

2FA

– PROTECTING THE FUTURE

Michael Robertson explains the role of two-factor authentication (2FA) solutions in controlling access to web applications and providing additional protection for user identities.

The internet plays a significant role in the efficient operations of both public and private sector organisations. This medium offers a fast and effective way to communicate with stakeholders who have become increasingly comfortable with sharing information and conducting transactions online. The web's evolving capabilities, together with this growing public engagement, has created a virtuous circle where more and more end-users are benefiting from a growing number of products and services that are now available online and which, ultimately, add value to their professional and personal lives.

This scenario, however, is threatened by one unwelcome internet user: the fraudster. Within the banking community, for example, the migration to Chip & PIN has improved security for payments where the card and its holder are present, but has driven significant financial crime online. APACS, the UK payments association, recently released figures that showed a 180 per cent increase in e-mail 'phishing' scams – more than 20,000 reported cases – for the first half of 2008 compared to the same period last year.

Although there is an obvious need for a high level of security when it comes to financial transactions, such as online banking and trading, the need to secure access and authenticate users is common to other non-financial, information-sharing operations across many sectors. The move towards e-government, for example, aims to encourage UK citizens to communicate with various government departments online. This inevitably means sharing private and confidential personal details via the web.

This glimpse of the future, together with

some recent high profile incidents where sensitive data has been lost by public sector departments or personnel, has led identity theft to become an understandably hot topic and one which will become increasingly debated as the government pursues its national identity card programme. Within government departments, local authorities and the private sector alike, implementing effective security for web applications and being seen to be doing so has never been more important.

e-Criminals go phishing

Drawn by the sheer volume of online traffic and the sensitive nature of information shared between parties, fraudsters have developed sophisticated methods to infiltrate systems and access secure data through a variety of spurious techniques.

Phishing, pharming and Trojan horse attacks are all methods used to obtain private information that defraud web users. The first two methods direct users to false websites – either via an e-mail request for information, or automatically redirecting web traffic by corrupting a victim's computer through the change of a host file or exploiting the vulnerability in the Domain Name System server (software which translates internet domain names into their real addresses). In both cases, the victim thinks they are using a secure website, when in fact their details are being stolen by a third party.

Trojan horse crimes are more sophisticated as they take over the user's entire PC. This happens when corrupted files – which appear to be useful and innocent programs when downloaded by the user in good faith – execute a malicious code that gives the fraudster complete

control over the PC while it still displays information the user expects to see.

Both pharming and Trojan horses can be used to deploy man-in-the-middle attacks where a third party intercepts a legitimate exchange and modifies information in real time before passing it on to the recipient. Details such as where a payment should be sent, and how much should be paid, could be changed with neither the original sender nor recipient aware of anything untoward.

Fighting the fraudsters

Such attacks will no doubt become increasingly aggressive as more and more transactions and activities go online, and fraudsters actively decipher more sensitive information to maximise the impact of the crime committed. As a result, it has become both difficult for organisations to be sure about a user's identity and, at the same time, for users to have the confidence that they are communicating with an authentic website.

In light of this, any organisation which communicates online with stakeholders, particularly where sensitive data is being exchanged, has a real need to control access and protect the identity of users in a way that applies the simplicity of traditional 'name and password' solutions but introduces an additional layer of personalised security. Any analysis of how to achieve this must take into account a number of factors, including effectiveness against known and foreseen threats, the cost and ease of implementation, flexibility, and how easy it is for end-users to understand and employ the technology.

A two-factor approach

Although different approaches have



The author

Michael Robertson is founding partner and managing director of Commerce Media Limited (www.commercemedia.net).

been developed, authenticating a user based on what they have and what they know is becoming the accepted security benchmark. This has led to a significant increase in the acceptance and deployment of two-factor authentication (2FA) solutions as a means to control access to web applications and provide additional protection of user identities.

2FA is characterised by the fact that the user knows something – such as a password or a passphrase – and possesses something which is hard to steal or counterfeit, and which provides additional identification. In most 2FA applications, ‘possession’ is demonstrated by knowledge of a one-time-password (OTP) that is generated either by a token, or at an initial log-in phase by the website’s server, and is communicated to the end-user via a device such as a mobile phone. As the name suggests, this password can only be used once - in real time – to authenticate the user for the associated data or financial transaction. This negates the possibility of a ‘constant’ password being lost or forgotten, or from being stolen via a phishing attack and then used to access a system illegally on a future occasion. The fact that the OTP is generated by a known source, communicated by an independent medium and not via the web, and has to be entered by the user before an operation is verified, makes it almost impossible for a man-in-the-middle attack to succeed.

Using a mobile phone as the device via which to communicate a OTP through SMS text messaging has many advantages. Users are familiar with mobile phone technology and, unlike other devices such as handheld readers, the public’s reliance on their mobile phones to communicate

and to calendar commitments, means that the interface is nearly always available. Another key advantage is that no additional hardware needs to be purchased or deployed, thereby reducing the cost of 2FA implementation. These benefits combine to make mobile phones the preferred 2FA tool of the future.

Protecting the future

With continuing developments in delivery methods and proven success in some high-profile applications (see case study), the future looks strong for 2FA. The NCC’s own Benchmark of IT Strategy

2007 survey revealed ‘a rapidly growing interest in improving authentication procedures’ amongst respondents, especially for remote access users, token-based or 2FA single sign-on procedures and password policy.

With the continued growth of the internet, the promise of huge economic and social benefits relies on users and providers alike having the confidence that their identity and activity is securely protected. Two-factor authentication is a simple, cost effective and easy-to-use solution currently available that will help ensure the war on internet crime is not lost.

CASE STUDY

From socks to jets: how the UK Ministry of Defence authenticates online sellers of military surplus

The Disposal Services Authority (DSA) is the agency within the UK Ministry of Defence (MoD) which is responsible for the disposal of surplus assets, maximising the financial return to the government and ensuring that items are reused or recycled with the minimum of waste. Annually the agency generates a return of in excess of £700m through its activities.

The DSA wanted to extend its conventional sales channels by introducing an online portal that would bring together contractors who are tasked with the resale of surplus stock and buyers who are typically members of the public. The nature of the MoD’s business meant that security had to be at the very heart of the solution. Never before had a transactional database been hosted outside the MoD’s internal restricted network.

In order to satisfy these extremely high security standards the DSA decided to deploy a 2FA solution. All contractors were required to log in using a OTP, generated by a token, before uploading stock information to the site. Following the success of this deployment, the DSA identified the importance of providing a 2FA option to the entire 6,000 plus user base. As tokens can be relatively expensive to deploy and support, alternative 2FA delivery mechanisms were examined.

The DSA selected Commerce Media’s Celo – a tokenless 2FA system which sends a OTP via SMS text messaging to users’ mobile phones. The solution was chosen as it was cost-effective, simple to deploy without the need to implement software and issue hardware, could adapt to future changes in user numbers from 1 to 100,000+, and, most importantly, provided robust security for all users logging onto the website.