GCN

09.15.08

The Technology Authority for Government

CASE STUDY / AUTHENTICATION

One password says it all

South Carolina agency's single sign-on system boosts authentication, security

BY WILLIAM JACKSON | GCN STAFF

DAVID O'BERRY, director of information technology systems for South Carolina's Department of Probation, Parole and Pardon Services, takes his role as a public servant seriously.

"If we are not enablers, we are not relevant," he said.

O'Berry's mantra is increased business efficiency for the 850 users of the department's network. "If I can add one or two minutes worth of savings a day per user, that adds up. I may have to spend some more on the IT side upfront, but I have to drop productivity to the bottom line," he said.

He said he also believes that productivity does not have to conflict with IT security. Ease of use results in better security, he said. "It's not rocket science."

Here's a case in point: passwords. The growth of remote access to applications and other resources hosted online has led to a proliferation of passwords for each user. The more passwords used, the weaker the security, because users create weak passwords or keep them written down for easy reference.

"Users make it easy on their part because we're not making it easy for them to log in," O'Berry said.

The problem is not new, and it is not likely to go away soon, said David Ting, chief technology officer of Imprivata. The typical enterprise user must manage between seven and 11 passwords. "That number is going to go higher as we have more Web services available to us," he said.

O'Berry selected Imprivata's OneSign Single Sign-on to manage passwords for his department's users, supplying the credentials automatically to applications at log-in.

With stronger authentication upfront, passwords for each application can become redundant, Ting said. "Why should the user have to know anything to get into an application if they already have been authenticated?"

That doesn't mean that eliminating passwords is simple. Most enterprises use applications from a variety of vendors and other sources, and the user ID and password combination is the standard method of authentication for logging on to them.

"You had to custom-build applications or you had to do custom scripting and find out where the log-in page was" to consolidate them into a single sign-on, O'Berry said.

The challenge is complicated for O'Berry because of the distributed nature of his network and its resources. For its 850 users, there are just 50 desktop PCs. The rest use remote access with their laptop PCs. The probation department has 56 offices around the state, and also provides network access from 46 courtrooms, where its agents spend a lot of their time. "We support our officers in the courtroom, but we don't own that infrastructure," he said.

Because of the mobility of the computers and sensitive nature of the data they carry, the department has been using whole-disk encryption for about three years, which adds another layer of complexity to the sign-on problem. "Most endpoint encryption vendors want to grab the log-in first and then pass it on," O'Berry said.

Flexible appliance

When O'Berry began looking for a solution to his password problems, he put a premium on simplicity and interoperability.

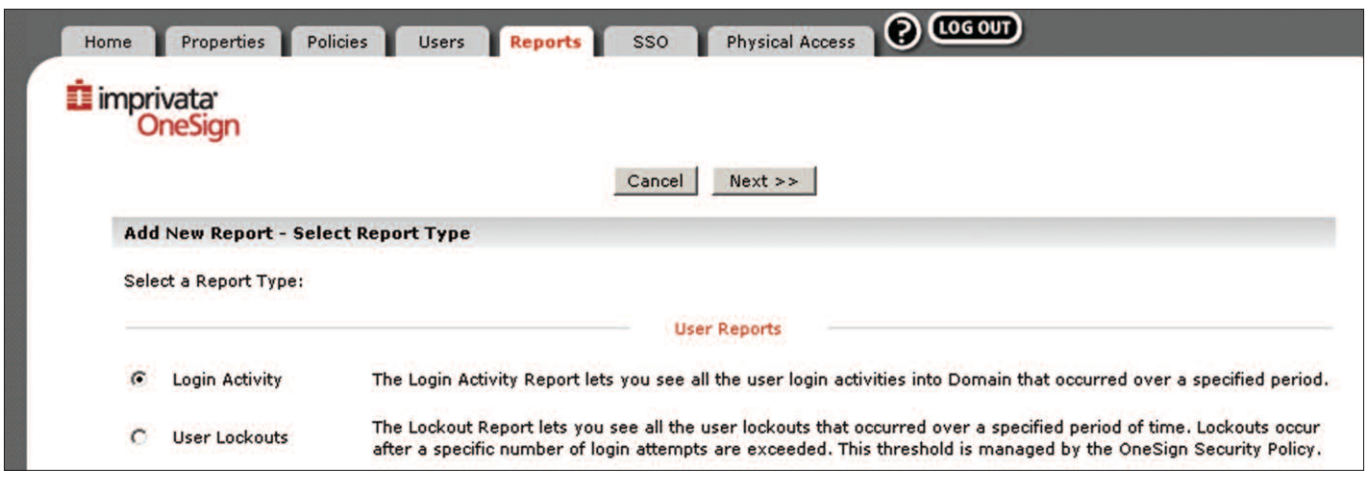
OneSign works with almost any application. The administrator tells the appliance what applications it will be signing on to and imports a user directory. It uses an Oracle 10g database, an enterprise-grade distributed database that can help with auditing and reporting because OneSign can recognize and consolidate a single user's multiple user IDs.

Primary authentication in the department is done through fingerprint readers built into the Lenovo ThinkPad X31 and ThinkPad X61 Convertible Tablet. Fingerprint authentication was the biggest hurdle in implementing single sign-on, O'Berry said.

"The technology has just gotten to the point in the last year that you can log in consistently with the hardware," he said.

The department is using two of the OneSign boxes, one only for backup. "They scale pretty well," O'Berry said.

One appliance can handle as many as 35,000 users and most customers use two for redundancy and load-balancing, Ting said. ■



CENTRAL CONTROL: In addition to helping organizations manage passwords, Imprivata's OneSign provides user access monitoring and reporting capabilities to help demonstrate regulatory compliance.

In the end, user acceptance is the real test

Maintaining security in increasingly complex networking environments requires working with users, not against them, said David O'Berry, director of information technology systems at South Carolina's Department of Probation, Parole and Pardon Services.

"We have to remember that our front-facing stuff matters more than anything," he said.

At the least, a new solution should not add to the user's burden. At best, it should make life easier — which is what single sign-on does. The key is doing the social engineering first.

"Make sure you know what your business needs are upfront" so that the products you buy meet those needs, O'Berry said. "Make sure you're not buying a horse when you need a cow." Get management's buy-in for the program and bring everybody to the table to explain the need for the change and its benefits, he said.

No matter how well conceived, change brings some discomfort, and that should be anticipated. When the probation department adopted a single-sign on product from Imprivata, it also wanted to implement strong authentication that used fingerprint readers so security would not be compromised by removing passwords from the log-in equation. That was not a technical problem, but fingerprint authentication was an additional step that would not be popular with many users.

So the department implemented single sign-on first to give the users a taste of the benefits and added fingerprint authentication later.

"Once it's properly implemented, it sells itself," O'Berry said. "But they have to be rewarded."

— William Jackson