

KIOSK Information Systems Integrates Intel Security

Intel Security Solutions Enhance Security
and Streamline Development

By Steve Hoffenberg, Director, with Chris Rommel, Executive Vice President
VDC Research Group

The Challenge

Although cybersecurity threats have been present since the early days of computing, hacking activity has ramped up dramatically over the past several years, as evidenced by numerous high profile and publicly embarrassing data breaches. These attacks are often driven by financially motivated gangs who are well organized and technically sophisticated. From networks of dedicated or compromised computers throughout the world, these hackers are constantly probing the Internet in search of vulnerabilities enabling them to procure sensitive information that is directly exploitable and/or saleable on the black market. Amid this rising threat, manufacturers of embedded systems—particularly those that deal in financial transactions—are at risk, perceived by hackers as real pots-of-gold at the end of virtual rainbows.

The potential for software vulnerabilities is highlighted in a recent survey of engineers at embedded device manufacturers conducted by VDC Research, in which a combined 61% of respondents rated security as “important,” “very important,” or “critical” in their current projects, yet only 29% of respondents’ projects required embedded security software components.

Self-service kiosks constitute a category of embedded systems that are not only connected to the Internet, they often conduct financial transactions and connect to internal networks of major corporations or institutions, where databases contain other financial records, intellectual property, or personally identifiable information.

In addition, self-service kiosks are frequently located in public spaces where their electronic systems may be exposed to tampering via USB, Bluetooth, Wi-Fi, or other means of local area connectivity. Such installation sites can provide attackers with repeated access to the systems over extended periods of time, as they attempt to exfiltrate stored data or reverse engineer security protocols with which to base attacks on additional kiosk systems elsewhere in the field or on the corporate networks to which they are connected.

Further complicating the development of secure systems by kiosk manufacturers is that many kiosk users have little or no prior experience with a specific user interface, have little time in which to learn and interact with a device, and cannot be subjected to overly intrusive security measures.

In short, kiosk security needs to protect against hackers both local and remote, while simultaneously remaining unobtrusive to neophyte users, a truly challenging combination for any equipment maker.

The Solution

Founded in 1993, KIOSK Information Systems (KIOSK) is one of the world’s leading manufacturers of self-service kiosks for retail point-of-sale (POS), financial services, vending, ticketing, gaming, border security, and numerous other vertical markets.

When KIOSK recently was designing a system of self-service devices for deployment of thousands of units by a prominent customer, the system not only needed to meet KIOSK's and the customer's own security requirements, it needed to be compliant with the stringent Payment Card Industry Data Security Standard 3.0 (PCI DSS 3.0) to protect user credit and debit card data within the terminal as well as segment cardholder data at the merchant from other IT infrastructure.

Retail and other POS devices are under increased attacks, and compliance with PCI DSS 3.0 is a vital step for manufacturers to better protect both their retailers' and their end users' valued data. The 3.0 version of the standard, to which compliance became mandatory in 2015 for systems handling payment card data, is comprised of 12 top-level requirements and more than 200 detailed sub-requirements and testing procedures.

To bring comprehensive security to the new KIOSK system and help enable PCI DSS 3.0 compliance, the engineering team turned to the Intel Security group within Intel. "We chose to work with Intel Security," says Charley Newsom, Chief Technology Officer at KIOSK, "because it offered a complete embedded security solution from a single, high credibility vendor who was readily able to tailor it to our system – in a fraction of the time it would have taken to integrate it ourselves."

After carefully evaluating KIOSK's security criteria, the two companies chose to implement a bundle of Intel Security embedded security technologies for retail systems, including:

- McAfee Integrity Control – a package of security solutions for retail POS with:
 - McAfee Application Control – ensures through centrally managed dynamic whitelisting that only approved applications can run in the device software stack
 - McAfee ePolicy Orchestrator (ePO) – centrally manages and monitors security status throughout the network, and assigns/enforces security policies for users, devices, and applications
 - McAfee File Integrity Monitoring – continuously monitors data files to detect and log changes by users and applications
- McAfee Anti-Virus – detects and prevents malware attacks via signature-based blacklists
- McAfee Firewall – establishes and limits connections between internal and external networks to block incoming attacks
- McAfee Device Control – prevents data loss via removable storage media

Intel Security engineers worked closely with KIOSK development staff to customize the security solution for the specific hardware and software stack in the devices, as well as for the host system to which it connects. The result was a self-service kiosk with improved resistance to tampering and malware, as well as greater control over updating and patching of embedded software, supporting crucial PCI DSS 3.0 requirements number 1, 3, 5, 6, 10, and 11.

