

FEATURE

AUTHENTICATION MARKET UPDATE

1540 words

May 07

By Ian Kilpatrick, chairman Wick Hill Group, specialists in secure infrastructure solutions.

Summary of feature

* Breakdown of network security perimeter. Growth in number of devices wanting to access company networks. Increasing number of remote users and laptops. Users want to access more and more different applications.

* Traditional passwords unsuited to this situation. UK lagging behind in developing suitable access management for current situation.

* Description of types of authentication

- weak single factor
- strong authentication
- two factor authentication
- three factor authentication
- biometrics
- single sign on

* Remote, mobile and wireless security. How to deal with this particular risk. Strong 2-factor authentication. SSL VPNs. Limitations of wireless standards. MAC filtering

FEATURE

The impact of the Internet over the last few years has meant fundamental changes in the way we access business systems. The network security perimeter has crumbled at all levels while the number of users wanting network access has grown. The geographical location of users has also widened to a situation where they can be, not just in a different department or company branch office, but anywhere in the world.

The devices for gaining access have multiplied and diversified. Users now want to access using mobile and wireless devices, including laptops. The information they want to access has widened to encompass all aspects of a business, including e-mail, a greater range of applications and various types of data.

While there are enormous productivity benefits available from increased access, the security risks have greatly increased. The traditional method of securing system access was by authentication through the use of passwords. Unfortunately, traditional password authentication is totally unsuitable for securing the access requirements of today's distributed users.

UK companies are considerably behind the curve in responding to this changing scenario. According to the DTI Information Security Breaches Survey 2006, UK businesses are still overwhelmingly dependant on user IDs and passwords to check the identity of users attempting to access their systems.

The Survey says that UK companies are poorly placed to deal with identity theft, with only 1% having a comprehensive approach for identity management (authentication, access control and user provisioning).



Types of authentication

Weak single factor authentication

This is the use of single static passwords and still employed by most UK companies. The benefit is that static passwords are easy to remember. However, when you have different passwords for different systems, they start to become very difficult to remember and have to be written down, making them vulnerable. A significant use of Post-It notes is rumoured to be password related.

The many disadvantages of single static passwords include how easy it is to crack them. They are short and based on topics close to the user, such as birthdays, partner names, children's names, etc; and they are typically letters only.

They are also vulnerable to social engineering i.e. people asking for your password or guessing it. Some highly publicised surveys carried out at railway stations have shown how easy it is to get people to reveal their passwords. They can also be picked up by spyware.

The alternative method of password management is to change passwords regularly. Operated correctly, this has the benefit of being more inherently secure than static passwords. A disadvantage of frequently changing passwords is that they can be easily forgotten, leading to very high support costs and significantly increased administration costs. This is particularly relevant for larger organisations with hundreds of applications.

Single Sign On (SSO)

Single sign on allows users to authenticate once and gain access, when required, to multiple (permitted) software systems. This is useful where users are wanting to access an ever increasing numbers of applications. SSO has major security and user benefits, as well as significantly reducing the helpdesk costs of password management.

There is a security risk with static password-based single sign on because a breach of password security means all systems accessible by a particular user can be compromised.

Typically, SSO deployments are in conjunction with some form of two factor authentication. SSO is now undergoing rapid growth thanks to new technology from companies such as Imprivata, which has dramatically lowered the cost of deployment.

Strong authentication

Strong authentication involves one of a range of elements such as hardware tokens, soft tokens, fingerprint recognition, swipe cards, etc. Most strong authentication deployments are used together with passwords (two factor authentication).

Strong two factor authentication

Strong two factor authentication is a much more secure means of authenticating users onto networks as it requires two separate security elements.

It comprises something you know (a password) and something you have (e.g. a token). Tokens are currently the most popular two factor solution, due to their low cost, ease of deployment, ease of management and the standard of security they provide. VASCO, one of the market leaders, provides hardware tokens which generate one time passwords (OTP). The rapid fall in the price of tokens means they are now available from only a few pounds per user per year

To put that in perspective, it's less than the cost of ONE password-related helpdesk call. With password-connected calls making up between 30% and 50% of all helpdesk calls (depending on whose research you accept), tokens can represent a cost-saving as well as an improvement in security.

Other two factor options include soft tokens which can be sent to your mobile, swipe cards, USB-based authentication and fingerprint recognition. Proximity authentication is another variation which simply means that once you have authenticated and are within wireless range, you don't need to authenticate again for another system.

