solutions CHANNEL BUSINESS

N° and issue date : 80601 - 01/06/2008
Circulation : 13000
Frequency : Monthly
ChannelBusiness_80601_55_326.pdf
Web Site: www.channelbusiness.com
Page : 54
Size : 85 %

Then there was one

Smarter, safer and exponentially easier for users and admins, Single Sign-on (SSO) answers almost every security question raised. So why aren't more companies deploying it then? By Adam Oxford.

With decades of history behind it, Single Sign-on (SSO) technology can hardly be called the next big thing. It is, however, rapidly becoming a 'must-have'. A change in direction for security buyers is coinciding with a new generation of technology used to create systems that offer security, ease of use and provable ROI. Believe the hype and it sells itself, once you start trying.

Depending on the survey data you read, the average employee has somewhere between five and ten separate passwords for essential business applications that they use on a regular basis. That's not counting Gmail accounts, Facebook log-ins or internet banking details, although all three of those activities make up a fair part of the working day too.

That's as things stand now. The nature of security is changing, though. Historically, perimeter defence of firewall and network log-in has been all important, keeping unwanted guests out of the system. In the minds of CTOs, though, that's changing, and fast.

For a start, the perimeter is collapsing under the pressure of the always connected worker, who's on the road or at home with his or her laptop. More importantly, the institutional data breaches which have hit headline news recently haven't been script kiddie crackers or gangs of heavily organised cyber criminals, they've been a result of 'insider threat'. People with legitimate access to systems who, through malice or negligence, have caused havoc.

Insider man

Ian Kilpatrick, chairman of security distributor Wick Hill, says that the locked front door method of current infrastructures simply isn't good enough any more.

"Insider threat represents between 70-80 per cent of all threats now," he explains, "That's not just criminal hacking, it's the misuse of information people have available to them. If you allow people access to areas on the network or applications that they don't need, then after a period of time they begin to become complacent about it and do things which are potentially criminal just because they have access to it."

It's not unusual when working with a large client, he says, to be standing in an office while someone shouts a manager's password across the room. Likewise employees who move around a company are likely to find that their access to critical systems they no longer need remains unrestricted.

Companies need to face up to a simple truth: the laissez-faire attitude towards security has got to stop. On top of the high level of risk exposure these behaviours lead to, legislation around data and fraud protection is tightening, further forcing their hand.

People are generally resistant to heavy handed encryption, though. Having to password protect everyday documents to share amongst a particular workgroup, for example, is a laborious task, and the more separate logins employees are required to remember, the more chance that they'll choose weak passwords or ones that are very similar to each other. Worse, they'll write them down on pieces of paper stuck to their desk.

Old habits

The UK sales manager for enterprise security at Aladdin, Gregg Hardie, recalls this anecdote about typical user behaviour.

"We spent a lot of time with one high level government department to make sure they had all their laptops encrypted, and that they all went out with very strong passwords [a mix of alpha-numeric characters and punctuation points]. What enterprising employees did, because they didn't like strong passwords, was to actually write those passwords down on a piece of paper, laminate it and keep it in their laptop bags."

The proliferation of multiple logins also compounds a second problem facing any business of moderate size. It's estimated that anywhere between 30-50 per cent of calls to internal helpdesks are requests for password resets from users who've forgotten their details or are struggling to access an essential system.

"If you attribute a cost to the phone call as being typically between £50-£100," says Hardie, "Then if you can significantly reduce the number of calls coming in, then you can free up staff to do something more useful than reset passwords."

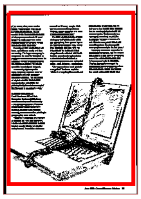
The simple sell

Given that employees are less likely to forget or lose one password, then, there's a strong ROI story in the reduction of helpdesk costs alone. The shift from a 'locked front door' mentality of generic log-ins to Network Access Control (NAC) based on user identity also combines the increasing number of automated tools for setting and revoking multiple application and service privileges makes SSO an elegant solution to a multitude of security problems.

There have been historical problems with cost and complexity for Single Sign-on, though.

"Any company over about a thousand users," says Kilpatrick, "Will have had somebody investigate SSO in the past. But most of the implementations they'll have heard

Copyright (Channel Business Solutions) No reproduction without authorisation



of, or worse, tried, were service based. Traditionally it was 80-90 per cent service based, and if I wanted to do 10 applications across a heterogeneous network I'd need to get in a really expensive coder from the vendor and they'd have to individually code each one."

Creating an SSO environment has been, up until now, costly and time consuming. The larger a company is, the greater the need for SSO; but at the same time the more likely it is to be running a number of legacy systems on obsolete hardware that require specialist knowledge to integrate.

"Historically, big companies have done what they had to do for compliance and then stopped," Kilpatrick continues, "I'm not aware of anyone who has implemented an organisation wide SSO. Yet philosophically the whole concept of SSO is that it is organisation wide."

Smarter integration

David Tomlinson, MD of Data Encryption Systems (DES), likens network security to airline security – the ad hoc integration of systems which weren't designed to work together, let alone work together securely, means retroactive patching is always going to be difficult.

