IEEE distributed systems ONLINE
Expert-authored articles and resources

IEEE DISTRIBUTED SYSTEMS ONLINE 1541-4922 © 2005 Published by the IEEE Computer Society
Vol. 6, No. 8; August 2005

Identity Theft Solutions Disagree on Problem

Greg Goth

Large-scale hacks into databases containing sensitive personal identification data are continuing to compromise personal data for thousands—and in some cases, millions—of individuals. Have these hacks become the flash point for converging legal and technological attempts to stem the data leaks?

At both the state and federal levels, lawmakers in the US as well as Japan are introducing tough new legislation intended to punish database proprietors whose security is substandard. On 30 June 2005, the credit card industry put strict new security guidelines into effect. Meanwhile, security vendors are finding new markets in ensuring that merchants, payment processors, and storage facilities are free from cybertampering.

Yet, some leading technologists, who might be considered visionaries, contrarians, or perhaps both, are calling these efforts short-term patches at best to networks that were never intended as secure transaction vehicles.

Outdated metaphors

"Everybody says we need encryption and decryption and data protection and firewalls and so on, and what we actually end up with is a fairly siegelike mentality," says Eric Norlin, vice president of marketing for Ping Identity (http://www.pingidentity.com), a vendor in the federated identity market. "We have this metaphorical moat and castle wall with the data inside, and try to make sure nobody breaches the castle wall. But really, in the modern enterprise, we're moving that information all the time. In fact, the business drivers of the modern world demand the castle wall has a whole bunch of holes in it."

Norlin acknowledges the purposes this kind of security serves but sees it operating under a way of thinking and methodology that are not aligned with the current business environment. In fact, in a recent Weblog posting (http://blogs.zdnet.com/BTL/index.php?p=1529), Norlin outlines his contention that the orthodox way of thinking about data security is a dead end.

"The real question to be asked," Norlin writes, "is: Why do all of these corporations need to store all of this personal data in the first place? Why does my credit card company need to store my social security number? Why does Amazon need to store my credit card number? Why shouldn't every company store only what I tell them they can store? And why shouldn't the data that they store be as little as they possibly need to conduct business?"

Federated identity

Norlin has some influential company. Kim Cameron, Microsoft's architect for identity and access, has written "The Laws of Identity" (http://msdn.microsoft.com/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-

us/dnwebsrv/html/lawsofidentity.asp) and, with colleagues at Microsoft, codified an *identity metasystem* (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebsrv/html/identitymetasystem.asp)—an open architecture in which end users retain control of their data according to the context of different relationships. Both of these visions extend the view of *federated identity*. This concept, which has heretofore resided mainly in the business-to-business realm, shifts the balance of control to the user.

"To me, it was a question of bringing things down to putting the user in control, which I think had largely been left out of the conversation," Cameron says. "The conversation had been taking place from the point of view of the commercial parties—and that's important, I'm not denigrating that. But you have to balance that out with the role of the individual user."

Global philosophical differences

Shifting to a user-centered approach is expected to take quite a while, no matter how promising its appeal. In the US, identity data doesn't belong to the consumer. Even after a spate of well-publicized hacks into databases, legal experts and technologists believe that the commercial and social entities will retain legal control over that data for quite some time.

"A lot of people ask if the US is moving toward the European Union model (http://www.edps.eu.int/01_en_presentation.htm), and I think answer is no," says Miriam Wugmeister, a partner specializing in data-protection law in the firm of Morrison Foerster. The US approach to privacy must emerge from a fundamental marketplace bias, where more information is better, Wugmeister says. "That's wholesale different than the European tradition because of misuse of information by fascistic regimes during World War II. Privacy of information is a fundamental human right in the EU. The US bills are still focused on rectifying misuse of data, while the EU approach says nobody should be collecting this information at all unless they have a good reason to."

Wugmeister says a new Japanese data privacy law (http://www.freshfields.com/places/japan/publications/pdfs/12343.pdf), which went into effect on 1 April 2005, might have a more significant impact on data security practices in the US.

"What's really interesting about the Japanese law is, it doesn't have a cross-border limitation like the European law does," Wugmeister says. "It says if you collect information, you can share it down the street or across the world, but you're responsible for it. So it puts the onus on the entity doing the collecting."

The Japanese law also has a lengthy section of explicit guidelines, and Wugmeister believes it might have a "significant downstream effect globally. If you're a Japanese subsidiary of a US company, in theory the subsidiary has to impose those security obligations on the US parent, so it will raise the bar from a security perspective around the globe."

Specter-Leahy proposal

However, in the US, both lawmakers and industry consortia have recently enacted sweeping data security reform proposals. On 29 June, US senators Patrick Leahy (D-Vermont) and Arlen Specter (R-Pennsylvania) introduced the Personal Data Privacy and Security Act of 2005 (http://leahy.senate.gov/press/200506/062905a.html). One day later, the credit card industry's new data security requirements, the Payment Card Industry Data Security Standard (http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf), went into effect.

The Specter-Leahy proposal would introduce stiff civil penalties for data-holding entities that fail to secure personally sensitive data. It mandates that companies notify consumers when a security breach affects their information. Entities holding data must also create a data privacy and security program that will "regularly assess, manage, and control risks

to data privacy and security consistent with the size, complexity, and scope of its business."

