



The Internet Authentication Service

'Passwords: Why they are so easy to crack'

~ a guide to the five favourite methods used by password pirates to penetrate your systems and how to combat them ~

Passwords are a problem

At present, the majority of companies use standard re-usable passwords to secure entry into their company systems or to log in remotely to their email, intranets, extranets, CRM and other line-of-business applications.

Standard, re-usable passwords are a very insecure way of keeping company or client information under wraps. Passwords can be easily cracked, stolen or guessed; and once someone's username and password has been hijacked, that person's entire digital identity is vulnerable: the attacker instantly acquires all the privileges of his/her victim.

All this can happen without the victim being aware that their password has been compromised and if the attacker is careful, no-one may ever know that the attack has happened. For companies it means confidential business information can be easily copied or read by unknown sources without the alarm being raised.

Most companies have a poor understanding of how easy it is for someone to enter their system. With standard password based systems, individuals re-use the same credentials each time they log in, and they are compared against a password database which is typically stored on the company system. So the password can be acquired either by snooping on the user's network connection, hacking the system's password file, or simply by copying a back-up tape. Passwords are normally stored in an encrypted or 'hashed' format, but there are now powerful password cracking tools, which can decrypt any password within minutes or a few hours using a standard PC.

Strong authentication is the answer

Ideally, companies need to eliminate use of re-usable passwords in favour of a 'one-time passcode' system. Under such a system, each passcode is only ever used once, then thrown away and a new one used the next time the user logs in. So even if an attack does manage to snoop the user's passcode, it is of no value as it cannot be used a second time.

The ideal solution is a one-time passcode system, which requires 'two factor' authentication: users must present two proofs of their identity: typically *something they know* - a secret PIN, and *something unique they have* - a token or smartcard.

In the most popular system: **RSA's SecurID**, the user's token creates a new code every minute, and this is combined with the user's secret PIN to make a unique one-time passcode. The SecurID system is favoured by users due to its simplicity and robust reliability and is currently used by over 7 million people worldwide. It ensures those gaining access to secure confidential company information really are authorised users - and not just a pirate who has stolen someone else's password.



The Signify SecurID keyfob token

However, strong authentication systems like SecurID, can be complex and require significant technical expertise and logistical resources to implement, so companies need to consider outsourcing the management of this service to a specialised service provider.

Until they do so, Signify has written this guide to help companies understand password cracking. This guide examines the five key areas where companies need to be particularly vigilant, including the methods of infiltration used and advice on how to tackle them.

The Password Pirate's "Top 5" techniques

1. Shoulder surfing

An extremely simple technique that people use to discover passwords. By peering over a shoulder or using readily available Web cameras, 'password pirates' can easily track the sequence of keystrokes used by the victim to log in. This is the most common method that work colleagues use to steal someone's online identity.

Solutions: The only way of preventing the above is to alert staff to the ease at which their password can be obtained. It is a modern courtesy for people to look away when a colleague is logging into a system, and people can reasonably request others to do so. If companies insist on using re-usable passwords, it is advisable to lay down a company policy. This should indicate to staff that they are not allowed to reveal their passwords to fellow staff members and must change it on a regular basis.

A recent example of this creating significant business problems is at Airbus. Airbus announced recently that it has introduced a company-wide policy forbidding staff to work on projects using their laptops when making aeroplane journeys. The rule, which could equally apply to train travel, has been introduced to maintain the integrity of the company's data after one of its managers reported he had covertly read sensitive project information off the laptop screen of the person in the next seat.

2. Guesswork and dictionary searches

A very simple method and often easier than you think. People usually choose passwords that are fairly obvious, such as their date of birth, mother's maiden name, partner's name or their pet's name. This makes it an easy hit for people to guess someone else's password. Most password cracking tools also come with pre-prepared dictionaries of commonly used passwords in multiple languages. It will then match and crack any password that it finds in its dictionary within seconds.

Solutions: IT managers should warn staff not to use passwords that are personal to them or that can be found in a standard dictionary. The company should set up a password management system, which is often built into NT and other operating systems. These systems will ensure that users change their password regularly and are using passwords which contain a combination of letters, numbers and other keyboard symbols to defeat dictionary search attacks. Not always the most user-friendly of systems, but a way of reducing the risk of passwords being guessed.



