TECHNOLOGY

Information Security Strategies for Healthcare—Defining the Roadmap: Part 3

Noam H. Arzt, PhD

At my son's middle school, students sign on to their Citrix environment with a biometric (in this case, a thumb scan), even though most of our clinical applications use a simple username and password to authenticate users.

We all know the basics of AAA: authentication (who you are), as distinct from authorization (what you can do), supported by accounting (an audit trail and management of these rights and responsibilities). We all have memorized the levels of authentication as if they were mantras (what you know, such as a password; what you have, for example, a hardware token; what you are, such as a biometric). Many of us have struggled to make progress with proprietary technology and inadequate standards. And we all fear the legal, political, and societal implication of an inappropriate disclosure of information from one of our systems.

Defining the Agenda

My first column, in the Summer 2003 issue, identified a set of important information security realities for healthcare IT leaders. They are:

- Security starts with principles and policies.
- Continue your move to the Web.
- Keep your basic infrastructure healthy.
- If you're not already doing so, start worrying about portable devices.
- In the end, it's all about AAA (authentication, authorization, and accounting).

Last time, I talked about portable computing. In this column, I want to discuss the struggle with authentication, authorization and accounting.

It's HIPAA, baby...

The Spring 2004 *JHIM* had two wonderful articles about AAA and HIPAA. One described the Mayo Clinic's struggle to deploy a single sign-on solution that did not unduly compromise the productivity of its workers while being unrealistically costly. The other reviewed key concepts about identity and access management, including the experience of Denver Health in securing its CPOE system.

> *"A more heterogeneous computing environment enables us to distribute risk over a number of products and players, as long as we have the capability to make compatible choices."*

Both articles chose to use HIPAA as the backdrop for these concerns, and rightly so. HIPAA legislation has not only pinpointed the exposure caused by these issues, but it has raised the stakes in terms of penalties for non-compliance and society's sensitivity to inappropriate disclosure.

Although these issues existed long before HIPAA was born, the somewhat coincidental coming-of-age of the Internet and mass-consumption of computing in the United States has raised the level of risk to many organizations. Broadband access has lead to additional exposures because persistent connections enable the "bad guys" to automate attacks more readily while exposing inadequately protected homes and small business partners to intrusion. Broadband penetration in the US surged to more than 40 percent, according to the January 2004 issue of *Broadband Report*.[1]

You think you've got it bad...

In an earlier article in the Spring 2004 issue of *JHIM*, I tried to find some silver lining within the reality of heterogeneous computing environments within our organizations. A more heterogeneous computing environment enables us to distribute risk over a number of products and players, as long as we have the capability to make compatible choices.

While this pragmatism may not be an obstacle in developing and implementing an organization's overall security architecture, uniformity leads to a more practical and supportable outcome when it comes to AAA. The more uniform the desktop, the more consistent the application architecture, and the more coherent the network, the easier it is to acquire and deploy an AAA solution.

Our concept of "user" is expanding rapidly. Hospitals are offering more online access to services, physicians, and specialties. Academic medical

centers are offering more educational content for aspiring health professionals and the public at large. Insurers aspire to be more efficient and customer-focused by providing access to information around-the-clock. But how do we incorporate these new, often transient users into our AAA plans?

There have been a number of efforts to provide more global AAA infrastructures, even though they have met with only limited success. Early adopters, especially in academic settings, looked to Kerberos as their standard, but it has yielded only a limited number of compatible applications and certainly is not for the meek. Public Key Infrastructure is touted as the underpinning of a pervasive authentication and authorization system, especially over the Internet. It has proven difficult to set up and costly to maintain and administer, and it has failed to provide a value proposition to certificate authorities and others who hoped to profit from its adoption and proliferation.

Other efforts aimed at developing the notion of a "federated identity" over the Internet also have had only very limited success (for a private sector example, check out the Liberty Alliance Project[2]; to see what the government is up to, look at the Federal Bridge Project[3]). Even Microsoft's Passport initiative does not seem to have reached nearly as many users as they had hoped.

Full steam ahead?

So where do we go from here?

Pilot, pilot, pilot. Healthcare organizations have to take this stuff for a test drive, simultaneously evaluating the robustness of the technology, the implications for administration, and end-users' experiences. These three perspectives may be at odds with each other and represent tradeoffs to be managed. Findings should be documented and discussed carefully with users, management, and technical staff.

"The more narrowly an organization defines its user population, the more success it will likely have in setting up a manageable implementation."

Recognize the limitations. Much of this technology is still in its infancy. The more narrowly an organization defines its user population, the more success it will likely have in setting up a manageable implementation. Administrators can consult with industry analysts, but they can't predict the future either.

Look to traditional vendors, but keep an open mind. While traditional Network Operating System (NOS), database or Web server vendors may offer compelling solutions, keep an open mind to alternatives that may interoperate better as pilot implementations expand to include other users and potentially other platforms.

This isn't going to be easy. As we get more tangled in the Web, our users' expectations for seamless integration increase, and mobility and wireless computing get more pervasive, but not necessarily more secure.

Sometimes, I try to gauge the future of technology through my 12-year-old's eyes, and he's usually on target: "Why can't this stuff just work the same way every day?"; "Why do I have so many passwords?"; "Faster, faster, faster!" Our challenge as IT professionals is to make it all seem as effortless as my son expects it to be. Maybe one day, he'll be there to help.

About the Author

Noam H. Arzt, PhD, is the president and founder of HLN Consulting, LLC, San Diego, CA. He can be reached at arzt@hln.com.

References

1. http://www.websiteoptimization.com/bw/0401/
2. http://www.projectliberty.org/
3. http://www.nbnn.com/vol19_no4/news/1389-1 for some information