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

Δελτίο 132
21 Οκτώβρη 2008

Cambridge Lab Sets Quantum Key World Record
Techworld (10/09/08), J. Dunn

Researchers at the Toshiba Cambridge Research Lab (CRL) have demonstrated the ability to shift quantum encryption keys at speeds of 1Mbps. The research makes it possible for secure Quantum Key Distribution to be used on optical networks with multiple nodes. Until this breakthrough, low secure key distribution speeds limited the technology to point-to-point links. The breakthrough was the result of engineers finding a way to make hardware better able to filter the "electron avalanches" that normally limit the technology. Quantum encryption uses principles from quantum physics to guarantee not only the data stream, but the keys used to encrypt the data stream. The bits that make the keys are encrypted into patterns of photons that, if intercepted in any way, corrupt the communication and alert the users that an attack has been made. The principle is sound, but relating the physics to semiconductor engineering is more difficult. The problem is that each photon used to communicate the key triggers an avalanche of electrons, which can become electronic noise that results in key errors. This problem can be prevented by turning off the equipment to dampen the effect, or limiting clock speeds to 10MHz. Both solutions limit throughput. The CRL researchers have developed a way to harness usable signals from much weaker electron fields without creating noise, enabling much higher clock speeds. The number of nodes is still limited to four, but the breakthrough is a major step forward.

Q&A: E-Voting Security Results 'Awful,' Says Ohio Secretary of State
Computerworld (10/08/08), B. Friedman

Ohio voters who do not trust touch-screen systems to properly record their votes will be given the option of a paper ballot thanks to a policy dictated by the results of Ohio Secretary of State J. Brunner's Evaluation & Validation of Election-Related Equipment, Standards and Testing (EVEREST) analysis, which uncovered "critical security failures" in every system evaluated by teams of both corporate and academic computer scientists and security specialists. Brunner says in an interview that the results of the EVEREST tests exceeded her worst expectations. "When I finally saw the results of our [EVEREST] tests, I thought I was going to throw up," she says. "I didn't think it would be that bad. And it was--it was awful." Vote dropping was observed in the tabulators of systems manufactured by Diebold's Premier Elections Solutions subsidiary. At the federal level, voting systems have to be certified as an entire end-to-end unit, and certification by the US Election Assistance Commission (EAC) requires companies to submit every piece of hardware and software to a single unit in order that tests can ascertain whether they all function together without problems. The EAC recently overhauled its certification process, but Brunner calls the process "very cumbersome." She notes that Ohio's boards of elections are instructed to tally the votes by hand if necessary, and sees value in such a practice, at least as a pilot program. "I'm not so sure I'd want to experiment during the presidential elections," Brunner says.

How Much Security Do You Expect From Your Pacemaker?

University of Massachusetts Amherst (10/03/08)

University of Massachusetts Amherst professor K. Fu is developing zero-power technology and low-power cryptographic protocols for implantable medical devices. Fu, who earlier this year showed that an implantable heart defibrillator is vulnerable to hacking, won a three-year, $449,000 National Science Foundation grant to improve the security in implanted cardiac devices without compromising their safety and effectiveness. Fu will research sharing data over the Internet and the use of wirelessly programmable implants. He says the research comes at a critical time because few, if any, implanted devices share patient data outside secure settings such as clinics, and none are re-programmable from remote locations. However, Fu says future devices could allow a patient with an implanted cardiac device to go on vacation while the device continues to deliver information to the patient's physician over the Internet, enabling the doctor to modify the electrical output as needed, similar to adjusting prescriptions. Maintaining privacy and security will be crucial. "With medical devices, we don't have the luxury to fix security after the fact," Fu says. "This is where our research comes in."

Researchers Show How to Crack Popular Smart Cards
InfoWorld (10/07/08), B. de Winter

Researchers at the Dutch Radboud University Nijmegen have published a cryptographic algorithm and source code that could be used to duplicate smart cards used by several major transit systems. The scientists presented their findings at the ESORICS security conference in Malaga, Spain, and also published an article with cryptographic details. The research demonstrated how to circumvent the security mechanism of NXP Semiconductor's Mifare Classic RFID cards, which are widely used to provide access control to buildings and public transportation. The researchers exposed the workings of the chip by analyzing communication between the chip and the reader. A RFID-compatible device, the Ghost, was designed to work independently from a computer, which allowed the researchers to obtain the cryptographic protocol. Part of the vulnerability comes from the fact that the RFID reader has to communicate in a predictable way. Once the mechanism was exposed, the scientists were able to crack keys in less than a second using an industry standard computer with only 8MB of memory. The researchers also examined another chip, the Hitag2, to crack Mifare. Information on a Hitag2 hack is freely available online, which helped the researchers crack Mifare. Another effort by German researcher H. Plotz cracked the Mifare Classic by removing a Mifare chip from a card and removing layers, photographing each layer under a microscope and analyzing all the connections.

