
White Paper: Two Factor Authentication

A brief overview of strong authentication

What is authentication?

In computer terms, authentication is the process by which a user – or another computer or application – confirms that they are who or what they claim to be. Usually this is to ensure that a person requesting access to computer resources is in fact a person authorised to use them.

Authentication and authorisation are related but different concepts. Effective authentication may prove that a user is John Smith. Effective authorisation will then ensure that he has access only to the resources that John Smith is entitled to use. Authentication has to be the first stage in the process.

This White Paper focuses on authentication.

Why have two factors?

Until fairly recently it was sufficient for most computer users to identify themselves with a simple password: they entered a username, then demonstrated that they were that user by providing the password associated with it. For particularly sensitive information more stringent rules were introduced about the passwords used: they might have to be more than 6 characters long, contain both letters and numbers, or be changed every month or so.

As computers became more connected, first of all in local networks and then by the Internet, it became both more difficult to define and secure the “boundaries” of the network, and more important to prevent unauthorised access because the amount and value of resources at risk grew exponentially.

It also became increasingly clear that even “strong” passwords simply did not provide sufficient protection. Passwords are lost, shared, stolen, cracked and compromised in any number of ways. Effective password-cracking software is freely available on the Internet: and a highly sophisticated industry has grown up specifically to dupe Internet users into revealing their passwords and online “shared secrets”.

All of this means that password protection involves management resources as well as security risks: authentication company Rainbow Technologies estimated in 2003 that “the cost of managing passwords is estimated to be from \$75 to \$150 per user, per year which does not count lost productivity due to downtime as the user waits to access an application.”

What is two-factor authentication (2FA)?

Password and PIN-based systems authenticate users by proving that they *know* a “secret” shared with the network. Two-factor systems demand that users also demonstrate that they physically *possess* something unique to them. This simple step increases the security of the authentication process by magnitudes.

HOW TO DEFEAT PASSWORDS

You have plenty of choices – and you don’t need to be technical

- Borrow someone else’s. Even if they won’t lend it to you, you can always “shoulder-surf” when they log on. Or read it off the post-it under the keyboard.
- Boss going away for a few days? Offer to check his e-mail. Of course, he’ll change his password as soon as he comes back...
- Use tools – you can get them free on the web. LOPhtcrack and NT Crack are classics – “for network admin only”. Network sniffers are useful too.
- Be really nice to your network administrator – nobody else will...
- Go phishing. Just send out a few million e-mails asking people to “confirm their passwords for security reasons”. Some of them will.
- Use a free kit to write a “Trojan” to recognise passwords as they are entered on someone’s computer, log the keystrokes and send them to you. They’ll never know.

YOU ONLY NEED ONE!

Most people use 2FA technology already, without thinking about it, in the form of their bank ATM cards. They have to prove both that they physically *possess* their card (by putting it in the machine) and that they *know* their PIN number.

This system works well with a closed system like ATM machines, when the banks control the access terminals. It is a lot more difficult to implement 2FA over the Internet when users may be using virtually any means of access from personal computers through WiFi connections to XDA's.

Types of 2FA: advantages and disadvantages

A number of systems have been developed to enable two-factor authentication over the Internet. The main categories are described below:

Smartcards

Smartcard based systems use a credit-card sized card with an onboard microprocessor. Typically the card is inserted into a reader and a password or PIN entered to gain access to data on the card, which is transmitted to the authentication server to confirm that the card is physically present.

Smartcards have the advantage that they may be used to store other, non-authentication information such as PKI keys, certificates or financial data. They may even be used to control physical access to buildings.

Their main disadvantage is the requirement for a reader at every access terminal used. This may be acceptable for users if only one machine is ever used for access: but for the system owner it represents a considerable initial capital outlay and an ongoing administrative and maintenance burden – as does the issue, recording and delivery of the smartcards.

An authentication server is required, and normally a separate smartcard is needed for each protected application.

Leading smartcard vendors include Gemplus, CryptoCard and Cardlogix.

USB tokens

USB tokens are plastic capsules around 7cm long, which are normally designed to be carried on a keyring. The token is plugged into a USB port on the access device, and operates in the same way as a smartcard.

Like a card, the USB token may be used to store unrelated data. Although no dedicated reader is required, the access device must have an available USB port – which can be inconvenient on an older machine. USB tokens are relatively expensive to purchase (typically around £30 per unit), and require initialisation, recording, delivery and ongoing maintenance. An authentication server is required on the protected site or network to handle interrogation and verification of the USB token on the client machine. The server requires installation, configuration and maintenance.

As more applications require strong authentication, users have to carry more and more tokens to provide access to their bank accounts, business networks and so on – a problem known as the “token necklace”.

Leading USB token vendors include Aladdin, Eutron and Rainbow Technologies.

Electronic “authenticators”

Authenticators normally take the form of “keyfob” tokens around 60mm x 35mm in size. Typically an LCD window displays a 6-digit number which either changes automatically every 60 seconds or is manually switched to provide a “one-time-password”, which is combined with the user’s static PIN to enable two-factor authentication. Authenticators are also available in “credit card” and USB token implementations working on the same principle.

Authenticators have the advantage of being “device independent”, since they are not connected to the access device. Like smartcards and USB tokens they require an authentication server, often with substantial licensing and maintenance costs. As well as the initial capital cost of the tokens there is a significant ongoing administration and maintenance overhead: although it is difficult to find published research, we understand from corporate

users that around 20% of tokens have to be replaced each year due to loss or damage, and tokens also need to be reset if they drift out of synchronisation with the authentication server.

