INFORMATION RESOURCES MANAGEMENT COLLEGE

Summer 2004
Volume 9, No. 3

Info Tech Talk

A Newsletter on Enabling Information Technologies by the IRMC E-Government and Technology Department

Inside this issue:

...the pen can afford a single student the opportunity to have a digital copy of their own notes. Furthermore, the individual can also share these notes with friends or colleagues.

The Digital Pen -- A New Tool for Education?

By Professor Paul Flanagan

The IRM College has purchased and evaluated a set of personal digital pens. The pens write just like any ballpoint pen, but the pen can also permanently record your words, sketches, and classroom notes in a digital form. This form can be transferred to a personal computer and if needed can be further manipulated using software.

The potential of these devices is most prominent in education. In a classroom setting or an educational briefing, the pen can afford students the opportunity to have a digital copy of their own notes. Furthermore, the individual can also share these notes with friends or colleagues. This is done electronically and does not involve having to share the original notes or to photocopy.

If a student is working as a member of a group, the pen allows the student to be the official scribe or note-taker. In this manner each member of the group can quickly have a copy of the "official" notes within minutes of the end of the group session.

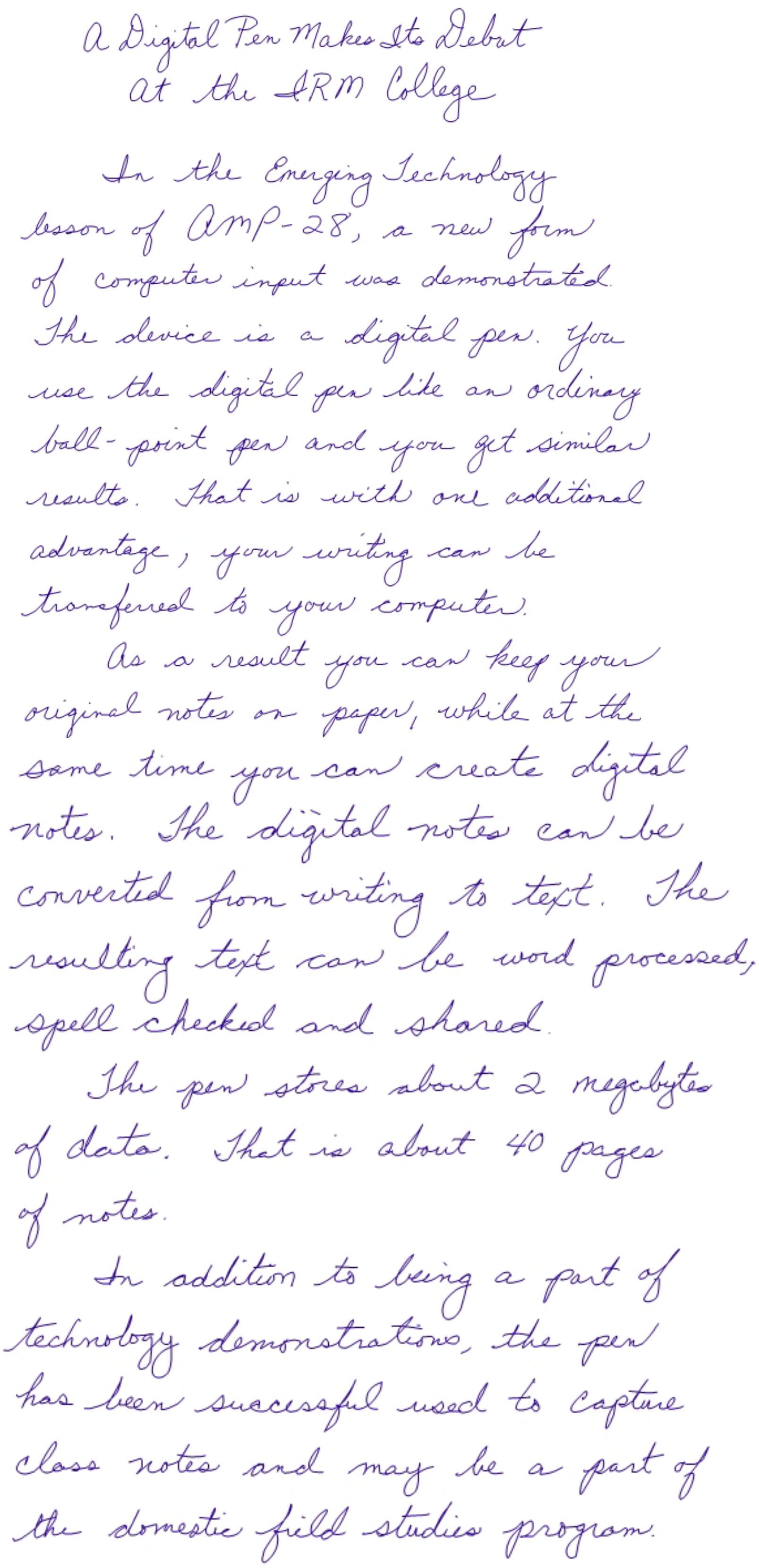
The pen requires special paper with fine blue dots on its surface. The paper and pen work together to store the strokes of the pen in the memory of the pen itself. As a part of testing this pen, Research Assistant Farzana Huq used the pen in a classroom at a local university. She attended class and took notes as usual. The next day she loaded the pen into an input / output cradle. Within minutes she had a digital copy of her notes including a sketch of the brain which was part of the psychology class. In an additional step she converted the handwriting into clear ASCII text. The resulting text can be further manipulated (i.e. spell-checked) using a word processor.

