|  |
| --- |
|  |

--------------------------------------------------------------

This story was printed from [ZDNet Australia](http://www.zdnet.com.au).

--------------------------------------------------------------

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Security with bite: 15 technologies tested**  By [Matt Tett, Technology & Business magazine](mailto:edit@zdnet.com.au) April 22, 2005 URL: <http://www.zdnet.com.au/reviews/hardware/peripherals/soa/Security-with-bite-15-technologies-tested/0,139023417,139189092,00.htm>  **In this special review, we round up the various authentication devices on the market. From fingerprint scanners, to single sign-on software and biometric technology -- we have the authentication market covered.**  Picture this if you will, some genius bent on taking over the world creates a malicious self-replicating stealth worm that has the power to infect every known PC in the universe via any network medium. Its sole aim is to install itself and remain resident while remaining on the lookout for key bytes of data that, when triggered, capture and send the information back to a series of well hidden previously compromised servers waiting there for the nefarious creator of this super worm to come along and collect the data to misuse in whatever way they see fit.  Organised crime syndicates would love to get their hands on some smart programmer who could make this dream a reality and capture all that juicy data. And what information would they steal -- credit card information? Bank account details and passwords? Username and password lists for multinational organisations? Potentially yes, but all that is really passed these days and the syndicates have moved on.  These days it is all about personal information, most of which is already publicly available on the Internet or in our garbage bins for those who are happy to search enough for it. If someone with malicious intentions can make enough of a personal profile about someone then they have effectively stolen that person's identity, commonly known as identity theft, which when used by unauthorised individuals becomes identity fraud.  Identity theft is nothing new, in fact it has been going on for years. Traditionally, not even associated with electronic crime it was used by people avoiding the law and tax, and claiming benefits they may not necessarily be entitled too. There are fraud taskforces setup by the Federal Police and ATO who investigate identity fraud full time. It is just that now with technology as an enabler it is easier, faster and able to be performed on a much larger and more anonymous scale.  And to complicate matters even more, in the ICT arena, it is not only humans that have an identity but pretty much any object on your network. Therefore there are a whole lot more identities to manage and decide who or which can or can't be authorised access to resources. This is commonly called IAM (identity and access management). The basic premise which must be understood is that authentication is actually quite different from authorisation.  **Authentication vs authorisation**  The definition for authentication as found in the [Webopedia](http://www.webopedia.com) is: "The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorisation, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual."  Authorisation, according to Webopedia, is: "The process of granting or denying access to a network resource. Most computer security systems are based on a two-step process. The first stage is authentication, which ensures that a user is who he or she claims to be. The second stage is authorisation, which allows the user access to various resources based on the user's identity." For the purpose of this review on data authentication, a "subject" is the identity attempting to access a device, and an "object" is the device.  **Factors of Authentication** There are several types of authentication, one of the most commonly used is a password or personal identification number (PIN). This is known as single factor authentication -- something the subject knows. One of the most secure authentication processes would use a combination of factors such as something the subject knows (password, passphrase, or PIN), something they have (smartcard, token, or tag) and something they are (fingerprint, handwriting, iris, or retina scan, and so on).  Other behind-the-scenes authentication techniques used are digital certificates and digital signatures. Pretty Good Privacy (PGP) uses keys and digital signatures to enable authentication of e-mail messages to ensure that they came from whom they said they did. Likewise, secure Web sites use digital certificates to let the subject know that they are whom they say they are and that they can be trusted.  **One-time passwords and token devices** One-time passwords are a good and relatively low-cost alternative. Like the name suggests, the passwords are used once only and if the same password is used again at a later stage in a login attempt then the subject is rejected.  The tokens are small devices that are synchronised with the authentication server system to issue the user with a password when a button is pressed on the device.  One-time passwords are an excellent choice if one is concerned about keyloggers or spyware infections that may be collecting data from compromised machines. Another benefit to one-time passwords is they can stop identity fraud occurring within the organisation.  Vasco Data Security shipped us a copy of its Radius server middleware and one of its token devices. Vasco has managed to include two-factor authentication with the tokens by having the user input a static PIN first, such as 1234 (something they will know) and then the one-time password supplied by the token (something that they have). Using this, the login would look like 1234 (code on the token). There are also options to interface with Web-based logons, Citrix, Lotus/Domino, Windows, and Novell. RSA, Verisign, and Giesecke & Devrient also supply one-time password generating token devices.   |  |  | | --- | --- | | http://www.zdnet.com.au/shared/images/tandb/gemsafe_200x150.jpg | http://www.zdnet.com.au/shared/images/tandb/vasco_200x150.jpg |   **Single sign-on (aka the Holy Grail)** Single sign-on is taking every existing authentication system used by an individual and changing it to a single authentication technology. So say a user has 12 disparate objects to access via passwords every day, they can reduce that to one password to access all 12.  