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

Δελτίο 122
29 Ιουνίου 2008

Compressed Web Phone Calls Are Easy to Bug
New Scientist (06/12/08), D. Robson

Johns Hopkins University researchers say compressing Voice over Internet Protocol (VoIP) phone calls could expose them to eavesdroppers. The team has developed eavesdropping software that can find chosen phrases in the encrypted data, without decoding a conversation. The software is capable of breaking down a typed phrase into its constituent sounds using a phonetic dictionary, pasting together a version of the phrase from audio clips of phonemes taken from a library of example conversations, and showing how the phrase would look in a real VoIP stream. A close match found in a real call prompts the software to alert the eavesdropper. The software had an average accuracy rate of about 50% in testing, but that increased to 90% for longer, more complicated words. "I think the attack is much more of a threat to calls with some sort of professional jargon where you have lots of big words that string together to make long, relatively predictable phrases," says C. Wright of the Johns Hopkins team. Many service providers plan to implement the variable bitrate compression technique to reduce bandwidth for VoIP calls. "We hope we have caught this threat before it becomes too serious," Wright says.

Beware, Your Computer May Betray You
New Scientist (06/07/08) Vol. 198, No. 2659, P. 26; C. Barras

Non-repudiation is a system whereby sensitive data sent over the Internet is digitally signed at the source with a signature that can be traced to the user's computer as a safeguard against fraud, but L. Sassaman of the Catholic University of Leuven warns that making this system the default setting for all traffic on a network would enable authorities to trace the source of any online activity and take away users' anonymity. Worse still, Sassaman and University of Ireland colleague M. Patterson say that the One Laptop per Child (OLPC) foundation is unintentionally engaged in establishing such a system throughout the Third World by supplying inexperienced users Internet-ready laptops. Theft of the laptops is discouraged with a security model called Bitfrost in which each laptop automatically phones an anti-theft server and sends its serial number once a day so that it can get an activation key, and any machine reported stolen is refused activation. Sassaman and Patterson caution that the security model's use of non-repudiable digital signatures could be exploited by oppressive regimes to identify and silence dissidents. "They may not intend for the signatures to be used for non-repudiation, but it's possible to use them for this purpose," Sassaman says. Although the OLPC laptops are primarily intended to be used for educational purposes, which some people claim would preclude government monitoring, Sassaman says it is unlikely that the systems will be used solely by children, and that conditions in some developing nations might actually encourage children to act as whistleblowers. Sassaman and Patterson are modifying the Bitfrost security model to enable the laptops to identify each other without compromising their users' privacy, based on existing cryptographic methods that cannot be employed for non-repudiation.

Technology Leaders Favor Online ID Card Over Passwords
New York Times (06/24/08) P. C8; L. Flynn

Microsoft, Google, PayPal, and several other companies; industry analysts; and technology leaders have formed the Information Card Foundation, an organization that aims to create an industry-wide identity verification system based on information cards instead of user names and passwords. Under the system, computer users would be able to gain access to Web sites by using a secure digital identity card overseen by a third party. Users would control the information in a secure place and transmit only the information needed to access the site. Burton Group's R. Blakeley says the information cards would be based on open standards and would reduce the number of phishing and fraud incidents because consumers would not have to rely on passwords to gain access to Web sites. Despite the advantages of using information cards, the group faces a number of challenges in establishing such a system. For instance, it will likely take the group several years to get the millions of sites on the Web to support the system, Blakeley says. "The mission of the group is to assure everybody that the industry is working together," he says.

University of Portsmouth Researchers Work on CCTV That Can Hear
Computer Business Review (06/25/08), B. Navuluri

University of Portsmouth researchers are working on a three-year project to incorporate artificial intelligence capabilities into visual recognition software that would enable CCTV cameras to turn in the direction of a certain sound and capture it in about 300 ms. "So, if in a car park someone smashes a window, the camera would turn to look at them and the camera operator would be alerted," says D. Brown, director of the Institute of Industrial Research. Portsmouth will not have the algorithms capture full conversations, but they will be capable of listening for specific words associated with violence. The idea is to develop shapes of sounds that can be recognized by the software of the CCTV cameras. "The software will use an artificial intelligence template for the waveform of sound shapes and if the shape isn't an exact fit, use fuzzy logic to determine what the sound is," Brown says.

Rogue Code Could Seriously Skew US Presidential Election Results
IT Business Canada (06/25/08), B. Jackson

Experts at A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE) say rogue programmers could disrupt US elections that use electronic voting systems. ACCURATE warns that a single rogue programmer writing code for one of the many elections that use e-voting machines could completely distort election results. "One programmer could make a change in the software that would affect 100,000 votes," says ACCURATE investigator D. Dill. The 2002 federal Help America Vote Act provided funding to replace traditional voting machines with direct-recording electronic (DRE) systems, and some states have been using e-voting systems since the 2006 Congressional elections. ACCURATE director A. Rubin says having the entire country vote on a single day presents quite a problem, and while he does not think the country should switch back to punch cards, he still cautions that the US should stay away from DRE machines. The main problem is that they cannot be audited, Rubin says, so the machines could produce the wrong results without anyone ever knowing. Rubin, who will serve as a poll clerk in the upcoming presidential elections, says the anonymous paper survey used to evaluate a training session he ran was more secure than the Diebold Accuvote machines that will be used to register votes in Maryland in the presidential election, because the machines could be compromised by a virus and it would be much more difficult to alter the survey on paper. ACCURATE is working on an open source

threat modeling system called AttackDog that calculates all the possible iterations of steps that would be needed to rig an election system to find key points where such efforts could be thwarted.