Research Assistant Farzana Huq uses a digital pen to capture handwritten notes.

The pen itself currently sells for $129. It costs about an additional $100 for the input/output cradle which transfers the data to a computer, the software, and a spiral notebook holding the blue-dotted paper. It works and is an interesting concept. At present we feel the pen itself is a little too heavy and bulky for most writers. We hope future pens can be smaller, lighter, and therefore more comfortable. We demonstrate these pens in the Critical Information Systems Technology course that is taught in residence at our home location of Marshall Hall on the Fort McNair campus.

(Continued on the next page)

Here is a comparison of the original notes as scanned by the digital pen and the finalized version which is in digital format.



A Digital Pen Makes Its Debut
At the IRM College

In the Emerging Technology lesson of AMP-28, a new form of computer input was demonstrated. The device is a digital pen. You use the digital pen like an ordinary ball-point pen and you get similar results. That is with one additional advantage, your writing can be transferred to your computer.

As a result you can keep your original notes on paper, while at the same time you can create digital notes. The digital notes can be converted from writing to text. The resulting text can be word processed, spell checked and shared.

The pen stores about 2 megabytes of data. That is about 40 pages of notes.

In addition to being a part of technology demonstrations, the pen has been successful used to capture class notes and may be a part of the domestic field studies program.

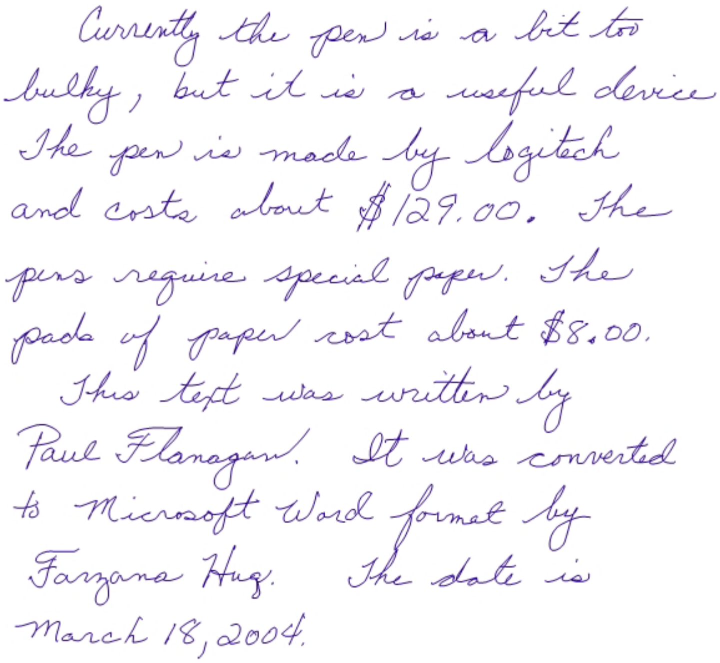
A Digital Pen Makes Its Debut at the IRM College

In the Emerging Technology lesson of AMP-28, a new form of computer input was demonstrated. The device is a digital pen. You use the digital pen like an ordinary ball-point pen and you get similar results. That is with one additional advantage, your writing can be transferred to your computer.

As a result you can keep your original notes on paper, while at the some time you can create digital notes. The digital notes can be converted from writing to text. The resulting text can be word processed, spell checked and shared.

The pen stores about 2 megabytes of data. That is about 40 pages of notes.

In addition to being a part of technology demonstrations, the pen has been successful used to capture class notes and may be a part of the domestic field studies program.



