Information Matters, Volume 4

Who are you? . . . and are you sure?
Of Secrecy and Identity

> *"Who are you, Master?" he asked. "Eh, what," said Tom, sitting up, his eyes glinting in the gloom. "Don't you know my name yet? That's the only answer. Tell me, who are you, alone, yourself and nameless?"*
> – J. R. R. Tolkien

Everyone on the security team at Oracle wears a trench coat and a fedora, just like everyone in disaster protection wears a HazMat suit. So it was easy to identify Mary Ann Davidson, Oracle's Chief Security Officer, as I strode over to interview her for this piece.

I was a little nervous going through the retinal scan to get into her office and I didn't think such a large hair sample was really necessary, especially since I have known her for five years. But she gave me a winning smile and agreed to answer my questions about security and identity. "You know me," she said. "I'm all sweetness and light!" With my lingering anxiety lessening somewhat, I offered: "Great. So can you take your foot off my chest now?" And off we went.

Well, I may have mythologized this encounter somewhat. In fact, I made all of this up, except for Mary Ann's winning smile. Mary Ann, like you and I, has a complex identity. Our identity is not just the sum total of the things we purchase or view on the Web. We are not our credit history, our medical records, our IQs, our last year's Halloween costume, or what we dreamt about last night. And why is this?

Because to a degree, we define our own identity. And I, for one, have a secret identity.

Human beings have a huge curiosity about identity, and an adoration of secret identities. Books, movies and tall tales are rife with stories about mistaken identity, doppelgangers, split-personalities, princes and paupers and the like. Cyrano De Bergerac, The Matrix, The Lone Ranger, and any decent soap opera thrive on secrets—and especially dirty little secrets, and secret identities.

Ironically, this pretty well reflects the direction of computer security: inspired by secrecy, but consumed with the question of identity.

Truthfully, only part of my identity is secret. Of course, I have my public, physical self out there in the world. But, more to the point, I have an online identity, an imprint on various databases, websites, email lists and online communities (nothing kinky, mind you). And so

do all of us. And so do companies, partnerships, government agencies, credit bureaus, and charitable organizations–a vast flickering imprint on the electrosphere.

And flicker we do. The Internet now conveys inconceivable amounts of wealth, meaning, and amusement to and fro, and it can only continue. We are e-waltzing our way towards an always-on, telepresent society, where our identity—real, secret or cyber—becomes a much more important and interesting concept.

Issues about secrecy, security and identity have pervaded the IT industry for decades. Back in the early 1980s, as widespread use of computer networks took hold, there was a corresponding rise in concern over computer security. In 1983, the US Department of Defense created the Trusted Computer System Evaluation Criteria (TCSEC), also known as the Orange Book. They established a method of categorizing and certifying computer security from "D Level," which provides some minimal protections, to "C level," which specifies discretionary access control (like file and directory permissions, password protection, etc.) to "B Level" (requiring mandatory protections), to "A level" which requires special helmets to prevent people from reading your mind. Okay, not really, but you get the idea. Each level contained sub-levels, with "C2" security now being the most common evaluation.

Back then, driven by the reality and the mentality of the times, many government agencies required their highly sensitive projects to comply with B1-level requirements. Years ago, I had some direct experience with this when I worked at AT&T Bell Labs, at a time when parts of the modern UNIX system were being developed. One of the critical projects we were involved in was the creation of a B1 level security-compliant UNIX operating system. At about the same time, Oracle – which already had well-established credentials in computer security – was working on a product called "Trusted Oracle," a B1-compliant version of the Oracle database.

As these technologies were rolled out, they faced a similar reception: Most if not all of the B1 features were not used. Why? Because a disciplined use of B1 technology imposes mandatory (and seemingly constant) checks, challenges, and passwords. The systems became practically unusable because the security was so intrusive and cumbersome.

