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

Δελτίο 91
23 Σεπτέμβρη 2007

UM Software Tools May Key Successful Antiterrorism, Military and Diplomatic Actions, University of Maryland (09/13/07), L. Tune

The University of Maryland Institute for Advanced Computer Studies (UMIACS) has developed computer analysis software to provide rapid information on terrorists and the cultural and political climate on the ground in areas of critical interest. The new computer models and databases could help policymakers and military leaders predict the behavior of political, economic, and social groups. UMIACS director and professor of computer science V. Subrahmanian says US commanders probably knew where Osama bin Laden was, but were unable to capture him because troops on the group did not have enough cultural knowledge to successfully negotiate with the locals. Subrahmanian says such failures can be avoided if decision makers have access to pertinent data and accurate models of behavior. The software tools developed by Subrahmanian and his colleagues track information on foreign groups in a variety of sources, including news sources, blogs, and online video libraries. The software can almost instantly search the entire Internet for information and links on a terrorist suspect or other particular person, group, or other topic of interest. Additionally, with help from social scientists at the University of Maryland, UMIACS computer scientists developed methods to obtain rules governing the behaviors of different groups in foreign areas, including about 14,000 rules on Hezbollah alone.

Scientists Use the "Dark Web" to Snag Extremists and Terrorists Online
National Science Foundation (09/10/07)

University of Arizona Artificial Intelligence Lab researchers have created the Dark Web project with the intention of systematically collecting and analyzing all terrorist-generated content on the Web. Some estimates place the number of Web sites created and maintained by known international terrorist groups at over 5,000, and many of the sites are developed in multiple languages and can be hidden in innocent-looking Web sites. To tackle the massive challenge of finding, cataloging, and analyzing extremist activities online, the Dark Web project will use a variety of techniques including Web spidering, and link, content, authorship, sentiment, and multimedia analysis. One of the tools developed by Dark Web is a technique known as Writeprint, which automatically collects thousands of multilingual, structural, and semantic features to determine who is creating 'anonymous' content online. For example, Writeprint can examine a posting on an online bulletin board and compare it to writings found elsewhere on the Internet, and through analysis, determine if the author has produced other content with 95% accuracy. Dark Web also uses Web spiders to search discussion threads and other content to find terrorist activities, but the terrorist can fight back by infecting the spiders with viruses that infect Dark Web computers. The project recently completed a study of online stories and videos intended to teach terrorists how to build improvised explosive devices.

Google Calls for International Standards on Internet Privacy
Washington Post (09/15/07) P. D1; C. Rampell

Speaking before a UN audience in Strasbourg, France, global privacy counsel for Google P. Fleischer said that fragmentary international privacy laws burden companies and fail to protect consumers, arguing for new international standards on the collection and use of consumer data. Fleischer said the United Nations should create standards countries could adopt and adjust to fit their needs. "The ultimate goal should be to create minimum standards of privacy protection that meet the expectations and demands of consumers, businesses, and governments," Fleischer said. Google has frequently been criticized for its privacy policies and is currently under investigation by the European Union for violating global privacy standards. Critics are also concerned that Google's planned $3.1 billion merger with online advertising broker DoubleClick would place too much consumer data in the hands of one company. Fleischer criticized US privacy law for being too complex and too patched-together because different laws apply to different industries and vary by state. Fleischer also called the European Union model "too bureaucratic and inflexible." Fleischer suggested adopting a model similar to the Asia-Pacific Economic Cooperation guidelines, but critics say the APEC standards are too lenient. "The APEC guidelines are far below what Google would be expected to do in Europe or the United States," said Electronic Privacy Information Center executive director M. Rotenberg. APEC does not limit data collects, for example, which is a significant problem and the key point in the dispute over Google's business practices, Rotenberg said.

NSF Researchers Produce RFID Random Number Generator
Government Computer News (09/12/07), J. Jackson

University of Massachusetts researchers, with funding from the National Science Foundation, have developed an inexpensive way of producing truly random numbers for radio frequency identification tags, as well as a technique that produces a unique fingerprint for each tag. Although encryption programs require a reliable source of random numbers, computers are incapable of producing truly random numbers. Algorithms have been developed that can help machines produce numbers that statistically resemble random numbers, but they contain subtle repeatable patterns that can be used to decipher a message encrypted with those digits. The technique developed by the researchers produces a set of random numbers from an RFID tag by reading the binary states of the tag's memory cells while the tag is being powered up. A typical Electronic Product Code Class 1 RFID tag has between 1,000 to 4,000 gates, which is typically volatile memory that loses all information when power is lost. Each time a tag is powered up, a certain number of gates fluctuate randomly between having a residual charge or not having a charge. These fluctuations can be used to produce a stream of random numbers. The researchers say the numbers produced by this process have passed the National Institute of Standards and Technology's test for statistical randomness. The variations in each tag's gates can also be used to uniquely identify each tag, ensuring information derived from each tag has not been altered by a possibly malicious source.

