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

Δελτίο 58
25 Γενάρη 2007

Ethics Dilemma in Killer Bots
The Australian (01/16/07) P. 29; P. Argy

Guard robots being deployed on the northern border of South Korea are capable of firing on human targets without receiving any direct commands from humans, and have brought up many important ethical questions. Each Intelligent Surveillance and Security Guard Robot will be equipped with a daylight camera capable of identifying targets within a 4-kilometer radius, and an infra-red night vision camera that has a range of 2 kms. While humans can use a joystick and touchscreen to control the robots, they are programmed to respond autonomously when an intruder does not provide a correct password. The robot's responses include sounding an alarm, using non-lethal force, or firing a machine gun or rifle; these would be the world's first robots with such capabilities. While the manufacturer says the robots are superior to human guards because they are immune to weather conditions and fatigue, many point out that a human soldier could utilize discretion and understand the consequences of his actions. Australian Computer Society's M. Bowern expresses concerns over the potential for "software and hardware defects" to "influence the robot's conduct." He also points out that little is known of the ethical considerations taken by the robots' designers, or any code they must follow, since Korea doesn't have an independent professional association such as the ACM or the ACS, and the Korean Ministry of Information and Communication seems to place greater importance on technical aspects than it does on professional or ethical concerns. Many worry that these robots could eventually be sold to private customers. Computer ethicist J. Moor points out the robots could not be held legally or morally responsible for their actions, leaving such responsibility up to technology professionals.

Interview With Bill Cheswick
Security Focus (01/15/07), F. Biancuzzi

In an interview with F. Biancuzzi, Internet Mapping Project creator and Lumeta chief scientist B. Cheswick says useful information about attacks could be culled through a combination of data about firewall probes and other information about an assault on an organization, and he notes that he prefers placing such logs in a big, cheap drop-safe. Cheswick describes network intrusion detection systems (NIDS) as an ongoing network monitoring effort, and notes that false negatives and false positives are a recurring problem for the technology; potential subversion of the NIDS is another significant minus. In terms of finding a solution to distributed denial of service (DDoS) attacks, Cheswick says, "I see no theoretical possibility of doing anything more than mitigating attacks, and ultimately throwing large amounts of computing and network capacity at the problem." Cheswick harbors doubts about intrusion prevention systems or reactive firewalls, which on the surface seem logical but are actually difficult to execute, and carry the danger of turning on their users through the machinations of a clever attacker. Network security research that has drawn Cheswick's attention or excitement includes a SANE paper at Usenix that rethinks intranet design by shifting from an end-to-end scheme to centralized control, which Cheswick thinks could be potentially useful for military and corporate networks; a paper detailing a proactive Microsoft project to find browser exploits on malevolent sites; and investigations into the use of virtual machines such as Xen and VMware. Cheswick anticipates the continued exploitation of susceptible machines for underhanded money-making schemes such as spam email, phishing, and DDoS extortion attacks, because the incentives remain strong. It is his hope that there will be fewer vulnerable systems with the implementation of Vista.

Computer Privacy in Distress
Wired News (01/17/07), J. Granick

Recent court cases have brought the question of computer privacy into the spotlight, as it pertains to the Fourth Amendment's protection against unreasonable search and seizure. Recent cases have proposed that border agents can search PCs of individuals crossing the border, without reasonable suspicion or a warrant. Though "routine" searchers are allowed to take place without reasonable suspicion, no court has directly addressed the question of whether searching a PC at the border is a routine or non-routine search. Due to the amount of private information on PCs, the length of time searches take, and the probability of finding contraband, courts may rule that reasonable suspicion is needed for such searches. US v. Zeigler, heard in the 9th US Circuit Court of Appeals, has stated that employees of private companies have no reasonable expectation of privacy, meaning no Fourth Amendment rights, concerning their workplace computers. Unless defense attorneys' requests for a rehearing are granted, the government could walk into an office without cause or a warrant and search the entire contents of the computer of any employee. The 9th Circuit is also trying to figure out a way to make sure authorities get the information they need without accessing or disturbing private, unrelated material that may be on the same disk drive. For example, in prosecuting US v. Comprehensive Drug Testing, the government obtained warrants and seized databases containing drug test results for the 10 baseball players suspected of taking steroids, as well as the test results for hundreds of other athletes, and despite a lower court ruling that said the government must return the unrelated information, the 9th Circuit upheld a government appeal. This case shows that warrants must not only state what authorities can seize, but what they may not access on these seized machines. Courts, and possibly Congress, have a complicated road ahead in crafting a computer privacy compromise that is supported by both privacy advocates and investigating authorities.

