SearchSecurity.com E-Guide

Tips for Overcoming Authentication Challenges in 2008

It's not secret that Internet fraud and identity theft threats have influenced the way consumers are conducting transactions online. Gartner reported that almost half of US adults were worried enough that in 2006 companies lost more than $2 billion in online sales.

This expert E-Guide takes a look at the challenges of effectively authenticating consumers and details what your company can do to ensure the security of its online customers. Read this E-Guide today and learn more about multi-factor authentication for high-risk transactions and what you can do to ease your consumer authentication burdens.

TechTarget
The IT Media ROI Experts

The second factor and beyond: Challenges in consumer authentication

By Carol Weiszmann and Susan Messenheimer

The risks of Internet fraud and identity theft are giving consumers pause. Some 46 percent of U.S. adults were sufficiently nervous about it that in 2006 businesses lost more than $2 billion in online sales, reports Gartner.

Many believe at least part of the problem is due to weak customer authentication that's far too easy to spoof. Many believe the answer—or piece of the answer anyway—lies in multifactor authentication. This would require customers to authenticate themselves in terms of more than just one of the three categories of authentication factors:

- Something s/he knows (e.g., password, personal identification number)
- Something s/he has (ID card, ATM card, security token)
- Something s/he is (signature, fingerprint, retinal pattern, voice pattern, DNA sequence)

Multifactor authentication for high-risk transactions

The push for multifactor authentication in consumer transactions is being driven by a 2005 directive from the Federal Financial Institutions Examination Council (FFIEC), whose agencies include the Federal Reserve Board of Governors, the FDIC, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. These guidelines don't actually require multifactor authentication in online banking transactions—but it's the upshot. Here's what the guidelines actually say:

> "Single-factor authentication, as the only control mechanism, [is considered] to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. … Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks."

While strong authentication can be achieved by requiring multiple responses to challenges from a single category (as in, say, password and account ID number), multifactor authentication means requiring responses from two or more authentication factor categories. "Using multiple solutions from the same category at different points in the process," notes a 2006 FFIEC guideline FAQ, "would not constitute multifactor authentication."

Enter a new generation of tokens

Perhaps the multifactor authentication experience consumers are most familiar with is using their ATM card (what they have) and PIN number (what they know).

The ATM card is, in effect, a token, and it works fine when a customer goes to an ATM machine, which includes a mechanism that can read the card. The challenge comes in extending this model to a world where transactions are conducted with a variety of banks and vendors from computers at customers' homes, jobs, and friends' homes.

Several barriers have hindered use of tokens for multifactor authentication. These include a lack of standards, which forces consumers to carry an impractical number of tokens. Consumers have balked at this. Nor do companies want to incur the high costs and inordinate complexity of deploying and maintaining tokens.

But that's starting to change, thanks to the Initiative for Open Authentication (OATH), which has released the Reference Architecture 2.0 standards for authentication tokens. OATH is supported by Verisign, IBM/Tivoli, Hewlett-Packard, Citrix, AOL, BMC, Entrust, Imprivata, SanDisk, and many others.

OATH supports use of one-time passwords (OTP) to reduce the possibility of password compromise by generating a new password for each transaction. When implemented on proprietary tokens, OTP is expensive. But the interoperability inherent in OATH has enabled vendors to offer a variety of OTP token options, including USB-connected tokens, credit card tokens, and software-based key generators that can communicate with mobile phones, and voice-enabled OTP.

Sharing authentication burdens

The result is enablement of a shared-service model—not unlike the ability to use an ATM card in many different banks' ATMs. Credentials can be shared among credential issuers and other relying parties. This means the token issued by a bank or a retailer to its customers can be used to conduct transactions with other web-based businesses. The ultimate result will be a single, open authentication network accessible by consumers. And the costs of this network can be shared by businesses.

Today OATH-based multifactor authentication is available as an Internet service, easing the burdens on companies of OTP token fulfillment, distribution, and support. Verisign's Authentication Service, for instance, enables a business to issue and/or accept multiple end-user credentials that are OATH-compliant. Those not interested in issuing credentials directly can have Verisign do it for them.

Of course, multifactor authentication alone cannot stop all online transaction fraud. Man-in-the-middle attacks, for instance—in which online sessions are hijacked by tricking customers into providing OTPs generated by tokens—can defeat even two-factor authentication.

That's why the FFIEC and security experts recommend deploying layered security. Software designed to detect online fraud—such as Verisign's Fraud Detection Service—uses a rules-based engine and heuristics (machine learning algorithms) to spot fraudulent transactions in real time. When this kind of capability is combined with OATH-based shared credentialing, businesses can benefit from participation in an extensive authentication network at minimal cost.

In the world of e-banking and e-commerce, multifactor authentication is a necessity. Making it part of a layered security strategy is a cost of doing business—and now the cost is becoming reasonable.

About the authors: *Carol Weiszmann and Susan Messenheimer are partners at aimpublications.com, a content consultancy at the intersection of technology and business. They analyze and write about how key information technologies impact enterprise security, compliance, infrastructure, productivity, and profitability.*