The new payment card standards expand on the broad strokes of Specter-Leahy by mandating security procedures for merchants accepting credit cards. For example, any merchant processing more than 20,000 credit card payments per year must undergo quarterly scanning of its external-facing network applications by a certified third-party security firm.

Security research

Joe Stewart, a senior security researcher at Lurhq, a managed security firm, expects his industry's business to increase as identity hacks gain more notoriety. Many exploits, he says, are not products of gifted malware writers but rather of continued user gullibility.

"From a technical level, we're seeing less and less ability to exploit things remotely just by port scanning, Stewart says. He attributes this difference to widespread adoption of Microsoft XP Service Pack 2. "The malware authors are trending to application logic vulnerabilities like Internet Explorer exploits and social engineering—because no matter how many times somebody tries the same old tired social engineering tactic, it seems to work."

Stewart believes successful security providers will give their data-holding customers pertinent information without drowning them in the minutiae of vulnerabilities. At the same time, they must stay on the cutting edge of *intrusion-detection signature* development. He says a community-driven technology, such as the open source Snort IDS, gives security technologists a good foundation but needs refinement.

"Lots of the signatures that exist in the standard Snort rule set are really bad, with lots of false positives, written by people who don't have experience watching real networks," Stewart says. "That can be a big time waster and quite devastating." Stewart nevertheless believes that community-built IDSs like Snort have performed better than many proprietary IDSs.

Public sentiment

Susanna Montemezolo, a policy analyst for Consumers Union, says the US Congress is considering five bills besides Specter-Leahy concerning data privacy. While Specter-Leahy seems to have built momentum, Montemezolo says the data-holding industry is lobbying for a fairly weak bill concerning breach notification instead of worrying about technical mandates. She believes privacy advocates have public sentiment on their side. "On the grassroots level, there's a lot of anger about this," Montemezolo says. "The marketplace clearly isn't working right now."

However, Marty Lindner, senior member of the technical staff at CERT-CC at the Software Engineering Institute, says he doesn't see any particular rise in consumer anger. "The people making money are not around you, they're elsewhere. The people losing money are actually your next-door neighbors, but they don't see the money being lost, because the banks and other financial service institutions are putting the money back."

Because the costs are absorbed in service fees, Lindner says, the average consumer isn't complaining about it.

Best practices

Whatever the prevailing mood is among consumers, attorney Wugmeister says the business community is adopting best practices with alacrity to avoid embarrassing publicity. "So many of our clients have said, 'We don't want to be the person in the *Wall Street Journal* tomorrow.' The fear of a reputation hit is so strong right now. I am now putting into agreements admissions of responsibility and financial obligation in case of a breach."

Wugmeister says one legislative route to reducing identity theft will be eliminating Social Security numbers as personal identifiers. Institutional system administrators have estimated the cost to change databases using Social Security numbers can run into the millions. Rutgers University, for example, estimated replacing Social Security numbers (http://senate.rutgers.edu/rucsssid.html) with an alternative student ID number would cost $1.2 million. But Wugmeister believes legislation stipulating a financial penalty per Social Security number exposed to hackers would provide sufficient incentive to data brokers with large banks of personal data to make those changes.

The user-driven network

The legislative and short-term technical fixes such as monitoring services can only go so far, says Microsoft's Cameron. The identity metasystem that he and his colleagues envision is an open architecture that builds on existing identity efforts, such as the Liberty Alliance (http://www.projectliberty.org/) and the in-progress WS-Trust (http://specs.xmlsoap.org/ws/2005/02/trust/WS-Trust.pdf) specification from the Web Services Interoperability organization. The architecture includes an identity selector component, which Microsoft will implement with the InfoCard. A WinFX component, the InfoCard is specifically hardened against tampering and spoofing to protect the end users' digital identities and maintain end-user control. Users can create a "lighter" version of the InfoCard, similar to current Web site registration configurations.

However, the identity metasystem architecture doesn't require implementations to use InfoCard. Cameron says Microsoft learned from its unsuccessful attempt to create a centralized identity clearinghouse with .Net Passport that an open architecture approach is far more likely to catch hold.

Mindful of the Passport lessons when he wrote "The Laws of Identity," Cameron wanted to define enduring system characteristics that would minimize pushbacks. "One pushback," he explains, "will be from the user who says 'I don't like this. I'm not going to use it.' Another is legislators who say, 'This is terrible, so we're going to legislate so it's closer to what an identity system should be like.'"

Conclusion

Ping Identity's Norlin, who has already successfully demonstrated a transaction between Microsoft technology and an open source SAML (Security Assertion Markup Language) identity implementation, says adoption of user-driven identity technology and philosophy is inevitable but gradual.

"I don't think there's any flash point," he says, "and certainly don't think we're going to have control over identity attributes at any time in the near future. I really would like to be able to go to Amazon and have them not have my credit card number at all. Give them permission to use it but not get it, but I think we're five years from that being a reality. There's a lot of IT computing work that needs to be done."

Related Links

- Online Fraud Gets Sophisticated (http://doi.ieeecomputersociety.org/10.1109/MIC.2003.1232512)
- DS Online Security Community (http://dsonline.computer.org/portal/site/dsonline/index.jsp

Cite this article: Greg Goth, "Identity Theft Solutions Disagree on Problem," *IEEE Distributed Systems Online*, vol. 6, no. 8, 2005.