Editor: Scott L. Andresen, sandresen@computer.org
Briefs editor: David Ladd, daveladd@microsoft.com

News

Santa Barbara Health Exchange: User-Driven Security Prevails

Greg Goth

A pioneering healthcare data exchange project in Santa Barbara County, California, could be an early example of how secure community-wide clinical data sharing can improve both personal healthcare and community-wide public health initiatives.

The Santa Barbara County Clinical Care Data Exchange (SBCCDE) is a countywide project funded by a grant from the California HealthCare Foundation, and gives the county's three hospitals—plus participating physician groups, laboratories, and the public health authority responsible for running the county's Medicaid program—instant access to patient records via a brokered peer-to-peer architecture.

Technology that gives physicians instant access to a patient's records might be critical in improving the quality of care. A 1999 Institute of Medicine report estimated anywhere between 44,000 and 98,000 people in the US die each year from medical errors, many of which could be prevented if better patient information were available to physicians at the point of care.

The technology also meets all requirements of the federal government's Health Insurance Portability and Accountability Act (HIPAA), which mandates security requirements for the electronic transmission of healthcare records. All except the smallest offices will need to be HIPAA-compliant by 20 April 2005. Some of the technical standards under HIPAA are required, and some are "addressable," meaning a system can opt for an alternative method that meets the regulation's desired goal.

In building the system, CareScience engineers worked closely with the county's physicians to craft a security architecture that met and sometimes exceeded HIPAA regulations without requiring physicians or their staff members to spend undue amounts of time logging in.

The Care Data Exchange is the broker between providers such as hospitals, payors such as insurance companies and government health and welfare divisions, and end users including physicians and patients. As a broker, the exchange contains no patient data itself. Its information-location service links to addresses for patient data behind providers' discrete firewalls, which "provides an additional level of security," says Nick Augustinos, vice president of the Care Data Exchange Group for CareScience.

The original design for the exchange included communications protected by secure HTTPS, secure FTP, the Secure Sockets Layer, and 168-bit DES encryption, as well as digital certificates for logon rights. However, physicians balked at the certificate requirement.

"Digital certificates can be fairly onerous from the management standpoint as well as the usability standpoint," Augustinos says, "and physicians did not want to jump through a lot of hoops as they tried to access this data. Digital certificates tie you in a lot of ways as an end user to a specific machine, and we have a very mobile environment."

As a result of physicians' complaints, certificates were eliminated in favor of password logons with each password subject to time limitations decided by the SBCCDE.

Other hallmarks of the exchange's security architecture include several provisions: only authorized users can access data according to rules established by the data provider; patient consent is required and logged by the data requester to view data; the data holder provider can override an authorized request and withhold data if requested by the patient; and access and consent are logged for patient review and routine auditing.

The system, which is expected to go live countywide in late 2004, also passed a "hack" test conducted by an independent security firm.

Augustinos says the project, in which 70 percent of the county's providers might participate, will en-

able instantaneous delivery of critical records.

"A large proportion of the county's inhabitants are migrant workers or otherwise move around in their jobs in the agricultural community," he says. "As they moved around, there was no way to move their records around other than phone, fax, or paper, which were often unavailable to the physician at the point of care."

DES Is Dead: NIST Declares Standard Officially Obsolete

Greg Goth

The venerable Data Encryption Standard (DES), called the "most important algorithm ever made" by one of the world's foremost experts in electronic security, has been declared officially obsolete by the US government.

"It invented cryptography," says Bruce Schneier, chief technology officer of Counterpane Internet Security, and author of *Applied Cryptography,* a standard reference work for the industry. "It was the catalyst for modern nonmilitary cryptography."

Adopted in 1977, the 56-bit encryption standard formed the foundation of encryption for a wide array of applications ranging from financial services to data-over-cable modem (DOCSIS), but it fell victim to Moore's law, according to William Burr, manager of the security technology group at the National Institute of Standards and Technology. A NIST special publication issued in May 2004 first declared DES no longer sufficient for encrypting data transmitted by government agencies and contractors. The obsolescence, stated in the withdrawal of the Federal Information Processing Standard (FIPS) that approved DES, was disseminated in the 26 July 2004 *Federal Register* (http://csrc.nist.gov/Federal-register/July26-2004-FR-DES-Notice.pdf).

