

**Why VOIP Needs Crypto
Wired News (04/06/06), B. Schneier**

Voice over Internet Protocol (VoIP) phone calls must be encrypted because the scope of the dangers VoIP is vulnerable too far exceeds that of threats to traditional phone calls, writes Counterpane Internet Security CTO Bruce Schneier. He notes that data packets can be intercepted at any point along the route of transmission, and eavesdropped on by governments, corporate competitors, hackers, and criminals. Schneier envisions a multitude of crimes that can be committed through VoIP call eavesdropping, including the hijacking of phone calls, the theft of account information, the accumulation of sensitive material for blackmail or industrial espionage, and insider stock trading. The author criticizes the US government's suggestion of permitting encryption by everyone, provided it owns a copy of the key; he calls this "an amazingly insecure idea for a number of reasons, mostly boiling down to the fact that when you provide a means of access into a security system, you greatly weaken its security." Schneier reports that there are many products that provide VoIP encryption, including built-in encryption from Skype, and P. Zimmermann's open-source ZFone. However, he cautions that encryption is not a cure-all, in that it cannot address the leading threat of endpoint surveillance. "No amount of IP telephony encryption can prevent a Trojan or worm on your computer--or just a hacker who managed to get access to your machine--from eavesdropping on your phone calls, just as no amount of SSL or email encryption can prevent a Trojan on your computer from eavesdropping--or even modifying--your data," Schneier says.

Wireless Sensor Networks Offer High-Tech Assurance for a World Wary of Earthquakes, EurekAlert (04/06/06)

City officials must make snap decisions about whether bridges can support the load of emergency-rescue traffic when they have been damaged in an earthquake or other disaster. To provide them with better information, Lehigh University assistant professor of civil and environmental engineering Y. Zhang is developing wireless sensor networks that could relay data about a bridge's performance and ability to support traffic. Wired networks could relay information in real time, but the wires are susceptible to electromagnetic signal interference and could themselves be damaged in an earthquake. Zhang, working under a five-year, \$400,000 NSF grant, is developing sophisticated data-compression algorithms to overcome the limited bandwidth available for wireless sensor networks, which can dramatically slow data transmission rates. The algorithms include the capability to filter out redundancies in the sensor data to maximize compression rates. "Using the sensor-data-compression algorithm I'm developing," Zhang said, "we can minimize data-downloading time and ultimately download data in real time and evaluate it in near real-time basis." As part of the grant, Zhang will build a test network to monitor a bridge in China that was damaged during construction in 2000, and conduct extensive validation testing in 2009 to assess its ability to carry traffic. Zhang says the data collected in the test could also benefit American engineers, and he will also incorporate his research into the classes he is teaching at Lehigh.

Cradle of Liberty Lags on E-Voting
IEEE Distributed Systems Online (04/06) Vol. 7, No. 4, G. Goth

The advancement of e-voting technology in England, continental Europe, and Australia is overtaking the US effort because of the first three regions' wholehearted movement to endorse standards such as Election Markup Language (EML) and make the e-voting process transparent, in contrast to America's laissez-faire attitude and policies. The latest version of EML, which was ratified by the Organization for the Advancement of Structured Information Standards (OASIS) Election and Voter Services technical committee in February, offers "a very generic set of XML schemas that handle data exchanges that will support--as far as we know--all the known voting regimes around the globe," according to UK Local e-Government Standards Body Chairman J. Borrás. Numerous British e-voting technology pilots have received generally good marks from the UK Electoral Commission, while the Australian Capital Territory (ACT) used e-voting in its 2001 and 2004 general assembly elections to satisfactory reviews from its own commission. ACT's e-voting system was designed to include open-source software, built-in security, the independent audit of software code, and a paper audit trail of electronic votes, and to fulfill such commission requirements as the casting of all votes in a public polling place over an isolated local network; the locking away and constant monitoring of polling place servers; the storage of votes on a pair of identical hard disks as a protection from hardware failure; and the encryption of vote data. U.S. elections officials, on the other hand, have drawn fire from voters' rights activists for sowing uncertainty among both vendors and government officials over what voting equipment is reliable through iffy, ill-defined guidelines and contradictory opinions. U.S. e-voting experts endorse paper ballot backups as a short-term solution to the reliability problem, while Borrás maintains that "What we've tried to build into EML is sufficient checks and balances so that your security regime, whatever that might be...can operate and see what's going on."

