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

Δελτίο 12
27 Φλεβάρη 2006

ITU Eyes Role in RFID Standards
RFID Journal (02/16/06), J. Collins

The role of the International Telecommunication Union (ITU) in assuring the successful adoption of radio frequency identification (RFID) and sensor technologies was the focus of a recent workshop in Geneva, Switzerland, attended by industry and academic leaders. "RFID is moving from closed systems of reader and tag to where we need a network capable of sharing the data," says Pierre-Andre Probst, who headed a number of sessions at the ITU workshop. "Billions of tags creating data to transmit over a network means a significant change in traffic for the network to handle. That will require new network capabilities, and there are specific new requirements as we move toward an Internet of things." Among the issues broached at the conference were network and service architecture, requirements for machine-to-machine communications, security, interoperability, and spectrum allocation. "Our main concern is to see the network requirements and capabilities developed to support the move from simple RFID applications toward more-complicated devices that include sensors," says Probst. Spectrum allocation will be addressed at ITU World Radiocommunication Conference scheduled for October 2007 in Geneva.

Calls Made Over Skype Internet Service Make Eavesdropping Tougher
USA Today (02/17/06) P. 2B; P. Svensson

The debate over the legality of the Bush administration's warrentless eavesdropping could become a moot point if more providers follow in the footsteps of Skype, which encrypts its free Internet calls, making them almost immune to eavesdropping. Though encryption techniques for Internet communication have been around for years, most users have not felt vulnerable enough to justify the hassle of security programs such as the cumbersome email application Pretty Good Privacy. Counterpane Internet Security CTO Bruce Schneier notes that Skype's ease of use made it popular, rather than its security. Skype boasted 75 million registered users of its freely distributed software at the end of last year. Talking over the PC is free, but telephone-based communication carries a fee. Calls placed through Skype traverse the Internet encrypted with 256-bit keys, twice the length of the keys typically used to transmit credit card numbers. "It's a pretty secure form of communication, which if you're talking to your mistress you really appreciate, but if al-Qaeda is talking over Skype, you have probably a different view," said Verso Technologies CEO Monty Bannerman. Schneier says that Skype's encryption is of sufficient strength to foil the eavesdropping efforts of the National Security Administration, as even a poorly encrypted call would take hours to crack. He adds, however, that the government could still track Skype's calls, even if it could not listen in on the content. Skype CEO Kurt Sauer claims the system has no back doors to get around the encryption, though he also reports that Skype is in full cooperation "with all lawful requests from relevant authorities," declining to elaborate further.

Understanding Elliptic-Curve Cryptography
Embedded Systems Design (02/06) Vol. 19, No. 2, P. 16; R. Lambert

Elliptic-curve cryptography (ECC) can contribute significantly to the performance of embedded systems. ECC, which is standards-based, comes with all the benefits of public-key cryptography, employs smaller key lengths, and offers more efficient implementation for both public and private operations. Because private-key cryptographic schemes assume knowledge of a shared secret key, systems that use them are hard to initialize or recover when the keys are lost or compromised. Public-key cryptography only sets up shared keys on an as-needed basis, which makes public-key systems more secure but less efficient than private-key systems. As a result, private-key and public-key schemes are often employed together to establish the private keys for encryption or to sign and confirm signatures on messages. The much smaller sizes of ECC keys mean security measures such as smaller signatures and certificates are more efficiently implemented. Increased efficiency of other ECC operations besides security can be realized through additional methods, with notable advantages to embedded systems. On systems that are flexible enough to add hardware, substantial gains in speed and power usage can be extracted from the addition of a hardware assist to carry out finite-field multiplications, which are the foundation of ECC.