"DES was first publicly cracked in 1997, in about five months—we can imagine that governments' intelligence agencies may have done it earlier—using a large network of computers," Burr says. "In 1998, the Electronic Freedom Foundation constructed a hardware 'DES cracker' at a cost of about [US]$130,000, including all the design costs. It took this machine about four and a half days to find a DES key typically. Following Moore's law, that machine, if it were designed and built today, ought to take about 12 hours to find a DES key, and would cost a few thousand dollars to build, if you built them in quantity. If you had a few million dollars to spend, you could reduce the time to a few minutes.

"Obviously, DES still provides some protection, because most attackers don't have a specialized DES cracker or a large network of computers at their disposal. But we're rapidly approaching the point, if we're not already there, where you could buy a computer off the shelf for a couple of thousand dollars that would be able to crack a DES key in a few months. An algorithm that a few thousand dollars of off-the-shelf hardware can break in a few months is not good enough for a federal encryption standard."

The May 2004 NIST specification (http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf) declares DES might be used only as a component of the Triple Data Encryption Algorithm (TDEA), which provides 112 bits of key strength. TDEA and the new Advanced Encryption Standard (AES) will coexist as federally recognized standards through 2030, although NIST recommends the earliest possible adoption of AES. NIST accepted comments on the new specification through 9 September 2004.

"Basically, the comments seem to fall into two camps," Burr says. "Those who have a lot of equipment that uses DES say, 'Please consider how much it's going to cost us to upgrade to AES or TDEA,' while the cryptographers say, 'This is past due, you should have done it long ago.'"

Even entities not involved in transmitting federal data, such as those responsible for DOCSIS, have advised their members that DES will need to be replaced sooner rather than later. In its latest specification for the Baseline Privacy+ Interface (BPI+) published in April 2004, Cable Television Labs surmised DES would be suitable for cable modem use for five years or more, but, they noted, "at some future date, DOCSIS cable modems will need to adopt a stronger traffic encryption algorithm, possibly AES."

Schneier says the obsolescence of DES should come as no surprise, and Burr says those who submitted comments against the decision are likely to be facing either great expense in replacing hardware such as DES-enabled radios, or else adverse publicity in adhering to the fading standard.

NIST will look closely at all the comments gathered, and "if we were to find a persuasive argument that we should continue with single DES, we might issue a revision, but I don't think that's very likely," Burr says. "We have to go with the world's collective cryptographic experience." □

***Greg Goth** is a freelance writer based in Connecticut.*

NewsBriefs

Security

South Korea, Japan, and China will work together (with other Northeast Asian countries) to create a **joint regional monitoring system against hackers** and strengthen cooperation with Australia's Computer Emergency Response Team (CERT). These countries will also form an antihacking task force consisting of 226 private computer-security companies to promote combined efforts against hacking, and coordinate between government agencies and private companies.

In a report issued by antivirus firm Sophos in August, **the US originates almost 43 percent of all unwanted emails**. The report also suggests that recent US antispam laws have had little impact on curbing spam. South Korea was second on the list, originating 15 percent, followed by China at 11 percent, Brazil at 6 percent, and Canada at 2.9 percent.

The Computer Security Institute and the US Federal Bureau of Investigations have released their annual computer crime and security survey. Overall, the 2004 survey indicates that **the frequency of successful attacks against corporate information systems is decreasing** and has been in steady decline since 2001. Fifty-three percent of respondents indicated that they had experienced unauthorized use of their systems in the past year—the lowest level since 1999. During the past year, there has been a dramatic drop in reports of system penetration, insider abuse, and theft of intellectual property. Last year, 80 percent of respondents noted that insider abuse of networks was the most common form of attack.

According to the Yankee Group, a communications and networking research and consulting firm, **nearly 90 percent of US companies will outsource their security to managed service providers** by the end of the decade. Companies will make this move to save money but also list legislative requirements (such as HIPAA and Sarbanes-Oxley), the accelerated attacks of today's threats, and the trend toward pushing out the network perimeter to include partners and remote workers as reasons for outsourcing. These and other factors are outpacing the average company's ability to keep up with the latest countermeasures and techniques to thwart attacks, the report says.