New Database Rejects Eligible Calif. Voters
Computerworld (04/07/06), M. Songini

California's new database of registered voters, once hailed as a model for other states by the federal government, could block thousands of registered voters from casting ballots in this June's statewide election, officials warn. Since the December implementation of the database, California's registration process has invalidated numerous attempts to register, typically due to minor data-entry issues. Between Jan. 1 and Mar. 15, 43% of the voter registration forms in Los Angeles County were rejected, causing election officials to wonder if eligible voters will be dropped from the voter rolls. The voter registration database, created to comply with the Help America Vote Act, accepts 74% of registrations on the first try, leaving the rest to be manually validated by election workers, according to a spokeswoman for Secretary of State B. McPherson, who runs the database. Voters must provide their county registrar with a driver's license number or other identifying information, which is then keyed into a database and uploaded to the new system, which cross-references the information with records from the Department of Motor Vehicles or other appropriate agency. If so much as a middle initial is missing, the new centralized system could reject the application. Given the lag time sometimes required to validate registrations in the new system, election officials fear that they may not be able to manually validate all the rejected registrations in time for the May 22 deadline to vote in the June 6 election. California State Sen. D. Brown, an outspoken critic of McPherson, believes the rejection rate should be no higher than 2%, and that the voter database has been fraught with problems from the outset. Meanwhile, McPherson has proposed legislation to "provide common-sense flexibility so that no eligible voter should be denied

the opportunity to vote because of a technicality," his spokeswoman said. ACM's US Public Policy Committee released an in-depth report regarding "Statewide Databases of Registered Voters."

**Researcher: Security Risks in Web Services Largely Ignored
IDG News Service (04/07/06), R. McMillan**

Security professionals should look more closely at Web services, which are being increasingly targeted by attackers, warned A. Stamos, a founding partner of Information Security Partners in San Francisco, during a presentation at the CanSecWest/core06 conference. "Web application security is the red-headed stepchild of the security industry," he said, adding that hackers could use Web services such as AJAX and the XQuery query language to uncover secret information and attack systems. He explained how a hacker could enter malicious code into a Web form, then have the code dial a customer service number of a company and trick the customer service representative into executing it unintentionally. Stamos also said an attacker could create malicious XML queries that use an enormous amount of memory or overwhelm database applications with requests, in order to carry out denial-of-service attacks. Including filtering capabilities in products, which would help them to detect requests that should not be performed, would be a way for Web applications vendors to help improve security, said Stamos. Web applications were linked to nearly 70 percent of vulnerabilities disclosed during the second half of 2005, according to security vendor Symantec.

**Research Reveals Phishing Hooks
BBC News (04/05/06)**

A recent study found that while most people could identify a phishing site as bogus, sophisticated scams could fool around 90% of users, most of whom tend to ignore the visual clues provided by their browsers. The study, which looked specifically at banking Web sites, was conducted by R. Dhamija of the Harvard Center for Research on Computation and Society and University of California, Berkeley, computer science professors D. Tygar and M. Hearst. The researchers concluded that Web designers must develop new ways of signaling to users that a site is unsecured. Approximately 5% of phishing recipients open the email, visit the bogus site, and furnish sensitive information, which provides ample incentive for phishers to keep up their efforts. The researchers recommend that users look at the address bar to check for fake sites that incorporate a well-known name into the URL to lend it an air of legitimacy. They also caution users to retype links instead of clicking on them, check the sites for spelling and grammatical errors, look for "https" on bank sites rather than "http," and to use an anti-phishing toolbar. On average, 40% of the 22 test subjects failed to recognize a fake Web site, and the most authentic-looking spoofed site fooled 90%. Most participants simply did not know what features typically distinguish fake sites from real ones. Most did not look at the address bar, status bar, or other identifying features, and many ignored explicit security warnings in pop-up windows. "The indicators of trust presented by the browser are trivial to spoof," the researchers concluded. "These results illustrate that standard security indicators are not effective for a substantial fraction of users, and suggest that alternative approaches are needed."

