

Rs 100

PCQUEST

Build your Own UTM Appliance

Strategies to Manage Datacenters

UNDERSTAND CHOOSE IMPLEMENT IT

MAY 2007

Subscriber copy. Not for sale

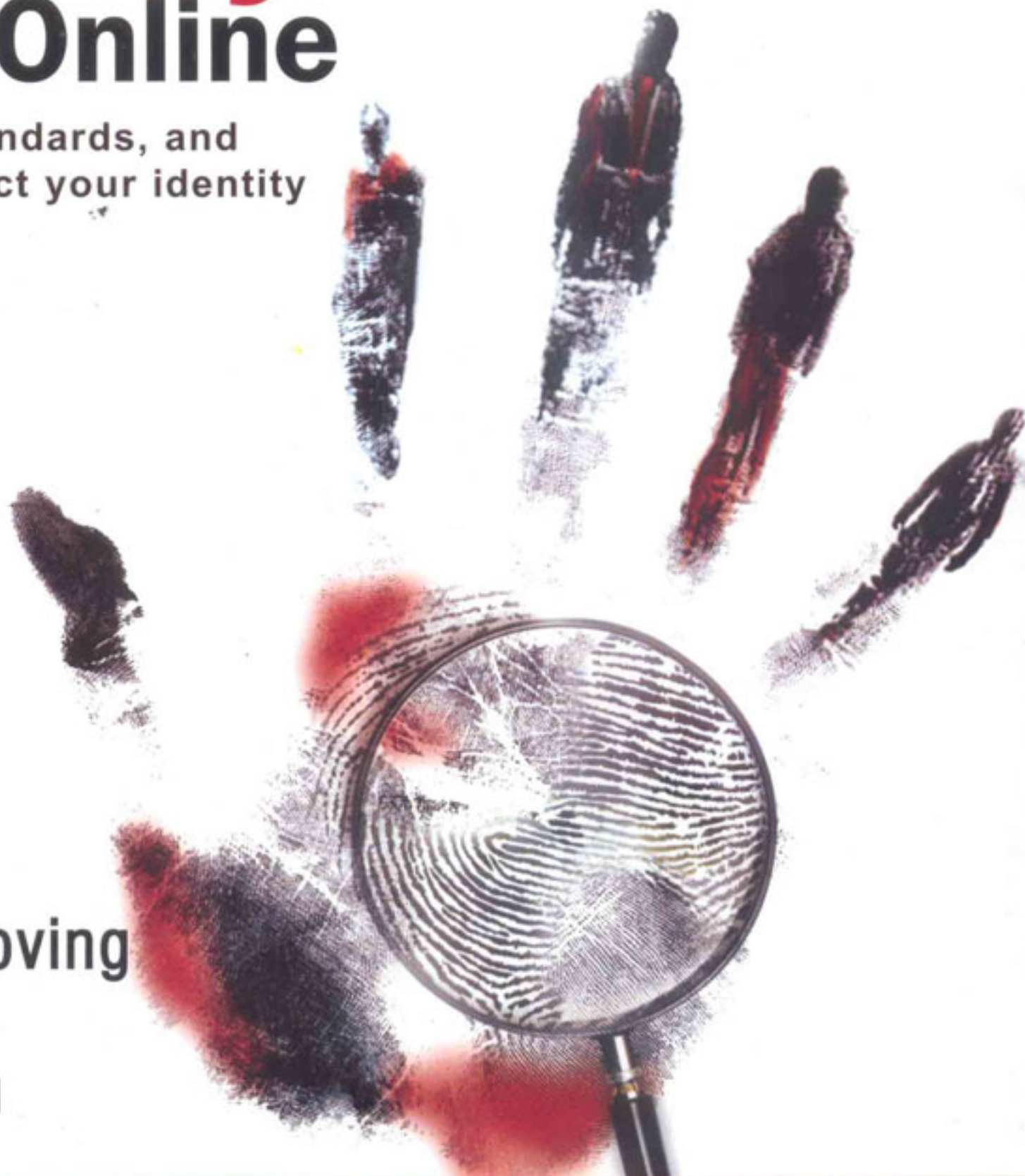
A **CYBER MEDIA** publication

Preventing an Identity Crisis Online

Technologies, standards, and products to protect your identity

Healthcare:
IT's in the Blood

New Age Graphics: Moving Closer to Photorealism



Laser Printers Buying Guide

Key Trends in Mobility

Troubleshoot your Network with Protocol Analyzers

If your disks are missing, please ask your newsagent or e-mail rsepcquest@cybermedia.co.in