University Program Targets Online Security
Augusta Chronicle (GA) (09/12/07), J. Few

Armstrong Atlantic State University is researching and developing software that will be able to intercept secret messages transmitted over the Internet and destroy any malicious content. As part of a demonstration of the program, professor R. Hashemi showed how a message can be hidden in a photograph and go unnoticed by the human eye. "A terrorist headquarters can send a hidden message to a sleeper cell in this photograph or music or the text of an email," Hashemi says. "What we did was develop a vaccine that is able to intercept the image; the sleeper cell will get the image with the message destroyed and the original can be held for a

government agency to analyze later." The university's School of Computing is developing the program for companies that provided its new Cyber Security Research Institute with equipment and other resources. The institute also demonstrated other top-secret projects that are unlikely to receive further public attention due to the sensitive nature of the work.

Quantum Threat to Our Secret Data
New Scientist (09/13/07) Vol. 195, No. 2621, P. 30; D. Graham-Rowe

Quantum computing's ability to decrypt the codes that safeguard banking, e-commerce, and business data has taken a step closer to realization with the development of quantum computers that can run Shor's algorithm by two research groups working independently. RSA is an example of a highly common encryption system that can be defeated by Shor's algorithm. RSA involves a widely distributed public key for encrypting messages and a secret private key for decrypting them, and the trick to solving the private key is to work out the large prime numbers that produce the key when they are multiplied together. Shor's algorithm dramatically reduces the time it takes to find the prime factors by searching for telltale patterns in remainders when a key is divided by a prime factor, but quantum computation is essential for performing the massive number of calculations that the algorithm requires to be successful. The first quantum implementation of Shor's algorithm involved the manipulation of nuclear spin, while the more recent experiments--one led by A. White at Australia's University of Queensland and the other by C.-Y. Lu of the University of Science and Technology of China--used quantum photonic computers. Photon pairs were produced with femtosecond lasers and passed through polarizing bismuth borate crystals to generate entangled qubits, which were coaxed by optical devices to run Shor's algorithm to factor the number 15 into its prime components. IT security specialist B. Schneier calls the development of techniques to run the algorithm using standard lab optics a significant achievement that could spell trouble for encryption down the road. White contends that cryptography would need to be fundamentally rethought if quantum calculations for much larger numbers could be carried out. "There are paths to a fully scalable quantum computer," he notes.

Group Says E-Voting Paper Trail Wouldn't Improve Security
IDG News Service (09/18/07), G. Gross

A report from the Information Technology and Innovation Foundation (ITIF) think tank concludes that requiring printouts as a back-up to electronic voting would not improve security and would increase the costs of US voting systems. The ITIF says that voter-verified paper trail ballots used with e-voting machines would prevent the use of more innovative voting technology that providers better security, transparency, and reliability than paper-only voting systems. The ITIF report also notes that people are willing to trust computers with many other important functions such as banking, medicine, and aviation. Supporters of paper-trail ballots dispute the report's findings. "The argument that people trust computers in other places is specious--safety-critical systems have been developed in other contexts using rigorous standards that are not applied to voting machines," says E. Spafford, chairman of ACM's US policy committee. ACM has not called for e-voting machines to be abandoned, but suggests that e-voting machines go through two levels of auditing, paper trails and random machine audits, says Spafford, who notes that beyond the hacking threat, "errors, bugs, and accidents can also result in problems unless there is an independent, durable audit trail." Meanwhile, VerifiedVoting.org President P. Smith disputes the report's suggestion that a growing technophobic movement is driving mistrust for e-voting. "The harshest critics of e-voting--in parti-

cular paperless e-voting--are computer technologists who are the literal opposite of technophobic," Smith says.

CS Profs and the DOD
Computing Research Association (09/18/07), P. Harsha

Recent policy changes at the Defense Advanced Research Projects Agency (DARPA) have reduced university participation rates in DARPA-funded computer science research projects. Between fiscal years 2001 and 2004, the amount of funding from DARPA to US universities for computer science research fell by half, and evidence suggests that funding for universities is currently lower still, writes the Computer Research Association's P. Harsha. Diminished support for university computer science not only creates a gap in federal IT research and development, but also weakens the "DARPA model" of research support. Since the early 1960s, the country has benefited from the two different approaches to research that the NSF and DARPA have taken. While the NSF focused primarily on small grants for individual researchers, DARPA worked to identify key problems of interest and to create and support communities of research to solve the problems. DARPA-supported research in computer science over the past four decades has established the U.S. economy and military as the most dominant forces in the world, Harsha says. Reducing support for academic computer science means some of the brightest computer scientists in the country are no longer working on defense-related problems. Many experienced computer science researchers say there is an entire generation of young researchers who have no experience working on DARPA and Defense Department projects. The Computer Science Study Group, managed by the Institute for Defense Analysis for DARPA, focuses on introducing researchers to the needs and priorities of the Defense Department by running workshops, mentoring, and hosting tours of DOD facilities, but the group does little to bring DARPA interests back into university research.

