

Secure device management prevents unauthorized access

By David Kleidermacher, Green Hills Software

The common criteria for evaluating the security of operating systems, firewalls, web servers etc have a leveling system assigning scores, 1 through 7, for the security confidence that users can have. This article shows how secure device management software can upgrade EAL4 level systems to EAL6+.

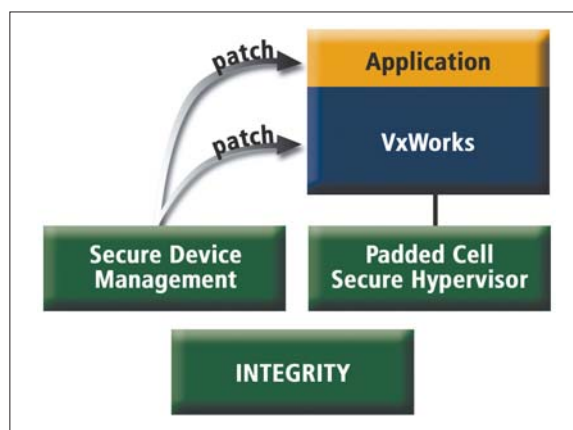


Figure 1. Device management architecture for legacy systems

■ When an embedded system fails in the field, developers (and sometimes government forensics teams) are tasked with determining the cause of failure. A flight recorder is a well-known field diagnostic system: the end product, an aircraft, is shipped with a built-in diagnostic capability, the black box. Yet a burgeoning class of embedded devices requires field diagnostic and management capabilities. Unlike the black box which is a purely forensic tool, many systems require a live connection. This connection enables technicians to inspect a fielded system to locate the source of anomalous behavior, such as loss of function or performance degradation, install patches or other software upgrades, perform automated audits, change configuration, or execute a plethora of other management duties.

Furthermore, with the increasing availability of network services built into embedded systems, device management can be conveniently discharged via the internet. Your home cable or satellite box has a network connection that most likely has been used to carry out both remote diagnostics and firmware upgrades. Device management functionality has been transformational, increasing product lifetime, reliability, serviceability, and customer satisfaction while reducing maintenance cost and total cost of ownership. The hacker's ambition is to locate a vulnerability that, when properly

manipulated, provides access into a computer system for nefarious purposes. Over time, exploits have become increasingly sophisticated. Just this past April, IBM security researcher Mark Dowd won acclaim with his 25-page report detailing an astoundingly convoluted set of steps that could be taken to exploit a vulnerability, previously believed to be innocuous, in the ubiquitous Adobe flash program.

Device management is the answer to the wildest dreams of hackers: the embedded system has been endowed not only with internet access, but also the means by which to remotely modify and patch software. No Byzantine attack vector is required: just get past the basic operating system controls, and the embedded device becomes your playground of iniquity.

So how difficult is it to circumvent common operating system security functions? How does one evaluate the strength of security? Luckily, there is an international standard for evaluating

security: ISO/IEC 15408, more commonly known as the common criteria. For more than a decade, the common criteria have been used to evaluate the security of operating systems, firewalls, web servers, VPNs, and more. The common criteria have a leveling system which assigns a numeric score, 1 through 7 (called EAL – evaluated assurance levels), to indicate the confidence that users can have with system security policies (table 1).

Most operating environments controlling computer systems come in at EAL 4. For example, Windows and Linux have been assessed to EAL 4. More recent enterprise system software applications, such as VMware, have yet to even reach this benchmark. The inability to exceed EAL 4 is due to the stringent demands that come with the higher levels and must be designed in from the beginning; according to the common criteria, EAL 4 is the highest level at which it is likely to be economically feasible to retrofit an existing product line. Windows and

EAL1	Functionally tested
EAL2	Structurally tested
EAL3	Methodically tested and checked
EAL4	Methodically designed, tested, and reviewed
EAL5	Semiformally designed and tested
EAL6	Semiformally verified design and tested
EAL7	Formally verified design and tested

Table 1. Common criteria security levels

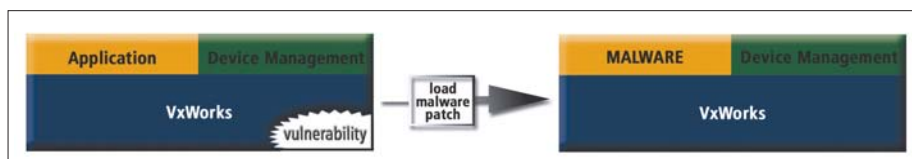


Figure 2. Vulnerability leading to malware insertion

Linux have been evaluated against a common criteria product class specification called the controlled access protection profile (CAPP), which specifies the EAL 4 security level. According to its authors, CAPP is only appropriate for an assumed non-hostile and well-managed user community requiring protection against threats of inadvertent or casual attempts to breach system security. But this level of security is not appropriate when protection is required against determined attempts by hostile and well-funded attackers.