Collaboration Will Investigate Vulnerabilities of Rapidly Growing Internet Phone and Multimedia Systems, EurekAlert (04/04/06)

The NSF has awarded four grants totaling \$600,000 to the University of North Texas to lead a consortium of universities in the development of a secure, geographically diffuse test bed for VoIP over three years. The project will focus on preventing voice spam and DoS attacks, improving the quality of service and 911 reliability, and exploring vulnerabilities that arise when using VoIP with traditional phone networks. "Proactively securing the next-generation infrastructure for voice communications is critical for us all," said Ram Dantu, the project's leader. "Our research will identify vulnerabilities in the technology and establish solutions--before damage is done." With Vonage, AT&T, and other companies aggressively rolling out VoIP services, one study has projected that about 24 million US households will use VoIP by 2008, while government agencies have already begun implementing VoIP strategies. In 1880, four years after inventing the telephone, A.G. Bell and C.S. Tainter patented the photophone, which transmitted sound via a beam of light in a similar fashion as today's optical-signal networks. Today, security is a much greater concern, and NSF program director R.V. Rodriguez hopes that the project will make significant strides toward providing both immediate and long-term solutions for securing VoIP calls.

Forging a National Cyber Security Strategy SC Magazine (03/01/06) P. 48; A. Purdy

Deputy director of the Department of Homeland Security's (DHS) National Cyber Security Division (NCSA) A. Purdy details his agency's mission of developing a comprehensive and cohesive plan to ensure the security of America's critical data through intense public-private collaboration and the various tools, resources, and insights this effort involves. He describes the first priority of the National Strategy to Secure Cyberspace as the development of a national cyberspace security response system, a core element of which is strong situational awareness in conjunction with information sharing among federal departments as well as between the government and the private sector. The NCSA, in partnership with the Office of Management and Budget (OMB), has released the US Emergency Readiness Team (US-CERT) Federal Concept of Operations (CONOPS) mandating agencies' reportage of cyberincidents, along with data on their initiatives to lower cyber risk in accordance with the Federal Information Security Management Act (FISMA), to the team. DHS also supports the multi-state ISAC to effect information sharing and collaborate on awareness-raising efforts among state and local governments. Pursuant to a national cybersecurity response system's situation awareness component is the construction of an international watch and warning network. Purdy writes that increasing reliance on cyber resources calls for effective disruption recovery planning by federal agencies, enterprises, and private networks. The National Recovery Plan (NRP) offers guidance on such areas as emergency support functions for communications. The DHS' Preparedness Directorate, of which the NCSA is a component, is concentrating on readiness and is working to guarantee proper coordination between the mission areas to expedite general preparedness.

Systems Let Families Monitor Loved Ones Myrtle Beach Sun News (SC) (04/10/06), K. Scharnber

Academic and commercial groups continue to research technology and innovate on ideas that would allow the parents of the baby boom generation to live at home as they grow older. Memory-aid systems, which would help seniors remember things they did during the day by producing instant digital photos of themselves, have been the focus of computer engineers at the Georgia Institute of Technology. Researchers at Washington University are incorporating artificial intelligence in a handheld GPS device that would be able to predict where an elderly

person is trying to go, and use oral prompts and directional instructions to help guide the individual to their destination. Smart floors that can sense a senior citizen has fallen and summon emergency help are available through home-builders in Florida. And the assisted living facility Oatfield Estates in the Portland area has deployed sensors throughout the buildings and grounds of its community, and has outfitted residents with intelligent badges. Its beds take weight readings throughout the day, analyse sleeping patterns, and can instantly alert a staffer to assist a "fall risk" resident who is trying to get out of bed. Family members in other parts of the country can monitor their elderly parents and gain their vital signs in real time throughout the day from a secure Web site.

