Ειδήσεις για την ΑΣΦΑΛΕΙΑ στις ΤΠΕ απ' όλο τον κόσμο...

Δελτίο 162
10 Νοέμβρη 2009

Scan of Internet Uncovers Thousands of Vulnerable Embedded Devices
Wired News (10/23/09), K. Zetter

A scan of the Internet by Columbia University researchers searching for vulnerable embedded devices has found that nearly 21,000 routers, Webcams and VoIP products are vulnerable to remote attack. They say there could be as many as 6 million vulnerable devices on the Internet. The scan also found that the devices' administrative interfaces are viewable from anywhere on the Internet, and their owners have not changed the devices' passwords from the manufacturer's default. The study scanned networks belonging to the largest Internet service providers (ISPs) in North America, Europe and Asia, and vulnerable devices were found in significant numbers in all parts of the world. Since starting the project last December, the researchers have scanned 130 million IP addresses and found nearly 300,000 devices whose administrative interfaces were remotely accessible from anywhere on the Internet. Devices with default passwords are most vulnerable, but others are theoretically vulnerable to brute-force password-cracking attacks. The researchers have provided ISPs with their findings, but Columbia professor S. Stolfo says product manufacturers are the real culprits. He says that they need to hide their administrative interfaces by default and give customers clear instructions on how to alter the configuration to protect themselves. Stolfo also says that vendors should be more vocal in encouraging customers to change default passwords.

In Industry First, Voting Machine Company to Publish Source Code
Wired News (10/27/09), K. Zetter

Sequoia Voting Systems, which has been criticized for resisting public examination of its proprietary systems, recently announced plans to make the source code for its new optical-scan voting system available to the public. The new voting system, called Frontier Election System, will be submitted for federal certification and testing in the first quarter of 2010. The system's source code will be released for public review in November, according to Sequoia's Web site. Sequoia's announcement comes five days after a non-profit foundation announced the release of its open source election software for public review, although Sequoia's M. Shafer says the timing of the announcements are unrelated. "Fully disclosed source code is the path to true transparency and confidence in the voting process for all involved," says Sequoia's E. Coomer in a press release. Previously, Sequoia had fought any efforts to examine the source code of its proprietary systems and even threatened to sue Princeton University computer scientists if they disclosed anything they learned during a court-ordered review of its software. The firmware for Sequoia's new Frontier optical-scan machines is written in C# and runs on Linux. "It's good to know the vendors are developing a new transparent optical-scan system," says Verified Voting president P. Smith. "That is probably the biggest recognition of the direction that the voting public wants to see the market going."

Thwarting Cyber Criminal
Norwegian University of Science and Technology (10/30/09)

Researchers at the Norwegian University of Science and Technology (NTNU) say they have developed a digital signature system that is 17,000 times faster than current systems used for verification and 10,000 times faster in providing a digital signature. They say the new system, MQQ, was developed as a way to address the biggest pitfalls in current data security systems. Existing systems, when used with smart card applications or at credit card payment terminals, are often slow, do not protect against quantum computing attacks, and have not been optimized for parallel processing. MQQ was developed using a trapdoor function, which is generated by quasigroup string transformations based on multivariate quadratic quasigroups. The researchers say that MQQ's security is enhanced by a signing speed that is 10,000 times faster than corresponding RSA and elliptical curves digital signatures. The researchers also say that MQQ is one of the first algorithms specially designed for parallel processing, which allows the system to benefit from the recent trends in multicore parallel processing. "Due to the nature of its design, MQQ is secure against quantum computing attacks," says NTNU professor D. Gligoroski. He says MQQ also has been found to be secure against all known multivariate quadratic attack methods.

US Cyber War Policy Needs New Focus, Experts Say
Computerworld (10/29/09), G. Gross

Three cybersecurity experts recently told a meeting of the Congressional Cyber Caucus that current US policies for protecting the United States against various forms of attack won't work for defending against cyberwarfare. Rand Corp.'s M. Libicki said a policy of cyberdeterrence modeled after the strategy for nuclear attacks is problematic, largely because it is difficult to identify attackers, particularly when some nations appear to be sponsoring private attackers. Libicki also said it may be difficult for the US to follow through with counterattacks when US cyberexperts do not know how much damage those attacks could do. Good Harbor Consulting's P. Kurtz said it is still unclear what the US's cyberwarfare policies will look like, which is particularly troublesome because the United States lacks a definition of what constitutes an act of cyberwar. Additionally, it may be unwise to label some countries as cyberadversaries, Kurtz said. For example, although the Chinese government is often blamed for encouraging or sponsoring cyberattacks, the US government needs to engage the Chinese about cyberdefense. US Cyber Consequences Unit director S. Borg said the US government needs to recognize that cyberattacks can cause "horrendous damage," and that attacks on targets such as electricity generators could have a long-lasting effect, primarily due to the US's limited ability to support new parts for damaged generators. Most of the parts for electricity generators come from China and India, and Borg said that emergency planners have not found a way to replace those parts quickly. He said shutting down electricity in a large area of the US for several months would have the same level of economic damage as a nuclear attack.

