Putting security back into passwords

Passwords may be the ubiquitous authentication method chosen by the business community, but the system is riddled with flaws that can leave critical information exposed. **Kevin Foster** of **NTA Monitor** outlines the steps that businesses can take to minimise the risks.

Whether logging onto the network in the morning as part of the daily routine or shopping online, we cannot escape the need to authenticate ourselves in order to use shared computing resources. For good reason, there is a great deal at risk. Companies entrust highly sensitive records to username and password authentication, and equally, we do the same with our identity and credit card records when we shop online.

Although this is the *de facto* method of authentication, does this method of uniquely identifying ourselves really provide the appropriate protection? We will consider below the common risks that simple username and password management present to users, customers, and organisations. We will also take a look at recent research into password attitudes and practices. Finally, the inadequacies of passwords are well known and documented within the security community. Yet why do we not use anything more sophisticated? After all, passwords have been around for centuries. Surely we can do better?

Risks through weak passwords/management

The primary risk associated with any authentication mechanism is whether the secret values used in the exchange between a client and a server remain secure, and whether it is possible for the authentication details to be accessed and used by an unauthorised person to gain privileged access to restricted data and resources. In evaluating such a risk consider:

1. The strength of the username and the strength of the password combination used

2. Procedures and practices to manage and protect account details

3. The security associated with the authentication channel used; and

4. The security of either the client or the server applications.

Username & password strength

Password strength (and weakness) is determined by a number of factors, including:

• Number of characters used

• Range of character sets used: upper and lower case letters, numbers, punctuation marks and extended ASCII characters

• Sequence length of one particular character type (ie. Aaaaaaa1 or 1234567b); and

• Avoiding 'guessable' phrases (dictionary words, slang, words spelt in reverse etc.).

The main threat then comes from users selecting weak or easily guessable passwords. The greater the number and variety of characters used, the stronger the password will be. But, remember that password authentication's ubiquitous use is due primarily to its ease of use and minimal per user costs. The cost savings are achieved by storing sensitive password data in the user's brain, not expensive electronic devices. We prefer to remember simple things; places, names, animals, not complex strings of characters, and numbers. Which is why users typically gravitate towards easily guessable dictionary words as passwords. At this point, the usability verses security dichotomy becomes apparent. Users will undermine the security of sensitive data if they are allowed to.

Dictionary words are to be avoided at all costs. They are easily guessed by automated password cracking software which can attempt hundreds of thousands of combinations per hour.

So here is the dilemma: users need to remember passwords, are advised not to write them down or store them online. The passwords should not be dictionary words, car registration plates, birthdays etc. but a random selection of letters, numbers and extended characters. How do users react to such constraints?

NTA monitor password survey results

NTA Monitor conducted a password survey of 500 users in December 2002 to investigate password usage attitudes and practice, and their implications on corporate network and e-commerce security (see www.nta-monitor.com). The key findings were:

• Users are compromising their personal security in a bid to manage an increasing number of different passwords, with an average of 21 passwords across multiple websites and IT systems for heavy users

• 84 per cent of computer users consider memorability as the most important attribute in selecting a password

• 81 per cent of users select a common password where possible

• 67 per cent of users rarely or never

change their passwords

• 22 per cent admit that they would only ever change their password if forced to by a website or system/IT department

• 49 per cent of heavy computer users write their passwords down, or store them in a file on their PC; and

• 31 per cent of lighter users write their password down, or store them in a file on their PC.

COMMON PASSWORD SECURITY ISSUES

Too many to handle? - It can be tough enough for users to protect just one account, imagine if you have to manage 5, 10, 20 or more accounts? NTA's results show that 8 out of 10 people use a shared or common password across multiple accounts - ie. the same password on their eBay account as their network login. If the home PC is compromised, the same account data could be used to plunder other accounts, including the individual's work accounts.

Writing down passwords - The cardinal sin. All password security policies mandate that you do not write down your password, but that it should be committed to memory. In practice, we have been to customer sites where key staff have multiple passwords written down in their notebooks, and even on the backs of picture frames. Security breaches result when these items are lost, stolen, or worse, simply copied and returned.