In 2007, IEEE Spectrum published a fascinating piece, *The Athens Affair*, in which authors Vasilis Prevelakis and Diomidis Spinellis detailed the recent wiretapping incident in which the Greek Prime Minister and a slew of other high ranking dignitaries had their mobile devices bugged. According to the article, the hackers took advantage of the cellular switches built-in field upgrade and device management features (normally used for network diagnostics, billing, lawful wiretaps, defect patching, etc) to inject software that maliciously redirected private communications. The investigators concluded that the switch software had been reprogrammed with a finesse and sophistication rarely seen before or since. The perpetrators used some serious programming chops to repeatedly reconfigure their malicious software and cover up the intrusion. This was not an inadvertent attempt to breach system security by a non-hostile user community.

Another aspect of this story teaches an important lesson. Modern telephone switches use encryption to protect communications between mobile devices and the central base stations. Yet within the central switch network, the communications were not protected. This is where the device management software resided and thus is what the criminals targeted. Other commercial device management solutions on the market today boast of using encryption, such as SSL, to protect communications between the device and the remote management software. Yet the device itself is not secure. Hacking the core software on the device renders the edge network encryption useless. This is akin to putting a padlock on a safe built from cardboard. Another example is found in arguably the most famous remote management system in the world: Windows Update. Windows Update is designed to unobtrusively and remotely feed your PC with the latest validated

security patches. Yet hackers have commandeered this facility to upload unauthorized software. Building functional field diagnostic, upgrade, and management facilities into embedded systems is not rocket science. As the authors of *The Athens Affair* report, field debugging and upgrade capabilities are stan-

dard fare in the networking and telecom world where devices may have a service life of many years with no tolerance for downtime. Availability is ensured by device management software incorporated into these systems. Another salient example (speaking of rocket science) is the Mars Pathfinder: device management software saved the 1997 mission from disaster when a malfunction was diagnosed as a software defect, remedied with a patch installed via radio link from Earth. Creating secure device management systems, however, is a challenge. The EAL 4 (certified hackable) operating systems running many devices provide an insufficient foundation upon which to build device man-

agement functionality. Figure 2 depicts vulnerability in an EAL 4 operating system (in this case, the popular embedded operating system VxWorks) which enables malware to be loaded via the operating system device management component.

The Integrity operating system is the first operating system accepted into a high assurance (EAL 6+) common criteria evaluation, performed under the auspices of a US government program to protect national secrets in environments with high risk of exposure to hostile, well-funded attackers. The software, the same as used in a wide range of critical embedded systems since 1997, was designed for the highest level of security and includes a formal, mathematical proof of the security policies. The system must also undergo penetration testing by the NSA expert hackers who have complete access to the source code and design documentation. These techniques are used to assure the security-critical components of Green Hills Software's recently announced secure device management solution. Secure authentication, encryption, and access controls provide end-to-end protection of the device management function. A secure device management solution protects against insider attacks. Without proper assurance, including testing at the binary level, secure delivery, and other controls, developers can insert backdoors using a wide range of proven techniques. A secure device management

solution prevents malicious code insertion by employing high assurance authentication and digital signatures: unauthorized IT administrators, technicians, janitors, and users cannot circumvent the mandatory access controls imposed by the system. In short, secure device management would have prevented the Athens Affair.

Of course, not every embedded device runs Integrity. However, an EAL 4 device can incorporate EAL 6+ device management capability. One way to do this is to employ virtualization technology, such as Green Hills padded cell secure hypervisor, to host the device EAL 4 software environment alongside the security-critical device management components that run natively on the EAL 6+ subsystem. In fact, the device management software can be used to monitor, configure, and patch the EAL 4 environment itself.

In many cases, a secure device management solution involves consulting services to ensure that the appropriate set of security components is integrated and deployed in a robust and cost-effective manner into end devices. Given the increasing financial, safety, and security risks associated with remote access, many embedded and mobile device makers are rethinking their device management strategy. The good news is that the state of the art in device management security has taken a big step forward with the advent of EAL 6+ infrastructure. ■