

**Call for Participation: 2008 ACM Workshop on Secure Web Services (SWS)
XML Daily Newslink (06/10/08)**

Organizers of the 2008 ACM Workshop on Secure Web Services (SWS) have issued a call for participation in exploring the security challenges of technologies such as XML and Web services security protocols and issues such as advanced metadata, general security policies, trust establishment, risk management, and service assurance. Experts will have an opportunity to present research results, discuss their practical experiences, and share innovative ideas about Web services security. Organizers are interested in topics such as Web services and GRID computing security; authentication and authorization; frameworks for managing, establishing, and assessing inter-organizational trust relationships; Web services exploitation of Trusted Computing; Semantics-aware Web service security, and Semantic Web Secure orchestration of Web services; and privacy and digital identities support. SWS is scheduled for Oct. 31, in Fairfax. The workshop will be held in conjunction with the 15th ACM Conference on Computer and Communications Security (CCS-15).

**'Herds' of Wary Cars Could Keep an Eye Out for Thieves
New Scientist (06/05/08), D. Robson**

Frostburg State University researcher H. Song together with Pennsylvania State University researchers have developed the Sensor-network-based Vehicle Anti-Theft System (SVAS-TS), a vehicle security system that uses networks of cars constantly communicating with each other using concealed wireless transmitters to prevent thieves from stealing one of the cars in the network. Song says multiple sensors hidden throughout a car would make it difficult, if not impossible, for a thief to disable the system in a short period of time. He says the design of the network should also produce fewer false alarms than traditional car alarm systems. To secure a vehicle, the driver uses a remote to switch on the transmitters, which then work to join a network of other nearby cars. The group acts as each others' sentinels, choosing partners that need the lowest signal strength for communication to prevent the system from consuming too much energy. The car continues to send and receive signals until the owner returns, at which point it sends out a "goodbye" signal to tell the other cars it is leaving. If the signal stops without the "goodbye" signal, the other cars report a theft by relaying a message to a central base station. The base station would notify nearby security guards, police officers, and the owner. The system was tested using a small number of cars, with researchers driving off in some cars to test SVATS response. The system detected all such "thefts" within just four to nine seconds.

**Researchers Say Notification Laws Not Lowering ID Theft
IDG News Service (06/05/08), R. McMillan**

The adoption of data breach notification laws by all but seven US states has done little to stem the tide of identity theft, according to a state-by-state analysis by Carnegie Mellon University researchers of data provided by the US Federal Trade Commission. The analysis, which covered ID theft complaints submitted to the FTC between 2002-06, looked for a

change in the rate of reported ID thefts before and after data breach ordinances were enacted. Though Carnegie Mellon Ph.D student S. Romanosky says the laws had no statistically significant effect on ID theft rates, other factors, such as state populations, gross domestic product, and fraud rate, did have a noticeable impact. Breach notification letters are often disregarded by consumers, and Romanosky thinks security firms' data protection efforts are still insufficient. "In so many of these cases, the breaches occur because of ridiculous security practices," he says. Gartner analyst A. Litan says the incompleteness of the reports to the FTC makes drawing definite conclusions from the data difficult, but she notes that many companies have responded to tighter laws and regulations by devoting more attention to compliance than security, which is frequently inadequate for shielding customers from ID theft. In a paper to be presented at Dartmouth College's Information Security Economics conference, the Carnegie Mellon researchers recommend the adoption by the federal government of a unified breach law designed to "reduce conflict between states laws and lower the barrier for compliance."

Space Station Could Beam Secret Quantum Codes by 2014 **Scientific American (06/08), J. Minkel**

