



Identity Management Summit May 17, 2006

Communiqué

Identity management is a significant concern for consumers and businesses as security breaches continue to lead to the loss of personal and sensitive information for large number of users. In a day and age where information is constantly at our fingertips, the task of defining and establishing “identity” is growing more complex and difficult to manage. As new threats that target both technical vulnerabilities and human nature continue to grow and as technologies that offer new identity management solutions for the individual and the corporation continue to evolve, the lack of well understood and accepted solutions for issuing and establishing identities remains a major challenge.

On May 17, 2006, the **Georgia Tech Information Security Center (GTISC)** hosted the **Identity Management Summit** to examine the security challenges for businesses and consumers in managing digital identities. During his keynote address to the summit, Howard A. Schmidt, visiting professor at GTISC and former Special advisor to the White House for Cyberspace Security noted that matters of identity management have changed for the better, but there is still plenty of room for improvement. After the keynote, a panel of executives from major corporations with a stake in online identity management echoed his sentiments as they provided Summit attendees with a “reality check” on the current and future state of identity management.

Panel Discussion

Moderator: Dr. Paul Judge, chief technology officer for CipherTrust, Inc.

Panelists:

- *Jeff Schmidt, chief executive officer of Authis*
- *Todd Inskip, senior architect for identity management of Bank of America*
- *Tony Spinelli, senior vice president for information security of Equifax*
- *Richard J. Lipton, professor at the Georgia Tech College of Computing*
- *Dr. Burt Kaliski, vice-president of research at RSA Security and chief scientist of RSA Labs*
- *Chris Meaney, vice president of secure networks, Siemens*

During the course of the panel, many questions were raised concerning the current definition of identity management, responsibilities for issuing and authenticating individual and corporate identities, as well as the future of managing digital identities for individuals and businesses. Fortunately, the panelists reached consensus on most of these issues, and recommendations resulted from the discussion.

The following outlines the questions addressed by the panelists, the resulting consensus that emerged at the Identity Management Summit, and the action items that will be driven by the Georgia Tech Information Security Center.

How do you define identity management? What are the goals of your company, as well as the industry, when it comes to identity management?

- At the onset of the discussion, panel members provided their perspective on the existing definitions of identity and current identity management solutions. The panel agreed that it is appropriate and even desirable for one person or business to employ multiple identities for different purposes, and because of this, there is no single definition of identity. They agreed that, as more people move online, their identities that have been used in the past do not necessarily translate to meaningful online identities, which often makes it more difficult to establish the “claimed” identities of parties involved in an online transaction..

There was strong agreement among the panelists that there is a difference between a user's identity and identifiers associated with the user. An identity defines who you are, and identifiers are attributes that are used to establish your identity . The panel stated that there are three main rules for an identifier: it must be issued by a trusted party; it must be usable in multiple contexts; and it must be difficult or impossible to forge and change.

The panel agreed that, from a corporate and industry perspective, the primary driver behind identity management is the customer's experience and that too much security can be just as bad as too little. Thus there is a need for standardized identity management. The panelists agreed that there must be a national dialogue to identify that standard and that it is imperative that the dialogue take place today.

Given where we are now, what are the existing problems or shortcomings?

- Security challenges that have recently exploded in the Internet space – identity theft, spam, rogue access points, spoofing, and phishing attacks – all impact a person or corporation's ability to manage his, her or its identity. The panel stated that there are three pillars of identity management: identification; authentication and authorization. But part of the problem today is the fact that there are multiple solutions and no standards. Also, there is no clear understanding of who should set the standards and determine the terms that constitute the three pillars of identity management.

Depending on the situation, it can be easy or difficult for an individual or corporation to prove his, her or its identity and gain authorization to use private information or services. The scope of the problem grows even more complex as people develop new identities online and as the global community becomes more intertwined because there is no common internationally-accepted set of identifiers.

The panel agreed that a framework must be created to determine the authenticity of the digital identity of a source that provides identity-related information, and a standard must be researched and defined to determine the best method for authentication and authorization. This research must span the national and international community as individual and corporate identities become increasingly global and Web-based.

What are some of the problems companies face deploying identity management today?

- The panel agreed that one of the largest problems in deploying identity management is determining if the source that provides identity information is a “good” source. Malicious sources can pose the threat of security breaches, like viruses or bots, which often strike without the operator's knowledge. Another issue faced by corporations is the consumer's lack of desire for complicated identification and authorization procedures to gain access to their information or services. The panelists noted that, while it is important for companies to secure the information of their customers, there is also a problem with too much security if it degrades the quality of user experience.

While future authentication techniques may include facial and computer recognition, these technologies have not yet been perfected, leading to a need for other and more-usable solutions. The panel agreed that there is also a need to define the level of security needed for access to private information and programs and to determine the level of access for employees in order to provide optimal customer service in a manner that secures their information and identities.

There are many different types of systems that call themselves “identity management,” where do industry standard efforts and products converge?

- The panel identified and explored a number of current “identity management” systems, programs and regulations, including Sarbanes-Oxley and HIPPA, that aim to better protect consumers and businesses when it comes to private identification information. However, it was also noted that there has not been a large market adoption of one identity management standard or system in particular.

Additionally, while consumers want their identities protected, they do not want to be inconvenienced by the methods used to protect them – complicating the situation for corporations charged with the task of protecting their customer’s digital identities. Over time there will most likely be a larger push for stronger authentication; but today’s obstacles to creating such authentication solutions remain development time and costs. The good news is that there is a growing market to develop “identity management” systems, and the competitive nature of an open market will likely lead to higher standards as companies and organizations vie for the best products to protect the consumer and the corporation.

The panel agreed that any approach to identity management needs to converge on an open standard as a platform for running best practices for security. This will better enable the information security industry to help consumers by reducing complexity, meeting regulatory standards and ultimately satisfying the customer.

Let’s talk about what we as the IT and research community need to do next. What collaborative efforts and research efforts are needed?

- The panel agreed that there are several efforts that offer an approach to identity management, but no one person or group is standing up as the authoritative source. The panelists noted that national dialogue is needed to define the authoritative source or sources and identify a standard by which secure measures can be practiced to ensure proper identity management. Some of the problems with identity management today include: the fact that not all authentication techniques are created equal; the willingness of the public to forgo certain aspects of security in the excitement of a new technology; and the use of too much personal information to authenticate a source.

The panel agreed that there needs to be a holistic approach to tackle the identity management challenge. Systems need to be scrutinized from a broad view down to specific aspects of security management to develop a single standard of identification, authentication and authorization that satisfies the customer’s need for simplicity and efficiency, as well as an individual and corporate need for security. Therefore, with the ongoing sponsorship and guidance from these key stakeholders, GTISC will continue to actively promote research and education initiatives to raise awareness, and will provide leadership to promote the critical technology and policy issues related to identity management.

Summit Outcome

All participants in the GTISC Identity Management Summit agree that any approach for tackling identity management issues MUST center on a national and international dialogue among all

stakeholder groups to raise a cohesive understanding of what identity is and how to ensure the secure management of individual and corporate identities.

With support from the Identity Management Summit panelists, GTISC plans to:

- Develop comprehensive research programs to explore many of the identity management concerns raised at the Identity Management Summit, including the appropriate identification authentication and authorization frameworks.
- Promote open dialogue of identity management in hopes of increasing national and international awareness about identification, authentication and authorization, thereby leading to a standard for the secure issuance and management of individual and corporate identities.

Ultimately, it is research and education that will lead to user empowerment and the ability of the individual and corporation to combat security attacks head on.