The Rise of the Gadgets

So you think that to protect your IT infrastructure effectively you merely need to deploy a streamlined assess, patch, and audit process for your routers, servers, and workstations? Think again! Although it is indisputable that we must constantly monitor and patch networking hardware, servers, and workstations against the latest and most threatening bugs, a slowly growing trend might prove that strategy to be flawed, or at least not comprehensive.

The emergence of networkable gadgets, ranging from printers and DSL routers to gaming consoles, cameras, and personal data assistants (PDAs), can pose serious risks to an otherwise secure infrastructure.

In this installment of Attack Trends, I examine sample vulnerabilities and research that might point to novel attack vectors that administrators should consider when planning a well thought-out information security strategy.

A vulnerable network infrastructure

Generally, discussions about protecting an organization’s or an entire nation state’s core IT infrastructure center on the basic building blocks of networks: routing and switching hardware and software. The line dividing software and hardware is starting to blur; in today’s network equipment, it is increasingly unclear which is which (and I will not attempt to clarify the differences in this article). Yet an analysis of recently published vulnerabilities can reveal interesting interactions between hardware and software if we consider the techniques and tools used to exploit them:

- Most exploits for vulnerabilities in network protocols yield results at the semantic level; that is, they modify the meaning of the information such protocols transport. Examples of these include route poisoning, IP spoofing, TCP session hijacking, DNS spoofing and domain name hijacking, and various forms of man-in-the-middle attacks.

- Most exploits for vulnerabilities in critical infrastructure software that run on computers with general-purpose operating systems (Microsoft Windows, Linux, and Unix variants) yield remote access to the underlying operating system. This allows arbitrary command execution with either privileged or unprivileged permissions. A smaller set of exploits gives the attacker denial-of-service (DoS) capabilities. It is sometimes impossible or too complex to exploit a given vulnerability in a more sophisticated manner.

- Most vulnerabilities in software that run on networking devices such as routers and switches are catalogued as DoS problems. Most exploits for these vulnerabilities are, in fact, for DoS attack execution, but it is not clear if attackers can exploit the vulnerabilities in any other, more meaningful or threatening ways that let them gain control of the vulnerable devices.

The latter point supports the assumption that network appliances running embedded systems—simple, small software and hardware components designed for a single or very few purposes—are inherently more secure than complex general-purpose operating systems and networking protocols. At most, network appliances will suffer from availability issues due to software security bugs and, although these are important issues for the core of an IT infrastructure, they are not as serious a threat as current attack vectors against servers and workstations.

The Phenoelit is a German research group (www.phenoelit.de/fr/tools.html) that studies, among other things, information security of embedded systems. Their recent research shows that the most widely used routing and switching equipment can be the target of direct compromise attempts from skilled attackers. This could be proof enough to counter the dubious assumption stated earlier—that networking equipment running embedded systems is not inherently more secure than general purpose operating systems running on personal computers and servers—but let us more closely examine the facts.

The “other” infrastructure

An embedded system is a combination of computer hardware and software,
either fixed in capability or programmable, which is designed for a specific application device. Industrial machines, automobiles, medical equipment, cameras, household appliances, airplanes, vending machines, and toys (as well as the more obvious cellular phone and PDA) are among the myriad possible hosts of an embedded system.

Thus, currently, we are unknowingly surrounded by embedded systems that assist us in our interaction with the increasingly technologically complex environment. Until recently, many devices with embedded systems did not provide any networking capabilities, except for those purposely designed for networking applications, such as the software running on network routers and switches.