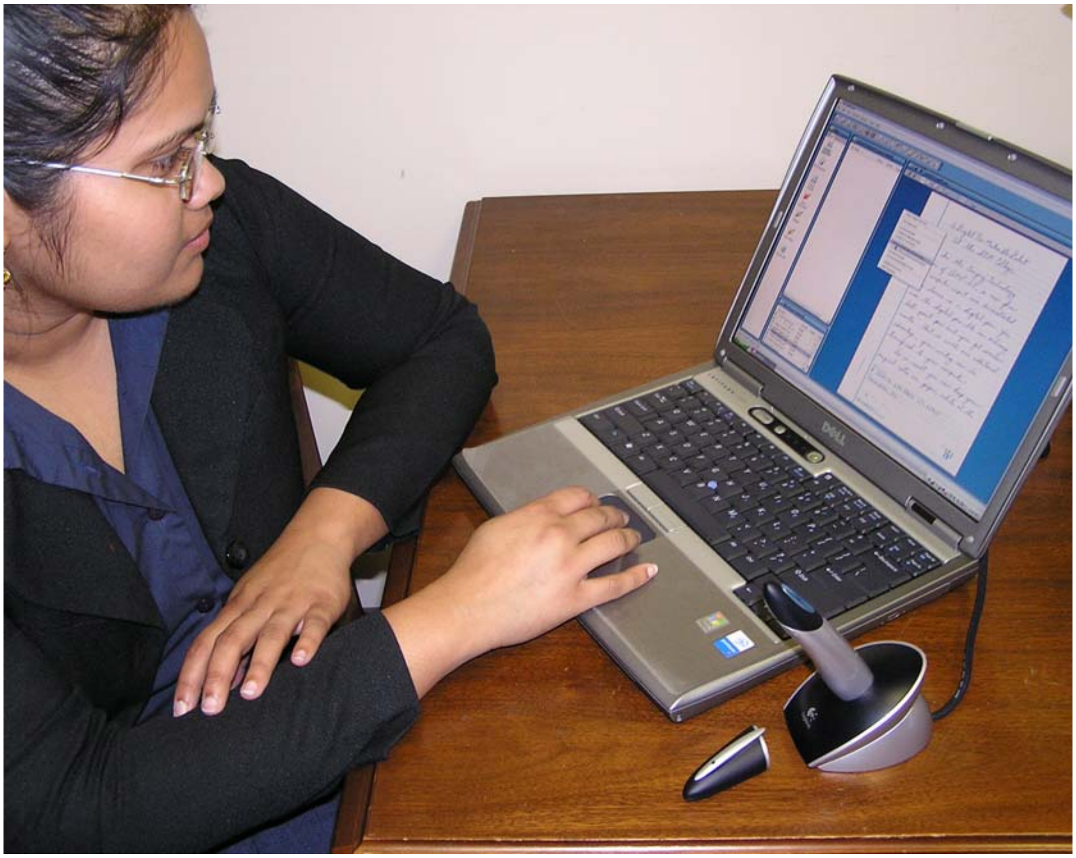
Currently the pen is a bit too bulky, but it is a useful device The pen is made by Logitech and costs about $129.00. The pens require special paper. The pads of paper cost about $8.00.

This text was written by Paul Flanagan. It was converted to Microsoft Word format by Farzana Huq. The date is March 18, 2004.

Currently the pen is a bit too bulky, but it is a useful device. The pen is made by Logitech* and costs about $129.00. The pens require special paper. The pads of paper cost about $8.00.

This text was written by Paul Flanagan. It was converted to Microsoft word format by Farzana Huq. The date is March 18, 2004.

** No endorsement of this product is expressed or implied.*



After placing the digital pen in its cradle, Farzana Huq is downloading the notes to a personal computer where it can be digitized, manipulated, stored, and shared.

Online Student Study Patterns

During a recent international conference, one paper presented the results of research on the study patterns of students attending Central Michigan University (CMU) who were taking an online class in introductory college physics. Homework activity was captured in log files and more information was gathered through surveys and institutional data.

A number of interesting trends were noted in this research:

◊ Students who did well in class tended to submit their assignments early.

◊ Students who regularly collaborated with others tended to complete their assignments earlier and did well in the course.

◊ Those who did not collaborate clearly did very poorly in the class.

◊ Where students lived and whether they had access to the Internet at home did not appear to be related to student performance or homework behavior.

◊ Female students tended to participate in study groups and complete their assignments earlier in the week than their male counterparts.

Study conclusions were as follows:

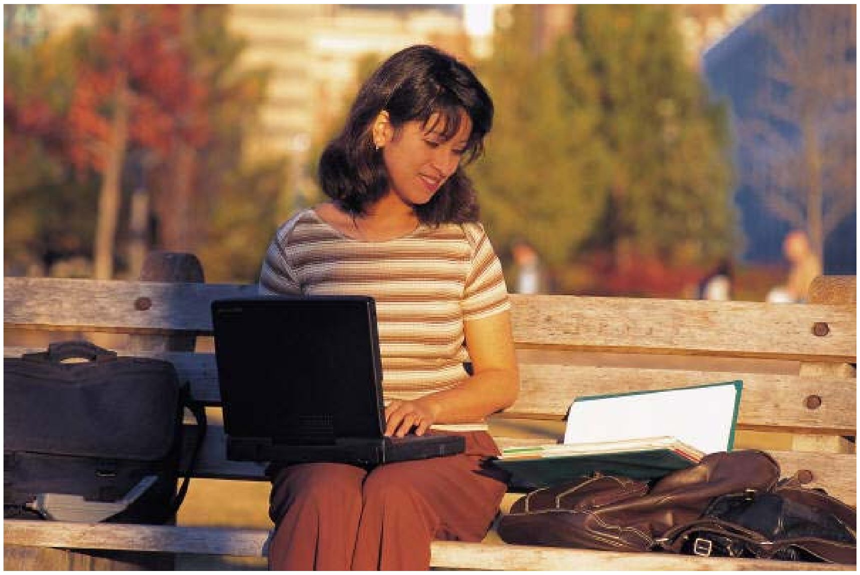
◊ Significant relationships exist between homework behavior and achievement.

◊ Collaboration on assignments is a significant factor related to achievement.

There are several implications of this research. First is the instructor's need to recognize the different learning styles among the diversity of students including gender differences. Second, an understanding of effective time management techniques should be a prerequisite to online learning. Third, an instructor should take corrective action immediately when a student does not turn in his/her homework assignment or turns it in late on a regular basis. Fourth, the need for collaboration needs to be emphasized to achieve success in the classroom.

Can we apply these results to the online students attending IRMC? The answer is uncertain because of differences in students, class size, curriculum, and culture between IRMC and CMU. However, the findings undoubtedly provide some good food for thought!

Reference: Finck, J.E. & P.M. Kotas (2004). Using the Internet to Examine Student Study Patterns. Proceedings from the SSCCII-2004 Conference.



Identity Management and Federated Identity: Keys to Successful e-Government

By Les Pang, Professor of Systems Management

What is identity management?

Identity management (IdM) is the process of managing the information for a person's interaction with an organization's information systems and assets.

There is a key fundamental business shift away from the traditional approach in which a user's identity was managed manually on a system-by-system basis. When a new employee was hired, accounts and permissions were set for the workstation, network, enterprise resource planning system and other corporate applications. Different administrators were responsible for configuring access to each of the different environments.

Today, there are a vast number of applications, platforms, services, and systems that an employee may access. Users have a difficult time managing multiple usernames and passwords. Security vulnerabilities occur when users select poor, easy-to-remember passwords or use the same password at a collection of independent sites. A key challenge is to provide access to external stakeholders such as customers, suppliers, and partners.

Organizations have looked at IdM to manage this complex process and to provide reliable, efficient and controlled access to resources. The goal is to provide the right people with the right access at the right time and prevent the possibility of identity fraud and theft. CIO Magazine estimated that identity theft crimes cost about $221 billion worldwide in 2003.

A new perspective is needed in the way organizations view identity management. It goes beyond resetting passwords and conducting other mundane account maintenance activities. It involves establishing new processes and standards, a new level of relationship and trust, and new technologies -- all of which cross organizational boundaries.

What are the basic components of IdM?

◊ *Authentication* – the process of verifying the identity of a person so that access to protected resources can properly granted or denied. Common approaches include passwords, digital certificates, biometrics, smart cards and smart tokens. These systems may be implemented as single sign-on system, where identity is verified once and access is granted to every application that the user accesses.

◊ *Authorization/Access control* – the process of ensuring that users are given access to applications or resources that are entitled to review or use. Access control can be user-based, rule-based, role-based, or a combination of these.

◊ *Enterprise directory* – a central data repository for holding and managing user identities and access privileges. It can also store rules and policies for the IdM architecture.

◊ *User management* – a collection of systems that support the creation, maintenance, suspension, deletion, and use of digital identities. This includes user self-service and the automation of the user management procedure.

What are benefits of IdM?

◊ *Minimizes cost.* An effective IdM solution can reduce the time users must wait to do their jobs by speeding up the provision process for permissions and access rights.

◊ *Better customer service.* For example, the successful implementation of single sign-on to multiple applications can reduce the irritation of creating user names and passwords for each individual application. IdM will also address the issue of users selecting guessable user names and passwords and repeating them at different sites.

◊ *Improved security.* When employees leave or change jobs, access rights need to be revised in a timely manner, making the organization less vulnerable to risks.

◊ *Reduces the privacy risk.* IdM solution can reduce the risk of privacy breaches. Recent legislation requires companies to safeguard user privacy, to guarantee the accuracy of corporate financial data, and to audit their efforts to ensure compliance. Those pieces of legislation include the European Union Data Protection Directive and, in the U.S., the Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act (HIPAA).

