DO NOT SHIP, OR RECEIVE, TROJAN HORSES (*)

Avoiding Network Vulnerabilities Potentially Introduced by Embedded Systems

Corey Hirsch

LeCroy Corporation, 700 Chestnut Ridge Road, Chestnut Ridge, New York, 10977, USA, Corey.Hirsch@LeCroy.Com

Abstract: Academic journals and trade press have explored several likely routes of malware contagion against which information security practitioners need to defend. These include traditional 'tunnels and bridges' that bypass the firewalled corporate perimeter, such as visitor's laptops, VPN tunnels, encrypted & zipped email attachments, unencrypted wireless, and weak authentication. A potential threat that has not been widely documented is embedded Windows ™ based systems and appliances. Corporate networks that are otherwise highly secure often have some tens of nodes that are not generally recognized as 'computers', however run networkable Windows ™ operating systems (OS). These devices range from smart phones to engineering microscopes, from oscilloscopes to print stations, and many others. They may have no single owner, and frequently generic or group user accounts are established on them. They have not been purchased by the IT department and may not appear on IT's lists of machines to patch and monitor. Vendor's practices vary widely, with results for their customers ranging from 'no issue' to 'serious risk'. This paper narrates the embedded appliance infosecurity lifecycle, to provide vendors of such systems with best-in-class precautionary measures they should take on behalf of their customers' security, and to provide purchasers of such appliances with a checklist to enable them to select secure products. LeCroy, a leader in safe and secure Windows ™ appliance engineering, provides the reference case for best-in-class practice. Research in this field is being conducted at LeCroy and elsewhere, in August 2005, by Dr. Julia Kotlarsky of Warwick Business School, and Dr. Ilan Oshri of Erasmus.

(*) Trojan Horse in this context denotes a hidden danger. It escapes detection because it is considered something other than a computer.

Key words: Embedded systems; Windows Network Security; Trojan Horse; Appliances;

1. SCOPE

Digital general-purpose computers have been in use for approximately 60 years. During this period, especially recently, many types of special-purpose machines that had previously been implemented using analog electronics, have been re-designed in digital incarnations, to take advantage of myriad inherent feature and user interface benefits, and design reusability. Numerically controlled machine tools, cameras, television, and scientific equipment are a few examples. Embedded microprocessor is the preponderant design, and therefore Operating System and application software are required, to convert a general-purpose machine to a special purpose one. Embedded system units far outnumber computer units in terms of total annual microprocessor and microcontroller production. Windows ™ based embedded appliance production unit volume is not believed to exceed Windows ™ based computer volume. Windows ™ based appliances in this paper are not limited to those employing Windows ™ CE and Windows ™ XP Embedded operating systems.

Initially, many special-purpose 'programmable appliances' operated with embedded proprietary programming busses, operating systems, and application software. These networks, operating systems and application programs very likely contained vulnerabilities such as buffer overflows and could potentially have been successfully attacked. However given the fragmented nature of the opportunity, few such exploits took place.

In recent years, many vendors have replaced proprietary busses and operating systems with industry standards, and many have offered these appliances as Windows ™ -Networkable machines. A decision to do this may appear to the vendor to offer only upside. The upside is less design investment required by the vendor in areas perceived as low value-add, such as writing hardware drivers and file management systems. Many vendors fail to grasp the corresponding requirement: to become far more sophisticated than the average organization regarding information security, and to provide a comprehensive security regime to protect downstream organizations. Doing one without the other changes the equation to one where the vendor benefits short term but the user assumes a risk over the lifetime of the product.

Today there remain some networkable appliances that still employ proprietary hardware and/or operating systems, as well as non- Windows ™ industry standards such as Linux, and they very likely present network vulnerabilities. In addition, the application programs in such machines, as well as application programs in Windows ™ appliances, likely present vulnerabilities. Anything with a TCP/IP stack may contain a vulnerability. These categories of vulnerability however are outside the scope of this paper.

This paper deals solely with recognizing and mitigating vulnerabilities associated with Microsoft Networking and Windows ™ Operating Systems in embedded systems and appliances (referred to hereafter as 'appliances').

