Some systems are out of sight - don't let them be out of mind

Challenges facing embedded systems security

kaspersky

Every embedded system is a target for cyberattack

We're surrounded by embedded systems, and whether we realize it or not, we use them every day. ATMs and POS systems, information kiosks, medical devices and old computers, all these disparate systems are an integral part of nearly every aspect of our lives. And every embedded system is a potential surface for cyberattack…

We all know that the current threat landscape requires that we protect every part of an IT infrastructure, including the perimeter (web and mail traffic), desktops, laptops, servers, virtual infrastructure, even mobile devices. But what about those devices that fall beyond this scope of protection – and even outside the scope of maintenance?

Embedded systems are produced in vast quantities, designed to perform a very specific task or set of tasks - to dispense cash, for example. But unlike ordinary PCs used by a single or few users, who are more likely to be tuned into maintenance and updates as they become necessary, embedded systems don't have a single user to rely on. And when one device is exposed and attacked, it can open the door to a world of opportunity to cause considerable damage and disruption.

Many embedded devices use old hardware and software, and because they operate smoothly, updating them isn't always a priority. As support for Windows 7 winds down – ending on 12 January 2020 – there is still time for companies to update the OS in their embedded systems, and take any additional protection measures necessary. However, older Windows XP - still an extremely popular OS for embedded systems – is still being overlooked, even though support for that OS ended in 2016. This is an open invitation to hackers.

Let's look at some of the most common scenarios that impact the security of these systems, and the businesses that run them - and how to keep them safe.

Finance

ATMs

It's not hard to see why ATMs are so enticing for hackers. They contain hard cash. They're everywhere, on nearly every street corner across the globe. And their security is often overlooked and inadequate…

There are a few reasons why this is the case. While ATMs are a familiar part of the banking infrastructure, banks frequently outsource the maintenance of their ATMs to third-party service companies, in effect putting them 'out of sight, out of mind', almost handing off responsibility. And although PCI DSS regulations require banks to secure ATMs with a set of specific measures, for older hardware and systems, it's not adequate or satisfactory. A significant number of ATMs still in use today worldwide are old, often more than 10 years old – a lifetime when it comes to IT and cybersecurity. These machines run outdated, unsupported Windows XP OS on this old hardware, leaving them vulnerable to modern threats and attacks.

Cybercriminals looking to attack ATMs can do so in numerous ways. The most popular approaches include:

- Infecting ATMs manually one by one, or through the network, and then inserting some hidden code that allows them to carry out jackpotting
- Either manually one at a time or through the network, infecting ATMs and using malware to steal credit card data which they then sell on the dark web
- Infecting an ATM and using it as a gateway to attack other network segments, computers, servers and applications.

ATM jackpotting is where jackpotting malware forces a machine, or multiple machines, to spew cash, similar to a slot machine. Two of the best-known ATM malware are WinPot and Cutlet Maker, both for sale on the Dark Web for as little as $500 – a trivial sum considering the potential jackpot in the event of a successful attack on a nice, full ATM machine. Almost anyone with even basic knowledge can mount an attack using these tools and the step-by-step instructions they're sold with.

In a globally coordinated attack over a period of two days, hackers stole the equivalent of over £10-million in nearly 15,000 ATM transactions from ATMs in 28 countries.

Retail, transportation and others

Point of Sale systems

Following its well-publicized NonPetya attack, shipping giant Maersk had to undergo an almost complete infrastructure overall.

Carphone Warehouse faces GDPR fines totalling £400-million after a massive data breach compromised customer data, including payment records.

Point of Sale (POS) systems are used wherever something is sold – milk from the supermarket, your train ticket at the railway station, paying for electricity. For the most part, POS systems accept cash and bank cards and therefore, follow PCI DSS regulations. However, as is the case with ATMs, many cash registers and vending machines are way past their sell-by date, running on old hardware and outdated, unsupported Windows XP OS.

A specific area of vulnerability for POS systems is the middleware they depend on. This middleware tends to be created by third-party vendors or in-house and functionality may well take precedence over security as a design consideration. As with ATMs, easy access to USB ports and CD/DVD drives may be seen as a convenience, rather than a security weakness.