3. Password Snooping and Cracking

Companies should be aware that password cracking technology exists and is a powerful and effective tool. It is extremely simple to use and readily available over the Internet.

An example of this technology is L0phtCrack, a very user friendly utility which can be used by anyone to break the MS Windows network password system. It provides a 'network sniffing' tool to collect encrypted passwords off the LAN and extensive dictionaries of commonly used passwords. L0phtCrack is then used to break each of these encrypted passwords.

Firstly, it tries dictionary searches, which is a very fast way of finding easily guessed passwords (names or any word in a standard English or foreign dictionary). Secondly, if it does not get a match on these it tries a brute force approach – trying every combination of letters, numbers and symbols to generate a match. Most passwords are found within seconds or minutes via the dictionary search techniques, but more complex passwords take longer – hours or a couple of days - but it will get there in the end.

One way of checking your system security is to run such technology and see what the results are. For example, L0phtCrack was used in an audit of a large hi-tech company. Although the company had enforced a rigorous password policy, L0phtCrack cracked 90 per cent of its passwords in 48 hours.

Solution: Carry out a full audit on your own system using these popular cracking tools before the hackers do it for you. That way you can check how robust your users' passwords are to these tools, and will give you the ammunition to justify investment in a strong, two factor authentication system.

4. Keyboard tapping

This technique works by infecting a PC with 'remote control' agent software such as NetBus, Back Orifice or PC Anywhere. These allow the hacker to take control of the user's machine remotely, across the LAN or WAN enabling them to capture every keystroke that the user makes on his or her PC.

Solutions: IT managers should be ensuring that virus protection software is up-to-date on all PCs. Such technology will be able to detect if a PC has been infected by a remote control agent. There are also intrusion detection tools, such as RealSecure from ISS, which can monitor your network in real time for this sort of hostile traffic and will highlight if such activity is taking place illicitly across your networks.

Stealth infection by "Trojan Horse" Virus

Viruses provide a powerful and simple 'hands-off' way to break into a company and install a 'Trojan Horse' password piracy program. Virus building kits are freely available and you only need basic programming skills to develop your own variant.

The virus masquerades as a friendly bit of fun: an image file, game or utility but the attacker has hidden a 'Trojan horse' program within it. This is then sent by email to someone at the target company. This script is often not detected by the anti-virus programme and is activated as soon as the email recipient opens it. The Trojan horse code quietly installs itself on the victim's machine and sets about capturing names and passwords from the system and surreptitiously e-mailing them back to the hacker. Importantly the virus is not designed to do any obvious damage, so no one is aware that it is sitting there in the background doing its dirty work.



It was this type of procedure that was allegedly used to penetrate Microsoft's defences recently. Using the well know QAZ Trojan it is suspected that the hacker had pirated the names and passwords and was using these log-in details to enter Microsoft's network. Using this method, the target organisation would be unable to establish whether the person entering the system was a disgruntled employee or a competitor.

Another classic Trojan Horse, which always fools users, is one that mimics the Windows operating system. It works by popping up a window on the user's PC when it sees the user accessing their network, which will display something like:

```
"network access failure - please log in."
```

It then presents a familiar network log-in prompt for the user's log-in details. Most people would simply assume that they had been logged off the network or that the system had crashed and innocently log-in again. They would fill in the details and the virus would capture the data and send it back to the password pirate.

Solution: It can be difficult to prevent such an attack from happening. The average virus scanners can only recognise known viruses and competent pirates will re-design a virus in such a way that it is not detected. IT managers must ensure that they are regularly updating their anti-virus software as well as prompting their users to do so.

Conclusion

All these are stop-gap measures that will never give adequate protection against the determined password pirate. The only solution is to eliminate the use of standard passwords and implement strong, two-factor authentication systems that generate throw away one-time passcodes which will really scupper those pirates.

For further information please contact Signify at:

Tel: +44 (0) 1223 472572
Fax: +44 (0) 1223 472573
Web: www.signify.net