Clock to Tick Down US Privacy
Washington Times (09/18/07) P. A3; A. Hudson

The American Civil Liberties Union's "Surveillance Society Clock" is counting down until the US government stops spying on private citizens as part of the war on terror, and the clock is quickly approaching midnight. "The extinction of privacy is a real possibility," says B. Steinhardt, director of the ACLU's Technology and Liberty Project. "We believe that privacy is not yet dead--it is a patient on life support." The ACLU clock is modeled after the "Doomsday Clock," created by the Bulletin of the Atomic Scientists in 1974 to warn against the possibility of a nuclear holocaust. Steinhardt says rapid advancements in technology and data mining are leading to the possibility of a "1984-style surveillance society" and creating a false sense of security. "The false security of a surveillance society threatens to turn our country into a place where individuals are constantly susceptible to being trapped by data errors or misinterpretations, illegal use of information by rogue government workers, abuses by political leaders--or perhaps most insidiously, expanded legal uses of information for all kinds of purposes," says a new ACLU report on mass surveillance by the government. The clock is currently set at six minutes before midnight, and will be updated as events warrant moving the time closer to or further away from midnight. "With a flood of new technologies that expand the potential for centralized monitoring, a president who believes he can unilaterally sweep aside the laws that restrain government spying ... we confront the possibility of a dark future where our every move, our every transaction, our every communication is recorded, compiled and stored away, ready for access by the authorities whenever they want," the report says.

New Research Seeks to Enhance Quality and Security of Wireless Telemedicine
Rochester Institute of Technology (09/17/07), W. Dube

Researchers at the Rochester Institute of Technology and the University of Alabama are working to advance the use of radio frequency identification (RFID) technology in cardiac sensor networks, a new wireless technology for telemedicine delivery. The researchers will work on improving the security of the systems, reducing the possibility of identity theft and cyber-terrorism. "Telemedicine technology can greatly increase the quality of medical care while also decreasing health care costs," says Rochester Institute of Technology assistant professor of computer engineering F. Hu. "Through this project we hope to increase the integration of RFID into existing cardiac sensor networks, ensure the overall security of the system and promote the implementation of the technology in nursing homes and adult care facilities across the country." One of the major challenges of the project is concern over the security of wireless networks used in telemedicine delivery. Hu and University of Alabama computer science professor Y. Xiao will research the use of anti-interference technology to reduce radio distortion on the networks, and design and test new RFID security systems that will decrease the chance of information being stolen. "There are well known security challenges associated with cardiac sensor networks and RFID," Hu says. "It is my hope this research will assist in better protecting these systems and allow greater numbers of doctors and patients to take advantage of the benefits of telemedicine."

If RSA Is Cracked, Here's Plan B
New Scientist (09/15/07) Vol. 195, No. 2621, P. 31; D. Graham-Rowe

Two research groups, one from the University of Queensland in Brisbane, Australia, and the other from the University of Science and Technology of China, in Hefei, say they have successfully created quantum computers that can run a routine called Shor's algorithm, a development that could have a profound impact on cryptography and how we protect our banking, business, and e-commerce data. Some say that quantum computing is nowhere near developed enough for real-world code breaking, but others say that cryptography will have to develop beyond current prime-number-based encryption techniques. The ability to run Shor's algorithm indicates the quantum computers are capable of using quantum processes to factorize large prime numbers. Almost every strong encryption system relies on a regular computer's inability to factor such numbers in a reasonable amount of time, exactly what the two groups claim to have done. However, J. Callas, head of technology at cryptographic software developer PGP, says the work done by the two groups is significantly behind current cryptography techniques. Callas says the researchers only used four qubits, whereas current cryptography uses about 4,000 bits, which would require a quantum computer with about 50 trillion qubits. Eventually, the number of qubits in quantum computing is expected to surpass the point where it can outperform traditional computers and the length encryption keys can reach, but that could be 50 years away. When that point is reached, however, there are other cryptographic systems that even quantum computing will have trouble with. Hash chains, for example, use a sequential encoding process, and there is currently no known way to break them using a quantum computer.