I'm Pc01002/SpringPeeper/ED288l.6; Who are You?

Susan Landau
Sun Microsystems

Deirdre K. Mulligan
University of California, Berkeley, School of Law

In considering identity management, the first issue is—What is identity? This is, of course, an issue that has plagued poets, philosophers, and playwrights for centuries.[1–3] We're concerned with a more prosaic version of the question: How does an entity recognize another entity? This important question occurs when access to resources, such as health or financial records, services, or benefits, is limited to specific entities. The entity in question could be a person, a computer, or even a device with quite limited memory and computational power. In this issue of *IEEE Security & Privacy*—the first of what we suspect will be several special issues on identity management—we have chosen to focus on identity management in which the entity being identified is a person.

There are several reasons for this focus. Most *S&P* readers are likely to face this sort of identity management system first (many of you have probably already done so). Competing, overlapping, and—to some extent—interoperable technical solutions are vying for market and mindshare in the public and private sectors. These technical solutions, which both reflect and implicate human values, must respond to demands of the political and legal landscape that will strongly influence the forms of identity management deemed desirable and viable in a given context.

A striking example of the issue's complexity and timeliness is playing out in the implementation of the highly-controversial US Real ID Act, a 2005 law that established federal mandates that states must follow when issuing drivers' licenses and identification (ID) cards. This law presents daunting technical and administrative challenges. It requires that a state first determine whether an applicant has an ID card in another state before issuing one of its own to that applicant. (Although holding multiple licenses was previously illegal, states hadn't been required to determine whether a person held a driver's license in another state before issuing one.) How can this be done securely? A centralized database isn't the answer, but performing real-time checks between 50 states in a nation of more than 300 million people presents serious reliability, interoperability, and security challenges. Standardization and broader policy challenges exist as well; for example, the law neither defines statutory limitations on what data can be included on an ID card's machine-readable side nor requires that such data be encrypted. The Real ID Act doesn't set limitations on who can read or capture a card's information. Once other states or third parties—such as supermarkets or bars—collect the data (and all of them have shown great appetite for it), its use and further dissemination is assumed, given that the practice is currently unregulated. The privacy and security implications of this lapse are immense. Due to concerns about the hard and soft costs of the Real ID system, several state governments have voiced strong objections—highlighting the political dimensions—privacy in particular—of managing people's identities.

The special issue

Complexity—and the shifting of complexity—underlies many aspects of identity management systems (as it does other efficiencies that computers and networked systems bring to our lives). Technologists are accustomed to looking at how technology simplifies

an overall system, but technologies that people use are complicated because people are complicated. Through technical, policy, market, and usability perspectives, the articles in this issue unpack and explore the complexities of identity management systems.

Technologists are accustomed to looking at how technology simplifies an overall system, but technologies that people use are complicated—because people are complicated.

Because *S&P* is primarily a technological magazine, we've focused on identity management's technological concerns. We can't cover the full panoply of issues surrounding identity management in six short articles; instead, our aim is to provide a range of perspectives on identity management systems that will enable readers to identify and understand relevant questions when faced with questions about such systems' suitability, constraints, design, deployment, and policy. The key questions are

- Where is the complexity in the system? (It depends on the application.)
- How do you design to avoid complexity? (If you don't, the users will find ways around it.)
- Which constraints cause complexity? Can they be avoided?

As any user of identity systems knows, the concern is how to manage multiple identities. A premier technical solution is to merge and federate them. Thus, we begin with Eve Maler and Drummond Reed's article, "The Venn of Identity: Options and Issues in Federated Identity Management," which examines three models of federated identity—SAML, OpenID, and Cardspace—and studies their varied focuses. Which is simplest to use? Which provides stronger security? How well do they interoperate? What are the technical challenges of federation? What new capabilities are on the horizon? Does federated identity work?

People are highly complex—and at times as stubborn as the most determined adolescent. As any sysadmin can tell you, it's important to account for human foibles and preferences when designing systems for people, or the systems won't work. Given that people are the entities at issue in the identity management systems we are considering, usability is the key to success. If system designers create complex, nonintuitive and distracting solutions, users are likely to create work-arounds (the ubiquitous yellow Post-It note stuck on the side of the computer terminal with the password written on it). Rachna Dhamija and Lisa Dusseault, in their article, "The Seven Flaws of Identity Management: Usability and Security Challenges," illuminate the usability challenges facing identity management systems, including the flaws and risks that can arise if design and deployment do not pay attention to the people who will use the systems.