Some prefer to store all their passwords in a secure excel spreadsheet stored on their PC or laptop. This is lethal if either can be accessed physically or across the network, given that user PCs are inherently insecure.

Lack of user awareness - Many security breaches arise through staff being unaware of the risks of why they need to keep their password secure and how they can achieve security. Generally, users are unaware of the likelihood of their account being breached, and the impact this could have on themselves or the organisation they work for, and hence get lazy and fail to keep passwords secure. This could range from being lax and writing it down somewhere obvious, hinting to colleagues that it is similar to a family name, even telling colleagues their password so they can access essential resources while they are on holiday.

Stale passwords - Passwords need to be changed regularly. If not, a compromised account could stay active for months (even years) allowing an attacker privileged access.

Crackers go for the weakest passwords and typically do not target a single account. Attackers targeting password accounts rarely attempt to crack just one single account. They run a brute force attack against a password file or login pages that allow unlimited attempts. Typically the cracking software will return a hat full of weak passwords which the attacker can use to gain deeper access. When we talk about the combinations required to crack passwords, it is every possible password using that scheme, including your one!

> Users are compromising their personal security in a bid to manage an increasing number of different passwords.

In practice, poor system restrictions, and user choice mean that password crackers can be tailored to hunt for common patterns - ie. the first character is a capital letter, the last character is a number. This means that passwords can be cracked in a fraction of the theoretical maximum time.

Software configuration errors and vulnerabilities undo all good user password practice - If the system you use to authenticate your identity has been poorly configured or has software vulnerabilities associated with either the authentication mechanism - eg. Microsoft's PPP (Point-to-Point Protocol) channel - or the application itself, no matter how strong the password, potentially all password information, and data can be exposed.

IMPACTS OF PASSWORD BREACH

Customer data stolen or exposed - For online transactions, this is perhaps the biggest fear for security managers and directors (see p.9). Exposure of sensitive customer records is highly likely to constitute a breach of national data protection laws, if the company has not taken due care to protect user data - resulting in possible compensation claims or enforcement action from the national data protection authorities.

Access to other users' records - Poor password system design can expose customer records to unauthorised users. A large UK public utility made the pro-active offer to 7,500 of its online users of £50 compensation each - totalling £350,000! (€520,000) - to change their credit card details after they exposed a subset of their customer records on one of their online billing sites a couple of years ago.

Financial theft - Access to board level staff or business trading accounts can result in financial theft, either through transferring online funds, or trading shares. There was a case of rogue share trading through a Malaysian online trading site earlier this year.

Intellectual Property - Intellectual property is the main asset for the majority of companies - specifically in fields that require ongoing research and development, from those involved in computer or software design, to pharmaceuticals, to racing car manufactures.

Network and system access disruption - Weak password access to any one of an organisation's key Internet systems - router, mail server, or e-commerce system - could result in dramatic disruption. At the router level, for example, an attacker could stop all Internet access outbound and inbound. No one would be able to access your extranet records, buy online or even send or receive an e-mail.

Access deeper into the network - A compromised administrator password on a perimeter system could enable an attacker to gain access deeper into the network, by 'sniffing' all password traffic visible to that host. Internal databases, financial or R&D systems could be compromised.

How can organisations tackle the problem?

Organisations need to approach this problem from both a technical and social perspective.

The appropriate technology must be in place and maintained to securely protect passwords. Enforce strong password selection (when creating accounts) using software that rejects weak passwords. Audit for weak passwords with password cracking software on a regular basis.

But technology alone will not solve this problem. An effective security policy needs to be implemented, maintained and enforced. The policy at the user level should be brief, and able to be read and understood by non-technical staff. As part of induction to the company, all staff should be educated on the risks of password exposure so they understand the need to maintain the security of passwords. Existing staff should be given refresher training each year. Security staff should perform a walkthrough of offices, checking for passwords being written down and stored on users' desks.