2. CONTEXT

This paper is written with enterprise networks in mind, especially those with several hundred, or more, nodes. Today, myriad tools including anti-spam, anti-virus, anti-spy ware, auto-patching, encryption, firewalls, intrusion detection/prevention, and others often protect such networks. Client computers in such organizations are often purchased, setup, and maintained by an IT group that is trained and equipped to reduce information security vulnerabilities and manage security risks on networks.

In addition to tools, processes are vital in locking down large networks, and many organizations have implemented policies regarding password strength, access control, patching and virus definition updating, and others, that rely on the concept of 'one machine, one owner'.

The tools, and processes, referred to above will probably not encompass network nodes that were purchased, for example, by the facilities department, or the engineering department, or by an individual marketer. The vulnerabilities they introduce are likely to by-pass these defenses, and your perimeter. For example, a shared microscope in an engineering group may offer a soft node in an otherwise hardened network, and a platform from which unauthorized access can be gained, internal reconnaissance conducted, and further damage propagated. A hospital with several medical imagers on its network, a university physics lab with 20 oscilloscope stations, a business with office staff's PDAs in cradles, or a document copy/print station, face the same potential threat.

At this time there is no standard or widely accepted third party certification of vendor's embedded security practices, as there is for example in the quality arena (ISO9000) or financial reporting controls (SAS70), and buyers at this time must therefore make their own enquiries.

This paper narrates the product lifecycle steps in which security should play a role, and implicitly offers vendors suggestions as to how to invest for safety at each, in order to elevate themselves in the vendor maturity model presented below in figure 1. Tests and questions for distinguishing between secure and insecure offerings are included for the consumer community. The text is written grammatically to address consumers as the audience.

3. VENDOR MATURITY MODEL

A tiered vendor classification scheme is introduced:

Best-in-class: Information security practices prominent in every stage of customer interaction and support.

Basic care in product manufacture and delivery: Information security practices prominent in production stage of customer interaction and support, such as AV shipped in package.

Tactical care: Information security practices are prominent if convenient for vendor, such as provision of XP SP2 mods files for customers when appliance's application code requires.

Worst-in-class: Information security not prominent at any stage of customer interaction or support.

4. LIFECYCLE MODEL

The following stages are examined here:

- Product Design
- Shopping; Selling and Demonstration Process
- Production
- Shipment and Receiving
- Deployment
- Service; Calibration or Repair
- End of Life; Disposal, Secure Transfer or Destruction of Data

A discussion of issues, and questions an alert buyer might ask, will be presented for each stage.

5. PRODUCT DESIGN

Design choices as fundamental as motherboard, processor, and chipset will affect the long-term security of the resulting appliance. Vendors may choose a line of commercial components, seeking latest revision processors, memories, busses and peripherals, in support of frequently improved banner spec claims. Or they may choose OEM lines, in support of stable, and more secure, platforms over time. Software will often track HW revision levels, hence the vendor's 'dwell time' on a given OS will be influenced by component choices made early in design. OS's have a security 'sweet spot' as they age; new releases have undiscovered vulnerabilities, while very old OS's are unsupported and without patches when vulnerabilities are found. Best-in-class vendors will have considered their customer's security needs carefully, and their security team will be able to articulate their adoption practices and how those optimize their tradeoff between processor banner specs and overall system security. Hardware security features, such as the Intel disable bit architecture, should play a part in the vendor's chip & chipset selection.

Other design choices reflect the vendor's security culture as well. These include design of ports such as USB, drives, Ethernet connectors, and also design of application software to be compatible with future OS patches. Accessories signal the vendor's thinking; is antivirus (AV) a standard accessory? Are other security options, such as dual factor authentication, or a firewall, available for the product? Are removable drives an option? Has the vendor considered customers' diverse requirements and preferences regarding security, such as sites that may prefer one AV package vs. another? Best-in-class vendors will have covered most bases above. Tactical-care vendors will have mixed coverage, as their strategy will not have been security-aware and hence each decision taken may fall randomly on the security spectrum.

Software licensing for the OS should be undertaken with security in mind. If the vendor's choices limit the user's ability to operate a secure appliance, for example by limiting the number of applications that can be run on the unit, this introduces needless, severe, security risks. The license for example might limit the appliance to two applications, in which case the appliance's application program would utilize at least one, eliminating for example the possibility of running both AV and Site Kiosk, or other risk management packages. The OS license may also impact allowed methodologies for automated OS patching.