Similarly with physical/logical security, physical swipe card entry systems linked to IT systems security, allow organisations to integrate access security with network security. Companies such as Imprivata are providing converged security systems in this area.

Three factor authentication

This is far superior and involves something you know (e.g. password), something you have (e.g. authentication token) and something you are (e.g. fingerprint, retinal scan, facial recognition). While biometric authentication is obviously more costly, it is appropriate for high security applications/departments such as pharmaceutical R&D, finance, etc.

Biometric authentication

Biometric authentication is a more recent and still developing technology. It can be either two factor or three factor. Examples of physical, physiological or biometric characteristics include fingerprints, eye retinas and irises, facial patterns, and hand measurements; examples of behavioural characteristics used for authentication include signature, gait and typing patterns. Biometric authentication is more appropriate than tokens for certain applications, such as some manufacturing environments; or where superior security is required.

Remote, mobile and wireless security

Static passwords, as mentioned above, are still the main way of authenticating users onto a network, but are woefully inadequate for remote and mobile computer users, with huge identity theft risks (particularly for wireless). The answer is to deploy strong two factor authentication, but other measures are also advisable.

Low cost encryption from companies such as Utimaco or PGP, can protect key mobile devices for less than £70 per device. Or, if cost is an issue and performance isn't a problem, there are free solutions available.

It is essential to ensure that network connections from remote users is via encrypted VPNs, which create a secure tunnel over the Internet from the user to the network and are authenticated through the network gateway. Either Secure Socket Layer (SSL) or IPsec VPNs are suitable.

SSL VPNs are more appropriate where you have large numbers of remote users as they are low cost and provide easier to manage connections than IPsec. SSL VPNs are a growing area and there is a wide range of solutions available from vendors such as WatchGuard, Array, Check Point and NETASQ.

Wireless is a particular security issue and it is best to ensure that, together with strong authentication, all wireless traffic is over VPNs and is encrypted. Don't use Wired Equivalent Privacy (WEP) for encryption because it is poor, insecure and weak. Use WPA or WPA2 (also known as 802.11i) and ensure that users always operate with it switched on - the default is with it switched off.

If you have remote wireless LANs, ensure that the service set ID (SSID) is changed from the default and is secured to prevent unauthorised wireless users connecting. Don't change it to something blindingly obvious like your company name (or "control tower", as seen by startled laptop users at a US airport).

Another authentication option is to implement media access control (MAC) filtering. A MAC address is a physical address, so if you restrict access to devices whose address you have authorised, you can eliminate many ID theft issues. Another variation of this is device authentication, where the device authenticates itself to the network.

The DTI Survey 2006 found that roughly 36% of UK businesses allow some staff to access their systems from a remote location (e.g. from home or via wireless hotspots). Four-fifths of large businesses allow this. Interestingly, respondents who allow remote access are twice as likely to have had an unauthorised outsider try to break into their network as those who do not; they are also more likely to have experienced an actual penetration incident.

Conclusion

The growth of the Internet, the increase in users requiring access to networks and the move to remote working has fundamentally changed the requirements for authentication over the last few years. However, users are still lagging behind developments and relying on single static passwords, which are wholly inadequate.

The need for strong authentication is greater than ever, the cost of solutions such as single sign on and strong two factor authentication has come down, and such solutions are now easier to use. It is time for companies to look at improving their authentication procedures, if they want to remain secure and avoid potential business disruption, financial loss and damage to reputation.

ENDS

For further press information, please contact Annabelle Brown on 0191 252 8548, email a_brown@dial.pipex.com. For reader queries, please contact Wick Hill on 01483 227600, web www.wickhill.com.

Bio - Ian Kilpatrick

Ian Kilpatrick is chairman of Wick Hill Group plc, specialists in secure infrastructure solutions for ebusiness. Kilpatrick has been involved with the Group for over 30 years and is the moving force behind its dynamic growth. Wick Hill is an international organisation supplying most of the Time Top 1000 companies through a network of accredited resellers.

Kilpatrick has an in-depth experience of computing with a strong vision of the future in IT. He looks at computing from a business point-of-view and his approach reflects his philosophy that business benefits and ease-of-use are key factors in IT. He has had numerous articles published in the UK and overseas press, as well as being a regular speaker at IT exhibitions.