www.pcquest.com

Preventing Identity Crisis Online

The number of online frauds is rising, and the prime reason for that is identity theft. End users need to take more precautions, and organizations need to consider deploying identity management solutions. In this story, we cover the key trends, technologies, standards and solutions for identity management of both individuals and enterprises

Anindya Roy and Swapnil Arora





For an end-user Identity management is about keeping his identity safe online. And as the nature of online frauds is shifting from technical to social in nature, it becomes more and more important for a person who has a decent net presence, to manage his ID properly.

We take a very live example of why ID management is necessary for an end user. Let's assume that Mr. Bean Patrick, the chairman of Olive Inc. has created an account on Yahoo and has added his photos and relevant details to that profile. Now one fine day he goes to orkut.com and does a random search for his name. He finds that a profile with his photo, name and vital details, already exists on orkut, but it hosts a lot of pornographic content and obscene language.

How did this happen needs no explanation. But think about the consequences. Not only is that becoming unpopular, but his reputation could also be at stake in the place he works. This is one of the reasons even ordinary users need to be aware of identity management.

If we shift focus towards enterprises, then identity management there is a completely different ballgame there. There are identity management solutions meant for enterprises as well, but implementing them is no bed of roses. For enterprises ID management is about managing three things: User provisioning; Single Sign On and User Access Control. And if any of the above three fails, ID management can't work for an enterprise. In the pages to follow, we will look at various technologies and standards available in identity management, how to protect your personal identity, and we'll even look at some deployment scenarios for enterprises.

Identity2.0

In real life you can prove your identity by showing your license, PAN card and other authentic government documents. But how do you prove your identity online? When you provide your details online by filling up an online form, the website has very few ways to determine whether your credentials are correct or

FAQs on Online Privacy

Question 1: If the Bank or transaction site shows a lock icon at the right bottom of your browser, and the address consists of "https" then is it supposed to be a safe website?

Answer: Not necessarily. It might be that the site which you are accessing is actually phished and the certificate (which shows the lock icon) of the site is also fake. Creating such a fake certificate is not at all rocket science and someone who has basic knowledge of website designing and web hosting can do it very easily.

Question 2: Then what should I do to make sure that the site I am accessing is authentic?

Answer: It is not sufficient to just check whether the Lock icon is there in the browser or not. You should also double click on the icon to check and verify the certificate of the site. If the site has a fake certificate then double clicking on the lock icon will pop up a Window that will have a cross sign on the certificate header. This should immediately ring alarm bells that you're accessing an unsafe site.

Question 3: Is it safe to use banking and financial websites from Cyber Cafes?

Answer: Not really, because it's very easy for the owner of a Cyber Café to capture all data that is going out from your machine. A person with malicious intent on the same network can easily play around with the gateway (which is not very secure in this case) and can redirect your entries to any phishing site by running attacks such as arpspoofing and dnsspoofing.

Question 4: How safe is online shopping with your credit card? Is it safer than shopping with a physical card?