The password policy must be integrated with staff contracts and backed up with defined disciplinary action if the policy is breached. Remember it could be the CEO that is compromising the whole company's security - do you want to tell him he is wrong? Better to direct staff to the appropriate schedules defined in their contracts.

Making a strong password

A strong password has the following characteristics:

1. Uses both upper and lower case letters a-z, A-Z - **52 combinations**

2. Uses a mix of numbers, 0-9 - **10 combinations**

3. Uses punctuation marks, and other extended characters (e.g. `!"£$%^&*()_+-={}[]:@~;'#|\<>?,./) - **34 combinations**

4. Uses short character sequence length - ie. using the format aR1%*d8Nu^? not Abcdef123

5. Is at least 8 characters long

6. Is not a word in any dictionary or language, slang or written in reverse etc.

7. Do not correspond to personal information, eg. national insurance or social security numbers, staff ID, family members, pets, license plate numbers.

8. Are not written down or stored online; and

9. Make each password uniquely memorable to you.

Given the advice above, this appears to be quite a task. But the length of passwords and their complexity can be increased by using the first letters of phrases/song titles and mixing up the cases of letters, swapping letters for numbers and inserting punctuation marks.

For example: 0TfD0CmT!GtM looks daunting to remember at first, but when you know it stands for "On The First Day Of Christmas My True Love Gave To Me" ('O's are replaced by zeros and the letter 'L' is replaced by '!') it becomes easier to commit to memory.

> Educate staff to never reveal their password to anyone who asks for it - even if they are from the IT help desk, or the CEO

The maximum theoretical number of attempts required to crack a password is calculated as: the total number of combinations possible for each character raised to the power of the number of characters used.

So adopting the advice above, our example would require a theoretical maximum of: 96 to the power of 14 attempts to crack this particular password. This equates to about 36,000 billion years, based on a supercomputer cracker working at 5 million attempts per second.

This is overkill but the most reliable way of increasing the security of your password is to increase the number of characters used. For example, using lower case letters alone - an 8 letter password could be cracked in just 11.5 hours. Use the same scheme but 14 letters, it would take 410,000 years.

Good password practice

A strong password alone is not sufficient, it needs to be supported by good password practice.

Passwords should be changed regularly, at least once per quarter. Usernames should not be trivial either, and should never be set the same as a password. Privileges for each account should be limited solely according to the reasonable needs of each individual user. Educate staff to never reveal their password to anyone who asks for it - even if they are from the IT help desk, or the CEO. And finally, password accounts should be disabled when individuals leave the company.

Password management options

The task of managing a personal collection of more than 5 passwords can be tough, leading to users compromising security, either by choosing guessable passwords, using passwords common to more than one account, or writing them down.

Single Sign-On

SSO has been touted as the silver bullet to resolve this problem for years, yet still has not reached mainstream acceptance. Perhaps one of the main problems, is the diversity of applications that need authentication. There are some interesting products on the market that address the problem of handling multiple business logon accounts, and seed them all to one master authentication action (see p.26 for more on SSO).

Other forms of authentication to consider

There are three main types of authentication:

• One-factor - something you know (eg. password, mother's maiden name)

• Two factor - something you have (eg. smart card or token); and

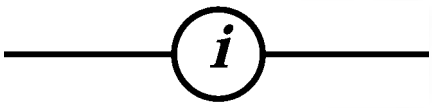
• Three factor - something you are (eg. unique - retina, fingerprint, signature).

Passwords use only one of these. The security is considered to increase with the number of authentication factors used. Two factor authentication includes products such as Axent's defender and RSA's Secure_ID tokens, which gener-

ate random password numbers that are only ever valid for one period in time. They have a relatively high unit cost, between €45 and €75 each, so this is a solution confined to government and business environments. Biometric scanning can authenticate based on: fingerprints, hand geometry, retina, iris, facial structure, signature and voice characteristics. The reliability of different methods vary, but have excellent potential for use in public spaces like office blocks and airports.