Beware the Smart Virus Byte and Switch (04/07/06), J. Rogers

Attendees at this week's Storage Networking World conference warned of a new kind of smart virus based on advanced mathematical theory that could disrupt storage networks and servers. "It's not far-fetched," said Interval International CIO S. Hamidi, who noted that researchers are already able "to create a living computer program and let it have intelligence". With that capability, a smart virus could mutate itself to get around patches and other security measures. Hamidi claimed that hackers could author the viruses based on cellular automation or game theory, among other scientific foundations. Evolutionary computing could lead to a threat that differs from traditional worms and viruses in its ability to alter its own code once detected and redirect the attack to another part of the network. "The code adapts itself to the environment," said Hamidi. This could be a worm that learns from the environment and becomes more intelligent." Since storage and many other computer resources are now IP-based, an evolutionary computing virus could wreak havoc on an organization after entering through a system's TCP packets. IT managers at the convention agreed that few people have the expertise in genetic algorithms to pull off an evolutionary computing attack, though they identified the 1988 Great Worm attack that brought down much of the Internet as an example. However, Hamidi argued that the industry's current lack of preparedness against such an attack is troubling. Even though most hackers currently lack the knowledge of advanced scientific theory to execute such an attack, the attendees grudgingly admitted that it is only a matter of time before the theoretical possibility of an evolutionary computing attack becomes a reality.

The Worried Executive's Guide: Disaster Recovery Planning for Mixed-Hardware Environments, InformIT (04/07/06), L. Wrobel

Protecting a company's computer and data assets is no longer simply about protecting corporate networks at the office because data these days extends onto mobile devices, such as laptops and PDA. This evolving computer web likely will extend into cell phones soon, opines L. Wrobel, and one important aspect of mobile technology is how much more vulnerable mobile technology is to physical theft compared to ensconced corporate data centres and server rooms. Companies can use security-minded operating systems to protect mobile data, and thwart data theft from a laptop that may have been taken for its market resale value. This is especially crucial for financial companies and others dealing with sensitive client information, because data theft can lead to bad publicity, and much worse. When a company is configuring how to protect itself, it should consider standardizing the type of programs used. This is easier to control and secure, and a company could standardize employee options into as little as three basic packages. Knowledge workers such as writers, lawyers, Web designers, and managers will need a flexible and diverse set of tools to accomplish their jobs,

and they likely will use these tools often. In contrast, production workers such as call centre operators, help desk employees, and telemarketers all can use standardized computing tools in a more limited array to accomplish their crucial revenue-generating tasks.

Pirates See Days of Yore

Washington Times (04/07/06) P. C10; J. Bacchus

Researchers at the University of Maryland at College Park believe they have developed new technology that will discourage people from using collusion attacks to steal copies of CD, DVD, or software. A collusion attack involves a number of people copying multiple versions of the same piece of digital media to weaken electronic watermarks embedded in the file and wash away the trace from the original file. The digital fingerprinting technology, developed by K.J. Ray Liu, a professor of electrical and computer engineering, and colleagues at the Institute for Systems Research, makes use of codes that will leave a unique impression on every illegal copy. The strategy would deter people from taking the collusion approach to making illegal copies of digital media because more than 100 pirates would have to work together to make a collusion-resistant fingerprint on a file untraceable. Moreover, the unique fingerprint would enable investigators to trace the crime. According to the researchers, the digital fingerprinting technology would not negatively impact the quality of audio or video, the speed of a computer or download unwanted programs.