

Sharing Data Bits and Pieces

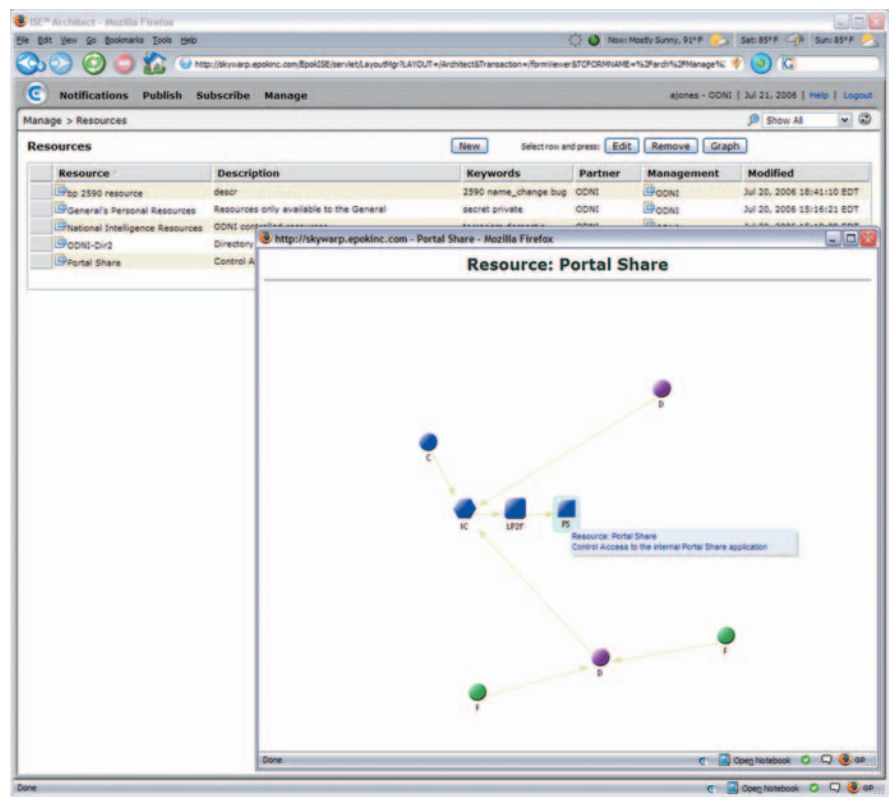
Information owners control who sees what, how and where.

By Rita Boland

New emerging ways to protect electronic data include methods to verify the identity of those who have rights to view specific material as well as to provide access to information through the Internet instead of through hard or soft copies. These approaches reduce the chances of personnel stealing or misplacing copies of confidential records, because data remains in one location. This capability is particularly important as the U.S. military shifts to a network-centric environment and officials look for ways to provide the right information access to the right people while prohibiting that information from the enemy.

Protecting information stored in electronic formats, yet making appropriate data available to allies and partners, has become vital to national as well as personal security. In network-centric operations, technology would allow for human and computer networks that provide information to all necessary parties; however, debates over policy, turf battles and legacy systems often prevent such networks from being put into place.

According to Chris Gunderson, research associate professor of information science, Naval Postgraduate School, Monterey, California, and principal investigator, World Wide Consortium for the Grid (W2COG) and Net-centric Certification Office Initiatives, in order for the government to sur-



Epok Incorporated's Information Sharing Enterprise (ISE) Architect, called AuthorityNet, manages information publication, user subscriptions and community collaboration in an information-sharing environment.

mount the policy obstacle, the government needs tools that allow personnel and managers to evaluate risk and reward quickly and to share information intelligently. Gunderson says the government protects its information well, but government agencies are not as adept at sharing it.

Gunderson works on a special project that studies e-business best practices to import them in process models. The goal is to help the federal