Making Every E-Vote Count
IEEE Spectrum (01/07) Vol. 44, No. 1, P. 13; S. Cherry

A team of graduate computing engineering students from US and Canadian universities presented a voting system two months ago that reportedly jettisons all the problems of commercial e-voting systems. The team is led by cryptography researcher D. Chaum, and the system, Punchscan, is easy to explain and can be deployed with commercially available equipment. Among the key problems with commercial systems that Punchscan addresses are ballots that cannot be recounted in disputed elections; vulnerability to malware and hackers; and the possibility of election rigging through the exploitation of secret computer code contained in commercial e-voting systems. The Punchscan ballot is designed so that it can be torn in half, with candidates' names and assigned letters on one half and a set of holes on the other that correspond to the letters, which show through when the ballot is folded. A unique number is assigned to the ballot and is printed on both halves, and the voter indicates the candidate of their choice with a special pen that marks both the hole on the top sheet and the number on the bottom sheet; either half of the ballot can be used to record the votes via a portable scanner, while the other half is shredded. Since letters are randomly assigned to candidates, no one can determine the voter's selections by studying just one half of the ballot, but Punchscan

can because the random assignment is recorded in a database keyed to the ballot number. No database connects the ballot number with the name of the voter, so the voter's personal choices are kept private. Since at no point in the voting process do the computers contain more than half the data needed to know how someone voted, there is no need to physically safeguard the machines.

Advisory Council Seeks Tighter Cyber Security Net
GovExec.com (01/16/07), J. Marino

The National Infrastructure Advisory Council will send a report to the White House that declares the need for greater cooperation between private and public interests in order to establish a cybersecurity network that can defend against an increasing terrorist threat. The report states that sufficiently critical cybersecurity is needed by 2015, and that the Dept. of Homeland Security (DHS) must work with infrastructure owners and operators to build sector-specific maps that could help organize efforts should a disaster or attack take place. Council member M. Grayson said during her presentation that regulatory oversight might be required to make sure the mandated tasks are being carried out satisfactorily by both the public and private bodies involved. The report follows the Homeland Security Advisory Council recommendation that DHS Secretary M. Chertoff extend the department's research to look into how a terrorist attack could utilize the Internet to obstruct homeland security.

Linux Guru Argues Against Security Liability
ZDNet Australia (01/19/07), T. Espiner

Red Hat developer A. Cox told a House of Lords committee on science and technology that a developer's obligation to create secure software is ethical, not legal. Cox, who was among the leading developers of the Linux kernel, spoke of both open- and closed-source software developers as he discussed the generally accepted fact that no one knows how a completely secure program could be built. Closed-source companies cannot be held accountable for breaches of their software because it would do great damage to relationships with third-party vendors, said Cox: "[Code] should not be the [legal] responsibility of software vendors, because this would lead to a combatorial explosion with third-party vendors," he explained. "When you add third-party applications, the software interaction becomes complex. Rational behavior for software vendors would be to forbid the installation of any third-party software." Stressing the communal nature of open-source code, Cox said, "Potentially there's no way to enforce liability." Since many companies implement open-source code in their products, the transfer of liability would cause many problems. Open source developer and security researcher A. Laurie told the committee that while manufacturers have an obligation to the public to make it easy for them to secure their computers, usability can trump security. He believes programmers must be held accountable for software that they claim is secure, yet has been proven not to be.