◊ *Personalization.* IdM allows the organization to personalize the content and delivery methods for the user as well as provide an improved self-service environment.

◊ *Infrastructure improvements.* By providing an IdM architecture with reusable integration and security components, an organization can reduce application development time and provide services more quickly.

What are the control risks associated with identity management?

Safeguards are needed at enterprise access points to prevent unauthorized entry and ensure compliance with government-

(Continued on page 8)

Highlights from Gartner's First Government Conference

The following are brief summaries of several key sessions attended by various IRMC professors. This conference was held in Washington, D.C. from May 3-5, 2004. This was Garter's first conference focusing on government.

Keynote Session with Clayton Christensen

The Harvard Business School professor and author of "Innovator's Dilemma" discussed innovation and its capability to disrupt successful business strategies especially in mature markets. He explained if mature industries ignore new, cheaper innovations from the upstart companies, these innovative products will evolve to replace their reigning products.

He gave an illustrative example of how mini-mills in the steel industry incrementally consumed the steel production industry. He also cited examples such as Toyota surpassing GM, Dell over IBM, and Sony over RCA. He listed a number of upstart and potentially disruptive technologies: Linux, Veritas, University of Phoenix, RIM Blackberry, salesforce.com, e-Bay, Sonosite, Amazon and Tensilica. He also applied the concept to terrorist groups which are making an impact against the American military infrastructure which is more accommodated toward addressing Cold War adversaries.

Upstart technologies should be on the radar screen of both established companies and budding entrepreneurs. They can rapidly develop into a competitive threat and dramatically transform the marketplace.

Mastermind Interview with Clay Johnson III

As Deputy Director for Management at the Office of Management and Budget, Mr. Clay Johnson III provides government-wide leadership to Executive Branch agencies to improve agency and program performance. Mr. Johnson stated that his organization's role is to help agencies be successful and define opportunities under the President's Management Agenda (PMA). He is pleased with progress of agencies over the past 3 years based on the Executive Branch Management Scorecard. The Scorecard is used to assess both agencies' overall status in achieving the long-term PMA goals as well as their quarterly efforts in working toward those goals. "Infantile but effective," the scorecard tracks how well the departments and major agencies are executing the five government-wide management initiatives using green-yellow-red light indicators. The approach offers no real penalties for under performance except public shame, humiliation and perhaps a President inquiry according to the Gartner moderator. To access the scorecard, visit: http://results.gov/agenda/scorecard.html

He outlined four things for agencies to be successful:

1. A clear definition of success
2. An action plan
3. Accountability – who is responsible for carrying out the plan
4. Unconditional commitment from the top

Other points he addressed included:

- Consultants should not be given the responsibility of establishing policy.
- The government needs to do a better job in performance-based contracting.
- There is a shortage of high-quality project managers and management competencies at the mid-management level.
- We all need to get a "results-oriented" mindset within the government

Mastermind Interview with Keith Kellogg

Serving as Chief Operating Officer for the U.S.-led Coalition Provisional Authority in Iraq, Keith Kellogg talked about his experiences with the reconstruction of Iraq. Some of the points he made included the following:

- Iraq's infrastructure was much more damaged than what was originally thought ("everything was broken.") For example, electrical towers were down and lines of fiber optic and phone systems often terminated unexpectedly. Also, past economic sanctions had an impact on infant mortality and food supply.
- Iraq citizens still trust Americans but cannot understand the slow progress of reconstruction --- Iraqis stated that, after all, Americans were able to "put a man on the moon." Their expectations were also heightened by the availability of satellite dishes bringing in global television images.
- A key lesson learned was that reconstruction funding should have been provided directly and immediately to Iraqi citizens. Historically, supplying jobs to the citizens help reduce violence.
- "Hire an A team to get an A solution" was his theme in recruiting his cross-discipline management team.

(Continued on page 7)

(Continued from page 6)

- One needs to be on the ground to understand the situation. He was very critical of the current procurement processes used by Government. He said he cannot run a business under the current process. It is time for Government to streamline.

World Leaders Panel

Karen Evans, Administrator of the Office of Electronic Government and Information Technology at the Office of Management and Budget, as well as representatives from the UK, Canada and the State of Virginia, participated in a panel to explore IT topics involving government. Key points included the following:

- There is a shift from a vertical to horizontal perspective in terms of citizen delivery, IT and administrative services. (Canada) Also, consolidation of services such as help desks and payroll systems is a key strategy. (US)
- Government must communicate the value and progress of a program to its constituents and Congress. (US)
- A multi-channel approach is often needed to deliver services. This can be done by establishing a portal using a travel agent metaphor. (UK)
- To achieve success, change starts at the top management level and technology is key in supporting new business processes resulting from the changes. (VA)
- IT will not be an issue in the next election except in terms of how IT can deliver in terms of enabling and supporting public services. (All)

Karen Evans, Administrator of the Office of Electronic Government and Information Technology at OMB, spoke at the Gartner Government Conference.

