



SECURING FIXED FUNCTION DEVICES



Security Connected

The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.

At the 2010 Black Hat Conference, a security researcher demonstrated how to hack an ATM machine and make it spew out cash.

Minimize Risk on Fixed-Function Devices

Challenges

Fixed-function devices are becoming mainstays in virtually every industry. They include: point-of-sale (POS) systems, ATMs, medical equipment, industrial control systems, mobile devices, multifunction printers, automotive and aeronautical systems, and beyond. Many are purpose-built and only capable of performing a few specific tasks, while others are more generalized and run atop common operating systems with standard services and capabilities available. In either case, these devices suffer from some key security issues.

- The underlying operating systems and applications are rarely, if ever, patched; many of these devices run out-of-date operating systems that are no longer supported which means that they can't be patched
- Because they are designed for a fixed purpose, they often lack system resources such as CPU, memory, and storage necessary for the installation and operation of additional security controls such as host-based intrusion prevention systems (IPS), firewalls, and related controls
- In many cases, the installation of additional software, such as security controls, or the modification of the system through patching, voids vendor warranties
- Many devices don't have network connections, have slow networks, or out-of-band network connections; this coupled with limited system resources means that even traditional blacklisting and signature-based antivirus is not feasible because:
 - » Updates are too frequent and consume too many network resources during download
 - » The storage footprint of the antivirus software and its updates are too large for installation

- » Scan-based solutions consume the limited CPU and memory resources needed for operation
- » Many solutions such as Microsoft Windows XPe, which is a popular POS operating system, won't even allow traditional antivirus to be installed

After being hacked, several restaurants sued the makers of their point-of-sale system, alleging they should be responsible for fines levied by payment processors.¹

Many organizations that operate fixed-function devices measure the lifecycle of those devices over decades, not over years, as is the case with most IT solutions. This means that swapping out older equipment isn't always practical and legacy and end-of-life solutions must still supply value. Those systems that can be patched can't be patched as often because of the above-mentioned issues. As a result, patch frequency and urgency must be minimized so as not to disrupt operations while security risks are kept in check.

Just because an asset is classified as a fixed-function device, it's not immune to auditors who are investigating compliance with regulatory mandates. Two prime examples are POS systems within the retail industry regulated by PCI DSS and industrial control systems within the electric industry regulated by NERC.



In 2010 Stuxnet was responsible for attacking programmable logic controllers around the world, with Iranian nuclear facilities being hit the hardest. The attack set their nuclear program back several years and cost the country millions of dollars.²

Solutions

Solutions for fixed-function devices can be applied by the vendor—through an OEM relationship, for example, or after the fact, depending on the solution. In whatever way these devices are protected, security shouldn't be an afterthought. There are three general controls that should be considered to help mitigate risk on fixed-function devices: dynamic whitelisting, change management, and integrity.

Dynamic whitelisting

In many scenarios, dynamic whitelisting can augment traditional blacklisting antivirus software. However, because of the specific security issues outlined earlier, dynamic whitelisting can be used instead of traditional antivirus products. These types of controls should require minimal system resources to operate. They should not require updating or even network connectivity to operate. They should protect even end-of-life equipment from known and zero-day attacks by not allowing processes, registry changes, software installation, file creation, and the like to occur without explicitly being allowed. Two of the biggest gains are that patch urgency will be reduced and malware can't be installed. This helps with ROI by maximizing the life of legacy equipment and not only stops the installation of malware, but it should also stop the installation of any unauthorized or unwanted software that might negatively impact the security and operations of the device.

Managing change

There is often a gap between authorized, documented change and actual change activity. Security solutions for change control should provide real-time, forensic situational awareness into any changes. There should be full accountability associated with every change and validation to ensure that the intended changes

were applied. Beyond detection, there should be preventative controls that disallow unauthorized changes. As an example, changes should be automatically evaluated against change policy, gold configurations, authorized administrators, time and date checks, and other parameters. For changes that meet these requirements, changes should be made and a record should be kept. Out-of-policy changes should generate an alert and a report of the changes made, or depending on organizational policies, the change should be blocked. For fixed-function devices, ensuring that changes are addressed through a secure, repeatable process is paramount when operational availability is essential.

Monitoring integrity

Integrity is critically important to security and compliance. Solutions in this area should help provide assurances that malicious or careless activity has or hasn't compromised the integrity of a system. Knowing the current state of a system—its trusted state—and tracking changes from that point on helps provide those assurances. Monitoring integrity needs to take place at the file and directory level for fixed-function devices. Further, these solutions should identify both changes to content and permissions. In addition to the security benefits, demonstrating compliance with regulatory mandates can also be achieved. Once again, consider PCI DSS requirements around file integrity monitoring. A solid solution geared for monitoring integrity should address items 10.5.5 and 11.5, which state that organizations are required to monitor the integrity of log data and generate alerts if an unauthorized modification of a critical system or content files is made. By doing so, the secure running state of the fixed-function device can be validated.

Best Practices Considerations

- Analyze the security capabilities of fixed-function devices and the security of OEM relationships they are employing
- For fixed-function devices and assets that interact with those fixed-function devices, apply controls for dynamic whitelisting, managing change, and monitoring integrity
- Protect from known and zero-day attacks
- Reduce in-field breakage incidents often caused by human configuration errors
- Eliminate or reduce patch urgency
- Monitor know good system states against existing run states
- Keep devices compliant with security standards

Human error, such as mistakes made to system configurations, can be caused by fatigue, increased work demands, insufficient training, inadequate supervision, insufficient time to double-check work, inadequate data, unclear instructions, and poorly designed technology user interfaces.

Value Drivers

The strategy and efforts of your security practices in this area can have a considerable impact on your operational value to the organization. Build a compelling business case to demonstrate the ability to manage risk and lower costs. For example, whitelisting and change management technologies in this area can provide direct cost savings as follows:

- Loss prevention due to downtime of critical systems due to patching
- Loss prevention due to downtime of critical systems due to unwanted or unauthorized change
- Increasing the length of use (useful life) of legacy operating systems

Related Material from the Security Connected Reference Architecture

Level II

- Protecting Information
- Controlling and Monitoring Change
- Obtaining Benefit from PCI

Level III

- Assessing Vulnerabilities
- Securing Automatic Teller Machines (ATMs)
- Securing Point-of-Sale (POS) Systems
- Securing Medical Devices

For more information about the Security Connected Reference Architecture, visit:

www.mcafee.com/securityconnected.

About the Author



Brian Contos, CISSP, is director of global security strategy at McAfee. He is a recognized security expert with nearly two decades of security engineering and management experience. He is the author of several books, including *Enemy at the Water Cooler* and *Physical and Logical Security Convergence*. He has worked with government organizations and Forbes Global 2000 companies throughout North, Central, and South America, Europe, the Middle East, and Asia. He is an invited speaker at leading industry events like RSA, Interop, SANS, OWASP, and SecTor and is a writer for industry and business press such as *Forbes*, *New York Times*, and *The Times of London*. Brian is a Ponemon Institute Distinguished Fellow and graduate of the University of Arizona.

brian_contos@mcafee.com || <http://siblog.mcafee.com/author/brian-contos/> || @BrianContos

1 http://www.pcworld.com/businesscenter/article/183499/restaurants_sue_vendors_after_pointofsale_hack.html

2 <http://blogs.mcafee.com/enterprise/critical-infrastructure-protection/stuxnet-a-view-from-an-energy-perspective>