Congress Lights Fire Under Vote Systems Agency
InternetNews.com (01/19/07), M. Hickins

The Election Assistance Committee (EAC), which has been advised to accredit two new independent testing labs by the National Institute of Standard and Technology, will most likely be the target of substantial congressional scrutiny during the coming year. Members of both houses have made their intentions to reform the way Americans vote. Senate Rules and Administration Committee Chairman Sen. D. Feinstein (D-Calif.) has announced that hearings concerning electronic voting machines will be held and corresponding legislation will be introduced. "One-third of voters cast their ballots in the midterm election using new electronic voting machines, and problems arose, not only in Florida, but in various jurisdictions across the country," said Feinstein. Rep. J. Millender-McDonald (D-Calif.) has said that "the integrity of electronic voting machines is a number-one priority for the Committee on House Administration," of which she is the new chairman. Millender-McDonald has asked Florida courts to grant access to the source code of voting machines in Sarasota County, where 18,000 people did not vote in the congressional election, yet voted in others on the ballot. She is expected to subpoena the source code if the Florida courts do not do so. As the ranking member of the Administration Committee, Millender-McDonald took part in hearings on verifiable paper trails this summer and fall, where she questioned EAC chief D. Davidson concerning suspected flaws in current voting systems guidelines and testing activities. More recently, the EAC has been criticized for not revealing that a lab used to test software for voting machines did not receive proper interim certification, yet continued testing software upgrades in the weeks preceding the November election.

Nordic Researchers Aim for Multiprotocol Multisensor RFID Tag
RFID Journal (01/19/07), R. Wessel

Nordic researchers developing a multiprotocol radio frequency identification (RFID) tag that could be used in a number of applications and regions will find out later in the year whether the project will be extended for another three years. Researchers involved in the IntelliSense RFID initiative plan to incorporate environmental sensor technology into the multiprotocol RFID tag, and expect to complete work on developing sensors for measuring humidity and pH later in the year. Launched in January 2006, the IntelliSense project is expected to have by the end of the year a fully operational RFID tag that supports the ISO 15693 and ISO 18000-6C protocols and is able to monitor air pressure, temperature, humidity, and pH. An extended project would allow the researchers to proceed next year with integrating the 18000-4 standard for tags operating at 2.45 GHz. "Today, there are different types of protocols for different types of applications, such as logistics or consumer applications," says project coordinator O. Vermesan. "Our goal is to merge these protocols so that one can use one tag for different applications." SINTEF in Norway and VTT in Finland are heading the project, which has received $3 million from the NORDITE research program.

Interview: Must-Know Security Insights for 2007
Business 2.0 (01/07) Fortt, Jon

Cryptography Research President P. Kocher outlines in an interview some electronic security threats that people may encounter, along with steps individuals and businesses can take to protect themselves from these threats. Kocher says that the hackers of years past who only wanted attention and bragging rights have been replaced by criminals looking to make money through electronic fraud. Furthermore, a great deal of the work being done to commit these electronic crimes is effectively outsourced to countries with very intelligent people but poor employment opportunities and weak economies, like Eastern Europe, he says. Kocher also explains a new system of attack that Cryptography Research discovered whereby a hacker can figure out a key code by reading the amount of energy a semiconductor chip uses while processing. To protect information, Kocher says you should encrypt all laptops in case they are lost or stolen; never reuse the same password; put a fraud alert on your credit history; ensure that firewalls and virus scanners are active; and put critical data on a physically separate network from the one used for email and Web browsing.

Brain Activity Provides Novel Biometric Key
New Scientist (01/16/07), W. Knight

Researchers at the Center for Research and Technology Hellas in Greece plan to test a biometric system that is able to identify people based on their brain activity this year as a security system for a laboratory in Germany. D. Tzovaras and colleagues make use of electroencephalography (EEG) to measure the electrical activity in the brain as part of the authentication process, in which individuals wear a cap to wirelessly communicate their uniquely identifiable brain data. The researchers believe such an authentication system could serve as a building or computer security system. Their work is part of a larger initiative in Europe, the Human Monitoring and Authentication using Biodynamic Indicators and Behavioral Analysis (HUMABIO) project, which is integrating various biometric strategies to develop a more effective security system. Although the approach has been found to have an accuracy rate of 88%, there is still some criticism that using the cumbersome and invasive EEG cap is not practical. "Wearing a wired helmet with sensors on one's scalp might change the ambiance of the workplace somewhat," says J. Daugman, a biometrics researcher at the University of Cambridge in the UK. Another Cambridge researcher, O. Hauk, questions its accuracy. "EEG varies greatly depending on a person's alertness, or mental operations," says Hauk, a neuroimaging specialist.