One-on-One Session with a Technology Guru

As one of Gartner's top technology gurus, Ms. Jackie Fenn identified the top three technologies in the next few years:

1. Service-oriented architectures such as Web Services,
2. Sensors and mesh networks, and
3. Improvements in managing e-mail.

She forsees security technologies making advancements in biometrics, pattern recognition using artificial intelligence, and quantum cryptography.

Open Source Software

There is increasing interest in open source software because of the beliefs that it is quick and inexpensive to implement; it is more secure; and it can be tailored to the organizational needs. In fact, about 63% of European public administrations use open source software. China has adopted an open source software policy.

However, an organization needs to look at the “total cost of ownership” which includes indirect costs such training, support, and maintenance. Also, consideration needs to be made toward migration costs that have often been underestimated, as well as political and cultural factors.

The European Union is exploring pooling open source components across European administrations. They envision this approach to be a service supporting high levels of quality and various languages.

An interesting open source project is the Public Sector Open Project, involving MIT and the Commonwealth of Massachusetts. This project looks at the sharing of open source components in government primarily at the state and local level.

Another project is SAKAI where a number of universities are cooperating to overcome difficulties in sharing course management systems and other tools and gaining cost savings by reuse of open source applications.

Identity Management (cont.)

> Citizens and businesses need to have a secure, simple-to-use and consistent method of proving one's identity to the government and avoid having to keep track of multiple sets of registration data.
>
> - The White House's website on e-gov

(Continued from page 5)

mandated privacy controls such as European Union Data Protective Directive and, in the U.S., the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), and Gramm-Leach-Bliley Act. If an identity management system fails to safeguard privacy, the affected organization may have to pay fines, become legally liable for damages, and suffer a damaged reputation and the loss of customers' trust and confidence. Financial consequences can result.

What is federated identity management?

This refers to the ability to establish trust relationships between various security domains to enable the passing of authentication, authorization, and privacy assertions. This is a key aspect of identity management in the context of business-to-business integration typically when Web services technology is used.

For example, if a company was using Web services to integrate its application with its suppliers, one approach would be to create additional user accounts for all of the eligible users in the various supplier companies. This can create an administrative nightmare for the company – having to manage the plethora of new accounts. One alternative is to implement a delegated user system in which each supplier has one administrative account and is responsible for managing the accounts of its individual users. An issue with this approach is that delegated accounts become more costly as more suppliers are added. Also, the supplier has an additional burden of maintaining the accounts of its users who are accessing the system. Federated identity would address this situation by enabling the suppliers to directly link the user information in each internal IdM system.

What are the primary features of a federated identity solution?

- A single sign-on (SSO) system that operates across different enterprises
- Capability to link and unlink an account in one system to another. This identity mapping feature tells an application that Johnd is the same as Jdoe – and that Jdoe is John Doe and not Jane Doe.
- A basis for trust between systems – having one company trust the information and identity credentials it receives from another.
- A secure system for sharing and managing user authorization data between organizations

What are Web services and why is identity management so important to this concept?

According to Gartner Research, "web services are software components that can interact with one another dynamically via standard Internet technologies, making it possible for enterprises to build bridges between IT systems that otherwise would require extensive development efforts. With Web services, an enterprise's systems can advertise the presence of business processes, information or tasks that can be consumed by other systems, providing immediate benefits to business-to-business and business-to-consumer relationships." Web services can integrate previously incompatible systems and shape a layer of abstraction around their software to support future development and integration efforts.

The key technologies which support web services include:

Extensible Markup Language (XML) - XML provides a set of tags for establishing text formats that allow you to structure data. It allows a computer to generate data seamlessly, read data, and ensure that the data structure is explicit. XML uses tags only to delimit pieces of data and leaves the application to interpret the data.

Web Services Description Language (WSDL) - WSDL is an XML format for describing web services that are being provided between the service requestor and the service provider.

(Continued on page 9)

(Continued from page 8)

Simple Object Access Protocol (SOAP) – SOAP is the web protocol to access services, objects, and servers in a completely platform-independent manner. One can query, invoke, and communicate with services provided on remote systems no matter the remote system's location, operating system, or platform.

Universal Description, Discovery, and Integration (UDDI) – UDDI is a specification for supporting distributed Web-based registries of Web Services. It serves as the "yellow pages" that allow businesses and other organizations to register information about the Web Services they provide so that other entities can locate them.

One of the significant challenges of Web services is to maintain security and privacy when connections are made among the IT systems. For example, service providers need to identify and expose the right Web service to only authorized requestors.

What standards are being used to support federated identity?

