Virtual Patching Solution:
Increased Protection and Reduced Maintenance for Process Control Systems
Table of Contents

Introduction .................................................................................................................................................................................. 3
Today’s Security Risks................................................................................................................................................................. 3
Virtual Patching Technique.......................................................................................................................................................... 4
How the Solution Works............................................................................................................................................................... 4
Method of Implementation ........................................................................................................................................................... 8
Conclusion ................................................................................................................................................................................. 10

Table of Figures

Figure 1: Function of vulnerability filters (Courtesy of HP TippingPoint).......................................................... 5
Figure 2: Solution behavior under rising ICMP traffic (Courtesy of HP TippingPoint) .................................. 6
Figure 3: Intrinsic high availability (Courtesy of HP TippingPoint).......................................................... 6
Figure 4: Zero power HA (Courtesy of HP TippingPoint) .................................................................................. 7
Figure 5: Transparent high availability configurations (Courtesy of HP TippingPoint) ................................ 8
Figure 6: Honeywell’s Virtual Patching solution ................................................................................................. 9
Introduction

In today's industrial organizations, patching process control system software to remove security vulnerabilities is a regular, ongoing activity fraught with risk. Significant issues, such as a software regression (i.e., a bug that causes a feature to stop functioning as intended), can be the result of installing a patch. At the same time, there is a potential for the system to become compromised if a patch has not been applied.

The calculation of whether to patch or not is governed by the tradeoff between the risk of installing a bad patch versus the risk of a penetration, which pits two equally important issues against one another. Patching a critical system may “break it” — but failing to do so could leave it open to security vulnerability.

In addition to the security risk tradeoff, there is a more pragmatic tradeoff on use of resources to complete the patching process. Whether it is mostly automated or done manually, it involves a certain amount of your valuable resources’ time that must be factored into the overall decision on how often to patch.

Today’s Security Risks

In manufacturing plants and other industrial facilities, the advent of open control system architectures and standard protocols has been a mixed blessing for enterprises. On the one hand, the evolution from isolated proprietary applications to open technology has expanded process and business information availability. On the other hand, open technology has exposed the manufacturing enterprise to a variety of electronic threats. With the further integration of manufacturing assets to Enterprise Resource Planning (ERP) systems, the risks become even greater.

The increased vulnerability of the enterprise resulting from open architectures, coupled with a rise in malware attacks, has made electronic security a major concern for manufacturers around the world.

Accidental or malicious attacks can cause significant risk to

- Health, safety and the environment
- Production
- Corporate reputation

In order to minimize risks to plant automation and information systems, it is important to implement a defense-in-depth strategy using multiple layers of protection. One such layer includes hardening of the servers and stations. As part of the hardening exercise, regular (monthly) maintenance of software is necessary to repair the various identified vulnerabilities of the Distributed Control System (DCS) operating system and applications.

Patching in a process control network (PCN) can be a time-consuming exercise, which apart from providing an increased resilience of the control system equipment against malware attacks, also introduces increased risk of failure during the patch installation process. Installing a software patch typically requires:

- Coordination with the process operations staff to determine the appropriate time slot for patching
- Actual installation of the patch
- Swapping primary and secondary server functions to allow patching on the secondary server
- Rebooting equipment to activate the modified software

Together, these factors result in an average patch processing time for a server/station of between 1-2 hours per node. This exercise soon becomes costly, since security patches are normally issued monthly and are not necessarily aligned (different
manufacturers have different patch release cycles). During the period the system is not patched, there is an increased risk of a successful exploit, an infection by a network worm in the majority of the cases.

**Virtual Patching Technique**

Thanks to an innovative technique known as virtual patching, industrial organizations can improve the patch process and raise the system’s security posture at the same time. The vulnerability filters that act on the network level provide security for the unpatched systems, allowing better alignment of the patch process with production requirements. Virtual patching, unlike traditional patching, protects the system without touching the application, its libraries, or operating system on which it is running. Additionally, “virtual patches” are available much sooner than the actual software patches. Within days after disclosure of a vulnerability, a virtual patch can become active, where the manufacturer might take weeks to months to modify and test the software.

Using a virtual patching solution, maintenance organizations can reduce the change frequency in a DCS, typically driven by the monthly distribution of the Microsoft security patches, and remain protected against network based attacks.

This solution is designed to place a shield around the control network that checks for the activity of known vulnerabilities. The virtual patching solution also offers good protection against so-called “zero-day attacks” not caught by protection mechanisms such as anti-virus software. The reason these attacks are not caught is because this same vulnerability is often exploited in various ways. A vulnerability filter is not impacted by this situation directly, since it filters the exploit of a vulnerability without being sensitive to changes in a particular signature.

Shielding works two ways. Not only does it offer protection against network based attacks or Denial of Service attacks, but it also stops the propagation of malware over the network. Often malware, both viruses and network worms, attempts to propagate to another node and frequently uses the network for this activity. The virtual patching solution can stop this propagation effectively without the need for physically disconnecting a network segment, which would have a much greater impact.

