



## IDENTITY MANAGEMENT: MORE ART THAN SCIENCE

10/08/08

By Wyatt Kash

The art of identity management is increasingly relying on shades of gray and off-kilter digital patterns, information technology security experts said Oct. 7 at a conference on identity management in government.

“Authentication is no long a binary decision,” said Bret Hartman, chief technology officer at EMC subsidiary RSA Security, referring to rules that either allow or prevent a user from gaining access to IT systems. Network administrators must strike a balance between the need to make their systems secure and the need to make them usable to a large number of users, he added.

The preferred approach goes beyond identity tokens and biometrics and involves dynamic risk-based authentication, in which the process that verifies the digital identity of a user also assigns a measure of risk that the user might not be who he or she claims to be, he said.

That risk assessment — similar to a credit score but established for each user session — might be based on whether an IP address or other data matches historical patterns associated with that user. If a data element looks suspicious, the system could redirect the user to a series of additional identity challenges, Hartman said. The approach, which is widely used with credit card transactions, would rout a small percentage of high-risk log-ins to more rigorous challenges while transferring the majority of low-risk users directly into their transaction sessions.

The additional scrutiny means applying “shades of gray to the authentication decision,” Hartman said.

He offered several principles for driving information assurance and authentication initiatives, saying they must be:

- Dynamic and intelligent, based on behavior as much as identity attributes, and content-driven.
- Transparent to the enterprise and user.
- Built into the product and the infrastructure.
- Risk-based and aligned with an agency’s mission.
- Holistic in nature, with a layered defense that extends from the data center to the user.

The challenge in developing those tools is keeping up with the vast amount of data created every day and the number of people accessing that data, said Stephen Coggeshall, chief technology officer at ID Analytics, who also spoke at the IT Association of America’s IdentEvent conference.

Coggeshall stressed the importance of analytics in understanding the nature and behavior of individuals accessing systems.

Part of that authentication equation involves understanding that an individual has multiple roles and, in effect, multiple identities, he said.

Another component involves assembling data elements that are knowable, unique and permanent — and can be revealed or discerned through transaction events, he said.

“We focus on the connectivity of [identity] elements by building linkage patterns” using a combination of fuzzy logic algorithms, he said. “Those graphs can provide substantial incremental information on how and to whom we connect, and improve identity management.”

By looking at variations in the patterns, such as an individual using multiple Social Security numbers or several individuals in different places using the same phone number or credit card, it’s possible to identify people who are misusing the system.

That approach can also help mitigate privacy issues by reducing data proliferation and having the authentication system use scores and recommended actions rather than extracting actual user data, he said.