Like USB token and smartcard systems, authenticators suffer from the “token necklace” problem.

Leading suppliers of authenticators include RSA (the market leader by far, with over 70% of the 2FA market in major sectors), Secure Computing and Vasco.

Pre-issued Two-Factor Authentication

This category includes Transaction Authorisation Numbers (TANs) and “security grids”. They operate by requiring the user to provide a unique number, either from a presupplied list or by derivation from an alphanumeric grid.

TANs are particularly popular with banks in Germany – although there have been recent instances of successful phishing attacks, where attackers have been able to lure users into divulging unused TAN numbers. Security grids are not susceptible to this attack because the grid references of the required pass number are generated on the fly for each log-in.

Although TANs and security grids are relatively cheap to manufacture, they are claimed to involve high help-desk costs and other administrative expenses. They require an authentication server.

TANs are frequently generated and provided by banks using their own proprietary software. Security grids may also be self-generated. EnTrust is the main commercial vendor.

Biometrics

Whereas most forms of 2FA rely on something you know and something you have, biometric systems look at something you know and something you are – using fingerprints, iris scans or other biometric measurements to provide the second factor.

The obvious advantage is that the right system will provide a very high level of identity verification. Disadvantages are high costs, both for the associated readers (which have to be available on every access device) and for the initial implementation of the system when users are enrolled. There are data protection and privacy implications which need to be resolved; and recent studies in the USA have raised questions about the reliability of fingerprint recognition in large user samples.

Vendors of biometric systems include Digital Persona and Identix.

Phone-based systems

Phone-based authentication systems fall into two main categories: one-time-password based and call signalling data based.

One-time-password based systems identify the user by first requesting a username and password. They then identify the phone number associated with that user, and use SMS texting or automated voice synthesis to provide a one-time-password to that phone. The password is then returned to the authentication server *via* the user’s browser to confirm that the user actually possesses the right phone. The phone therefore effectively becomes an authentication token.

Identrica has invented and patented a unique system which uses signalling data, created by the telephone companies when a call is set up, to prove that a user possesses the right phone. Typically, the user will enter their registered phone number and password into the browser and make a phone call from that phone to an Identrica service number. The phone call will not be answered (and so costs nothing), but this provides enough information for the Identrica service to confirm that the user possesses the right phone.

Both systems have the considerable security advantage of using an “out-of-band” factor – employing the telephone infrastructure rather than the existing IP channel from the user’s browser to carry authentication data. This provides an effective defence against “man-in-the-middle” attacks in which an attacker intercepts data passing between the user and the authentication system, and effectively hijacks the session. This technique can be successful against many conventional forms of 2FA.

Because users effectively administer their own “tokens”, and use them constantly, they are much less likely to forget to carry them and much quicker to notice if they are lost or stolen.

The main advantage, of course, is that there is no need to purchase, initialise or deliver any new user hardware in the form of tokens or readers. However, SMS and voice synthesis systems incur a cost every time the user logs on: since this happens more often than is normally realised (because of time-outs etc.) running costs are difficult to predict. These systems need an authentication server.

Because there are no SMS messages or completed calls with the Identrica system, there is no per-logout cost no matter how often users access the system. Since Identrica is normally provided as a fully-managed service, no authentication server is required and the only cost is the annual subscription for each user.

Phone-based systems have to deal with the problem of enabling authentication in areas with no mobile phone signal. This may be done by providing a time-limited “emergency PIN” – as used in many other systems to cope with lost, forgotten or broken tokens. Because it does not rely on SMS messaging, Identrica allows users to use a landline rather than a mobile phone when appropriate.

Digital certificates

Strictly speaking digital certificates identify access devices rather than users. They are blocks of data installed on individual machines and can be thought of as “pre-installed tokens” proving the identity of the machine, rather than the user, to an authentication server. They may form part of a full PKI suite allowing encryption, digital signature of documents, non-repudiation etc.

Digital certificates are frequently complex to administer and use, and are inflexible in that they restrict use to the machine that they are installed on. Although the user are normally has to enter a password to activate the certificate, in most environments they do not provide a high level of user authentication.

Conclusions

- Passwords provide trivial protection against determined hackers and fraudsters.
- Two factor authentication is currently the only viable means of safeguarding users and network administrators from ever more sophisticated forms of online identity theft.
- There are many different ways of achieving two factor authentication. All increase security by magnitudes compared to simple password protection.
- Smartcard, token-based and biometric authentication systems all carry relatively high costs for equipment purchase and implementation, and have significant ongoing administration and maintenance overheads.
- Users normally have to carry a separate token, smartcard or authenticator for every protected application that they use.
- Phone-based systems reduce or eliminate the cost of client hardware provision and solve the “token necklace” problem. However, “one-time-password” systems have unpredictable running costs for SMS or voice messaging.
- Identrica is a new phone-based system that uses telephone signalling data instead of one-time-passwords to provide strong authentication without any new hardware or per-logout running costs.



Simple, secure, affordable authentication

Identrica Ltd., Cipher House, Silver End, Olney, Bucks, MK46 4AL
T: +44 (0)1234 714138 F: +44 (0)870 0529238 E: info@identrica.com