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

Δελτίο 135
20 Νοέμβρη 2008

Cops Enlist HAL in Fight Against Crime
silicon.com (11/05/08), N. Heath

In an effort to explore how artificial intelligence (AI) can improve digital forensics, the UK-funded Cyber Security Knowledge Transfer Network (KTN) will examine the use of AI in Web counter-terrorism surveillance, preventing Internet fraud, protecting identities online, and online data mining. KTN will examine how artificial neural networks can intelligently combine evidence from different online sources and databases, and how particle swarm intelligence can probe information shared by groups on social networks. KTN also will research how autonomous agents could preserve images of hard drives and extract useful information from networks. KTN expects that AI will be a necessity for businesses and law enforcement looking to understand the massive amounts of information being generated on the Web, in public databases, and on corporate networks. To achieve this level of AI, KTN is establishing an AI and forensics special-interest group to enable forensics and AI experts to discuss how AI can shape digital forensics in the future. KTN director N. Jones says that today's vast, distributed networks offer access to a wide variety of data, but processing and mining that data is problematic. Jones says KTN also will propose a framework for how AI tools should be used in criminal investigations to ensure evidence remains admissible in court.

E-Voting Backers, Watchdogs Hope to Smooth Out Bumps Next Time
Computerworld (11/10/08), T. Weiss

Electronic-voting watchdog groups reported no major technological failures during last Tuesday's US presidential election, although there were a few scattered problems with touch-screen and optical-scan voting machines. For example, Ohio officials reported minor problems with voter-verifiable paper printouts generated by tough-screen systems, while Michigan, Pennsylvania, and New Jersey also reported minor voting machine breakdowns during the election. National Association of State Election Directors executive director D. Lewis said it was a normal election day and dismissed the few problems as "not systemic." Nevertheless, Fortify Software chief scientist B. Chess called on Congress to pass strict national standards for e-voting systems. "We need to test ways the machines could fail and the reliability of the machines in a true election environment," Chess says. ACM US Public Policy Committee chair E. Spafford says it is unclear whether fixing voting systems will be a top priority for incoming government officials. "We have so many other pressing national concerns that are going to require attention first," Spafford says. "I wonder whether this will bubble up high enough to get addressed soon."

North Carolina Uses Bar Codes to Match Voters With Ballots
Government Computer News (11/03/08), W. Jackson

A new bar-code scanning voting system was used by more than 2 million voters in North Carolina since the polls opened in that state on Oct. 16 for the US presidential election. "It is an extremely simple solution," says M. Burris, IT director for North Carolina's Board of Elections. "The poll workers are already taxed with so many duties, so we wanted a simple and economic solution." The front end of the system is a handheld bar-code scanner that matches the voter with the proper ballot. The back end is a geographic information system tied to the statewide voter-registration system that assigns the appropriate ballot type to each voter, depending on their home jurisdiction. Burris says this is the first time this type of system for ballot distribution and management has been used for an election. The board initially considered using a personal digital assistant to do the scanning, but the devices were too expensive, were ergonomically impractical over long periods of use, and were generally too complex. The bar-code scanner was chosen because the system is simple to use. A poll worker scans a bar code on the voter's affirmation card and a corresponding code on the ballot being issued. The scanner turns on a green light and gives an audible tone if they match, and displays an error message if there is a mismatch. The back-end of the system is linked to the registration system to indicate the proper type of ballot for each voter based on where they live.

Why Veins Could Replace Fingerprints and Retinas as Most Secure Form of ID
Times Online (UK) (11/11/08), M. Harvey

Finger vein authentication is starting to gain traction in Europe. Easydentic Group in France says it will use finger vein security for door access systems in the United Kingdom and other European markets. The advanced biometric system, which verifies identities based on the unique patterns of veins inside the finger, has been widely introduced by Japanese banks in thousands of cash machines over the last two years. Hitachi developed the technology, which captures the pattern of blood vessels by transmitting near-infrared light at different angles through the finger, and then turns it into a digital code to match it against preregistered profiles. Veins are difficult to forge and impossible to manipulate because they are inside the body, according to Hitachi. The company also says finger vein technology is more affordable than iris scanning or face/voice recognition and has a lower false rejection rate than fingerprinting. Finger vein authentication is primarily used in Japan for ATMs, door access systems, and computer log-in systems.