The questions below are likely to uncover key indicators of vendor maturity (the salesperson may have to refer these questions to a security team member):

- What is your design-for-security strategy with regards to hardware, mechanical, and OS?
- What product HW and SW options are provided or supported to reduce security risk?
- What EULA (end user license agreement) is provided with this product?
- What steps have been taken to insure the application program will be compatible with future security patches?
- Have any of the standard features of the OS been disabled? (best-in-class answer would be 'yes', or 'optionally')
- Does the application have any back-doors or hard-coded passwords?
- How is the application code tested for bugs?
- Is regression testing performed on new OS and new application updates?
- Are application updates digitally signed?
- What strength encryption, if any, is employed in the appliance? Is NTFS encryption supported?
- Are all unneeded services switched off (such as Telnet)?
- If Internet Explorer is part of the shipped appliance, can it be disabled or replaced by another browser?
- Can the application program be run without Administrator privileges?
- Can the user replace the Windows Firewall with a third party firewall?
- Are performance specifications offered with, and without, AV installed and running? Will running AV (or AntiSpyware) real-time protection interfere with the application program?
- Is the application software compatible with a screensaver?
- Does the application program perform user authentication, and if so does it employ secure methods?
- Does the appliance have potentially insecure access, such as a CD-ROM that will accept a Windows recovery CD?

6. SHOPPING; SELLING AND DEMONSTRATION PROCESS

You may first 'touch' your potential vendor on their website. The odds of a best-in-class vendor having a website that avoids discussing info-security is low, as are the odds of a worst-in-class vendor's site providing comprehensive security information of interest to prospective customers. The shopper in your organization may not be focused on security, for example an engineer looking for a test & measurement tool may not have network security in mind. It is important that CIOs raise awareness of security broadly inside their organizations.

Two critical pages to look for on a vendor's site are the company's privacy policy, and their information security page. These should both be easy to find, normally clickable directly off the home page. They should both be informative and broad, but not deep (truly secure providers do not broadcast technical details of their defenses). If either or both of these pages are not available, this is your first red flag of an immature vendor.

A best-in-class vendor will have trained and equipped its sales-force, such that they will not introduce information security risks during the demonstration or sales process. The appliance they bring along to your site for a demonstration, has presumably been to several other locations recently. Was it connected directly to another prospect's LAN, or to the public Internet? Demonstration or evaluation units should be inspected/evaluated by your IT/security function as well as by end application users.

Questions to ask the salesperson:

- What precautions do you take prior to connecting the appliance to my network, to insure there is no malware contagion?
- What precautions do you take with regard to your laptop PC to insure there is no malware contagion?
- How does your firm guard against spam, malware and spyware on company networks in general, and in particular with regard to demonstration units and salesperson's PC's?
- Ask to see any training documents, brochures or materials on infosecurity that the salesperson has received in the prior year.

7. PRODUCTION

Unless this is a key business partner, you likely are not willing to visit their plant to see first hand what precautions they take during production. However, they should be willing to host such a visit if you wish (and it does not hurt to enquire). You should still be able to find out a good deal, without travel, by asking to be put in touch with the head of the vendor's security team. The questions to ask include:

- Is this product manufactured in your own facilities, or those of a contract manufacturer? If a contract manufacturer is used, how do you insure their production line is secure?
- Are isolated networks in place for production (and for later servicing) of the product?
- Do production and/or service networks contain out of support (old) nodes? Is the equipment used in production certified to be malware-free?
- Is each box externally scanned just prior to shipment? With what tool? (Internal scanning tools introduce difficulties for customers who do not prefer the particular tool which the vendor chose to embed)
- How often are master images updated to reflect most recent patches?
- Do recovery CDs reflect recent images?

For those of you going through Sarbanes-Oxley compliance testing, consider this process parallel to, and as important as, checking the SAS70 of your key infrastructure vendors.

8. SHIPMENT AND RECEIVING

On opening the shipping box there will be several immediate clues as to the security and maintainability of your new asset.

- How long ago was it shipped? If the product was manufactured long ago, and sat in a warehouse or at a distributor for many months, it is more vulnerable when first put onto the internet. Is there a document in the package that gives you the date the unit was last scanned, and packed for shipment?