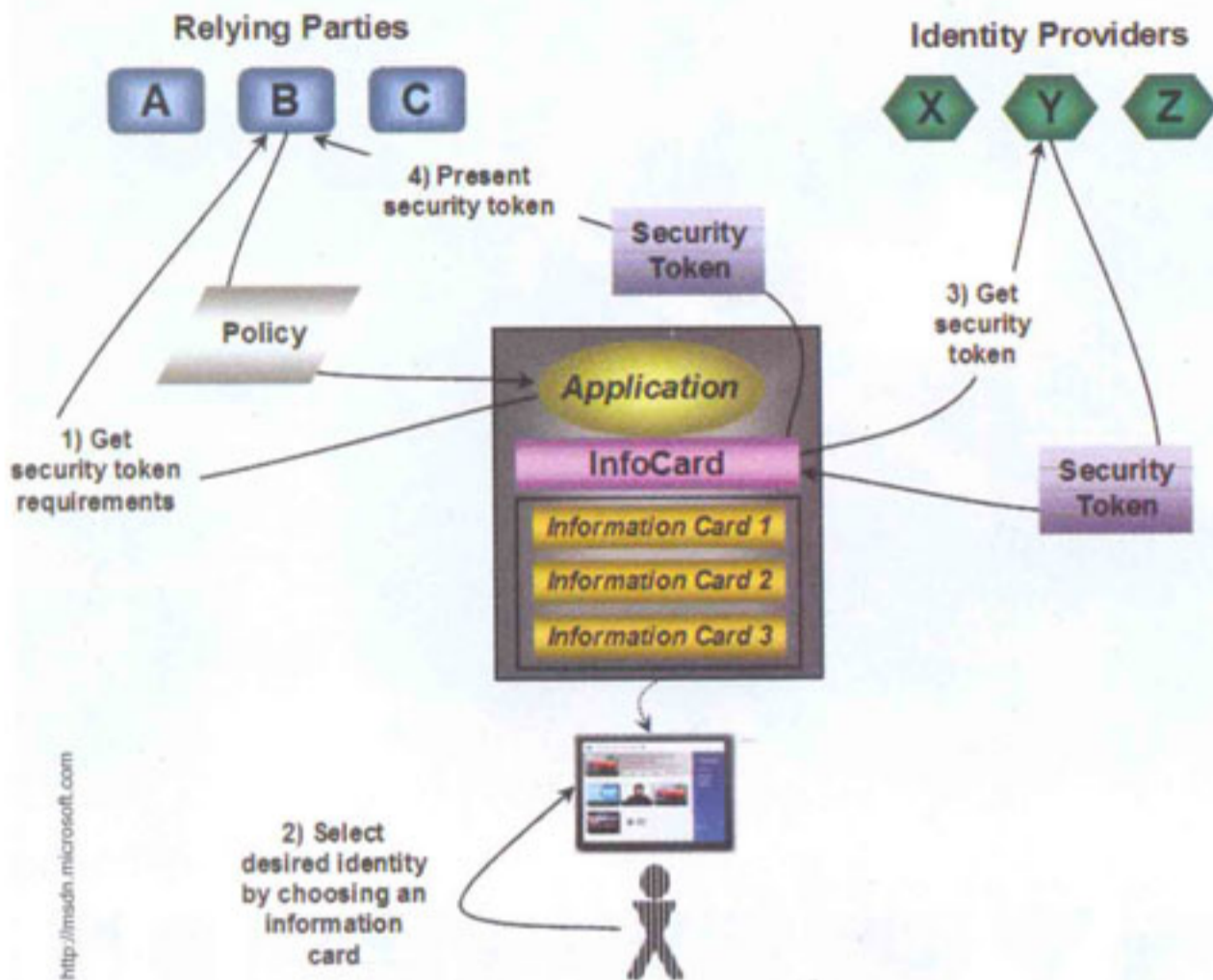
Answer: Contrary to belief, shopping online is much safer than shopping with a physical credit card. The reason for this is simple. When you shop with a physical card, you're leaving an imprint of your card's details with the vendor. The vendor could then use this to pose as you online and shop. There have been many such cases of fraud, indicating that it's not safer to shop with your physical card against shopping online. When you do shop online, then at least your credit card is with you both! The only thing you have to worry about is a fake website, but then there are many precautions you can take to ensure that. Many banks also have worked out various mechanisms to help ensure the safety of your online identity. Of course, one also presumes that the machine you're using yourself is free from all malware.

not. Identity 2.0 claims to provide identity verification on the World Wide Web using OpenID standards. In identity 2.0, a user controls his identity, also known as user a centric model.

The term identity 2.0 was made popular by sxip.com, who have also developed some tools related to identity 2.0. Microsoft is also in this space with Windows Cardspace, also known as infocard, that we have talked about later in the article. Another popular Identity2.0 model is OpenID. Then there are IBM and Novell supporting an open source project called Higgins managed by Eclipse Foundation. Higgins will provide an easy way through which many identity management systems will be able to interact. All of these together and some other players are supposed to make identity2.0 happen. Right now there are not too many websites supporting identity2.0. For instance, not even Microsoft is supporting infocard yet, for eg MSN. Lets start with OpenID first.