Due to their pervasiveness and age, and the valuable data they hold, POS systems are also extremely attractive targets for cybercriminals, who use them to carry out illegal activities, including:

- Stealing payment card data in 'hidden' mode, so that bank security has no evidence that a compromise has taken place
- Stealing authentic personally identifying information (PII) – name, address, contact phone numbers, email information, etc., that can be used to identify or locate a specific person – to sell to the highest bidder. Identity theft is a booming industry.
- Using the POS as an entry point for a wider, targeted attack on an organization and its systems.
- Using ransomware to block normal POS operation and disrupt an entire company from carrying out its normal business, with severe consequences, including losses in revenue – and staff...

Interactive kiosks

Researchers discover 19 previously unknown vulnerabilities in management system kiosks.

Unlike POS terminals, interactive kiosks and self-service terminals, in airports and shopping malls, for example, don't accept cash or use payment cards but they can offer an entry point into the wider network – and because they don't have card payment functionality, they aren't required to follow PCI DSS, and are even more likely to have little or no protection. These systems make an ideal entry point for a targeted attack or a disruptive attack that can have a knock-on effect on the wider system and business.

Healthcare

Medical devices

Researchers say that unpatched, out of date medical devices are dangerously vulnerable to attack.

The healthcare sector lags behind other sectors when it comes to protecting its data and systems, despite suffering numerous attacks globally over the years. One of the most high-profile attacks was the WannaCry cyberattack on the NHS, which cost the UK's health system £92-million.

Hospitals around the world have thousands of Internet-enabled devices connected to their networks, covering almost every aspect of patient care and including medical records. Medical equipment must be fault-tolerant, stable and available 24/7, yet these devices face risks associated with being part of the corporate network, as well as those unique to the embedded systems which they're based on. Significantly, many medical devices still run old operating systems on old hardware, and vulnerabilities in legacy technology attract cybercriminals who use these outdated, unpatched devices to gain access to devices and systems.

In this environment, cybercriminals are typically most interested in:

- Accessing medical data. Theft of medical data is arguably the most serious type of data theft of all – after all, who needs a credit card number when you can have an identity? Hackers can change even one line of code to alter a treatment plan, use ransomware to encrypt data and extort ransom, or blackmail patients about disclosing their medical conditions. For these reasons, cybercriminals love medical data – in 2018, it was reported that huge bundles of the medical data of up to 140 million patients were for sale on the Deep Web.
- Interrupting, or even stopping completely, the normal operation of a hospital or clinic.

In the last few years, there has been a 525% increase in vulnerabilities in medical devices[1], yet today, most hospitals don't even know how many embedded devices they have. How can you protect what you don't know you've got?

Manufacturing

Production control systems

Almost one in two industrial systems show evidence of **attempted malicious hacking activity** - usually due to inadequate security.

The number of cyberthreats targeting manufacturing **keeps rising** as hackers continue to penetrate outdated technologies.

Any automated terminal, whether controlling assembly line processes or orchestrating the flow of goods, relies on the stability and fault-tolerance of the embedded system at its core. If a device fails or its performance is disrupted, the impact can be devastating. The cost of unplanned downtime as a result of a cyberattack can cause a manufacturer serious problems. Embedded systems used in manufacturing also usually run on the obsolete Windows XP OS, are rarely updated, and typically reside within an internal network.

Embedded systems in automated control systems are prime targets for cybercriminals looking to:

- Cause maximum disruption and financial losses by interrupting, or even stopping completely, normal operations in targeted sabotage.
- Carry out industrial espionage and steal secrets, passing on information to competitors or holding the data, and the organization, to ransom.

Embedded systems in manufacturing present a classic entry point for targeted attacks in particular – the infamous Stuxnet, for example. According to US ICS CERT classification, in 2018 there were more vulnerabilities in various automated controls system components in manufacturing than in any other industry.

All sectors

Old hardware, old software

Not keeping your OS and apps up to date is **good news for hackers** who exploit commonly known vulnerabilities with software that delivers ransomware and then holds the encrypted data to ransom – which can run from a few hundred dollars into the millions...

We've specifically highlighted healthcare and manufacturing here because they're so essential to the normal functioning of our everyday lives. But there are embedded systems and old hardware in every other vertical, presenting the same or similar challenges when it comes to protecting them.

Many organizations still use PCs for basic, non-critical functions, using old hardware and software that haven't been updated for a decade or more. Everything seems to work well enough, so there's often no real motivation to go through a time-consuming, expensive and often impractical (in both cost and practical terms) upgrade. Some examples of this scenario include school libraries, state institutions, hotel registration desks, airport counters, the flow of goods in warehouses, and so on.

