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

Δελτίο 146
23 Απρίλη 2009

Our Ears May Have Built-In Passwords
New Scientist (04/13/09), P. Marks

University of Southampton researchers are investigating a possible biometric security technique that uses the subtle noises produced by the human ear to verify the user. The human ear makes noises, called otoacoustic emissions (OAE), which are only detectable by supersensitive microphones. OAE could be unique to each individual, potentially leading to a biometric security technique that call centers and telephone-banking operations could use to identify callers. OAE emanate from within the spiral-shaped cochlea in the inner ear. Southampton engineer S. Beeby says OAE can be provoked when a series of clicks are played into the ear. The resulting sounds comprise signals between 0-5 KHz and vary in amplitude. Click tests are used to check newborn babies for signs of hearing difficulties. The power and frequency distribution of the OAE provoked by a specific series of clicks are highly distinctive between people due to the internal shape of each person's ear. Beeby is researching whether OAE patterns can be used like iris scans or fingerprints. In the controlled conditions of a lab, everyone's OAE emissions are unique, but whether this is a practical security measure in the real world is still undetermined.

Implementation Plan for Voting System Requirements Set
Government Computer News (04/07/09), W. Jackson

The US Election Assistance Commission (EAC) is expected to complete work on a revised set of voluntary guidelines for voting systems later this year. A total rewrite of the guidelines is expected to be finished in 2011. EAC's Voluntary Voting System Guidelines establish a set of standards that states can use to certify voting equipment. Although the guidelines are voluntary, most states require that their voting systems are in compliance with some version of them. The EAC's Technical Guidelines Development Committee and the National Institute of Standards and Technology (NIST) have been working on a major rewrite of the guidelines, called the Next Iteration, for the past year. The NIST also is developing a series of standard tests for the Next Iteration guidelines that would replace current proprietary tests currently used by accredited laboratories to test voting equipment. The guidelines and the tests are intended to address concerns about the reliability and security of voting systems, particularly electronic-voting systems, which critics say are vulnerable to security flaws. Some of the major issues addressed by the Next Iteration include developing a threat assessment of voting systems, possibly developing requirements for a common interface language for peripheral voting equipment such as e-pollbooks, and addressing recommendations such as software independence in voting equipment and open-ended vulnerability testing.

UCL Study: Natural 'Barcodes' Help Us Recognise Faces
UCL News (04/04/09)

Humans recognize faces by organizing facial features such as eyebrows, eyes, and lips into simple black and white lines of information, say S. Dakin of the University College London (UCL) Institute of Ophthalmology and professor R. Watt from the University of Stirling. The researchers manipulated the images of celebrities and found that their facial features could be rendered in horizontal stripes of information that are similar to the barcodes used on commercial products. Dakin and Watt also studied other natural images, such as flowers and landscapes, but found that faces are unique in conveying useful information this way. They say the barcode pattern is recognized efficiently by the visual parts of the brain, is easy to locate in complex scenes, and may be resistant to changes in the overall appearance of the face. Their research has the potential to improve face recognition software and CCTV cameras. "To improve face recognition software, we need to look towards biology and see how we have solved the problem," Dakin says. "If we are looking for barcode-like images to tell us that 'this is a face,' then software could be developed to mimic this skill."

Control of Cybersecurity Becomes Divisive Issue
New York Times (04/17/09) P. A16; J. Risen; E. Lichtblau

The US National Security Agency (NSA) is lobbying to head the government's cybersecurity programs, and some officials are concerned that such a maneuver would grant the spy agency too much sway over government computer networks. R. Beckstrom, who resigned in March as director of the Homeland Security Department's National Cyber Security Center, said in an interview that if the NSA gained that much power, it would have the authority to collect and analyze every email message, text message, and Google search performed by every worker in every federal agency. "Power over information is so important, and it is so difficult to monitor, that we need to have checks and balances," he stressed. Beckstrom said he assumed that an intelligence agency designed to contend with outside threats should not be given so much influence over information traffic in the US government. Detecting threats against the computer infrastructure requires cybersecurity guardians to have virtually unlimited access to networks, and Beckstrom argues for the division of those responsibilities among agencies. National intelligence director D. Blair recently told Congress that the NSA should oversee federal cybersecurity, claiming that the group possesses the computer "wizards" with the skills needed. "The NSA's expertise, which is impressive and very, very deep, is focused primarily on the needs of the military and the intelligence community," said University of Pennsylvania computer security expert M. Blaze. "Their track record in dealing with civilian communications security is mixed at best."

Eyeball Spy Turns the Tables on Big Brother
New Scientist (04/14/09), P. Marks

The performance of closed-circuit television (CCTV) operators could be improved by analyzing their gaze, according to researchers in Turkey. U. Vural and Y. Akgul of the Gebze Institute of Technology have developed a gaze-tracking camera system to watch the eyeballs of CCTV operators as they work. The gaze-tracking system would train a webcam-style camera on the irises of people who watch CCTV images in the control room. CCTV operators could miss criminal or antisocial activity because they have so many screens to monitor simultaneously. After the system uses an algorithm to analyze where CCTV operators are looking, it uses software to create a video of sequences missed during the shift. "This increases the reliability of the surveillance system by giving a second chance to the operator," the researchers write in the journal Pattern Recognition Letters. The gaze-tracking camera system runs on a standard PC and processes the images in real time, making summary frames ready to browse, similar to a fast-motion flip book.