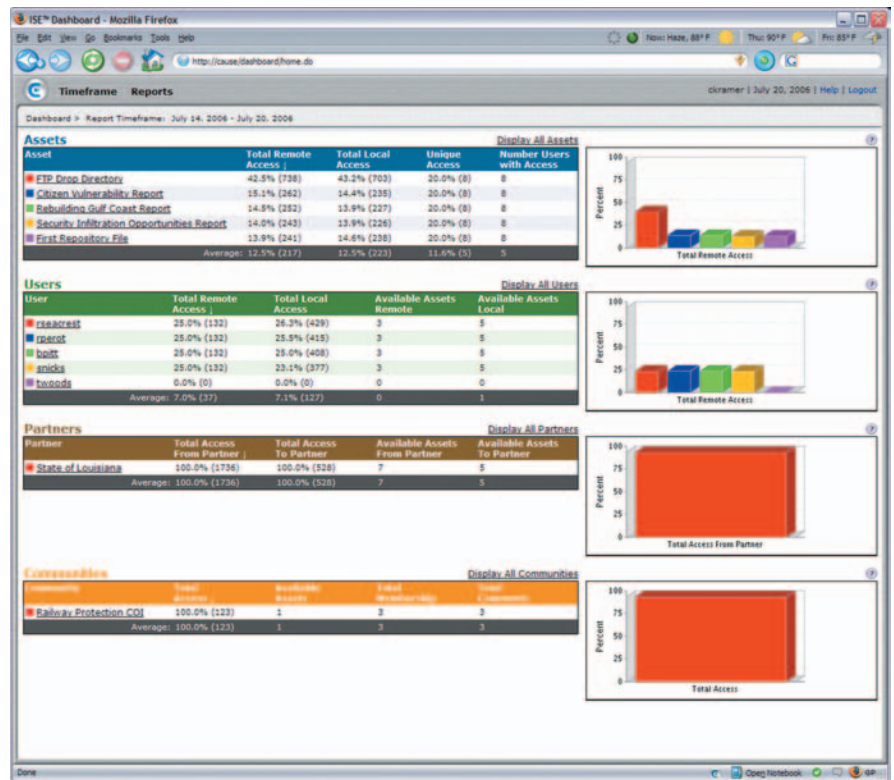
government to influence the commercial development of information-processing technology more effectively. The Defense Information Systems Agency's Joint Interoperability Test Command sponsors his work.

As the government digitizes more tools and processes, security measures for information will become more important, he relates. After events such as the September 11, 2001, terrorist attacks and Hurricane

Katrina, the government learned that various agencies have difficulty sharing information as effectively as they must. Increases in capabilities of technology provide more information all the time and contribute to information overload. According to Gunderson, the government must adopt methods and technologies that enable distributed trusted transactions to deliver valuable information at the right time to meet these challenges.

In addition to the technical capabilities necessary for sharing and securing information, the government needs methods to overcome procedural barriers. According to Gunderson, rather than promoting the current static and monolithic policy, the government should focus more on providing granular security, and it needs a dynamic policy that weighs emergent policy as well as emergent perishability and criticality to determine releasability. This will work only if the government embraces technology and techniques that expose applications and information solely to the users with dynamically authorized access and that provide only information that a busy user would consider valuable, he adds. "Implementing these ideas requires a shift from infrastructure protection to information protection," Gunderson asserts. "We need to shift emphasis from the need to protect to the need to share. All these ideas are co-dependent and equally important."

Developers in the commercial sector have been working on methods to improve security and accessibility. The Information Sharing Environment (ISE) system, developed by Epok Incorporated, Bethesda, Maryland, uses an Internet-based environment called AuthorityNet to control the access to and discovery of sensitive information by distributing access authorization and metadata rather than distributing the information itself. Kristofer Younger, chief technology officer, Epok, explains that AuthorityNet is the main tool his company uses to create the authorization connection between



The ISE Dashboard's window into AuthorityNet audit data interface clearly displays who has access to what, when and with what authority. Key metrics report on the effectiveness of information sharing.

people and resources. "It's a connection authorization layer between organizations," he states.

The ISE system attacks the problems of privileged access by designating authorization instead of information. Users can attach policy at various points in the information-sharing process and require information consumers to acknowledge the terms and conditions if they want to access the data. The system tracks who views the information and who granted access to it. Access can be restricted down to a single Web page.

Organizations can choose to turn off the tracking if necessary for security or other reasons. For example, users involved in black or covert operations might need to remain anonymous. The system is secure enough for Top Secret information to be shared over a Top Secret network but is not intended for sharing Top Secret files over wires secured at a lower classification. "You could easily use it within a Top Secret envi-

ronment and give yourself even more granular control," Younger shares.

To use the ISE, an application called the ISE Architect allows the information owner to log in. The architect enables the visual interface for creating links between published information and individual users and groups. The information owner then decides to share a group of publications under a certain set of conditions and can select a list of partners with which to share it. The login and password are not an issue for the owner. For the user, the viewer organizations' architect applications receive messages when new information is available. The program specifically allows users to create applications and to share subscriptions between business partners.

