

Safe and Sure

Oklahoma City finds an easy, inexpensive way to implement two-factor authentication for 5,000 users.

An information system protected by passwords isn't really all that safe. Simple passwords can't ward off invaders who employ sophisticated hacking tools. And longer, complex passwords might actually make a network less secure, not more.

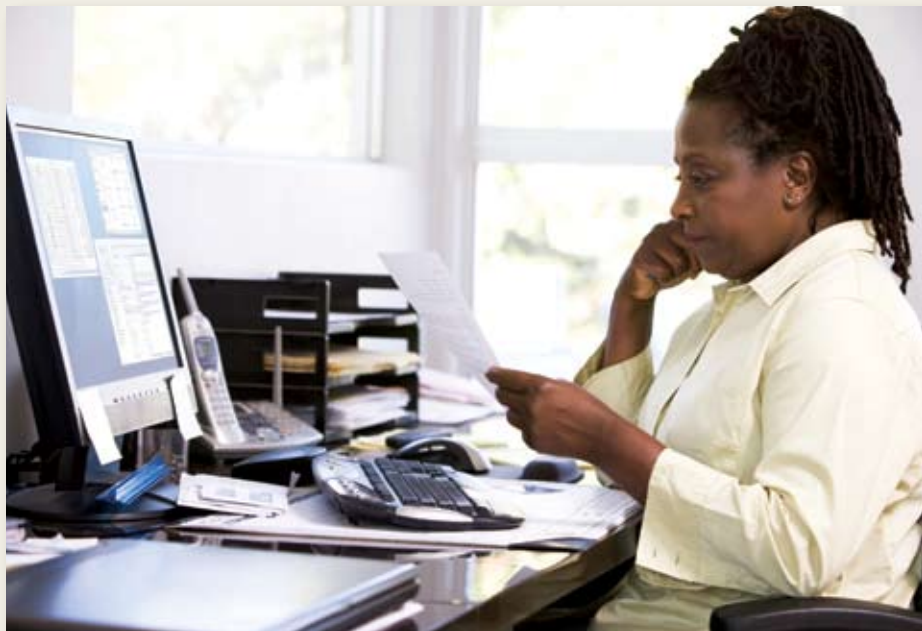
The problem arises when complex passwords become so hard to remember, users have to write them down. "They're sitting there with a sticky note on their monitor containing their password," said Steve Eaton, information security architect for Oklahoma City. The supposedly secret key that unlocks access to sensitive information systems goes on display for all to see.

Anticipating security gaps of that kind, Oklahoma City's IT officials decided passwords were no longer up to the job of controlling access to the city's information systems. Those systems include a 620-square-mile Wi-Fi mesh network that serves more than 900 police officers, firefighters and other city employees. So the IT department started to investigate two-factor authentication.

In two-factor authentication, a user who wants to access an information system must present two distinct forms of identification. The first is something the user knows — often a personal identification number (PIN). The second is something the user has — such as a smart card or electronic token — to prove that he really is the person he claims to be.

Oklahoma City already had some experience with this technology. A small number of city employees used hardware tokens for remote access through a virtual private network (VPN). Those tokens were expensive, though. "They weren't cost-effective to deploy throughout the entire organization," Eaton said.

Smart cards would be less costly, but they raised another challenge. The city would have to connect a card reader to each computer. That second piece of hardware would be cumbersome to deploy, especially on mobile computers.



"Vendors can log in one time and make the fix. When they log out, they can't get back in. So we have better control over our vendors accessing our network."

— STEVE EATON, INFORMATION SECURITY ARCHITECT, OKLAHOMA CITY

City officials then focused on token-based systems. In their evaluations, they considered several criteria.

AD Integration

First, the technology had to integrate well into the city's IT environment. "Primarily we wanted to integrate with Active Directory, so we could leverage our current infrastructure," Eaton said. Oklahoma City already used Microsoft's Active Directory to manage systems and users throughout the enterprise; IT officials wanted to use that same service to manage authentication.

Not every authentication system on the market offers that option. "A lot of systems have their own internal user identification systems," Eaton said. Administrators must

populate those systems with data that already resides in Active Directory. If they can't replicate the data automatically, they have to enter it by hand. "That provides a lot of management overhead," he said.

The city needed an inexpensive system, and one that was compatible with the encryption software it planned to deploy on the wireless network. Also, since 5,000 people would be using the new solution, it had to be easy to implement.

And users had to be able to register their tokens themselves. "That was one part of the deployment strategy that was critical, and there weren't too many systems that had that," Eaton said.

During the registration process, a user chooses a PIN and receives a token. IT

administrators didn't want to know users' PINs, so if users couldn't self-register from their desktops, they would need to visit the IT department to do the transaction in person. Administrators wanted to avoid that cumbersome process.

After evaluating five candidates, Oklahoma City's IT department chose Quest Software's Defender two-factor authentication solution. "It met all of our criteria and more," Eaton said.

One of the extra benefits Defender provides is the ability to use software-based tokens. Instead of carrying a hardware token that generates a random number for the user to enter as a second form of identification, a user can receive random numbers on a wireless phone or other mobile device. "They have BlackBerry tokens that we can issue to a user who might not want a hard token because they travel a lot and might lose it," Eaton said.

"Defender supports such a vast array of options that it provides our customers the flexibility to use whatever works for them in their particular deployment," said Troy Morvant, solutions architect at Quest.

Temporary Passcodes

Another feature of Defender that the IT department found attractive was its centralized help desk. Among other functions, it lets

an administrator issue temporary passcodes to users who don't have tokens. That's particularly helpful if a user accidentally comes to work without a token. "The only option you had with some of the other systems was to send that user home to get their token, or issue them another one," Eaton said.

Not only does Defender solve that problem for employees, but it also offers a way to give a vendor temporary access to the city's IT systems without issuing a hardware token. "Vendors can log in one time and make the fix," Eaton said. "When they log out, they can't get back in. So we have better control over our vendors accessing our network."

Quest's Zero IMPACT implementation process simplified the job of rolling Defender out to all of Oklahoma City's employees. "We can deploy this with little risk to the environment, and definitely no impact on a user," Morvant said. "They're unaware that there's anything new."

To self-register, a city employee goes to a Web site, enters the token's serial number and then enters a PIN. "Once they're registered, we just drop their computer into a particular group [in Active Directory]. They reboot their machine, and the software is automatically installed on their machine," Eaton said. "Once that system comes up, then they're using the two-factor authentication."

One of the key elements that makes Defender a cost-effective solution is Quest's hardware token, which is far less expensive than many competing products. The tokens that Oklahoma City bought for its previous authentication system on the VPN cost about seven times as much as the Defender devices, Eaton said.

Besides charging less for its tokens, Quest — unlike many other vendors — doesn't attach a time limit to its token licenses. "You can keep using ours as long as the battery is working," Morvant said. "We don't require you to buy tokens over and over again."

Also, because Defender works with any hardware token that conforms to the Open Authentication (OATH) standard, Oklahoma City isn't restricted to buying tokens from a single vendor. Using Defender, the city saves money by continuing to use the tokens it purchased for use on the VPN. In the future, city officials can shop around for the tokens that best meet their needs.

Three and a half months after Oklahoma City started implementing Defender, nearly all of its employees were operating on the new system. The transition was smooth, and the solution makes the city's information systems safer. "We've been very pleased with it," Eaton said.

Quest Software

More than 100,000 customers worldwide have selected Quest's enterprise management solutions to improve efficiency, boost productivity, control costs, enhance revenue, ease compliance and reduce risks.

For more information visit www.quest.com
Call 800-306-9329 or Email: DigitalCommunity@quest.com