Giant Database Plan 'Orwellian'
BBC News (10/15/08)

Britain has proposed creating a central database of all mobile phone and Internet traffic in an effort to fight terrorism and other crimes. Although critics have called the plan "Orwellian," the UK's Secretary of State for the Home Department J. Smith says the data warehouse is necessary to help police and security services deter crime. Smith says the content of conversations would not be stored, just the times and dates of messages and calls. Liberals say the idea is "incompatible with a free country," while the Tories say the government has to justify its plans first. Details on the times, dates, duration, and location of mobile phone calls, numbers called, Web sites visited, and email addresses used are already stored by telecom companies in the UK for 12 months under a voluntary agreement. That data can be accessed by the police and security services on request, but the government is looking to take control of the process in part to comply with a European Union directive. Information would be kept for two

years, and would be held centrally on a searchable database. Smith says without increasing the capacity to store data, police and security services will have to consider a significant expansion of surveillance practices. "Our ability to intercept communications and obtain communications data is vital to fighting terrorism and combating serious crime," Smith says.

E-Voting Report: Several States Still Vulnerable
IDG News Service (10/16/08), G. Gross

Several US states are not doing enough to ensure the accuracy of electronic-voting machines, concludes a report from three voting security advocacy groups, which gave 10 states inadequate grades in three out of four safeguard categories. The report, released by Common Cause, Verified Voting, and the Brennan Center for Justice at the New York University School of Law, predicts that some voting systems will fail on election day. "Unfortunately, we don't know where," the report says. "For this reason, it is imperative that every state prepare for system failures." Verified Voting president P. Smith says that state protections against voting fraud and e-voting machine failure have improved greatly since the last US presidential election in 2004, but several states still refuse to take basic precautions to protect the integrity of voting systems. Colorado, Delaware, Kentucky, Louisiana, New Jersey, South Carolina, Tennessee, Texas, Utah, and Virginia all received failing grades in three of four voting security areas. Of the 24 states using direct-recording electronic machines, only California, Indiana, and Ohio received satisfactory grades in all four categories. Colorado, Delaware, Louisiana, Nevada, Texas, Utah, Virginia, and West Virginia have no state-mandated requirement for emergency paper ballots to be available in precincts that use e-voting machines should those machines fail. Eighteen states, including Florida, New York, Texas, and Virginia, do not have adequate requirements in place for paper-record backups to e-voting or other non-paper methods, and 27 states do not have adequate provisions in place for conducting post-election audits of voting results.

Tools That Will Discreetly Tap a Shoulder to Offer Help
Financial Times Digital Business (10/08/08) P. 4; M. Branscombe

Microsoft Research's Adaptive Systems and Interaction group is developing interruption-alerting technology. "We want to build our applications to be courteous and intelligent about the nature and timing of interruptions," says Microsoft researcher E. Horvitz. "We need a better alerting model that understands how busy you are and when to defer alerts till later." Horvitz uses tools so that when he is in a meeting only the right people can interrupt. These tools prioritize messages and contacts and predict how busy Horvitz is going to be based on his calendar and working habits. One tool learns who to respond to immediately and who to put off, while another uses economic models for the value of information and the cost of being interrupted. The tools combine into a notification platform that acts as a virtual receptionist, postponing email alerts and calendar reminders until Horvitz finishes an important task, and redirecting calls and instant messages that it perceives as interruptions. Horvitz's group is working closely with the team developing Outlook to manage alerts using such methods, and Microsoft's Office Communicator team is using these tools to build a better model of "presence" to determine how to route messages to users in the right way at the right time. Horvitz wants to advance such systems to the point that they can help users work on long-term projects by scheduling time to work on the projects and automatically bringing up resources they are likely to use.

Feds, Industry Announce Centre for Identity Management Research

GovExec.com (10/07/08), J. Aitoro

Security leaders from government, academia, and corporations have formed the Center for Applied Identity Management Research in an effort to improve how government and industry organizations control access to information and data stored in networks. The new center will study ways of improving the practice of identity management, the ability to verify computer users' identities, and how to safely store sensitive information on a network. The Office of Management and Budget recently reported that the number of federal network information security incidents more than doubled in fiscal 2007, while federal networks have experienced a 70 percent increase in unauthorized access. The centre's backers, including IBM, Lockheed Martin, Indiana University and the US Secret Service, revealed several areas of research the centre will focus on. Public safety research will focus on cybercrime, organized criminal groups, and detecting sexual predators. National security efforts will focus on cybersecurity, cyberdefense, human trafficking and illegal immigration, and terrorist tracking and financing. Financial and corporate fraud research will focus on mortgage fraud, data breaches, and insider threats. Finally, individual protection research will focus on identity theft and fraud. The research objective will be to develop strategies and policies for protecting data and personal privacy to ensure individual civil liberties are respected.