OpenID

OpenID is a decentralized URL based identity management system in which every user is identified by a URL just like websites. In openID architecture, once you have acquired an OpenID from any of the OpenID identity provider, this openID will be your username when you go to an OpenID enabled website. The OpenID enabled website will send you back to your openID provider where you will have to authenticate yourself. Once authenticated, the provider will send you back to the website ▶



source: <http://msdn.microsoft.com>

How Windows CardSpace Works

with the information required for logging in. This is a like a single sign on over Internet and saves you the hassles of registering with so many websites and remembering all those passwords and other information. In the OpenID framework, users can control

what part of their identity is shared by the identity providers like thier name, phone number, e-mail etc.

Windows CardSpace

This is also made to replace usernames and passwords and the registration forms that need to be filled on every website. When a digital identity is sent over the network, it uses some kind of a security token. A security token is made of a collection of claims about that identity. A claim can be a username or first name, last name, address, e-mail, phone no, etc. Now to prove that all these claims belong to the user, a password is sent with the claims or some parts or all parts of the claims are digitally signed using a private key.

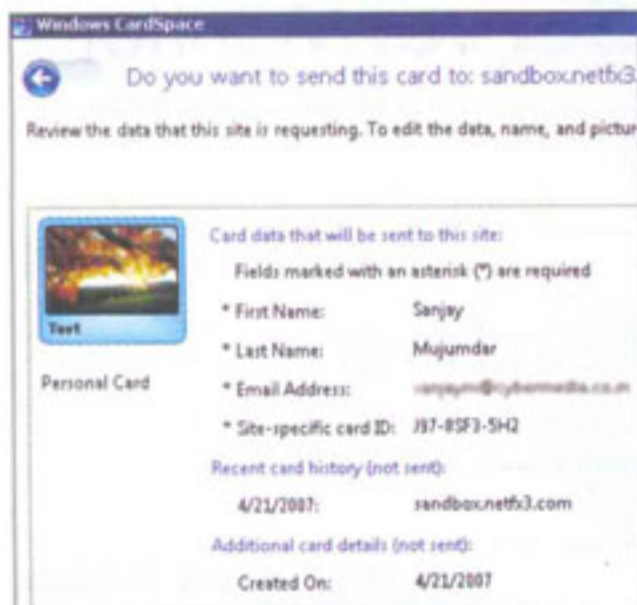
The information card can contain various things such as an im-

age files which can be a photograph of the user, data and time of when was that information card created. So, what if you are using infocard on your laptop and it gets stolen? In that case your infocards are stolen along with their identity provider. According to Microsoft, all information stored in cards is encrypted and you also protect it with a password. Also the user will have the choice to manually inform organizations about the loss of the card and cancel accounts at every relying party.

CardSpace is built in Windows Vista and add-ons for Windows XP and Windows 2003 server are available. To use CardSpace you will require IE7.0 and .net framework 3.0. In vista using Cardspace is simple, just go to the control panel and open Windows CardSpace.

Now click on Add card, a wizard will appear, just follow the wizard and your infocard is ready. Now when you go to a website which accepts information through CardSpace, you can choose to upload your infocard instead while filling up the form. Windows Vista will issue a pop-up telling that particular website is trying to get your infocard, once you allow it, you will be signed-in using your infocard.

Similar to infocard is Sxipper, which is more like a form filler but lets you multiple identities. Whenever you go to a website, it pops up asking you which identity you would like to use to fill up the form. It will then automatically fill the form and submit it. Here also you, you are the identity provider. Sxipper's firefox extension can be downloaded from Sxip's website. ▶



In Windows CardSpace, you can have an infocard through which you can transact online

Using Cyberoam for identity based access control

Let's say that you have deployed identity management solutions in your organization and have enabled features such as SSO, access control, user provisioning. Now one very important thing which you require here are granular policies based on users for your security devices. For instance, how do you make it possible for your HR team to access job sites from your organization but at the same time disallow the same job sites to normal users. Or let's say if you are a school or a college, how to make sure that, students below 18 years should not be allowed to visit certain websites.