Innovation: Harnessing Spammers to Advance AI

New Scientist (04/17/09), C. Barras

Some Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTCHA) security systems are already being solved by spammers, but CAPTCHA co-creator L. von Ahn says that when a software program is written that can solve all CAPTCHA it will be a cause for celebration as well as concern. He says that when spammers are finally able to break any CAPTCHA it will mark a major milestone in artificial intelligence (AI). Von Ahn says he has seen offers as high as $500,000 for anyone capable of writing software that can break reCAPTCHA, an improved system used by several major Web sites. The $500,000 prize is enough to attract people with the skills to accomplish such a feat, and is 5 times bigger than the Loebner Grand Prize that is offered to the programmer who designs a computer that passes the Turing test. Von Ahn says if spammers are able to write a program that reads distorted text they will have solved an AI problem, and security groups will be able to switch to alternative CAPTCHA systems, such as one based on pictures, which will give spammers another AI problem to solve. For example, a system Google will present at the International World Wide Web Conference asks users to correctly orient images that are randomly rotated, a task computers struggle with when an obvious horizon is unavailable. The ability to easily change security measures could make using spammers as an AI resource tool a viable option.

Software Improves P2P Privacy By Hiding in the Crowd
Northwestern University News Center (04/08/09)

Northwestern University researchers have identified a "guilt-by-association" threat to privacy in peer-to-peer (P2P) networks that would allow an eavesdropper to accurately classify groups of users with similar download behavior. To counter this threat, the researchers released open source software that restores a user's privacy by masking their download activity to disrupt classification. Northwestern professors F. Bustamante, L. Amaral and R. Guimera found that only the patterns of connection, and not the data itself, are sufficient to pose a serious threat to user privacy. The researchers studied connection patterns in the BitTorrent file-sharing network and found that groups of users formed communities in which each member consistently connected with other community members more than with users outside the community. Bustamante says this trend was surprising because BitTorrent was designed to create connections at random. After identifying the community behavior, the researchers demonstrated that an eavesdropper could classify users into specific communities using a relatively small number of observation points. The information could be used to launch a "guilt-by-association" attack in which a hacker only needs to determine the downloading behavior of one user to convincingly argue that all users in the community are doing the same things. The researchers released an extension to BitTorrent called SwarmScreen, which downloads randomly-selected content to prevent eavesdroppers from distinguishing that content from the content users requested.

Study: People Manage Their Privacy on Facebook Naturally
Helsinki Institute for Information Technology (04/20/09) Noronen, Visa

Trust is a key factor in the way people manage their privacy when using social media tools, according to researchers at Finland's Helsinki Institute for Information Technology (HIIT). Although users cannot control what other people publish on Facebook and similar sites, they tend to provide only information about themselves that they want other people to see, and they avoid publishing negative information about other people, say researchers Airi

Lampinen, Sakari Tamminen, and Antti Oulasvirta. People will limit their number of friends, and also will exchange private messages within more defined closed groups when they need to update their status, the researchers discovered during interviews with users of social media. "People protect their own privacy and other people's privacy instinctively, often almost without noticing," Lampinen says. "To support these activities, social networking sites need to provide users with easy-to-use privacy management that is interlinked with the overall use of the sites."

Dialect Detectives
MIT News (04/16/09), D. Ryan

Massachusetts Institute of Technology Lincoln Laboratory engineer P. Torres-Carrasquillo and his colleagues are developing a dialect identification system that could assist translators in identifying multiple variants of a spoken language. The researchers say the system could be used by law enforcement agencies to identify the origin of an intercepted phone call detailing a drug shipment, based on the dialect spoken and the region that dialect is from. Previous work at Lincoln Laboratory on dialect information focused on building models that mapped the audiowave frequencies of phonemes, the individual sounds of a spoken language. However, Torres-Carrasquillo has focused on lower-level acoustic systems that use the basic spectral similarities of small pieces of spoken utterances. "We are not looking for the types of data linguists deal with--larger units such as phonemes and words," Torres-Carrasquillo says. "We're looking at the statistical distributions of basic frequency spectra of small pieces of sounds." The researchers are building a model that classifies the training data and finds markers that discriminate the frequency chrematistics of the data. They are using pattern recognition and classification methods known as support vector machines and Gaussian Mixture models, which use models trained to emphasize the more distinctive tiny features seen in the frequency patterns of small pieces of the dialects in question.

Once Smartphones Become Truly Common, So Will the Viruses That Attack Them
Northeastern University News (04/14/09), R. Nyul

Northeastern University researchers say that smartphones will soon be targeted by viruses on a massive scale, but a study by the researchers could provide a way to negate these attacks. Northeastern University physicist and network scientist A.-L. Barabasi and fellow researchhers tracked the spreading potential of Bluetooth and multimedia messaging service viruses, and predicted that these viruses will become a significant threat to smartphones that gain at least a 10% market share. The user base for smart, handheld devices is still small and fragmented, making a large virus outbreak impossible. However, Barabasi warns that once smartphones are more widely used and one of the operating systems increases its market share, the users of the system will be targeted by mobile viruses in only a matter of minutes. He says an outbreak on a smartphone could be worse than any outbreak on a traditional computer. P. Wang, a Ph.D. candidate at Northeastern's Center for Complex Network Research, says understanding the basic spreading patterns of the viruses could help researchers find ways of minimizing their impact, estimate the realistic risk carried by mobile viruses, and develop measures to avoid the costly and damaging effects of outbreaks.