However, it does mean there is a single point of failure if static passwords are used. But combined with other forms of more secure authentication, such as tokens, smartcards, biometrics, and so on, single sign-on is a very attractive option.  There are two main types of single sign-on concepts. The first is enterprise-wide single sign-on; the second is Web single sign-on or federated (usually via Web interfaces) single sign-on. Enterprise single sign-on is what every company, particularly ICT departments that havee been operating for more than a few years, is trying to pursue. Consider how many applications employees have to log in to every day just to do their work -- accounting systems, stock control systems, operating systems, CRM applications, e-mail systems, intranets, extranets, Internet proxies, even old legacy apps.  Most of these applications are somewhere in the grand scheme of lifecycles, and at the end of the day cannot be replaced in one fell swoop, or indeed ever, with a nice directory compliant application (X.500, LDAP or otherwise).  This is why a middle ground needs to be established to head towards true single sign-on and a balance of smart programming and compliant standards-based applications needs to be achieved.  Vendors, such as Citrix with its MetaFrame Password Manager Access Suite, have taken some of the heartache out of this by developing very powerful tools that enable administrators to capture and set many forms of password controls and even enforce quite complex password policies on legacy applications which never would have had these options in the past, and all without rewriting the application or the interfaces.  Federated single sign-on, however, is where multiple Web sites have an agreement to accept and trust authentication of a user at one Web site and carry it across to the others. This means the user only has to sign in at the first Web site it visits.  Computer Associates has the best of both worlds in both enterprise and federated single sign-on.  It has a truly enterprise-scale directory service in the form of its eTrust eDirectory, which has the options to run with its range of IAM (identity and access management) applications for enterprise single sign-on and with the recent acquisition Netegrity it now has a federated single sign-on product called eTrust SiteMinder.   |  |  | | --- | --- | | [http://www.zdnet.com.au/shared/images/tandb/citrix_screenshot_200x150.jpg](http://www.zdnet.com.au/shared/images/tandb/citrix_screenshot_500x400.jpg) | [http://www.zdnet.com.au/shared/images/tandb/ca_screenshot_200x150.jpg](http://www.zdnet.com.au/shared/images/tandb/ca_screenshot_500x353.jpg) |   **Smartcards/Proximity Cards**  Smartcards and proximity cards have been around for many years.  Proximity or magnetic cards (mag cards) traditionally have been used more for physical access controls rather than for the authentication of people. Smartcards have been used for everything from mobile phone SIMs, to satellite decoders.  Smartcards are now becoming quite popular for use in authentication technologies providing the something a user has factor of authentication. So while it technically is possible to steal or copy a user's smartcard it adds another level of complexity to the equation for those with malicious intentions.  Smartcards, like mag cards, can also be printed on and used as company and photo IDs for security checkpoints and visual user identification.  Smartcards can also be used for storing biometric information or digital signatures/certificates and encryption/VPN codes.  The benefits of storing these types of information on a smartcard are fairly significant; firstly it removes the need for that information to be stored all together in a single database. It also removes the need to send that information from a server to a client where it may potentially be intercepted by a man-in-the middle attack; this is particularly relevant in the case of encryption handshaking.  Many vendors are now integrating smartcard readers into some of their devices such as HP and Acer in their notebook range. In a review we performed last year Sun Microsystems had a thin client terminal (Sun Ray 150) which used smartcard technology not only for authentication but in an innovative way by switching the entire user environment from one terminal to another terminal simply by unplugging the card and plugging it into another terminal.   |  |  | | --- | --- | | http://www.zdnet.com.au/shared/images/tandb/keycorp_200x150.jpg | http://www.zdnet.com.au/shared/images/tandb/sunray_200x150.jpg |   An example of the added functionality and versatility of smartcards is their ability to be incorporated with other card technologies such as magnetic swipe for use as physical access devices or even bank cards, they can also be printed with photos and other identification information.   |  |  | | --- | --- | | http://www.zdnet.com.au/shared/images/tandb/bqt_200x150.jpg | http://www.zdnet.com.au/shared/images/tandb/g&d_200x150.jpg |   **Biometrics**  Like most authentication technologies there are several flavours of biometric technology: from the advanced handwriting and facial character recognition systems to the more common fingerprint scanners and quite a few technologies in between (iris, retina, and palm scanners).  There are almost as many uses for biometrics as there are types. While all five of the devices that we were sent from vendors for this review were fingerprint scanners, most of them had very differing uses. From simple desktop management of passwords, through to three-factor authentication purposes.   An important tip when using fingerprint scanners is once authentication is complete, the finger must be slid off the scanning window to smudge the print. It has been known that some scanners return false positive IDs when a breath of air is blown onto the device or bag of water applied to a scanner with a residual imprint.  There are various other ways of "tricking" a fingerprint scanner and Steve Turvey sums these up in his [biometric review](http://www.zdnet.com.au/reviews/hardware/printersscanners/0,39023422,39116195,00.htm) in the February 2004 edition of T&B. Another problem is remembering which finger was used during the registration process.  When considering the biometric route look at a vendor's crossover error rate. This is the point where the rejection of legitimate users intersects with the false acceptance of unauthorised users. If a system is configured too tighty then legitimate user frustration can result in too many rejections/re-authentication requests coming through.   |  |  | | --- | --- | | http://www.zdnet.com.au/shared/images/tandb/apc_200x150.jpg | http://www.zdnet.com.au/shared/images/tandb/comsec_200x150.jpg | |