The traditional method requires you to set machine level or IP level policies defined at your

level of content filter or bandwidth shaper. But now we have more options. Take for instance the UTM device from Cyberoam which can do user level filtering. It provides policy-based filtering that allows defining of individual filtering plans for various users in the organization. It lets you assign individual policies to users (identified by IP address), or a single policy to a number of users (Group). User level authentication can be performed using the local user database on Cyberoam, or it can be integrated with ADS and LDAP. It is well known that stronger the policies implemented, the better is the performance given by the device and also harder is the device to bypass. By default, Cyberoam has plenty of policies for bandwidth management. It has at least one policy for every situation. Surfing Quota

policy lets you define the duration of Internet surfing time for particular users or a group of users. Internet policy lets you specify which user has access to which sites or applications, ie, you can deny access to messengers and offensive websites. All these policies are pretty easy to configure and manage. All configuration and reporting is done through a Web console.

This appliance also lets you view the live connections in a network. You can view live connections either application wise, or user wise, or LAN IP Address wise.

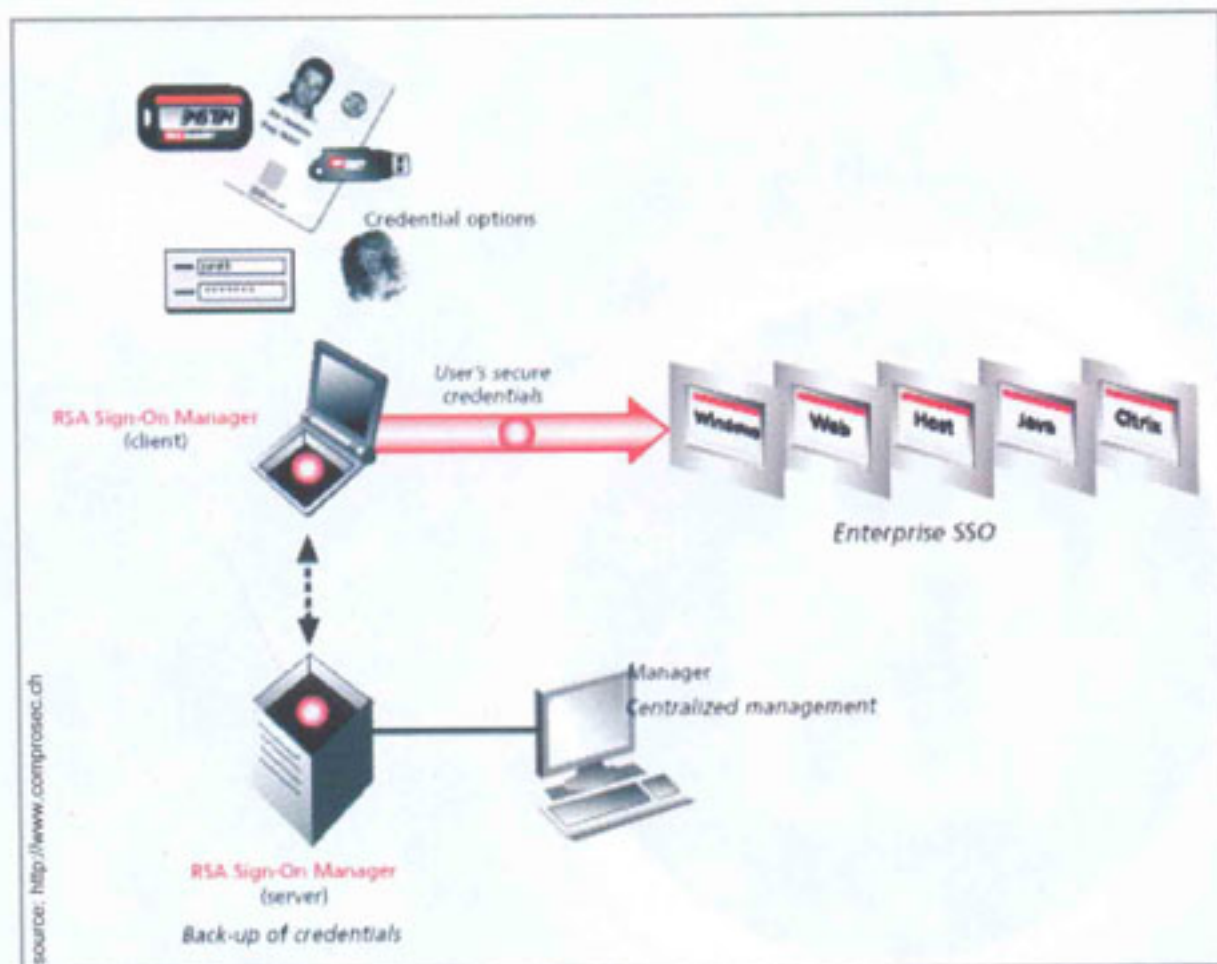
Data transfer and bandwidth usage details of every connection can also be seen. The Cyberoam box also provides detailed reporting. By default, it creates seven reports, which include reports for web browsing, cache reports, mail usage, Internet usage and printer usage. But the benefit here is that you can generate reports based on the users. For instance you can actually create reports where you can see which person is visiting which website or sending how many mails per day. This makes user auditing a breeze.

