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

Δελτίο 163
25 Νοέμβρη 2009

Researchers Develop a Facial Biometrics System Capable of Creating a Facial DNI
Carlos III University of Madrid (Spain) (11/04/09)

Researchers at Carlos III University of Madrid (UC3M) have developed a facial biometrics system based on individual models. UC3M study author D.D. Gomez says the objective is to create a model for each person that highlights the most distinguishing features on each face. Delgado says one way to describe a person is through traits that other people do not have, and their new system aims to apply that approach to an algorithm. The researchers say the most complicated part is combining facial geometry and facial texture. "With only the geometric information, very low classifications are obtained, which is why we combine this information with that of facial texture to obtain a more robust model, and a statistical way of combining them occurred to us, which offered very good results," Delgado says. The researchers have shown that when their system is used in a controlled environment it can achieve 95% accuracy. The biggest challenge to facial-recognition systems is lighting, which can change the color of a person's face. Aging also is a challenge as people's faces can become heavier, thinner, or more wrinkled.

Is AES Encryption Crackable?
TechNewsWorld (11/03/09), J. Germain

The Advanced Encryption Standard (AES) system was long believed to be invulnerable to attack, but a group of researchers recently demonstrated that there may be an inherent flaw in AES, at least theoretically. The study was conducted by the University of Luxembourg's A. Biryukov and D. Khovratovich, Hebrew University's N. Keller, and the Weizmann Institute's A. Shamir. In their report, "Key Recovery Attacks of Practical Complexity on AES Variants With Up to 10 Rounds," the researchers challenged the structural integrity of the AES protocol. The researchers suggest that AES may not be invulnerable and raise the question of how far is AES from becoming insecure. "The findings discussed in [in the report] are academic in nature and do not threaten the security of systems today," says AppRiver's F. Touchette. "But because most people depend on the encryption standard to keep sensitive information secure, the findings are nonetheless significant." AirPatrol CEO O. Diaz believes that wireless systems will be the most vulnerable because many investments in network media are wireless, and there is no physical barrier to entry. Diaz says that exposing the vulnerability of the AES system could lead to innovations for filling those gaps. Touchette says that AES cryptography is not broken, and notes that the latest attack techniques on AES-192 and AES-256 are impractical outside of a theoretical setting.

Rutgers Computer Scientists Work to Strengthen Online Security
Rutgers University (11/09/09), C. Blesch

Rutgers University computer scientists are developing an alternative to online security questions that is designed to be easier for legitimate users and more secure. "We call them activity-based personal questions," says Rutgers professor D. Yao. "Sites could ask you, 'When was the last time you sent an email?' Or, 'What did you do yesterday at noon?' "Initial studies suggest that questions about recent activities are easy for legitimate users to answer but harder for attackers to guess or learn. "We want the question to be dynamic," Yao says. "The questions you get today will be different from the ones you would get tomorrow." Initial results from the system will be presented at ACM's Conference on Computer and Communications Security, which takes place Nov. 9-13 in Chicago, Ill. Rutgers researchers found that questions related to time were more robust than other questions. Yao says online service providers can create security questions using data from a user's email, calendar, or transactions, though computers would need to use natural language processing tools to synthesize understandable questions and analyze answers for accuracy. Yao has proposed additional studies to determine the practicality of the new approach and how it could best be implemented.

Web Security Tool Copies Apps' Moves
Technology Review (11/09/09), C. Mims

Microsoft researchers have developed Ripley, a way to secure Web applications by cloning the user's browser and running the application remotely. Ripley, announced at ACM's Computer and Communications Security Conference, which takes place Nov. 9-13 in Chicago, prevents a remote hacker or malicious user from changing the behavior of code running inside a Web browser by creating an exact copy of the computational environment and running that copy on the server. Ripley also relays all of the user's actions, including mouse clicks, keystrokes, and other inputs, from the client to the server as a compressed event stream. The behavior of the clone code is compared to the behavior of the application running on the user's browser. If any discrepancies occur, Ripley disconnects the client. "You cannot trust anything that happens in the client," says Ripley lead developer B. Livshits. "It's basically the devil in the browser from the developer's point of view." Livshits says Ripley is completely invisible to the end user and will not affect the normal function of a Web application. Ripley can even enhance the performance of Web applications, because the clone program is written in .Net, which is 10 to 100 times faster than the JavaScript used on the client side. University of California, Berkeley researcher A. Barth says Ripley is part of a larger trend to protect the integrity of client-side programs. "The work suggests that security would benefit if we validated more than we're validating today," Barth says.