If we're concerned about identity management for people, we'll want to know how to authenticate users. Many people think that biometric authenticators are the be-all and end-all in authentication because unlike secure tokens or passwords, they can't be lost or stolen. But biometric authenticators are more difficult to handle than you might expect, and they present specific challenges, including being uniquely hard to replace and recall. Jim Wayman's article, "Biometrics in Identity Management Systems," presents a clear description of what works—and what doesn't—and maps out the challenges facing the use of biometrics within identity management systems.

Federated identity systems are all about sharing user information, but what is shared, through which technology and under what constraints, is critical. By keeping individual pieces of an identity separate, federated identity systems can preserve privacy. But done poorly, they can magnify existing risks and create new vulnerabilities for personal information. Identity management is an issue with large legal and policy implications, as well as constraints (what is legal to collect or disclose in one jurisdiction might not be legal to collect in another). In their article, "Privacy and Identity Management," Marit Hansen, Ari Schwartz, and Alissa Cooper give views from both "sides of the pond" on key issues of identity management systems and provide useful guidance on ways to implement good privacy practice.

Like many other network technologies, identity management systems create efficiencies and shift costs from one place to another. Understanding the economics is crucial for what considerations should underlie design. Alessandro Acquisti, in "Identity Management, Privacy, and Price Discrimination," clarifies the relationship between privacy, personalization, and price discrimination. He explains how identity management systems can support various forms of information disclosure and thus can reduce the tension between the three—offering the potential for better aligning individual and merchant objectives.

We close with an article that examines identity management

systems in practice. We chose to include an article on e-government, in part because of its rapid development and surprising diversity but also because e-government systems illustrate how policy, markets, people, and politics influence—and sometimes drive—the solution space. If you thought that an identity management system was an identity management system was an identity management system, think again; they can be as different as New Zealand is from the US is from Scandinavia. In "Use Cases for Identity Management in E-Government," a case study of a New Zealand government system, Robin McKenzie, Malcolm Crompton, and Colin Wallis point out how social policy can create a sharp focus on user-centric systems with a high emphasis on privacy. This stands in stark contrast with the US's Real ID effort, which concentrates on authenticating users and virtually ignores the privacy issues surrounding personal data. In briefly discussing other systems around the globe, the article shows how a society's values can limit the type of an identity management system that is viable there. Developers must understand and respond to social values in a system's technological development and participate in sorting out the related policies and procedures. This is an important and unusual lesson for technologists.

Identity management is a complex issue, and we have sought to tease out its various strands so that users, developers, implementers, and regulators will know to ask—and begin to answer—the key questions: What is the application? What are its uses? What is the larger context? If this series of articles broadens readers' understanding of the conceptual space in which identity management systems reside, then we will have succeeded. □

References

1. Emily Dickinson, *Collected Poems of Emily Dickinson*, Thomas H.Johnson, ed., Little, Brown and Company, 1960, p. 133.
2. T. Macchius Plautus, *Menaechmi*, third century BC.
3. W. Shakespeare, *Twelfth Night*, 1623.

Susan Landau *is a distinguished engineer at Sun Microsystems, where she works on security, cryptography, and public policy, including surveillance issues, digital rights management, and identity management. She is coauthor (with Whitfield Diffie) of* Privacy on the Line: the Politics of Wiretapping and Encryption, updated and expanded edition *(MIT Press, 2007). Landau has a PhD from MIT, an MS from Cornell University, and a BA from Princeton University. She is an AAAS fellow and an ACM distinguished engineer. Contact her at susan.landau@sun.com.*

Deirdre K. Mulligan *is a clinical professor at the University of California, Berkeley School of Law, where she is the director of the Samuelson Law, Technology and Public Policy Clinic. Her research interests include information privacy and security, intellectual property, and technology policy. Mulligan has a JD in law from Georgetown University Law Center. Contact her at dmulligan@law.berkeley.edu.*

Lower nonmember rate of $29 for *S&P* magazine!

IEEE Security & Privacy **magazine is the premier magazine for security professionals. Each issue is packed with information about cybercrime, security & policy, privacy and legal issues, and intellectual property protection.**

Top security professionals in the field share information you can rely on:

- **Silver Bullet podcasts and interviews**
- **Intellectual Property Protection and Piracy**
- **Designing for Infrastructure Security**
- **Privacy Issues**
- **Legal Issues and Cybercrime**
- **Digital Rights Management**
- **The Security Profession**

Subscribe now!

www.computer.org/services/nonmem/spbnr