Researchers hope to be running an experiment on the International Space Station (ISS) by the middle of the next decade that would allow for transcontinental transmissions of secret messages encoded using the quantum property of entanglement, which is when two particles, such as photons, are created by the same event and can communicate instantaneously no matter how far apart they are. Transmitting entangled pairs of photons reliably is the foundation of quantum key distribution, a procedure that converts those pairs of photons into potentially unbreakable codes. Photons can travel maybe 100 miles on modern fiber-optic cables before their quantum character breaks down, but that limit disappears above ground. Last year, a team of researchers led by physicist A. Zeilinger from the University of Vienna successfully transmitted quantum keys up to 89.5 miles between a pair of telescopes in Spain's Canary Islands. Now they want to send quantum keys hundreds of miles or even more. The group is leading an international project called Space-QUEST, or Quantum Entanglement for Space Experiments, with the intention to prove that a system for generating pairs of entangled photons can fit the constraints imposed by the ISS. Quantum keys distributed from the ISS could be transmitted to any two points within the station's line of sight, limited only by the ability of transmitters and receivers to maintain a tight lock on one another and isolate entangled photons from background light. Zeilinger and his colleagues demonstrated they could detect single photons reflects off a satellite 3,700 miles above Earth earlier this year. Space-QUEST hopes to build a prototype device and gather preliminary data in time for a meeting of the European Space Agency in November, where officials will decide what projects will receive funding and earn the chance to be run in space.

Can Computer Scientist Dream Team Clean Up E-Voting? **Network World (06/10/08)**

Electronic voting has become a source of concern and controversy, with many e-voting systems proving to be security black holes. A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections (ACCURATE) has received a \$7.5 million National Science Foundation award to bring the latest research, insights, and innovations from the lab to the voting booth and make e-voting systems more secure and accurate. ACCURATE unites computer experts from across the country and academic disciplines to find areas that need additional research and to determine how to apply existing technology and research findings to voting

systems. ACCURATE members from Rice University have designed and implemented a system called "Auditorium," which forms the base of a voting system prototype called "Vote-Box." Auditorium is a networked logging and auditing system built using timeline entanglement and broadcast messages. Auditorium allows anyone to audit the events, in the order that they occurred, with strong cryptographic guarantees to protect against tampering with the timeline. Additional research on secure logging is examining how log verification could be scaled for an entire election in real time. ACCURATE members at the University of California, Berkeley, are examining methods for building trustworthy audit logs in electronic voting systems. Their goal is to design a mechanism that records the entire user interaction between the voter and the voting machine to allow auditors to replay a "movie" of the interactions after the election. Challenges include ensuring that the audit log does not compromise ballot secrecy and that it is a trustworthy system.

Information Accountability

Com. of the ACM (06/08) Vol. 51, No. 6, P. 82; D. Weitzner, H. Abelson, T. Berners-Lee

Accountability for the misuse of personal information must be enforced by systems and statutes, as the openness of the information environment makes protection via encryption and access control impossible. "Information accountability means the use of information should be transparent so it is possible to determine whether a particular use is appropriate under a given set of rules and that the system enables individuals and institutions to be held accountable for misuse," write the authors. Rules are needed, both in the US and internationally, to address the permissible use of certain types of information, in addition to simple access and collection restrictions. The authors say that the information-accountability framework is more reflective of the relationship between the law and human behavior than the various initiatives to enforce policy compliance via access control over information. Supporting information accountability requires a technical architecture that features policy-aware transaction logs, a common framework for representing policy rules, and policy-reasoning tools. "One possible approach to designing accountable systems is to place a series of accountable appliances throughout the system that communicate through Web-based protocols," the authors suggest. The authors conclude that perfect compliance should not be the standard for evaluating laws and systems that aid the enforcement of information accountability. "Rather we should ask how to build systems that encourage compliance and maximize the possibility of accountability for violations," they write.

New Intrusion Tolerance Software Fortifies Server Security

George Mason University (06/16/08)

Researchers at George Mason University are taking a different approach to intrusion detection and prevention. A. Sood, professor of computer science and director of the Laboratory of Interdisciplinary Computer Science, and Y. Huang, senior research scientist in the Center for Secure Information Systems, accept the likelihood of someone trespassing on computer servers, but believe limiting the time of continuous connection to the Internet can serve as an additional layer of defense. Sood and Huang have developed Self Cleansing Intrusion Tolerance (SCIT), and they use virtualization technology to create duplicate servers. The idea is to periodically cleanse an online server and restore it to a known clean state, regardless of whether an intrusion has been detected. Regular cleansings occur in sub-minute intervals. "SCIT interrupts the flow of data regularly and automatically, and the data ex-filtration process is interrupted every cleansing cycle," says Sood. "Thus, SCIT, in partnership with intrusion detection systems, limits the volume of data that can be stolen."