Breaking the Botnet Code
Technology Review (11/11/09), R. Lemos

Researchers at the University of California, Berkeley and Carnegie Mellon University (CMU) have developed a way to disrupt botnets by automatically reverse engineering the communications between compromised computers and the controlling servers. The researchers say that automatic reverse engineering can decipher the structure and purpose of the communications between the controlling server and the botnet. Their new technique translates both the commands received by a client and the responses it sends. "The communications protocol of the botnet is the core of the botnet," says CMU PhD student J. Caballero, the lead author of a paper on the research. "That is how the attacker sends commands to the botnet." The researchers ran botnet code on a virtual machine and analyzed the movement of information between a computer's registers before it was encrypted. Watching for changes in the memory registers enabled the researchers to derive the structure of the botnet communications and infer the function of the various components of each command. The researchers have built Dispatcher, a tool that can analyze botnet communications and inject new information into the communications stream. Security researchers say Dispatcher could them help reverse engineer botnets. "It would solve a problem that the world has--having enough people to analyze botnets," says SecureWorks senior security researcher Joe Stewart. "You have a cadre of enthusiasts who could use this to help them."

NIST Test Proves 'the Eyes Have It' for ID Verification
National Institute of Standards and Technology (11/03/09), E. Brown

National Institute of Standards and Technology (NIST) computer scientists have released a report that demonstrates the ability of iris recognition algorithms to maintain their accuracy and interoperability with compact images, which means they could be used for large-scale identity management applications. The success of iris recognition largely depends on the ability of recognition algorithms to process standard images from the cameras currently available, which requires images to be captured in a standard format and prepared so they are compact enough for a smart card or for transmission across global networks. The images also must be detailed enough to be identifiable by computer algorithms and be interoperable with any iris-matching product. NIST scientists are working with the international biometrics community to revise iris recognition standards. NIST launched the Iris Exchange IREX program to encourage the development of iris recognition algorithms that use images conforming to the ISO-IEC 19794-6 standard. The international standard, currently under revision, defined three competing image formats and three compression methods. The first IREX test narrowed the field by determining which ones consistently performed at a high level. Two of the image formats that centered and cropped the iris were found to be the most effective, while two compression formats were found to create small enough file sizes for storage and transmission while retaining enough detail.

How Secure Is Cloud Computing?
Technology Review (11/16/09), D. Talbot

The recent ACM Cloud Computing Security Workshop, which took place Nov. 13 in Chicago, was the first event devoted specifically to the security of cloud computing systems. Speaker W. Diffie, a visiting professor at Royal Holloway, University of London, says that although cryptography solutions for cloud computing are still far-off, much can be done in the short term to help make cloud computing more secure. "The effect of the growing dependence on cloud computing is similar to that of our dependence on public transportation, particularly air transportation, which forces us to trust organizations over which we have no control, limits what we can transport, and subjects us to rules and schedules that wouldn't apply if we were flying our own planes," Diffie says. "On the other hand, it is so much more economical that we don't realistically have any alternative." He says current cloud computing techniques negate any economic benefit that would be gained by outsourcing computing tasks. Diffie says a practical near-term solution will require an overall improvement in computer security, including cloud computing providers choosing more secure operating systems and maintaining a careful configuration on the systems. Security-conscious computing services providers would have to provision each user with their own processors, caches, and memory at any given moment, and would clean systems between users, including reloading the operating system and zeroing all memory.

