection and cross-site scripting that tools like AV do detect and are (so far) not addressed by application whitelisting [vi].

Whitelisting can be quite restrictive and requires compatibility and interoperability testing by industrial control system vendors (much like AV tools have required). When implementing whitelisting for control system endpoints, allowing only certain applications to run, you need to understand the execution environment. For instance, if an approved executable that creates a new file that must be executed, such as a batch or script file, that new file must also be allowed to run. Therefore, Application Whitelisting must be tailored / tweaked for all use scenarios when used on an Industrial Control System. This understanding of the implications of whitelisting is particularly important on a mission critical server.

Regardless of the depth of initial usage in control systems, whitelisting is a technology that provides another layer of defense for process control systems.

---

[i] Storm is a backdoor Trojan Horse distributed through an email message, with a subject line about weather and storms. It is suspected to be of Russian origin and accounts for as much as 8% of global malware infections.

[ii] Conficker is a computer worm targeting Microsoft Windows operating system, first detected in November 2008 that exploited a software flaw and propagated, while forming a botnet. Its combined use of many advanced malware techniques made it particularly difficult to counter. Conficker is the largest known computer worm infection since the Welchia worm in 2003.

[iii] (PDF) McAfee Threats Report: First Quarter 2012. Page 6 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf

[iv] (PDF) "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies," Control Systems Security Program, National Cyber Security Division, Department of Homeland Security, October 2009. Page 5.

[v] "Cybercrime statistics wildly inaccurate, says researcher," Homeland Security Newswire, June 29, 2011.

[vi] Automation World article: "What about Whitelisting?", March 31, 2012

For More Information

Learn more about Honeywell's Industrial Cyber Security Solutions and how they can enhance the security of your operations, visit our website www.becybersecure.com or contact your Honeywell account manager.

Honeywell Process Solutions
Honeywell
1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB

Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

www.honeywellprocess.com

WP-12-19-ENG
November 2014