- Was it shipped with an AV package in the carton? If so, was AV installed on the system drive? (best-in-class answer is, surprisingly, no). AV packages are complex to un-install, so the best-in-class vendor will not pre-judge the user's organizations' preference in AV product, rather they will supply one in the box, and allow the user the choice of installing it or not. This in turn implies the vendor needs a system for scanning the machine from the outside, which is a nontrivial capability.
- Is the Ethernet connector covered with a warning label directing you to a source of detailed security information prior to connection to a LAN? (best-in-class answer is yes)
- If WinXP SP2 or newer, was it shipped with the firewall enabled?
- Is there a restore CD, or hidden partition for emergency recovery? If so, is it at the same level of patching as the disk image? Does the vendor keep this image current (surprisingly, not the best practice)? Best practice is to keep the image current only as of the most recent critical update (defined for embedded appliances as vulnerability to a passive threat).
- What user accounts have been set up by default on embedded Windows system? Does the documentation explain how to alter the default passwords? Are administrator-level access rights easy to protect? Are there instructions for how to reset account access should the unit need to be shipped back for repair? If the answers to these questions are all positive the vendor is probably best-in-class.
- The unit may have been 'off the network' for an extended period, especially if you purchased it from a stocking distributor (see above). Is there provision for safely connecting it to the internet the first time, despite this delay?
- Was it shipped with a certification as to its malware scab results and patch status as of shipment?
- Was it shipped with clear instructions for safe usage over time when networked?
- What choices did the vendor make in the security setup of Windows™? Try running Microsoft's Baseline Security Analyzer for a clear set of security diagnostics.

9. DEPLOYMENT

An 'owner' should be designated for each network node of this type. Often such machines are shared assets, not on the IT team's lists of computers, and if a responsible manager is not identified no one will be aware of its security status.

In settings such as universities, where users will be transitory and difficult to vet, you may need an option to restrain appliance use and/or user access to the underlying Windows ™ OS. Programs such as Site Kiosk, or in-built restriction or access control options can provide this facility. Best in class vendors will have some solution for these settings.

Things to check for:

- Does the product appear to be 'phoning home' to its manufacturer? If so, what information is transferred? If in doubt, ask the vendor and insist on an authoritative response (the salesperson may have no idea).
- How easy is it to get firmware and software updates for the product? Are the source sites for these secured using login credentials? (If this process is insecure, you are at risk every time you download, and just as worrisome this indicates the vendor hasn't thought through the security process for its customers over the whole product lifecycle).
- Does the vendor provide active (such as via email), or passive (such as posting on their website) security updates, such as advice on taking service packs or patches?
- Can disk drives be removed in order to protect data?

10. SERVICE; CALIBRATION OR REPAIR

This stage is the ultimate indicator of best-in-class. Look for these factors:

- What warranty period is offered? How does it compare to industry average?
- What is the long-term support period provided? How does it compare to industry average? The 'sweet spot' is about 7 years; long enough to fully utilize the asset, not so long as to require the

vendor or contract manufacturer to maintain unsupportable OS's on the production or service networks in their factory.

- What is the software support and version update process?
- Does the vendor scan your product prior to connecting it to a network during repair?
- Is the repair network isolated?
- Does the vendor scan your product prior to return shipping it to you?
- If a security problem is discovered, does the vendor contact you to offer a range of possible methods to deal with it?
- How does the vendor insure the privacy of any data you have stored on the appliance during the service process?
- Are instructions provided to facilitate administrator account access during service in a secure manner?

11. END OF LIFE; DISPOSAL, SECURE TRANSFER OR DESTRUCTION OF DATA

If the appliance is one, such as laboratory equipment, that has gathered or stored important data for the customer, then secure disposal is important.

Consider:

- Are storage media removable?
- Are methods for data backup/restore/archive provided?
- Ask the vendor what their WEEE compliance strategy is (**WEEE** is the abbreviation for the Directive on **W**aste **E**lectrical and **E**lectronic **E**quipment being implemented by the European Union. The **WEEE** Directive aims to reduce waste through the re-cycling and reuse of electronic products.)

12. SUMMARY

Vendors opting for standardized networking and OS solutions should consider every step of the customer interaction cycle carefully from a security perspective.

Pending adoption of a third party security certification process, the buyer must beware and make appropriate enquiries to avoid introducing network vulnerabilities into an otherwise hardened corporate network.