New Techniques Easier, More Secure
Columbian (WA) (11/09/08), T. Vogt

University of Idaho scientists are working to create computer passwords that are not only easier to remember but will provide better security as well. "Humans are good at remembering meaningful things, but bad at remembering arbitrary sequences of digits," says University of Idaho psychology professor S. Werner. Consequently, people tend to have trouble remembering the most secure passwords, which link together letters and number in random order, but may have more success with a sequence of pictures as a password. Werner says the challenge is to make a password that is memorable for the user yet as unpredictable and random as possible. Fortunately, people's visual memory is quite good, as people can extract a lot of information from a picture very efficiently, Werner says. He and his research team showed images to test subjects for about a minute, and then showed them nine-character strings of random numbers and letters. After 30 minutes, subjects were fairly successful in recalling both the images and the numbers and letters, but after about a month, the subjects could only identify 25-35% of the alpha-numeric sequence, but were still able to identify 90% of the images. In the system Werner is exploring, a password picture might include images in nine categories, such as a man, a woman, a child, a pet, another animal, a piece of fruit, an instrument, and a background. The user would select an image from each of these groups, and when logging on again later be asked to identify the image they selected from each group. Werner does not see this system becoming a password for day-to-day accounts, like email, but it could become a log-in system for accounts that are accessed less frequently, like retirement accounts.

An Algorithm With No Secrets
Technology Review (11/18/08), E. Naone

The National Institute of Standards and Technology (NIST) is organizing a competition to find an algorithm to replace the Secure Hash Algorithm 2 (SHA-2), which is becoming outdated. NIST plans to release a short list of the best entries by the end of November, the beginning of a four-year-long process to find the overall winner. In 2005, Tsinghua University Center for Advanced Study professor X. Wang found weaknesses in several related hashing algorithms, and since then Wang and others have found faults in several other hashing schemes, causing officials to worry that SHA-2 also may eventually be found to be vulnerable. A hash algorithm creates a digital fingerprint for messages that keep them secure during transit, but it is only considered secure if there is no practical way of running it backward and finding the original message from the fingerprint. There also cannot be a way of producing two messages with the same exact fingerprint. The weaknesses discovered by Wang and others relate to this problem, which cryptographers call a collision. It is impossible to completely avoid collisions, but the best algorithms make collisions extremely hard to produce. "Hash functions are the most widely used and the most poorly understood cryptographic primitives," says BT Counterpane's B. Schneier. "It's possible that everything gets broken here, simply because we don't really understand how hash functions work." NIST already has received 64 entries and is counting on cryptographers to narrow the list.

The First Metropolitan Quantum Cryptography Network Will Be Available in Spain by 2010, Universidad Politecnica de Madrid (11/07/08)

Universidad Politecnica de Madrid School of Computing researchers have developed a prototype metropolitan quantum-key distribution network that will be ready for deployment by Telefonica on any Spanish urban telecommunications network by 2010. The prototype is being developed as part of the Security and Confidence in the Information Society research and development project, which includes a consortium of 12 companies and 15 public research institutions. The project's goal is to create a new generation of integral security solutions capable of dealing with telecommunications security risks currently threatening conventional networks. The security of conventional public-key cryptography methods is based on the confidence that any attacker does not have enough computing power or mathematical knowledge to decrypt the message. However, this method is becoming less secure as computing power increases and mathematical models become increasingly sophisticated. Quantum-key distribution relies on quantum mechanics and provides a completely different way of creating cryptographic keys, providing much higher levels of security. The researchers' metropolitan quantum-key distribution network can coexist with traditional communications networks, which they say is a major advantage as networks already have all the key components and have been successfully tested in experiments.