However, we can identify two new trends that are relevant to information security:

- **More complex software.** Software running on network devices has become increasingly complex, rapidly leaving behind the notion of a simple embedded system with fixed or programmable—but still limited—capabilities in terms of scope and field of application and adopting the features and functionality of full-fledged general purpose operating systems. Examples of this include Cisco’s IOS operating system (www.cisco.com/warp/public/732/Tech/), which almost all Cisco networking equipment uses and the VxWorks real-time operating system (www.windriver.com/products/vxworks5/index.html), which many small- and home-office DSL routers, high-end network switching, and voice over IP (VoIP) devices use.
- **Consumer devices adopting embedded systems.** A wide range of consumer electronic devices and small appliances have adopted embedded systems with networking capabilities to provide users with seamless interaction with networked workstations and servers. The Embedded Linux initiative (www.embedded-linux.org), Microsoft Windows embedded (www.microsoft.com/windows/embedded/default.asp), and Palm OS (www.palmsource.com/palmos) operating systems, which many PDAs and cellular phones use, exemplify this trend. In addition, several of these new gadgets use wireless networking technologies such as the IEEE 802.11 standards and Bluetooth (www.bluetooth.org), adding another layer of weakness.

Traditionally, embedded systems running on highly specialized or mission-critical devices have far more stringent security requirements than those of general-purpose operating systems because they are highly sensitive or operate under harsh environmental conditions. However, these requirements are more related to fault tolerance, reliability, and accuracy than the privacy and security issues that arise in a threat model.

Due to the continuous introduction of new networkable gadgets, a new information technology infrastructure has appeared, composed of a range of potentially vulnerable and generally unprotected networked devices. This new infrastructure could become the target for direct attacks, and attackers could use them as stepping stones to launch further attacks into an organization’s traditional IT infrastructure of servers and workstations.

To better understand the risks of vulnerabilities in this new infrastructure, let’s take a look at the components that compose it.

### Network appliances

Network infrastructure vulnerabilities in the most traditional sense bring to mind routing and switching equipment. According to the Common Vulnerabilities and Exposures dictionary (http://cve.mitre.org), Cisco Systems’ routers, switches, and VPN appliances—the most widely used networking technology today—had 31 vulnerabilities reported so far during 2003. Of these, 17 are DoS vulnerabilities derived from poor processing of malicious...
Vulnerable gadgets

The list of recently disclosed security vulnerabilities includes a wide range of popular devices with networking capabilities.

- Cell phones from leading companies in the industry such as Nokia (http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0103) and Siemens (www.securityfocus.com/bid/7004).
- Personal data assistants (PDAs) running the Palm OS (http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0116).
- Short-range wireless access points using Bluetooth technology (www.eweek.com/article2/0,3959,6772,00.asp).
- Microsoft's Xbox home-entertainment system, which could be locally compromised to boot a different operating system (www.securityteam.com/securitynews/5BP0220AKG.html), bypassing all software integrity checks.

user input or malformed network packets. From this, we can conclude that the most serious threats to network infrastructure affect its availability but also could directly compromise networking equipment.

At the recent BlackHats Briefings 2003 conference in Las Vegas, Nevada, the Phenoeil group demonstrated that contrary to popular belief, attackers can effectively exploit Cisco IOS buffer overflow and format string vulnerabilities to gain control of the device on which it is running. In light of this, we wonder: how many previously reported DoS vulnerabilities are actually exploitable bugs that could yield access to network routers and switches? A real and present danger is now clearly evident. The building blocks of almost all modern networks are not only vulnerable to DoS attacks but should also be considered as assets that attackers can directly compromise and use to escalate more sophisticated attacks.

The ability to exploit software vulnerabilities on network appliances is not a “feature” exclusive to high-end networking equipment. Routers, low-cost DSL modems, and wireless network access points with embedded systems that provide HTTP and other IP-related configuration interfaces suffer from some of the same trivial vulnerabilities as their counterparts. For example, we at Core Security Technologies recently released a security advisory that demonstrates that stack- and heap-based buffer overflows and authentication bypass vulnerabilities exist in proprietary embedded systems that netizens worldwide use to access the Internet (www.coresecurity.com/common/showdoc.php?idx=276&idxsection=10). We should see this as a symptom of a greater problem: Millions of end users’ DSL modems and routers are vulnerable and can be directly compromised. Once compromised, attackers could use these devices as staging points to launch attacks on private home local area networks (LANs), corporate networks accessible from home VPN endpoints, and any other networks on the Internet. To make things worse, installing patches and fixes on home computers and servers does not suffice anymore—Internet users must now patch and maintain more esoteric items such as firmware and small Internet appliances’ configuration settings.