The US Federal Communications Commission (FCC) **plans to review the US Emergency Alert System (EAS)**, which lets officials instantly interrupt radio and television broadcasts to provide emergency information during a crisis. According the FCC, the EAS suffers from security holes that leave it vulnerable to denial-of-service attacks, and could even permit hackers to issue their own false alerts. The EAS was originally launched in 1997 without basic authentication mechanisms; as a result, it is activated locally by unencrypted low-speed modem transmissions over public airwaves, which places radio and television broadcasters and cable companies at risk of being spoofed. FCC regulations state that unattended stations must automatically interrupt their broadcasts to forward alerts, making it possible for false information to be forwarded without first passing human inspection.

Microsoft Research has set aside US$1M over a two-year period for colleges and universities **to add secure computing topics to their curricula**. Microsoft plans to conduct a competitive Request for Proposal program with eligibility limited to three- and four-year universities that have nonprofit status. According to the announcement on Microsoft Research's Web site, the funds are designed to stimulate the creation, testing, and dissemination of new security-focused content into technical, business, and legal curricula on the condition that successful applicants place the content in the public domain for nonprofit use by other educators.

Privacy

At a US House of Representatives subcommittee on Commerce, Trade, and Consumer Protection hearing, a representative from Wal-Mart stores said a **US law enforcing privacy rules for radio-frequency identification (RFID) isn't necessary** because companies using the technology are committed to protecting privacy. Wal-Mart continues to move forward with plans for case- and pallet-level tagging of products with RFID chips, but most item-level tagging, in which individual products are identified with RFID chips, is roughly 10 years away.

The **Induce Bill**, a copyright bill recently introduced in the US Senate that would make anyone who intentionally violates copyright law legally liable for those violations—effectively banning file-swapping networks—**has competition**. SBC Communications, Verizon Communications, and the Consumer Electronics Association have introduced their own proposal: **the Don't Induce Act**. Its scope is narrower,

saying that only someone who distributes a commercial computer program specifically designed for widespread piracy on digital networks could be held liable for copyright violations. The American Library Association, the Computer and Communications Industry Association, DigitalConsumer.org, the Home Recording Rights Coalition, and Public Knowledge also back the new proposal.

The Dedicated Cheque and Plastic Crime Unit (DCPCU), a United Kingdom police squad dedicated to fighting credit-card fraud, **has recovered 36,000 cards in its first two years of operation**. Set up in April 2002, the DCPCU targets organized gangs responsible for the majority of UK credit-card fraud, which amounted to recovering £402 million (approximately US$720 million) in 2003. In the two years leading up to April 2004, the unit made 171 arrests, resulting in 52 convictions over the period.

Several countries are preparing to launch trials of passports and visas that contain biometric information about the holder—such as a digital image of the citizen's face that can be compared to a facial scan conducted at the airport—alongside the traditional photo and passport number. The first country to take the plunge will likely be Belgium, which plans to conduct an e-passport trial later this year, with possible real-world implementation by next year. The UK, New Zealand, and Canada are also looking into conducting trials.

Policy

The FCC wants to make progress on regulating voice over Internet protocol, although bills that clarify VoIP's role won't go up for consideration in the US Senate and House of Representatives. The issue is **whether VoIP should be treated as a telephone service or an information service**. Sen. John Sununu (R-N.H.) introduced a bill that would exempt VoIP from most regulation, and a similar bill has been introduced in the House of Representatives by Charles "Chip" Pickering, Jr, (R-Miss.).

Microsoft won a second victory in its dispute with Eolas, a spinoff research company of the University of California. The US Patent and Trademark Office rejected Eolas's browser patent request, which claims ownership of the way Web browsers open third-party applications or plug-ins.

The North American Electric Reliability Council, a not-for-profit industry group responsible for keeping electricity flowing throughout the US and Canada, released a list of **measures that must be taken to shore up electric grid reliability**. NEARC also voted to renew the Urgent Action Cyber Security Standard 1200, which sets minimum cybersecurity requirements for US and Canadian utility companies.

The US Government Accountability Office (GAO) submitted a report to Congress in early August, stating its belief that **the US Department of Homeland Defense "does not yet have the necessary architectural blueprint** to effectively guide and constrain its ongoing business transformation efforts and the hundreds of millions of dollars that it is investing in supporting information technology assets." The GAO says that the DHS's IT blueprint doesn't have the content necessary to be considered a well-defined architecture, which the DHS acknowledged, adding that the GAO measured its progress against unrealistic expectations.