Rise From the Machines: Surveillance Software Gets Smart
National Geographic News (02/22/06), B. Harder

While lawmakers and advocacy groups debate the legitimacy of the Bush administration's domestic surveillance program, a host of new technologies are emerging that could revolutionize the scope and method of eavesdropping. New data mining programs are appearing to help intelligence analysts cull through the massive volume of written, audio, and video communications in search of information that could be relevant to the war on terror. Advanced applications can even mine several intercepts at once, offering far more efficiency and vigilance than human agents, as well as being uninfluenced by biases and prejudices. Automated sound analysis tools can almost perfectly distinguish between a child's voice and an adult's, and can usually determine the speaker's gender, age, and other characteristics. Determining that the speaker calling in a bomb threat is a child would call into greater question the seriousness of the threat than if it were an adult, and programs might one day be able to determine with certainty the speaker's country of origin, though SRI International's Venkata Gadde believes that there will always be limitations to the program's precision. Automated analysis is also proving more accurate in detecting when a speaker is lying through the excessive use of 'junk words'--articles, prepositions, and pronouns, while the use of 'exception words,' such as "not," "but," and "except" is usually indicative of honesty, though this analysis does not come with a guarantee of success, either. Similar computer programs have been used to gauge truthfulness in news stories and other writing, and to determine the author of a ransom note. The University of Arizona's T. Meservy and his information-system colleagues are developing a program to analyze non-verbal cues in video transmissions by analyzing the motions of the speaker's head and hands, though computers still have difficulty determining whose body parts belong to whom in a crowded scene.

Guarding the Wire: A Career in Computer Security
Science (02/24/06), A. Fazekas

University of California, Berkeley, computer scientist David Wagner believes that as long as business, government, and consumers use computers, security will always be a necessity. Given the error-prone process of software development, Wagner argues that the best approach to security is to create applications that protect software as it is being developed. With cyber crime having exceeded the drug trade in overall profitability, security experts such as Wagner are in high demand, with a recent survey projecting that the number of information-security professionals around the world would increase from 1.3 million in 2003 to 2.1 million in 2008. The Labor Department shares Wagner's view that security is a burgeoning field, where threats emerge faster than security experts can address them. Wagner gained his first bit of notoriety as a graduate student at Berkeley in 1995 when he and a friend decided to test Netscape's claim that its method of encryption enabled customers to securely send credit card information over the Internet through its browser. When they discovered how easy it was to intercept credit card numbers protected by Netscape's random cryptographic key generator, Wagner and his friend were soon contacted by the media and Netscape shipped out an overhauled version of its browser with a different security algorithm. Since opting for a career in academia, Wagner has devoted considerable attention to e-voting systems, noting that the relatively small commitment made by the private sector into developing the machines precludes advanced security research. Wagner believes that a secure, paperless voting system is the biggest challenge facing the industry today, one that, he notes, no one in the private sector wants to take up. "Probably the only place that I could do work in e-voting security is in a university because there's not much profit to be had in securing elections. It's crucial to democracy, but it's not a big moneymaker."

Fingerprint Advances Will Fight Cybercrime
University at Buffalo News (02/22/06)

A team of University at Buffalo biometrics researchers has determined the degree of security afforded by fingerprint scans that typically only capture a partial print, which had been a major stumbling block for the practical implementation of biometric identification in lieu of passwords. "Thus research paves the way toward efficient methods of preventing unauthorized access to handheld devices, such as cell phones, wireless handheld devices, and electronic audio players, as well as to secure Web sites," said Buffalo computer science and engineering professor Venu Govindaraju, adding that the technology could also have applications in forensics. The researchers' technique, the Automated Partial Fingerprint Identification System, defines the keypad sensor dimensions to specify the level of required security, pinning down for the first time how much of a fingerprint that is required to provide a degree of security comparable to a six-letter password. The system relies on an algorithm that determines if two images are a close enough match to verify the identity, recognizing that fingerprints and most other biometric information are incomplete, and that, unlike passwords, biometric data can be slightly different with each use. Securely matching biometric scans requires an algorithm that can adjust for factors that could cause variations in a person's fingerprints, such as how firmly the person pressed and the level of moisture in the finger. Govindaraju notes that the system relies on a transformation of the image, rather than the image of the fingerprint itself, making reverse engineering all but a mathematical impossibility.