Ilantus Password Management Portal

This product is a self service account unlock and password reset tool for Active Directory. With this software, any user can login to its main console, authenticate himself by answering a few questions and then reset the forgotten password. The benefits of the product include reduced help >

Manage Live Users						
Concurrent Sessions: 117		Tue, Jan 10, 02:45 PM		Next >>		Show
User name	Name	Connected From	Public IP	Start time	Time (H:MM)	
ben (S)	Ben Taylor	192.168.1.165 /	206.72.135.195	Tue, Jan 10, 12:45 PM	01:	
biren	Biren Patel	192.168.1.175 /	206.72.135.195	Tue, Jan 10, 12:45 PM	01:	
denise (S)	Denise Butler	192.168.1.179 /	206.72.135.195	Tue, Jan 10, 12:45 PM	01:	
dennis (S)	Dennis Deacon	192.168.1.132 /	206.72.135.195	Tue, Jan 10, 12:45 PM	02:	
edward (S)	Edward Morrison	192.168.1.163 /	206.72.135.195	Tue, Jan 10, 12:45 PM	01:	
fangyin (S)	Fangyin Zhou	192.168.1.190 /	206.72.135.195	Tue, Jan 10, 12:45 PM	01:	
frank	Frank Connor	192.168.1.103 /	206.72.135.195	Tue, Jan 10, 12:45 PM	01:	
fred (S)	Fred Billings	192.168.1.82 /	206.72.135.195	Tue, Jan 10, 12:44 PM	02:	
ivan (S)	Ivan Izquierdo	192.168.1.159 /	206.72.135.195	Tue, Jan 10, 12:44 PM	02:	
jane (S)	Jane Washington	192.168.1.56 /	206.72.135.195	Tue, Jan 10, 12:45 PM	01:	

From this interface, the administrator can see who all are logged into the Internet alongwith their IP addresses, and also how much data transfer is taking place. He can even terminate the session of any user



This diagram shows how RSA SSO enables single sign on across multiple applications

desk costs as there will be no tickets for resetting passwords and it also eliminates the possibility of errors by helpdesk. However, if an organization still wants to use helpdesk or if the user cannot reset the password for some reason, the software does have a helpdesk console through which helpdesk personnel can perform required tasks. It also has activity tracking and auditing features, and provides administrator with built-in auditing and activity tracking. The Password Management Portal provides the administrator a comprehensive and immediate notification of the password reset activity by the end users.

The software has three kinds of consoles: namely, a console for End users; an Administrator console; and a Helpdesk console. The end user can login and reset its pass-

word by answering a set of challenge questions correctly. Through administrator console, other than resetting a user's password, administrator can set password policies, Add challenge questions, view activity logs etc. Using the software is pretty straightforward. Users can also edit the answers to the challenge questions from the user's console. To use the software you will require a Windows 2003 Server Standard, Web or Enterprise Edition, Microsoft SQL Server 2000 or higher version, ASP.NET Framework 2.0 and IE6.

