What's in a Name?

"What's in a name? That which we call a rose
By any other name would smell as sweet;"
—Romeo and Juliet, Act II, Scene ii

In ancient times, when the economy was agrarian and people almost never traveled more than a few miles from their places of birth, most people made do with a single personal name. Everyone you met generally knew you, and if there did happen to be two Percivals in town, people learned to distinguish between "tall Percival" and "short Percival."

Marc Donner
Associate Editor in Chief

The development of travel and trade increased the number of different people you might meet in a life time and led to more complex names. By the Greek classical period, an individual's name had become a three-part structure including a personal name, a patronymic, and a demotic, which identified the person's deme—roughly, one's village or clan.

This represented the end of the line in the evolution of names for several thousand years. During that time, people developed a range of concepts to enrich names with extra capabilities. Letters of introduction enabled travelers to enter society in a distant city almost as if they were locals. Renaissance banking developed the early ancestors of the letter of credit and the bank account, allowing money to be transferred from place to place without the attendant risk of physically carrying the gold. In response to these innovations, clever people invented novel ways to manage their names, for both legitimate and illegitimate purposes, giving us the alias, the doing business as, and the cover name. Americans invented personal reinvention, or at least made it a central cultural artifact, and developed a strong distaste for central management of the personal namespace.

Enter the computer

With the computer era came the user ID: first one, then two, and then infinity. With the Internet boom, we got retail e-commerce and the proliferation of user IDs and passwords. The venerable letter of introduction reemerged as an identity certificate, and the bank account evolved into dozens of different glittering creatures. While enabling online services to an increasingly mobile population, this explosion in user IDs created inconvenience and risk for people and institutions. As shopping and banking moved online, identity theft went high tech. We responded with two- and three-factor authentication, public key infrastructure, cryptographically strong authentication, and single-sign-on technologies such as Microsoft's Passport and federated authentication from the Liberty Alliance.

We're currently trapped between Scylla and Charybdis. On one side, civil libertarians warn that a centralized authentication service comprising a concentration of power and operational and systemic risk represents an unacceptable threat to a free society. On the other, we have a chaotic morass of idiosyncratic user ID and password implementations that inconvenience people and invite attack.

The King is dead! Long live the King!

With its controversial Passport technology, Microsoft attempted to address the visible need by offering a single user ID and password framework to sites across the Internet. With eBay's recent defection, it's increasingly clear that Passport isn't winning large ecommerce sites. Ultimately, Passport failed commercially not because of competitors' hostility or civil libertarians' skepticism—or even because of the technical problems in the software—but rather because enterprises proved unwilling to cede management of their clients' identities to a third party. This is an important lesson, but not a reason to give up on the effort to create a usable framework.

Who or what will step up and make the next attempt to meet the need? Did we learn enough from the debate about Passport to clearly identify the salient characteristics of what comes next? Have we made enough progress toward a consensus on the need for "a" solution that the next company up to bat will be willing to hazard the amount of treasure that Microsoft spent on Passport?

Now is the time for a vigorous dialogue to get clarity. We aren't likely again to see a comparable exercise of courage, however misguided, so it behooves us to reduce the risk for the next round of competitors.

A successful Internet identity service framework must include admitting multiple independent authorities. Some industries have a strong need to establish a common identity and will insist on controlling the credential. Some governments will decide to do likewise, whereas others will leave it to the private sector. But identity services shouldn't be tied to any individual vendor, country, or technology. They should allow the dynamic assembly of sets of privileges, permitting participating systems to assign rights and augment verification requirements.

Thus, a level of proof sufficient for my ISP to permit me to send a social email could be overlaid with an extra layer by my bank before allowing me to transfer money. It should be possible to migrate my identity from one ISP to another without losing all of my privileges, although I might have to re-verify them. It should be possible to easily firewall segments of my identity from others so that losing control over one component doesn't result in the loss of the others.

This can't be all that's required, or we wouldn't still be scratching our heads about it at this late date. It's clear that there are thorny policy issues in addition to some very challenging technical questions. Getting to a workable Internet identity framework will take hard work, so let's get going. □

Erratum

In Stuart Schecter's "Toward Econometric Models of the Security Risk from Remote Attacks," (Jan/Feb. 2005, v. 3, no. 1, pp. 40–44), the symbol $\hat{Y}_i$ dropped out due to a font problem, leaving only question marks in some places on page 40. We regret any confusion stemming from this.

New in this issue

Be sure to check out this installment of ClearText as Daniel Geer Jr. takes over this issue from Bruce Schneier to discuss problem statements.

How to Contact *IEEE Security & Privacy*

Writers

Visit www.computer.org/security/author.htm or log onto Manuscript Central at http://cs-ieee.manuscriptcentral.com/. Authors must use Manuscript Central to upload their submissions. First-time users must create a new account.

Letters to the Editors

Send letters to Kathy Clark-Fisher, Lead Editor, kclark-fisher@computer.org. Please provide an email address or daytime phone number with your letter.

On the Web

Access www.computer.org/security/. To visit our community forum, access www.ieeecommunities.org/securityandprivacy.