Companies have used proprietary federated identity solutions for years such as Covisint for automotive suppliers and Yodlee for financial institutions. A recent development is the incorporation of standards to help facilitate the integration of the different means to implement SSO across different domains. The key underlying standard is the Security Assertion Markup Language (SAML).

Security Assertion Markup Language (SAML) – This language provides the basic definition and structure of security "assertions" that are trusted statements used to communicate authentication and authorization information of a user to a remote service. These assertions contain information about end users, Web services, or any other entity that can be assigned a digital identity. Developed by the Organization for the Advancement of Structured Information Standards (OASIS), SAML 1.0 is a specification for an XML-based security framework that will enable a federated network of identity management for operation across distributed hosted services and websites.

The specification allows instant recognition on determining whether the prospective user is a person or a machine, and what that person or machine can access. SAML documents can be wrapped in a Simple Object Access Protocol (SOAP) message for the computer-to-computer communications needed for Web services. Alternatively, they may be passed between Web servers of federated organizations that share live services.

There are two leading approaches to federated identity that promise to deliver the benefits of a federated SSO solution: Liberty Alliance and WS-Federation specifications. SAML is foundational element of both approaches.

Liberty Alliance – The Liberty Alliance 1.1 standards extends SAML by adding processes for the creation of "circles of trust" where an organization takes on the role of identity provider to manage a log-in facility that is shared among its business partners. Liberty Alliance 2.0 specifications adds significant functionality for sharing user information between organizations and so that the shared information could be used for making decisions on access control.

Established in 2001, the alliance includes about 160 member companies, such as technology suppliers Intel, Sun Microsystems, and Sony, as well as consumer-oriented businesses such as Fidelity Investments and American Express. Membership also includes most of the major identity management vendors -- RSA Security, Novell, Oblix, Sun, Waveset, and Netegrity.

WS-Federation – Similar to Liberty specification, WS-Federation uses SAML as a base and builds upon it a framework for creating a network of trust between parties. Using this model, a token issued by one domain can be trusted by another domain given that trust relationships are set up at the domain level. WS-Federation focuses on Web services while Liberty 2.0 has Web services as a subset of its scope. There is an overlaps with the Liberty Alliance specifications with WS-Federation includes more functionality than Liberty 1.1 in terms of sharing the credentials of the user and in sharing additional user data. IBM, Microsoft, BEA Systems, RSA Security and VeriSign back the WS-Federation.

About fifteen standards are planned under WS-Federation including WS-Security (basic security standards for SOAP messages), WS-Trust (defines the means for establishing trust relationships among web services) and WS-Federation (federated identity using a range of authentication methods). These WS-* standards enables web services to enforce security policies by requiring other web services to authenticate themselves with security tokens such as passwords, digital certificates, SAML or Kerberos tickets.

What is the U.S. Government doing in the area of identity management?

The U.S. Federal Government is committed to having its citizens and businesses access government services using the

(Continued on page 10)

Identity Management (cont.)

(Continued from page 9)

web rapidly and easily. Many of the government web sites require some form of identity verification before a transaction can be made. Citizens and businesses need to have a secure, simple-to-use and consistent method of proving one's identity to the government and avoid having to keep track of multiple sets of registration data. The public should not be expected to complete a separate registration process (e.g., user name, password, or other electronic credential) for each government agency with which they want to conduct on-line transactions. In providing a new authentication system, government agencies should aim to reduce system costs.

The General Services Administration is responsible for the E-Authentication Initiative which promises a trusted and secure standards-based authentication architecture to support the 24 government-wide E-Government initiatives called for under the President's Management Agenda program. This initiative will provide a uniform process for establishing electronic identity and eliminate the need for each initiative to develop a duplicate approach to verify identity and electronic signatures. E-Authentication's distributed architecture will also allow citizens and businesses to use non-government issued credentials to conduct transactions with the government.

The General Services Administration is responsible for the E-Authentication Initiative which...will provide a uniform process for establishing electronic identity and eliminate the need for each initiative to develop a duplicate approach to verify identity and electronic signatures.

GSA has set aside its original plans for creating a centralized government-wide gateway. The General Accounting Office warned that it would be risky for GSA to take on a central role as an online authentication broker. The gateway architecture could not scale to meet the demands of government entities and constituents it was intended to serve. As a result, GSA officials began revising their plans and are now proposing a decentralized, federated approach to e-authentication. The officials plan to focus on Liberty Alliance standards as well as the WS-* specifications.

Citizens will use electronic credentials issued by commercial entities, such as banks, to authenticate themselves. Authorized credential services companies and, in some cases, government agencies will issue electronic credentials to users before they submit address changes to the Social Security Administration as an example.

Approved commercial products for e-authentication must demonstrate interoperability with the SAML 1.0 artifact profile in a federated environment.