RSA SSO

If you are coping with the problem of managing multiple logins in multiple applications in your enterprise then you require a Single Sign On manager to solve this problem. For instance, let's sup-

pose that you have 10 different applications such as your corporate and personal e-mail accounts, the corporate Directory Service, your corporate Intranet, the ERP Solution, etc and none of them are integrated in terms of authentication. Then in that case you have to manually login to each and every application whenever you want to use or access them. And this is not all, you also have to manage the account for each of these applications—for instance you have to reset your passwords before they get expired or too old, and while resetting them you have to keep in mind the type of password policy the application has and then give the new password accordingly. And on top of it you have to remember all those passwords.

But with a Single Sign On manager such as the RSA SSO which we tested out in Labs, you can forget about managing multiple passwords. Now, all you have to do is to login with just one password to your workstation and RSA SSO will take care of the rest. It will automatically send the username and the password whenever you want to access any application.

Additionally, the software will automatically trap messages from the application which asks for password reset and will reset and save the password for you. The whole process of login, password reset, etc becomes completely transparent to the users.

With SSO you just have one password for all your applications, and this password becomes more than important for the user. Because if this password is stolen then all his applications be- ▶

come vulnerable. To solve this problem, RS SSO has support for two factor authentication with RSA Tokens. You can even go ahead and add biometric security with it. All these features make it pretty much secure and can help in making your organization Sarbanes-Oxley or HIPPA compliant without much effort. Because if you want to introduce SSO (which is a prime requirement for the HIPPA or Sarbanes-Oxley compliance) natively inside your DS then in that case you have to do a huge amount of modification in all your applications, so that they can become compliant with your DS and can read the users and policies directly from there.

Deploying RSA SSO is not at all a piece of cake. Rather it can give you some real hard experiences. While testing out the product in Labs we took around three day to make the thing work. So make sure that you get a service engineer along from RSA in case you plan to deploy this software.

The list of pre-requisites is not too long. All you require is a Windows 2000 or 2003 machine with IIS installed, for the RSA SSO server. Additionally, the server software requires that you have a directory

Identity 2.0 Resources on Web

<http://pip.verisignlabs.com>
Personal identity provider.

http://www.identityblog.com/?page_id=352/#lawsofiden_topic3
Laws of identity.

<http://voucher.com>
A community of vouchers, who verify web user identities instead of government agencies.

<http://lid.netmesh.org/>
LightWeight Identity - URL-based user-centric digital identity.

<http://sigly.com/>
A standard method for legally collecting e-signatures online.

<http://numly.com>
Numly assigns electronic serial numbers for all digital things.

<http://www.trufina.com>
Online identity provider.

<http://www.rapleaf.com/>
A ratings system for commerce. You can look people up before you buy or sell, and rate them afterwards.

<http://yadis.org/>
Yet another decentralized identity interoperability system


service running. This DS should be either a Microsoft ADS, or Novell eDirectory or a Sun One Directory. The RSA SSO manager then takes the users from the DS directly and reduces the need of creating users afresh. Once the server is installed and configured, you have to install

the client agent on all workstations. Installing the clients is nothing more than running a simple wizard. Once installed, connect the client to the server by providing the IP address of the machine where the RSA SSO server is installed and it will start working for you. □

PRESENTING LCD MONITOR
WITH




WORLD'S ONLY F-ENGINE TECHNOLOGY.

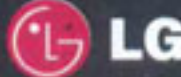
NOW ENJOY A NEVER BEFORE EXPERIENCE THAT BRINGS IMAGES TO LIFE.



CON:LOWE 04071191
for more details visit us at www.lgusa.com
or mail at Freshmint@lg.com

L17525

<p style="font-size: x-small;">Normal Monitor</p>  <p style="font-size: x-small;">F-ENGINE Technology</p>	<p style="font-size: x-small;">F-ENGINE</p>  <p style="font-size: x-small;">Ultra-Fast Response Time</p>	<p style="font-size: x-small;">Normal Monitor</p>  <p style="font-size: x-small;">Ultra-High Contrast Ratio</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Life's Good

LG FLATRON
LCD TFT MONITOR