The virtual patching solution can be used to shield the following security zones:

- Control network (for example, an Experion PKS community)
- Level 3
- DMZ

The most important protection offered by this solution encompasses vulnerability, Denial of Service, and threshold filtering.

**How the Solution Works**

The virtual patching solution (which is an Intrusion Prevention System (IPS) in network terminology) filters the traffic between two points, using vulnerability filters. These filters are designed to detect and block traffic that violates application protocols (e.g., a Remote Procedure Call (RPC) vulnerability) and/or satisfies conditions known to compromise application software flaws (e.g., a buffer overflow, SQL injection). This approach is used to shield the control network (or a subnet, for example, an Experion PKS community) from traffic coming from Level 3 or above, or traffic flowing between communities. The solution cannot be implemented to guard real-time traffic within a Fault Tolerant Ethernet (FTE) community, since acting on traffic within the control network directly impacts DCS performance and functionality.
The virtual patching (VP) solution employs vulnerability filters, which behave like a network-based virtual software patch to protect downstream hosts from network-based attacks on unpatched vulnerabilities. The vulnerability filters are created as soon as new vulnerabilities are discovered to pre-empt any attacks. These intrusion prevention system filters operate on reassembled Layer 7 information to inspect application flows fully (See Fig. 1).

![Diagram of vulnerability filters](image)

(1) A vulnerability is a security flaw in a software program.
(2) An exploit is a program that takes advantage of a security flaw to gain unauthorized access to a vulnerable system.
(3) Simple exploit filters are written only to a specific exploit, resulting in missed attacks, false positives and continued vulnerability risk.
(4) Vulnerability filters act as a virtual software patch and cover the entire vulnerability, with no false positives or false negatives.

Figure 1: Function of vulnerability filters (Courtesy of HP TippingPoint)

The Threat Suppression Engine of the VP protection device enables the traffic anomaly filters used to detect changes in traffic patterns also to detect and prevent threats, such as denial of service, peer-to-peer attacks, unknown worms, rogue applications and zero-day exploits. These filters are adaptive and learn about normal traffic patterns for the particular environment in which the VP solution is placed. Once traffic is baselined, the VP filters will detect statistical anomalies based on tuneable thresholds.

Of particular importance is the solution’s ability to rate-shape traffic flows based on application types, protocols or IP addresses. Protocol anomaly filters run simultaneously via the Threat Suppression Engine to detect out-of-spec network traffic. The filters detect conditions that are both necessary for an attack’s success and guaranteed never to occur in normal traffic. They can detect multiple attacks without false negatives or false positives.

Threshold filters establish a baseline of normal traffic levels by monitoring network traffic for a specified number of hours or days. These filters are configured to take specified actions when the traffic rises above or drops below a threshold. For maximum flexibility, four thresholds are available from the solution: minor and major thresholds either above or below normal.

Assume the normal level of Internet Control Message Protocol (ICMP) traffic is 2 Mbps. An administrator could configure two thresholds: one to send an alert when ICMP traffic rises to 200% of normal level, and another to rate-shape the traffic when it rises to 350% of normal. Figure 2 shows the effect of the solution when ICMP traffic begins to rise.
For example, the Nachi worm has the potential to cripple network performance by flooding the network with ICMP traffic. This could create excessive CPU load (>95%) on a router or host. The VP solution will limit the traffic on the Level 3 network toward the Level 2 control network and force CPU utilization to normal stable levels to prevent system downtime.

Thresholding features enable security policy implementation based on the number of bytes in a particular stream, as well as connections and packets from particular hosts with user-defined time frames, from per minute to per month.

The virtual patching solution also supports several modes of operation for redundancy. These include:

- Intrinsic High Availability
- Zero Power HA
- Transparent High Availability Configurations

**Intrinsic High Availability**: The virtual patching appliance has been designed as a redundant device from the ground up. Internal low-level system monitoring maintains operation. Upon system failure, the device will fail open, bypassing internal security processing, but allowing network availability. This process is termed Layer 2 fallback and can be configured to fail open or closed on a per segment basis. The default configuration is open (See Fig. 3).
This level of protection enables a single device deployment while allowing for high availability when budget prevents the deployment of redundant units or when redundancy is not warranted. When in Layer 2 fallback, no attack protection or detection occurs, but the device is not blocking traffic flow.

**Zero Power HA:** The Layer 2 fallback operation described above requires power and allows traffic flow on both copper and fiber segments. It prevents an internal device failure from stopping all traffic flow, but requires power. Zero power HA is an external copper unit designed to pass traffic around the VP device at Layer 1 upon power failure. It consists of twenty RJ45 interfaces, and five groups of four interfaces, to cover five segments. These interfaces are wired, pin-to-pin, through switches that are open when receiving power and closed when not powered. The unit as a whole receives power through a USB cable connected to the VP device. When the zero power HA device loses power, traffic flows without being impeded, but no security processing is accomplished. In Figure 4, the dark lines represent the cabling of such a deployment.