These tasks usually involve client software that does little more than send and receive requests from a server, and doesn't require too much power. But there's a problem – these older systems may still be in use, working properly, but they are vulnerable to modern threats. A chain is only as strong as its weakest link, and a single exposed device can infect an entire company infrastructure. Clearly, embedded systems must be protected, even as upgrades are being planned and rolled out.

How to protect embedded systems effectively – now and in the future

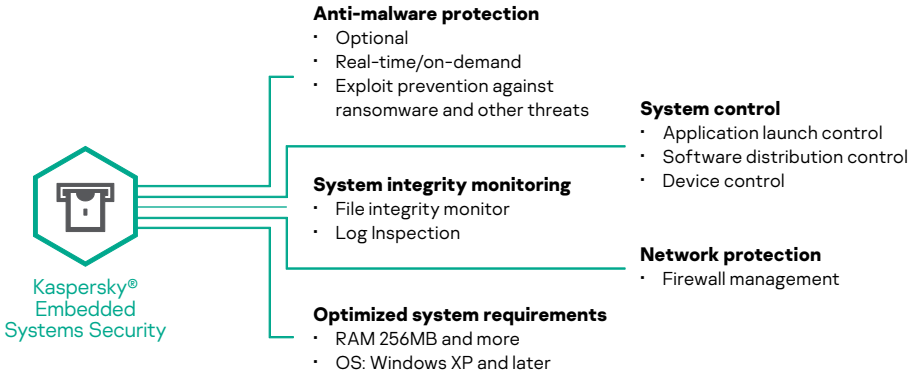
As we've seen, whether we're talking about medical devices, ATMs or critical infrastructure, embedded systems have some unique challenges while all sharing one big shortcoming: they frequently run on outdated software and old hardware. There are additional difficulties, too – their physical location, product design and wide application areas can make installation and deployment of security extremely impractical.

In this environment, a one-technology approach – just antivirus or Default Deny only (the most common methods) – is not effective; it simply doesn't deliver the necessary protection for these systems and leaves them exposed to cyberattacks.

Only multi-layered protection that has been specifically designed to tackle the unique requirements and challenges of embedded systems can secure and protect them against modern threats.

Kaspersky Embedded Systems Security

Kaspersky Lab Embedded Systems Security has been speci cally designed for organizations operating embedded systems, and the threat environment they operate in. It protects the attack surfaces unique to these architectures, re ecting their unique functionality and OS, channel and hardware requirements, while fully supporting the Windows XP family.



Anti-Malware and Memory Protection

Proven cloud-assisted protection from the industry's leading antivirus engine, capable of detecting even the most aggressive attacks.

Application and Device Controls

The basis of e ective protection for embedded systems, where everything (apps drivers, libraries, USB drives) not explicitly permitted is blocked.

File Integrity Monitoring

File Integrity Monitoring tracks actions performed on speci ed les and folders within scope. You can also con gure le changes to be tracked during periods when monitoring is interrupted.

Log Inspection

Kaspersky Embedded Systems Security monitors possible protection violations based on inspecting Windows Event Logs. The application noti es the administrator when it detects abnormal behavior that may indicate an attempted cyberattack.

Windows Firewall Management

Windows Firewall can be con gured directly from Kaspersky Security Center, giving you the convenience of local rewall management through a single uni ed console. This is essential when embedded systems are not in domain and Windows rewall settings can't be con gured centrally.

SIEM Integration

Kaspersky Embedded Systems Security can convert events in application logs into formats supported by the syslog server, so these can be transmitted to, and successfully recognized by, all SIEM systems. Events can be exported directly from Kaspersky Embedded System Security to SIEM or centrally via Kaspersky Security Center.

Flexible Management

Kaspersky Embedded Systems Security can be managed from the command line, the local GUI or the centralized policy-based management of Kaspersky Security Center.

Security policies, signature updates, anti-malware scans and results collection are easily managed through a single centralized management console – Kaspersky Security Center. In addition, clients in a local network can be managed through any local console – particularly useful when working in the isolated, segmented networks typical of embedded systems.

Licensing Options

Kaspersky Embedded Systems Security is available in two types of commercial licenses:

- Kaspersky Embedded Systems Security standard
- Kaspersky Embedded Systems Security Compliance Edition, an extended license that includes File Integrity Monitor and Log Inspection.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Cybersecurity for SMB: kaspersky.com/business
Cybersecurity for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Known more at kaspersky.com/transparency

Proven.
Transparent.
Independent.