One benefit of such a system is that information stays at its original Web location, preventing security breaches that result from stolen hardware or lost disks. The location of the information never changes.

The technology also allows content owners to correct their mistakes if they send URL address information to the wrong person or people. Owners can cut the link before anyone accesses the page and reauthorize it for the intended viewers. The servers on which the information resides will allow authorized viewers access and enable the link.

In a standard browser, anyone who tries to view the Web pages behind AuthorityNet will receive a “forbidden” message. “As long as you have a pretty standard Web browser, our technology is a small plug-in,” Younger says. “AuthorityNet invokes itself.”

Epok’s product developers also are working on several application program interfaces so users can plug into custom applications for functions such as accessing images, as well as control access to those items. An alternative to this approach may be to allow guests on the system to view links.

Gunderson believes that technologies inherent in the ISE system meet several of the government’s needs. They attack the problem of providing privileged access by delegating authorization in a decentralized manner. They also keep information at its source—with its owner. “So instead of distributing the information itself, it distributes the authorization to the information,” he explains. ISE also allows the information owner to attach the policy governing information usage directly to the information and can even compel the information consumer to acknowledge those terms before allowing the information to be accessed.

Another important aspect of the ISE, according to Gunderson, is that organizations share information in a natural and familiar manner. They enter into a contract with each other, which establishes a level of trust. Management representatives at each organization take responsibility for their organization’s commitments and determine the individuals within their organizations who need access to the data and which information



Michael Chertoff, secretary of the U.S. Department of Homeland Security (c), and other federal officials are briefed on the U.S. Army’s rapid deployment of mobile communications systems. Systems such as ISE could help resolve some of the information-sharing problems that government agencies experience.

resources they need to share with their partners, he explains.

Oscar Fuster, vice president of marketing and strategic alliances, Epok, explains that several applications commonly available—such as e-mail and other collaborative tools—allow information sharing but in an unsecured way; professionals responsible for enforcing compliance with the terms of the information lose control of the information. With ISE, personnel responsible for maintaining control of data can intervene, so misuse can be thwarted immediately.

By providing detailed access and sharing controls, ISE would enable government agencies to share necessary information around certain policy restrictions as well as allow various levels of government—federal, state, local and tribal—to interact among themselves and with other partners. This capability addresses previous disagreements about whether certain information should be shared because of its classification as either intelligence or law enforcement data. For example, ISE would enable a federal agency to share information with a local agen-

cy for anti-terrorism purposes, or a state agency might share some of its information for counterterrorism purposes but not for law enforcement work.

In addition, the environment permits the same information to be shared with various people for various reasons. Certain federal agencies are prohibited from sharing all their data with state or local authorities; they can share only certain types of information through a third party. ISE provides a chain of evidence that shows that the federal agency first shared the information with a third party. The third party then shares it with a state agency, but only under very specific conditions that were decided beforehand. As a result, information can be reused for many purposes by attaching various restrictions on access to it.

Gunderson says the capabilities inherent in ISE could enhance the United States’ ability to share information with its allies. The U.S. military operates on classified networks available only to U.S. forces and some classified networks available for collaborating with formal allies. Other countries, including coalition

members, cannot use these systems and often operate on the unclassified Internet, as do many terrorists.

“It is extremely painful or impossible to transfer information from one to the other,” Gunderson states. “We Band-Aid the problem by cutting and pasting from the various networks, generating paper products and PowerPoint slides, and ponderously sharing information by sheer brute force. This is despite recognition by all players that streamlined information sharing is critical to success.”

Gunderson believes that if the federal government uses tools such as ISE and

works with companies to improve them, coalition partners could connect when necessary and information owners could control access appropriately. Information partners could then discover relevant data in context.

ISE also has applications in the commercial sector. In the pharmaceutical industry, companies that are competitors on one drug may be partners on another and therefore must precisely and tightly share specific information. Epok officials say there are parallels between this type of collaboration and the work that goes on within the government. “One thing that happens

in both government and pharmaceuticals is multiple relationships with the same people,” Fuster says.

. . . — . . .

WEB RESOURCES

Epok Information Sharing Environment System:
www.epok.net/products.html

Naval Postgraduate School:
www.nps.edu

Joint Interoperability Test Command: http://jitc.fhu.disa.mil/jitc_dri/jitc.html

Reprinted with permission from *SIGNAL* Magazine,
February 2007, Copyright 2007
AFCEA
4400 Fair Lakes Court, Fairfax, Virginia 22033-3899.
(703) 631-6100. Printed in the U.S.A.