The zero power HA option was designed for deployments where a redundant unit could not be used due to budget constraints, or where it was not warranted, but higher redundancy requirements were in place. The use of this solution must be weighed against the security benefits gained from a redundant implementation where the network is always protected.

Two zero power HA models are available: one with fixed copper ports and another with modular slots for copper or fiber ports. Any given zero power unit cannot be shared between two or more VP devices, since a single USB cable connected to a single VP device powers it. However, a single unit can protect multiple segments.

**Transparent High Availability Configurations:** The final scenario is the most encompassing. The virtual patching solution platforms can all be implemented in a redundant configuration, either active-active or active-passive. The units can be configured to maintain state across the two devices so attacks are blocked on both sides (See Fig. 5).
When using these methods of path determination, it is possible for the redundancy protocol to not detect the path down due to the physical connection being lost on the far side of the VP device. The link from the VP device to the router/switch/firewall is maintained. Only monitoring link status defeats the purpose of the redundant architecture. The solution utilizes a work around solution to this issue, called link-down synchronization (also called Sympathetic HA). This approach allows configuring the virtual patching device to force both ports down on a segment when the device detects a link state down on one of the ports. When link-down synchronization is enabled, the appliance monitors the link state for both ports on a segment. If the link goes down on either port, both ports on the segment are disabled. This functionality propagates the link state across the VP device.

For example, in the case of redundant routers A and B, if the link to Router A goes down, then both ports are disabled, resulting in the link to Router B becoming the primary path.

If the link goes down on one port, link-down synchronization can be configured to maintain the partner port. It is also possible to have the system disable the partner, requiring a manual restart to bring them both up or to bring up the ports automatically when the link is restored.

In addition to the ability to enable link-down synchronization for each segment, it is possible to change the amount of time after detecting a link is down before forcing both ports down on a segment. The default is 1 second and can be configured from 0 to 240 seconds. Once link-down synchronization is enabled for a segment, monitoring of that segment begins only after link up is detected on both ports.

**Method of Implementation**

Plants seeking to implement the virtual patching solution can obtain assistance from Honeywell Process Solutions (HPS). This virtual patching solution is aligned with the HPS Industrial IT Solutions security perimeter management service, which provides remote management and maintenance of the solution. Activities included in this service are:

- Use of a virtual patching and intrusion prevention system that filters network traffic at critical conduits in the process control network.
- Monitoring security events and responding to events when detected.
- Consultancy on the subject of filter selection and configuration.
- Updates of the filters and alerts for raised attack activity requiring enabling of specific filters.
The virtual patching service provides an effective approach to shielding the PCN and DCS from being infected by network worms. It enables users to minimize patch installation frequency while staying protected. The service also provides support on device failures (e.g., troubleshooting, parts replacement) and saves time and money by reducing in-house staffing requirements, training, maintenance and infrastructure costs.

As part of the virtual patching service, the Honeywell Remote Service Center (RSC) performs continuous security monitoring of PCN traffic and maintains security filter policies and vaccine. It also provides security and compliance reporting, as well as software maintenance for appliances. Certified security engineers trained on the solution application carry out implementation.

As an option, the virtual patching service can have a remote connection to the Honeywell Security Response Center (HSRC). In case of emergencies, clients with a 24 x 7 contract extension can also rely on support of the HSRC during non-office hours. The VP device is managed from the HSRC (part of a remote security perimeter management service) or locally (See Fig. 6).

Implementation of virtual patching solution comprises several phases:

- Design– determine which security zones to shield and what level of availability is required.
- Installation and tuning– after initial setup, the solution provides immediate value by offering protection for many known vulnerabilities. However, the solution can be tuned to allow traffic to pass unfiltered (i.e., a backup data stream) and to set special filters for site specific traffic.
- Maintenance– after installation and tuning, maintenance of the vulnerability filter database and configured security policies is required. The solution reports back to a management server at the Honeywell Security Response Center to retrieve new filters and provide for 24x7 monitoring and advanced reporting.
The solution provides:

- One or more VP devices with Zero Power HA modules that segment traffic for the indicated security zones/conduits
- Services to design and implement the solution
- Optional services for remote management of the solution
- Documentation of the solution

Conclusion

The virtual patching solution, as implemented and maintained by Honeywell Process Solutions, offers industrial operations increased protection against the risks of zero-day attacks and can significantly reduce the impact of a malware infection. This innovative technique reduces the rate of change induced by security patches for the shielded control networks, providing increased reliability while improving security posture. Clients can improve the patch management process by having more control over the moment of security patch installation and, consequently, achieve significant cost savings.