The Impact

The KIOSK system secured with this new combination of solutions developed by Intel Security was able to pass the rigorous penetration testing mandatory for PCI DSS 3.0 compliance without issue on the first try, a significant achievement. The system then similarly passed a subsequent round of penetration testing for PCI DSS 3.0 compliance independently commissioned by the customer.

The KIOSK system has since been deployed in the field for over a year. With more than 2,100 units now in service, thus far the system has experienced no known security breaches. Furthermore, this multi-layered security approach is invisible to end users who have relied upon it to protect millions of credit and debit card data transactions.

The customized Intel Security security solution has been so successful that KIOSK now offers it to other customers as a standard product called Enhanced Security Suite. Working with Intel Security to create the Enhanced Security Suite has furthered KIOSK Information Systems' position as a trailblazer in the self-service industry, and VDC believes that in today's heightened threat environment, it represents a competitive advantage over kiosk systems from other vendors.

Recommendations

For device makers across vertical markets—especially those whose systems deal with financial transactions or other sensitive data—the KIOSK partnership with Intel Security exemplifies several VDC recommendations for security best practices that make the IoT safer for both device makers and end users.

Consider Security From Day One

OEMs need to take security into account right from the start of a project, as security can greatly impact both hardware design choices and software development requirements, not to mention bill of materials costs and engineering schedules. A desired security feature could, for example, dictate the need for Trusted Platform Module hardware in the microprocessor, an increase in available RAM, or the procurement and integration of third-party code modules.

Gone are the days when an engineering group could design a product, then tack on security as an afterthought, or worse, not tack it on at all.

Know What's Required Before Starting

Many industries require certifications or compliance to regulatory security standards, which may apply not only to completed systems, but also to the processes by which those systems are developed. Software developers

should know in advance, for example, if they have to submit source code for compliance assessment, so they don't license any software for which only compiled binaries are available.

Standards can vary by country or geographic region, so prior to beginning development, OEMs need to know which standards apply to the category of product they're planning to build for which vertical market and country.

Plan to Get Hacked

Security measures should be designed to handle the worst case scenarios that hackers could throw at a system: compromised passwords, stolen hardware, breaches elsewhere in the network, etc.

OEMs need to consider not just how to keep out hackers, but also how to minimize the damage that hackers could do if they are able to penetrate a system. Perimeter security is necessary but not sufficient. For devices which handle sensitive data—or are merely connected to networks which handle sensitive data—a multi-layered approach is recommended to protect the hardware interfaces, operating system, middleware, application software, data storage, communications channels, datacenter, and cloud services.

Call in Security Experts, Twice

Even engineering teams that have experience implementing security features may have overlooked critical vulnerabilities. Electronic design engineers, software developers, and QA testers are not necessarily experts in embedded system security. Whenever possible, engage security experts—either company internal or third-party—early in the product development process, to provide input into product design.

Commercial vendors of security solutions, such as Intel Security, can offer software and services that have passed specific compliance tests when integrated into otherwise compliant systems. Leveraging solutions pre-validated for compliance with particular standards can save considerable time and expense compared to developing solutions in-house then testing them for compliance and possibly reworking any security deficiencies.

Then, when prototypes are available, OEMs should call in experienced penetration testers to attempt to hack their devices and assess their vulnerabilities and risks of attack. These experts use many of the same tools that hackers use to find and exploit connected devices. Although penetration testing doesn't guarantee impenetrability, it may uncover a number of security flaws that can be fixed prior to product release. Don't let hackers (or customers) find these vulnerabilities first.

About VDC Research

Founded in 1971, VDC Research provides in-depth insights to technology vendors, end users, and investors across the globe. As a market research and consulting firm, VDC's coverage of AutoID, enterprise mobility, industrial automation, and IoT and embedded technologies is among the most advanced in the industry, helping our clients make critical decisions with confidence. Offering syndicated reports and custom consultation, our methodologies consistently provide accurate forecasts and unmatched thought leadership for deeply technical markets. Located in Natick, Massachusetts, VDC prides itself on its close personal relationships with clients, delivering an attention to detail and a unique perspective that is second to none.

For more information, contact us at info@vdcresearch.com.

Product, brand, and company names contained in this document are trademarks or registered trademarks of their respective holders.