And so the challenge remains: how can we maintain tight security, but not hinder our operations or overburden our staff? Oh, and by the way, there are 70,000 employees to deal with (or 700,000 customers or 7 million citizens).

Built into this equation is the basic requirement of mitigating risk. "Business is about taking acceptable risk. So is security." said Mary Ann. "The question is 'how can we manage risk?' and specifically, determine and manage what is acceptable risk?" There is an inherent balance to be struck in any implementation.

The truth is, we have pretty good locks these days. Information secrecy, at least in terms of encryption, biometrics and related strategies, is practically (dare I say it?) unbreakable. But Mary Ann would remind us that our security is only as good as our security practices. She

had an interesting take on Biometrics. “Technology is nothing, implementation is everything,” she said. “Since a fingerprint is unique, you would assume it makes a great way to uniquely identify you. However, unique not does mean secret – you leave your fingerprints everywhere. If somebody manages to hack your biometric, they are ‘you’ and there’s not a dang thing you can do about it. What are you going to do, reset your fingers?”

Of course, given available technology and good implementation, we can completely lock our information in virtual bunkers, yank out the network cables and sit on top of them – dangling our legs and waving our e-shotguns. But security today is less about keeping hugely sensitive information out of enemy hands. Security discussions have moved from simply protecting sensitive information to securing a trusted flow of information and identity among individuals and other cooperating entities.

Follow the money and you’ll see why. One of the major inhibiting factors of online commerce is that identity must be established and re-established for every new place you want to shop. Companies face this same problem when two or more businesses want to create a circle of trust. As a result, the concept of *federated identity* was born. A federated identity enables two organizations to transfer a trust relationship from one to another. For example, if a hotel chain has a partnership with a rental car agency, and they share a customer, why can’t the customer go from one virtual desk to another and take their trust relationship with them?

The business community drove the requirements for these federated identities because they already had these kind of relationships and they wanted to be able to express them technically. “Federated identity is business-driven,” Mary Ann points out. “Customers are saying, ‘We have existing relationships, we just need the technology to support them.’”

Standards such as Security Access Markup Language (SAML) are emerging to enable web services to swap these kinds of trust credentials. SAML mimics the same kind of business practices that have been in place for millennia. You shake hands, you establish a public contract: “You give me that cow, and you get the silver”. This transaction is first an exchange of identity (I am a seller, you are a buyer), and then an exchange of goods on the basis of this agreement. That is exactly the same kind of one-to-one business relationship that SAML enables.

It’s very likely that this type of technology will soon extend beyond business transactions to accommodate social interactions as well. Web sites devoted to music, entertainment, politics, hobbies and gaming can all benefit from a managed exchange of identity.

In the real world, you are the author of your identity. Your personal, public identity is a contract that you renew every day. What you say, how you act, and what you wear are all personal choices that you make, consciously or unconsciously. On the other side of that contract is everyone else and their perception of you. For instance, try as I might, I could not get Mary Ann to call me Agent Demarest, much less Special Agent Demarest. Identity is a personal choice, but there has to be agreement or collusion on the other end. Our

manners, customs and behavior are the protocols that get us through the day without being arrested, slapped or institutionalized.

There are, of course, conventions and protocols in the online world as well. But as we have seen in the headlines lately not everyone plays by the rules. There is a shocking amount of information collected about us, alternate unknown identities bought and sold in the online world that are well beyond our control. This is a troubling notion that raises real questions about privacy, security and civil rights in our society.

Consequently, we have to be just as deliberate about our online identity – perhaps even more so, given the increasing interconnection of our networks, our devices and ourselves. Whether it is identity theft, lost eBay auctions, lost privacy, or lost businesses opportunities, the implications of being careless with your cyber-self are immense.

On the other hand, successfully establishing appropriate circles of trust for our friends, employees, partners and customers promises to help close the distance between us. At that point, maybe the constant electronic prompting of "Halt! Who goes there?" will swiftly and silently be answered by, "It's me!"

And the doors shall open …