(Continued on page 11)

(Continued from page 10)

What are the best practices for identity management?

Identity management systems need to include business rules that characterize the level of access to information for employees based on their role within the organization. Organizations also need to identify ways they can share information freely with their partners without breaching the privacy rights of both employees or customers.

The strength of the authentication method used should be proportional to the value of the data that is being safeguarded. For example, low-risk transactions can be accessed using basic passwords and PINs.

Information being provided must be trusted in terms of accuracy and validity if it is to be shared with other organizations.

Records must be produced and maintained to ensure an audit trail for subsequent investigations.

Anonymity needs to be provided where appropriate. Beyond being compliant with all privacy laws, information controls must meet the privacy expectations of the customers.

Systems need to have the proper controls necessary to prevent identity fraud and identity theft. Identity fraud involves stealing another person's identity for a single transaction whereas identity theft involves multiple transactions where false identity is used for opening accounts, acquiring numerous goods and services, and so on.

What is an example of a successful identity management/federated identity implementation?

To do their jobs effectively, mechanics at Southwest Airlines need timely access to electronic repair manuals maintained by their partner Boeing. Using identity management, the mechanics can get to these repair manuals through their normal logon to Southwest's network via their notebook computer in the maintenance hangar. The implementation supports thousands of users at Southwest Airlines which operates 350 Boeing 737s in 58 cities. Boeing called this effort an implementation of a "seamless business Web" that will streamline business-to-business relationships and illustrate the integration capabilities of Web services.

Boeing now has a centralized, scalable, extensible, and secure standards-based means that it can reuse among its many business partners to provide Web-based access to internal systems. Their single sign-on system used Security Assertion Markup Language (SAML) to streamline access to its MyBoeingFleet Web portal where it supplies partners access to key information to operate and maintain Boeing aircraft.

After logging on to the Southwest Airlines website as normal, the user is passed a Southwest encrypted cookie that is SAML-enabled. When the user clicks on the links to the Boeing manuals, the system initiates the swapping of SAML credentials. Southwest generates a digitally signed SAML assertion that holds information on the user and his access rights.

This assertion is delivered by the browser to the Boeing SAML service, which is located outside the firewall of the Boeing network. The SAML service verifies the assertion and matches it to an entry for that user stored in a Boeing access server. Previously, Web services were used to upload users' identities to the access server. This server supplies a Boeing encrypted cookie that is passed back to the user's browser. The user is then linked to the appropriate application within the Boeing network. The user is authenticated using the Boeing SAML-enabled cookie and provided access to the application behind the firewall.

What does the future hold for federated identity ?

Demand for identity management will continue to grow. Unfortunately, some hardships are expected such as technically complex user name mapping; a number of the vendor products are not as interoperable as marketing personnel will suggest; and

(Continued on page 12)

Identity Management (cont.)

(Continued from page 11)

non-technical issues such as executive buy-in, establishing agreements with partners, passing legal reviews, and risk assessments for the new way of doing business.

The vision for the future is employees, customers, partners, vendors and other appropriate users securely accessing enterprise applications and conducting seamless data access using single sign-on. Customers would be the owners of their profile information and they would decide with whom to share information and to what extent. Enterprises are clearly heading toward attaining this goal.

> *The public should not be expected to complete a separate registration process (e.g., user name, password, or other electronic credential) for each government agency with which they want to conduct on-line transactions.*
>
> *- The White House's website on e-gov*

References

Electronic Government – Planned Authentication Gateway Faces Formidable Development Challenges, General Accounting Office, GAO-03-952, September 2003.

Federated Identity: Seizing Business Opportunities by Sharing Trusted Electronic Identities, RSA Security, Inc.

Identity and Access Management, RSA Security Inc.

Information Security – A Strategic Guide for Business. November 2003. PriceWaterhouseCoopers.

Web Services: 2002 and Beyond. Gartner Report No. COM-15-0588

Websites

http://www.fcw.com/fcw/articles/2004/0322/pol-retool-03-22-04.asp

http://www.nwfusion.com/news/2003/0714boeing.html

http://www.uddi.org/whitepapers.html

http://www.whitehouse.gov/omb/egov/ea.htm

"The views expressed in this publication are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U.S. Government."

Here's Our Web Address!!!
http://www.ndu.edu/irmc/elearning/infotech.html
CHECK OUT OUR PREVIOUS ISSUES!

INFORMATION RESOURCES MANAGEMENT COLLEGE

The World Leader in Information Resources Management Education

300 5th Avenue Marshall Hall (Building 62)
Fort Lesley J. McNair, DC 20319
(202) 685-2096
http://www.ndu.edu/irmc/

Director: Dr. Robert Childs

Dean of Faculty & Academic Programs: Dr. Elizabeth McDaniel

Newsletter Editor: Dr. Les Pang