NC State Research Shows Way to Block Stealthy Malware Attacks
NCSU News (11/03/09) Shipman, Matt

North Carolina State University (NCSU) researchers have developed a way to block rootkits and prevent them from contaminating computer systems. Rootkits often work by hijacking a number of hooks, or control data, in a computer's operating system. "By taking control of these hooks, the rootkit can intercept and manipulate the computer system's data at will," says NCSU professor Xuxian Jiang. To prevent a rootkit from taking over an operating system, Jiang's research team determined that all of an operating system's hooks had to be protected. "The challenging part is that an operating system may have tens of thousands of hooks--any of which could potentially be exploited for a rootkit's purposes," Jiang says. "Our research leads to a new way that can protect all the hooks in an efficient way, by moving them to a centralized place and thus making them easier to manage and harder to subvert." By placing all of the hooks in one place, the researchers were able to leverage hardware-based memory protection to prevent the hooks from being hijacked. The research will be presented at the ACM Conference on Computer and Communications Security in Chicago on November 12.

First Test for Election Cryptography
Technology Review (11/02/09), E. Naone

An election in Tacoma Park, Md., held this November will be the first to use Scantegrity, a new vote-counting system that uses cryptography to ensure that votes are cast and recorded accurately. Scantegrity's inventors say the system could eliminate the need for recounts and provide better assurance that an election was conducted properly. Scantegrity allows voters to check online to ensure their votes were counted correctly, and officials and independent auditors can check to make sure ballots were tallied properly without seeing how an individual voted. Scantegrity developer D. Chaum says the system uses a familiar paper ballot, which requires that voters fill in the bubble next to the name of their preferred candidate. The ballot is then fed into a machine that scans it and secretly records the result. The difference from other systems is that a special type of ink and pen are used, and when the voter fills in a bubble on the ballot a previously invisible secret code appears. The voter can record the code or codes and check them online later. If the code appears in the online database, the ballot was counted correctly. Every ballot has its own randomly assigned codes, which prevents the process from revealing which candidates a voter selected. Auditors can ensure all votes were counted correctly by comparing a list of codes corresponding to votes and a list of the results. University of Maryland, Baltimore County professor A. Sherman says Scantegrity is fundamentally better than other systems in regards to integrity, and makes it possible to audit elections with much greater accuracy and certainty.

New Honeypot Mimics the Web Vulnerabilities Attackers Want to Exploit
Dark Reading (10/29/09), K. Higgins

Glastopf is a new open source Web server honeypot project that enables researchers to study Internet attacks by acting as Web servers with thousands of vulnerabilities that provoke cybercriminals into attacking. Glastopf creator L. Rist says the program dynamically emulates vulnerabilities that attackers are looking for, so the decoy is more realistic and can gather more detailed information. "Many attackers are checking the vulnerability of the application before they inject malicious code," Rist says. "My project is the first Web application honeypot with a working vulnerability emulator able to respond properly to attacker requests." Rist built Glastopf through the Google Summer of Code program, in which student developers write code for open source projects. Glastopf uses a combination of known signatures of vulnerabilities and records the keywords an attacker uses when visiting the honeypot to ensure they are indexed in search engines, which attackers regularly use to find new targets. The project has a central database to collect Web attack data from the honeypot sensors, which are installed by participants who want to share their data with the database. "The project will contribute real-world data and statistics about attacks against Web apps--an area where we do not have good collection tools yet," says Rist's project mentor T. Holz. He says Glastopf tricks an attacker by returning content that is often found on vulnerable versions of Web applications, such as characteristic version numbers or similar information.

A New System Preserves the Right to Privacy in Internet Searches
Platforma SINC (11/05/09)

Researchers from Rovira i Virgili University, Autonoma of Barcelona, and Oberta of Catalonia have developed a system that protects the privacy of Internet search engine users through a new computer protocol. "It is a model based on cryptographic tools, which distort the profile of users when they use search engines on Internet in such a way that their privacy is preserved," says Rovira i Virgili University's A. Viego. The researchers note that there are systems that provide anonymous navigation, but say their system provides a significant improvement in response time over anonymous systems, though it still delays searches slightly. The new protocol has already been tested in both closed research center intranets and on the Internet, and the results have made the researchers optimistic about a global implementation model. The researchers are currently working on the development of a final user version, and believe that it will soon be easy to integrate the system into the major platforms and browsers.