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

Δελτίο 172
17 Απρίλη 2010

Security Researchers Hacked iPhone
University of Luxembourg (03/25/10)

The University of Luxembourg's R.-P. Weinmann and Zynamics' V. Iozzo chained existing code bits using the "return-into-libc" or "return-oriented-programming" technique to compromise the iPhone during the PWN2OWN hacking contest in Vancouver, Canada. The security researchers were able to bypass the iPhone's code signing and data execution prevention technologies a year after previous contest participants were unable to hack into the device. Iozzo and Weinmann were able to execute code on the iPhone when a user visits a malicious Web site, and the attack code steals the iPhone's SMS database.

Feds Developing Cloud Security Program
InformationWeek (03/31/10), N. Hoover

A US federal interagency working group is developing a unified, governmentwide risk-management program that could greatly decrease the amount of security work agencies must do to access cloud services. The proposed new effort, called the Federal Risk and Authorization Management Program Pilot (FedRAMP), would give agencies a centralized approach to solving security problems such as certification and accreditation. FedRAMP will develop common security requirements for certain systems, provide ongoing risk assessments, and carry out governmentwide security authorizations. Agencies also will be able to see what security controls have been conducted for different products and services. The program would make certification and accreditation processes simpler because they would only need to be carried out once per cloud service, and agencies could share security management services. Initially, the program would focus on public and private cloud computing technologies, but could eventually expand to cover traditional Web hosting and other domains.

Tubingen Computer Scientists Develop a Comfortable and Secure Login Method
AlphaGalileo (03/29/10)

Tubingen University's B. Borchert has developed a new method that saves smartphone users the trouble of memorizing, and typing, passwords and login names. The new approach provides a solution to the issue of keyloggers, which are trojans on the computer a password is entered into, and could later be misused for criminal purposes. The user downloads the application software to a smartphone. In order to access an account, the user can open the login page in a browser window on any computer. The user will be shown a two-dimensional code that must be scanned with the smartphone's camera. The data is processed by the application and the smartphone contacts the account server, which checks the data and connects to the browser window on the computer and opens the user's account.

After Google-China Dust-Up, Cyberwar Emerges as a Threat
Computerworld (04/07/10), J. Vijayan

Recent cyberattacks originating in China against Google and other tech firms highlight concerns about adversaries' ability to launch a full-fledged cyberwar against the US. Many see the hacks as an indication that the US is already engaged in an undeclared cyberwar--and losing. Such worries are spurring action in the form of a pair of cybersecurity bills, one of which would link US financial aid to a nation's willingness to combat cybercrime, while the other would bolster domestic cybersecurity and mandate that the president work with private industry on responding to a cybercrisis. Meanwhile, the US State Department is mulling the establishment of a cybersecurity ambassador for the United Nations--a key issue, as no settled definition of cyberwar exists and various countries are already trying to determine the implications, declaration protocols and counter-strategies of a cyberwar. A. Yoran, former director of the US Dept. of Homeland Security's National Cyber Security Division, says there increasingly appears to be a point of connection between perpetrators of cybertheft and cyberespionage.

Researchers Trace Data Theft to Intruders in China
New York Times (04/05/10), J. Markoff; D. Barboza; V. Bajaj

Over the past eight months a team of US and Canadian researchers have spied on a gang of intruders that stole sensitive information from the Indian Defense Ministry and traced them to China. A report from the researchers indicates that the ring extensively employed Internet services such as Twitter, Yahoo! Mail, and Google Groups to automate the control of computers once they had been commandeered. The investigators gained access to the control servers used by the gang to monitor the theft of a broad spectrum of material, and traced the attacks to intruders that appeared to be based in Chengdu. Among the stolen material were documents related to the travel of NATO forces in Afghanistan, which demonstrated that many nations can be put at risk of exposure by a single computer security hole. "An important question to be entertained is whether the People's Republic of China (PRC) will take action to shut the Shadow Network down," the report says. "Doing so will help to address long-standing concerns that malware ecosystems are actively cultivated, or at the very least tolerated, by governments like the PRC who stand to benefit from their exploits though the black and gray markets for information and data."

Steganography Discovery Could Help Data Thieves, But Also Improve Radar, Sonograms, Network World (04/09/10), T. Greene

The technology for instruments used to see through fog also could be used for optical steganography, according to a team of researchers at Princeton University. Radar instruments rely on the refractive properties of crystals, which combine the energy of light noise with the weak energy of the signal, to make a clear image of an object. Jason Fleischer and colleague D. Dylov used a ground-glass filter to simulate fog so they could control the statistical properties of the noise, but they say the same principles could be used in natural environments. Thieves might try to store stolen data on CD in a way that prevents it from being detected by corporate security professionals. A coating on the surface could diffuse the signal from the data so conventional CD players would interpret just noise. However, a device with a tunable crystal could be adjusted to read the signal behind the noise. "There could be a signal there, but unless you know it's there you wouldn't even know to look," Fleischer says. The technology also could improve sonograms and night vision goggles.

Battling Botnets With an Awesome OS
University of Illinois at Chicago (04/08/10), P Francuch

Computer security and cryptography experts at the University of Illinois at Chicago are laying the foundation for more secure computer operating systems (OS). J. Solworth and D. Bernstein are developing the Ethos OS, which they say could become the blueprint for a new generation of robust OS that are able to fend off bugs, viruses, and other kinds of malware. They hope to address the heart of computer vulnerability by enabling Ethos OS to guard against attacks on applications that would run on the OS. Ethos OS will be designed for virtual machine computers that run one or more OSes together, and will be able to simultaneously handle applications such as online banking and other sensitive business transactions. Solworth says an OS with no vulnerabilities will enable software developers to focus more on making applications work better. "This is a huge undertaking, with complex scientific aspects," he says. "If we succeed, we'll have achieved what many thought couldn't be done."

Exposing Hackers as an International Deterrent
Technology Review (04/13/10), D. Talbot

An international group of computer scientists, law professors, military leaders, and others recently met at Russia's Moscow State University for a conference on methods of deterrence for online hackers. Naval Postgraduate School computer scientist J.B. Michael argued that surveillance on computer networks and other forms of intelligence can provide the clues needed to expose a potential hacker, and this exposure may often serve as a deterrent. Retired Russian General V. Sherstuyuk announced a new research collaboration consisting of government officials from Russia and China, as well as academic institutions including the Indian Institute of Information Technology, Allahabad, and the State University of New York (SUNY) at Albany. The agreement will "undertake common research on international information security," Sherstuyuk says. The collaboration reflects an increased international concern over the potential devastation that computer attacks can cause. "The US needs to work with Russia because it is one of the hotbeds of crime and hacker activity," says SUNY Albany computer scientist S. Goel.