A New Tool for Real-Time Credit Card Fraud Prevention
Universidad Politecnica de Madrid (Spain) (11/12/09), E. Martínez

Researchers from several European institutions, led by the Universidad Politecnica de Madrid's School of Computing, are creating a services development platform that will be able to process millions of data per second. The researchers say the new technology could help fight real-time credit card fraud, mobile telephony SIM card cloning, and fraudulent unpaid telephone calls. Banks and credit card companies have several systems in place to detect fraudulent credit card use, but they all detect fraud after it has been committed, aiming to identify the fraud and prevent cardholder losses. The new system will implement real-time fraud detection, preventing improper credit card use and cardholder losses because improper payments will not be authorized. The same technology can be applied to mobile phones, where SIM card copying or the fraudulent use of telephone lines is only detected after the crime. The real-time system is being developed as part of the Scalable Autonomic Streaming Middleware Project (Stream), which aims to build a platform for real-time processing of massive data flows. The major technological innovation is that Stream uses large node clusters to process massive data throughput of millions of data per second.

Facebook Offers Poor Personal Data Protection
SINTEF (11/17/09)

A study of Norwegian Internet users and social media found that people are willing to post their personal information on social media sites even when they are not aware how it will be used. Conducted by SINTEF for the Norwegian Consumers' Council, the researchers found that 60% of Norweigan Internet users are on Facebook. SINTEF's P. Brandtzaeg and M. Luders conclude that Facebook offers relatively poor personal data protection due to the service itself, its design, the level of competence of its users, and their lack of awareness of how to protect themselves. "Facebook has become an important arena for social participation in our personal environment," Brandtzaeg says. "However, it is becoming ever more easy to gather and aggregate personal information, outside the control of users." Still, people are willing to post their personal information because so many other people use Facebook, and they rarely hear of unfortunate incidents. Respondents were usually not aware that Facebook uses personal information for commercial purposes, and their personal information also can be used against them, such as when they apply for a job. The researchers say that people and objects will be woven together ever more closely by the next wave of Internet media such as Google Wave and mobile smartphones. "This can make us even more vulnerable to failures of personal data protection," Luders says.

Hackers Create Tools for Disaster Relief
CNet (11/15/09), E. Mills

The first-ever Random Hacks of Kindness recently took place in Mountain View, California, bringing software developers together to focus on how technology could be used to help people get information and find each other during emergencies. Organized by Google, Microsoft, Yahoo, NASA, the World Bank and SecondMuse, the event is viewed as a way to bring technologists together to solve real-world problems and create a community of developers to build tools to help emergency workers. "We're trying to seed the community," says Google Crisis Response's J. Martin. "We're saying, partner with the private sector and we can push technology forward and innovate." Developers used social media sites such as Twitter and SMS for information sharing to build about a dozen tools. One project would use laptops, routers, mobile devices, USB keys, and Wi-Fi to create a mesh network during a disaster. A group primarily from NASA took first place with a mobile application for easily notifying loved ones that "I'm OK" via SMS by clicking one button. The organizers plan to hold the next Random Hacks of Kindness event in early 2010 in Washington.

Are Nations Paying Criminals for Botnet Attacks?
Network World (11/17/09), E. Messmer

Countries that want to disrupt other nations' government, banking, and media resources can simply hire cybercriminals to launch botnet attacks, according to new report by McAfee that interviews 20 cybersecurity experts. McAfee's D. Alperovitch says botnet attacks are hard to trace because of the anonymous nature of how they are requested and paid for. William Crowell, former deputy director of the US National Security Agency, says that "anyone can go to a criminal group and rent a botnet. We've reached a point where you only need money to cause disruption, not know-how, and this is something that needs to be addressed." The July 4th, 2009, cyberattacks launched against South Korea and the United States prompted Rep. P. Hoekstra (R-Mich.) to urge the United States to "conduct 'a show of force or strength' against North Korea for its alleged role in the attacks," the report says. Alperovitch says there is no concrete evidence that North Korea was behind the cyberattacks, but points out that it was unusual that the botnet was concentrated entirely in South Korea. Alperovitch also notes that North Korea gets its Internet link from China because North Korea never took ownership of the top-level domains it was assigned by ICANN. Countries that are known to be expanding their cyberwarfare capabilities include the United States, France, Israel, Russia, and China, according to the report. Major cyberconflicts have the potential to hurt businesses and individuals, indicating a need for greater public discussion about such issues.