Hackers Beware! New Technique Uses Photons, Physics to Foil Codebreakers
University of Toronto (02/22/06), N. Wahl

Researchers at the University of Toronto have used a quantum decoy technique to encrypt data transmitted over fiber-optic cable. Quantum cryptography makes use of laser light particles (photons) to deliver encryption keys over fiber-optic cables, and employs Heisenberg's Uncertainty Principle, in which the act of observation alters a quantum object. As a result, a hacker who attempts to eavesdrop on a data stream to determine the encryption key would prompt a change in the photonic decoys, which would indicate that an effort was made to tamper with the data. The experiment involved sending photonic decoys over a 15-kilometer telecommunications fiber, and then transmitting a second broadcast to let the receiving computer know which photons carried the signal and which photons were decoys. The quantum decoy technique changes the intensity of the photons. "Quantum cryptography is trying to make all transmissions secure, so this could be very useful for online banking, for example," says professor Hoi-Kwong Lo, a specialist in physics and electrical and computer engineering at the university's Center for Quantum Information and Quantum Control. "The idea can be implemented now, because we actually did the experiment with a commercial device," adds Lo, senior author of the study on the technique.

Buyer Beware: Online Shopping Hazards Exposed by Amherst Computer Scientist
University of Massachusetts Amherst (02/21/06)

University of Massachusetts Amherst computer scientist K. Fu was critical of the use of cookies by Web sites during a mid February American Association for the Advancement of Science meeting in St. Louis, questioning their use as a log-in method. Fu said the use of client certificates in SSL or "secure socket layer," the system often used by universities, for example, to allow students to look up their grades, is a better log-in method. He described SSL as using a signet ring to stamp a seal in wax, but not sending the ring itself to a Web site, which is the case when cookies are used to authenticate a user who is shopping online. Cookies allow users to bypass a Web site's log-in page, but someone who has access to a series of cookies on a hard drive has the opportunity to find a pattern and determine their algorithm. "It's the kind of thing a bored teenager could do in a few hours," Fu said. Retailers have not embraced certificates for their Web sites because transactions would no longer be as quick and easy, said Fu, adding that people do not have much of a choice when it comes to shopping online. "Even if you shop by phone, the attendant often enters your data on the same page you are trying to avoid," according to Fu.

Invasion of the Computer Snatchers
Washington Post Magazine (02/19/06) P. 10; B. Krebs

Hackers are commandeering unprotected computers or "bots" to deliver spam or adware programs that users unwittingly install on their systems. Adware, also known as spyware, mines data about the user's online browsing habits that marketing companies can use to direct targeted advertising, or can be employed to gather sensitive information for more nefarious purposes. Adware distribution companies recruit hackers or "affiliates" to help install their software, luring them with the promise of a hefty paycheck. These companies state in their "terms and conditions" disclaimer that affiliates will not be paid if they install their products without computer owners' permission, but hackers have devised crafty and often simple ways to surreptitiously install adware. Making money is increasingly becoming the No. 1 goal of hackers, who often perceive their victims as too stupid or lazy to take basic precautions. The latest hacker generation was brought up with the Internet, and learned how to hack for profit with a minimum of cost or effort. Hackers control their adware installation through networks of compromised computers or "botnets," and cracking down on botnets is difficult because hackers can easily switch their botnets onto different servers or ISPs. Prosecution against botnet operators is another arduous challenge, given that their crimes and networks often transcend national boundaries.

Beyond Bar Codes: Turning Up Plastic Radio Labels
Science News (02/11/06) Vol. 169, No. 6, P. 83; P. Weiss

Researchers in Europe have developed plastic radio frequency-identification (RFID) prototypes that operate at the industry-standard frequency of 13.56 MHz. At the 2006 IEEE International Solid-State Circuits Conference in San Francisco this week, researchers from Philips Research Laboratories in Eindhoven in the Netherlands presented an all-plastic device that responded with an 8-bit code when queried via radio waves by a nearby reader. And Markus Bohm of PolylC in Erlangen, Germany, discussed the experimental 13.56-MHz tag the company developed last fall. Each of the plastic RFID tags "constitutes an advance toward making a manufacturable RFID tag," according to K. Dimmler of Organic ID in Colorado Springs. Plastic RFID tags would be cheaper to produce than silicon-based tags, which are found in smart cards. The use of plastic could allow for the emergence of RFID tags in the labeling of consumer products, electronic tracking, and transactions as well. However, researchers would still need to use printing technology to make production of all-plastic RFID tags cost-effective, and the devices need to broadcast more powerfully.