“All your printer are belong to us!”

The introductory—and badly translated—speech of Zero Wing, a cult video game of 1989 (www.allyourbase.net) provides us with the perfect heading title to investigate the security threats brought about by a 15th century invention.

Is it possible that Johann Gutenberg’s revolutionary invention, the printer, is a threat to present-day corporate networks? Indeed, the new incarnations of Gutenberg’s mechanical marvel have turned into potential attack vectors against organizations’ networks: IP-capable printers running proprietary embedded systems are vulnerable to the most simplistic DoS and unauthorized reconfiguration attacks (www.securityfocus.com/bid/7001).

Web, telnet, and simple-network-management-protocol-based configuration and monitoring capabilities—with their own history of security bugs—have made it possible for attackers to access printers on LANs they populate. Many printers and other devices that feature rich embedded systems open new dimensions for attackers who use them as the launching pad for network mapping, port scanning probes, and more sophisticated attacks (www.securityfocus.com/bid/5332).

Although no publicly available tools currently exist that use network printers as a source of further attacks, they can become the perfect staging point to escalate attacks or launder connections to otherwise well-secured networks because they are generally disregarded as a threat. Therefore, network administrators and security officers should consider printers, like any network device, as part of the infrastructure to secure.

Consumer electronics

Routers, switches, and printers are not the only vulnerable devices in this new infrastructure. A wide range of other gadgets with security vulnerabilities and complex remedia-
tion issues are emerging as a possible target of direct attacks (see the “Vulnerable gadgets” sidebar).

The most obviously vulnerable gadget is the cell phone. Modern cell phones run fully-fledged operating systems such as Palm OS and provide IP networking capabilities for Web browsing, email synchronization, and instant messaging. In most cases, we don’t consider cell phones to be possibly hostile network devices; at most they are possible attack targets but certainly not originators of them. Or are they? @Stake, a security consulting company, recently released a set of penetration testing tools that run on a Sony Ericsson cell phone.

PDAs represent another possible target and attack vector into home and corporate networks. With performance and feature sets equal to those of small personal computers and with their ability to connect to any IP-capable network using a series of new—and, therefore, not mature in terms of security—wireless protocols, PDAs running Microsoft Windows CE or the Palm OS could very well become launching pads for almost untraceable attacks. Vulnerabilities in PDA software packages can provide attackers with an open door to launder attacks and originate them from unsuspecting users’ devices.

Home-entertainment systems, set-top boxes, surveillance cameras with embedded Web servers, and various other networkable gadgets are equally important in this new infrastructure’s overall security—if we understand that they can be permanently or intermittently connected to networks and so must be secured.

Where do we go from here?

We can use the discovery that high-end routers and switches are vulnerable to more serious threats than DoS attacks to support a statement of greater importance: Network equipment can be the subject of direct attacks and compromise.

This discovery is then complemented with another one: The rapidly increasing number of networkable gadgets suffer from similar problems. For any sound information security strategy, administrators should consider these as part of the IT infrastructure.

The rise of the networkable gadgets and their pervasive characteristics demand responsible security behavior from both their users and manufacturers, but the latter should carry the greater load in order to provide manageable security capabilities to millions of untrained users.

It should be evident by now that vendors of special purpose embedded systems should have as much concern about information security as the major software vendors whose software packages’ vulnerabilities make the headlines every day.

Iván Arce is chief technology officer and co-founder of Core Security Technologies, an information security company based in Boston. Previously, he worked as vice president of research and development for a computer telephony integration company and as information security consultant and software developer for various government agencies and financial and telecommunications companies. Contact him at ivan.arce@coresecurity.com.