"Security in airports at the moment is catching up - it's after the event. Had air travel been designed with the kind of security measures required today in mind, it would be a lot more streamlined. It's very easy to think you've understood the problems involved, design a solution and miss some fundamental aspect."

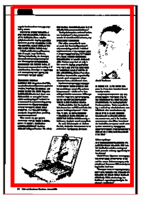
The DES solution is based around storing up to 64 passwords, which can be anything from system logons to document encryption files, locally on a protected USB key. This not only relieves the pressure of true integration with software front ends, but also provides strong two factor authentication in which both a memorised password and a physical token – the USB stick – are required.

"Our approach has been granular encryption," Tomlinson explains, "Which is encrypting files, emails and discrete items on demand. For the last year or two there's been this push that we must equip laptops with full disk encryption. That prevents you from doing something stupid, like leaving your laptop in the back of a taxi. Granular encryption lets you do something clever, like sharing with other people securely in the first place."

Hardware tokens are expensive to distribute and replace, but it's easy to argue that the total cost of ownership over a few years can be recouped in those saved calls to helpdesk. They're also easily managed by automated back end systems, which can dynamically renew and update the actual passwords stored on a

Copyright (Channel Business Solutions) No reproduction without authorisation

solutions CHANNEL BUSINESS



N° and issue date : 80601 - 01/06/2008
Circulation : 13000
Frequency : Monthly
ChannelBusiness_80601_55_326.pdf
Web Site: www.channelbusiness.com
Page : 56
Size : 85 %

regular basis without the user even being aware.

Importantly, argues Tomlinson, it also puts security back in the hands of the managers. Since only the people involved in sharing a sensitive document or email are involved in the key exchange, even IT staff won't be able to gain access 'accidentally'.

"I don't want to take anything away from IT people," says Tomlinson, "But they're facilitating the delivery of information: the people working with that information should be deciding what's sealed and who can read it. At the moment, anyone who's working in IT administration, who might be disgruntled and one day away from leaving, has access to all his boss' emails."

Appliance science

Traditional SSO integrators, like RSA, are also threatened by newer appliance vendors. Imprivata, for example, has created a black box which plugs into a corporate network and stores user passwords in an encrypted format which can't be pinged, installed into or accessed via command line, unlike a secure server. Rather than trying to synchronise and secure active directories, the Imprivata OneSign simply sits alongside them providing access as requested.

"That means we can put this structure in without having to modify any of the servers, desktops or network applications" explains Imprivata's Wayne Parslow. "It's utterly non-invasive, and adds an extra level of security to the password database."

The Imprivata system, reckons Parslow, can be deployed in days, compared to months for a traditional SSO solution, and is much easy to administer.

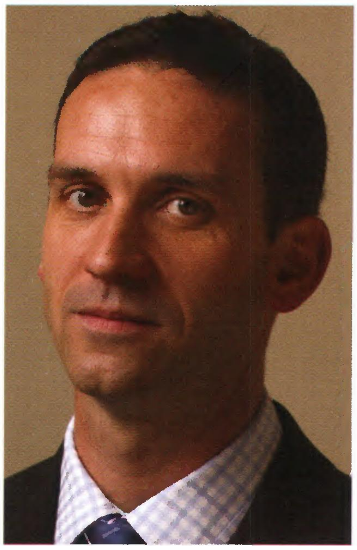
Part of the reason for its ease of use is that the OneSign doesn't rely on scripting code for individual application front ends. Instead it uses a pattern recognition algorithm based on a log-in screen's appearance and code base to provide password data. Parslow says that not only is this easier to deploy, since the box only has to see the front page once to recognise it again, it's harder to fool with phishing attacks than other solutions, because the page identity is made up of many more unique elements than a few lines of code.

Imprivata's system uses two factor authentication based around a USB key containing a smart chip and one time password – similar to the best selling of Aladdin's solutions. USB keys are more expensive than smartcards, but can be deployed more widely without buying-in special readers.

Parslow explains that the key itself can also contain an RFID coil to double up as a building entry card – this is vital, he says, as more companies in the financial sector especially are finding that location-based security is necessary simply to remain compliant.

He uses the example of Jérôme Kerviel, the junior future trader who defrauded the Societe Generale of almost 5bn Euros earlier this year, to show how location-based security works.

"It is pretty widely known that one of the pieces of information that he had was three or four other people's credentials into the trading systems," Parslow explains, "So he was able to log in and set-up a trade between two individuals who were both actually him. In order to do that he had to move around. In the front office he was one person, and in the back he was someone else. When he entered the back office our system would have queried the building management system and double checked that the ID trying to log in was physically present in the room."



David Tomlinson

Other options

All of the companies we spoke to are predicting strong growth for SSO over the next twelve months, and agreed that it presents a strong opportunity for the channel.

Wick Hill's Ian Kilpatrick summed up the current state of the market for us, and the reason that encouraging early adoption of these new SSO techniques is good for business.

"The opportunity for the channel is to get in early, because it's a great add-on sale and it still has an aura of perceived complexity. While a technology has that there's a great opportunity for the channel to add value."

Copyright (Channel Business Solutions) No reproduction without authorisation