CONCLUSION

In summary, it is clear that username and passwords can provide strong security but rely on users selecting complex passwords and committing them to memory. Organisations can help users keep passwords secure by implementing the correct policies, training and system controls. It seems achievable for a small number of passwords but the problem becomes impractical to manage when users are required to use large numbers of accounts. This often leads to users' compromising good password practice in favour of memorability. Ultimately, organisations need to consider alternative solutions if they require users to manage large numbers of passwords.



AUTHOR: Kevin Foster is strategy director for NTA Monitor.

ABOUT NTA MONITOR: NTA Monitor (www.nta-monitor.com) is a European market leader in Internet security testing with hundreds of blue-chip clients in Europe and Asia across all sectors. The company provides a full-service security testing range including, Regular Monitor for external Internet and Extranet penetration, e-Commerce service for application security, On-site Perimeter Audit service for additional layers of Internet security assurance, and War Dialling to detect rogue modems. NTA delivers consultancy and perimeter protection solutions to help organisations implement an effective defence, preventing unauthorised access to company networks and sensitive online data.

Privacy Laws & Effective Workplace Investigations
April 23-24, Vancouver, Canada
This two day event will tackle issues such as employee monitoring, medical data, and drugs and alcohol use.
Contact: Insight Information
Tel: +1 888 777 1707
E-mail: order@insightinfo.com
Website: www.insightinfo.com

European Privacy Officers Network (EPON)
April 29, Madrid, Spain
Featuring presentations from Spain's new Data Protection Commissioner, Professor Dr Pinar Manas and his staff. A full programme is available on the *Privacy Laws & Business* website (www.privacylaws.com).
Contact: Stewart Dresner
Tel: +44 208 423 1300
E-mail: stewart@privacylaws.com

Infosecurity Europe 2003
April 29-May 1, London, UK
Infosecurity is the world's premier series of IT security forums, bringing together IT professionals with suppliers of security hardware, software and consultancy services.
Contact: Infosecurity Europe
Website: www.infosecurity.co.uk

Cybercrime and Privacy Conference
May 8-9, Namur, Belgium
This conference will focus on a number of issues, including the legal implications of investigating cybercrime and will examine several areas including data protection, IT forensics, and digital piracy.
Contact: Maria Veronica Perez Asinari
E-mail: veronica.perez@fundp.ac.be
Website: www.ctose.org/info/events-/workshop-8-9-may-2003.html

Guernsey Data Protection
May 13 (public sector), May 14 (private sector), Guernsey
Featuring privacy consultants, lawyers, the European Commission and the Guernsey data protection community.
Contact: Lynne Bougourd, Guernsey Training Agency
Tel: +44 1481 721 555
E-mail: admin@trainingagencyguernsey.com

The Financial Services Data Protection Conference 2003
June 25, Droitwich Spa, UK
This conference is the fifth joint financial industries conference to be held, and features Richard Thomas, the Information Commissioner, as the keynote speaker.

Issues covered include the electoral register, the directive on privacy and electronic communications, the Lord Chancellor's review of the subject access request requirements, and an update on issues in Europe.
Contact: Emma Johnson, Council of Mortgage Lenders
Tel: +44 207 440 2219
E-mail: Emma.johnson@cml.org.uk
Website: www.cml.org.uk

PL&B 16th Annual International Conference - Transforming Risk Assessment Into Everyday Compliance With Data Protection Law
July 7-9, Cambridge, UK
Contact: Shelley Roche
Tel: +44 208 423 1300
E-mail: shelley.roche@privacylaws.com
Website: www.privacylaws.com/whats-newframe.htm

The UK Data Protection Act Explained - Basic Training for Beginners
Leeds - April 30; London - May 28; Manchester - 11 June
Contact: Sandra Kelman, Privacy Laws & Business
E-mail: sandra@privacylaws.com

How to use the UK Information Commissioner's DP Audit Manual
London - May 12-13; Cambridge - July 8-9, London - September 15-16
Contact: Shelley Malhotra, Privacy Laws & Business
E-mail: shelley@privacylaws.com