GCN

SEPTEMBER 17, 2014

Technology,
Tools and Tactics
for Public Sector IT

DC tests ID management for first responders

By John Breeden II

When an emergency occurs on federal property, responders from different agencies and jurisdictions arrive on the scene to help. Whether it's putting out a fire, inspecting a suspicious package or helping the injured get to a hospital, there are often a lot of boots on the ground and physical access is difficult to manage.

Without good access control, first responders could be walking into a situation they are not properly trained for. Even worse, an attacker could don a fireman's jacket and use the emergency to cover his entrance into a secure facility.

The problem of incident security ultimately will be solved with a nationwide network of standard first responder credentials, according to Karyn Higa-Smith, program manager of the Cyber Security Division of the Homeland Security Advanced Research Projects Agency. As part of the DHS's Science and Technology Directorate, she is working with state and local agencies to build just such a system.

"The idea is that when there is a large-scale incident, responders from state and local jurisdictions will come together," Higa-Smith said. "There will be a long line and a short line. The short line will be for those with identity cards linked into a unified bridge. The long line will be for those who have to go through a manual process like they do today."

But tying all state and local jurisdictions into a single system is not easy. To test the feasibility of such a system, DHS partnered with the Washington, D.C., government to set up a pilot program designed to control access to DC government buildings.

Higa-Smith explained that while the nationwide first responder ID system had been tested successfully in a lab, the DC program provided an opportunity to show it operating in daily use in a real-world environment. Then when an emergency occurs, the system will be ready.

For the access control pilot, DC's Office of the Chief Technology Officer used the open source ForgeRock Open Identity Stack, which it was already using for high-volume queries sent from identity cards to a backend database.

ForgeRock's Open Identity Stack works with any sized population and can use almost any device and token combination. The stack consists of three integrated products: OpenAM, OpenDJ and OpenIDM. OpenAM is a single, unified access management program that provides authentication, authorization, federation, security and entitlements.

OpenDJ is an LDAP directory server that supports Representational State Transfer (REST) for use with almost any device. And OpenIDM is a lightweight user administration and provisioning solution.

In addition, ForgeRock offers Open Identity Gateway (OpenIG), which enables consistent enforcement of enterprise access policies for applications and APIs on premises or in the cloud.

The DC government had already issued cards to its workers and citizens for everything from access to schools and libraries to recreation centers and government buildings, according to Stephan Papadopulos, managing director of The Triage Group, which helped to implement the new system in DC.

ForgeRock's OpenAM was used to tie everything together into a single card. "The local DC government used ForgeRock to manage those identities across many systems, which can be accessed using a kiosk," he said. "Before that, they needed multiple logins and access cards to get into government buildings and IT systems."

Papadopulos explained that government visitors with PIV, CAC or even civilians with PIV-I cards could also use the system to gain access to DC buildings.

"Let's say someone from the FBI needs to go into a DC government building," he said. "They call ahead and have their identity confirmed. Then they are given access for a certain time. When they show up at the kiosk, they do a biometric scan and scan their card. The system reaches out and grabs their credentials and if it all matches up, they are given access to the building."

"Using the installed kiosk reader and controller, we were able to show that not only could the ForgeRock system work for physical access, but also logical access," Higa-Smith said.

The new system in DC can also support access based on conditions. In the example given by Papadopulos, the FBI agent would be granted access based on his credentials, but also because he had scheduled an appointment to be in the building at that time. In a first responder situation, the conditional element would be some type of declared emergency. Firefighters couldn't enter a government building because they were firefighters. An emergency would have to have been declared.

Working out the conditional elements within the system will be a key to its ultimate success, according to Higa-Smith. If there is a hazardous materials spill, for example, operators should be able to tell the system that only firefighters with hazmat training should be allowed on site, which would both maintain security and ensure that only responders trained for the situation are allowed access.

"We want to get to a situation where [access can be controlled by] a law enforcement officer with a handheld device at the physical point of access to an emergency response," Higa-Smith said. "The mobile device will be capable of reading the cards and verifying the identities and authorizations of everyone who responds to that incident, regardless of what jurisdiction they come from."

Higa-Smith says that the Personal Identity Verification-Interoperability/First Responder Authentication Credential (PIV-I/FRAC) Technology Transition Working Group, currently made up of 15 state and local government entities, is studying best practice solutions for PIV-I/FRAC credentials. They are also looking at technology gaps and solutions for sharing attributes with backend databases. Right now, she expects FRAC to leverage the backend attribute exchange system, as FRAC is universally recognized by the emergency and law enforcement communities.

Whenever a first responder completes new training, such as becoming hazmat certified, updating his credentials would allow him access to those situations he is qualified for.

"While some information is kept on the card, the majority of it would be updated in the database," Higa-Smith said. "The handheld device could simply reach out and obtain those credentials quickly in an emergency."

While the first real-world test of the system is taking place in the calm of DC office buildings, the next step will be to conduct pilots and demonstrations for an actual emergency. Higa-Smith said the Federal Emergency Management Agency plans to use a version of the prototype system to control access during the next event. Her hope is that as the successes of the FEMA National Continuity Programs and PIV-I/FRAC working group are shared, more state and local jurisdictions will sign up to be a part of the program, and the identity and access control standards can begin to be deployed nationwide.

About the Author

John Breeden II is a freelance technology writer for GCN.