Halkyn Consulting Ltd
15 Llys y Nant, Pentre Halkyn
HOLYWELL, Flintshire, CH8 8LN
http://www.halkynconsulting.co.uk
info@halkynconsulting.co.uk

Password Security

By T Wake CISSP CISM CEH

20/06/2011

Contents

Halkyn Consulting is a security & risk management consultancy based in North Wales. Our consultants have over 18 years' experience delivering security and risk management advice to Government agencies, home users and all size of private sector business.

Executive Summary

Smart use of passwords is an integral part of information security management.

As single factor authentication controls, passwords are vulnerable to several forms of malicious attack. However, the alternatives to single factor authentication tend to be more costly and may interrupt workflow. On the other hand, effective password policies and procedures can bring direct security and financial benefits.

This paper discusses how organisations can best integrate passwords into their security plans. It presents practical guidance on best practice in using passwords.

About Passwords

Passwords have been with us since the dawn of modern computing. In the 1960s the large university computer systems used passwords as a method of authenticating which user was accessing the time sharing system at any given moment.

Even in the earliest days, security issues were identified and measures taken to minimise the risks. 1961 saw the introduction of a hidden character entry for passwords that remains with us today, as most systems will replace any password characters you type with an asterisk or star symbol.

Today, passwords are still one of the most common implementations of single factor authentication[1] and drive the vast majority of login systems across the globe. These provide simplicity for both the user and the administrators and, as they come built into almost every server application, they are cheap to implement.

In recent years, steps have been taken to attempt to standardise good practice for passwords – for example, compliance with the PCI-DSS standard for payment cards requires a 7 character password as a minimum – and common practice is for passwords to be made from a mix of upper and lower case letters, mixed with numbers and other special characters.

Passwords are such an integral part of most online business related functions today that, in May 2011, the US state of Tennessee passed a law making it illegal to share passwords with others, punishable by up to a year in jail[2].

Password Issues

Although a very useful single factor authentication control, passwords have shown to be subject to multiple weaknesses which can be exploited to allow unauthorised individuals access to sensitive data.

As a single authentication factor, passwords are vulnerable to several forms of attack. The risk to the enterprise is that if any form of attack succeeds, the hacker now has a way to get legitimate access. In turn, this will frequently bypass significant parts of the network security.

Attacks can come in many forms – the most widely known is the "brute force" attack, where a powerful computer (or a network) is used to try all the possible combinations knowing that eventually one will succeed.

With the increase in modern computing power, it can be shown that even passwords meeting the PCI-DSS requirement are likely to fall to a brute force attack in a matter of hours, rather than the 30 or 60 days normally selected as a password change interval. As hackers become more sophisticated (such as using Rainbow Tables) the attack times drop even more – it is accepted

[1] There are three "factors" of authentication – normally described as something you know (e.g. a password), something you have (e.g. a token or smartcard) and something you are (e.g. retinal scans). It is generally accepted that the more factors you use the stronger the authentication.

[2] http://www.latimes.com/business/la-fi-login-law-20110601,0,5685350.story

that a 7 character password made from letters and numbers is likely to be cracked in less than 5 days[3].

Other types can range from social engineering – where the hacker contacts the user and tries to get them to part with the log-on details – to fairly simplistic guess-attacks, although often this will be informed by an attacker studying what the target is likely to pick as a password (often this is a spouse or child's name, pet, etc.).

Another issue, although not so much an attack, is the frequent complaint that "strong" passwords are too difficult for users to remember so they either forget (locking themselves out of the system) or store the password in an insecure manner – thereby compromising its whole purpose.

The broken solution

As understanding of these risks grows, there are more and more calls for organisations to abandon single factor authentication and buy into two or three factor methods. The most common of these was the RSA SecureID, which provides a second factor in that you need to have the token present (and enter the corresponding code). Other solutions involve fingerprint readers, retinal scanners and similar technologies.

The biggest problem with multifactor authentication is cost. Not only do you have the cost of purchasing and implementing the system, but you need to constantly ensure all people who need access have current equipment / tokens. When users lose or break them, they must be replaced and you have to constantly guard against loss, theft or compromise of the additional factors.

For most businesses this is never going to be a cost-effective solution, yet all too often companies feel passwords have failed them and end up spending money unnecessarily. It is significantly more cost effective to take the time to build a proper password security process into your business – and until you have done so, you should never consider changing to two- or three-factor authentication.

How to properly use password authentication

Passwords, used properly, provide a more than adequate method of authentication for almost every business application. While there are limitations, a sensible approach factors these in and helps build a robust security model.

By following some simple steps you can take maximum advantages of the cost effective, and secure, authentication provided by passwords.

Identify threats and risks

The first step of any security plan should always be to determine what it is you are trying to protect and what you are trying to protect against. User authentication is likely to be something you will need in multiple locations, so you should carry out a threat & risk assessment for each implementation.

---

[3] http://www.lockdown.co.uk/?pg=combi

When carrying out a threat assessment it is important to be realistic and thorough. It is just as important to know if your system is vulnerable to internet-based attackers or if there is a real chance that an attacker will get onto your premises to find log-in information.

Design your security

Passwords are only part of the picture when it comes to building your authentication model. Whatever you choose for your password standards has to fit in with your overall security design.

Is it through this process that you can ensure your password isn't masking other vulnerabilities, such as SQL injection weaknesses. There is no point building an incredibly complex password rule or even implementing two- / three-factor authentication if the attacker can bypass your access control.

Very few security breaches happen via a direct attack on the password, in most cases it is a system weakness that is exploited to grant the attackers access to the passwords. This should always be designed out before the system goes live.

Establish a password standard

Once you know what you are protecting, what you are protecting against and how passwords fit into your overall security model, you can set the standard for your users.

A password standard needs to address three critical areas and a forth area optional but certainly good practice. Depending on your situation there may be compulsory password standards you must implement (such as PCI-DSS) but if not you can establish your own following these simple steps:

Password Length

This is the first thing you need to decide upon. The longer the password, the harder you make it for an attacker to brute force, but you must also consider how you designed your system to deal with failed logins.

While it is reasonable to assume an attacker can try 100 million combinations of password per second, if you have set your system up to lock for 30 minutes after 3 failed retries, it doesn't matter how powerful the attacker's computer is, they can only try 6 combinations an hour (around 144 per day).

Remember, you should also be encouraging your users to choose passwords that are longer than the minimum and to use memorable phrases – don't allow people to fixate on the idea that a password is a single word.

Password Complexity

Once you know how long you want your passwords to be, you need to decide on what characters are to be used.

Unless you have an overwhelming reason (such as application coding flaws), you should allow and even encourage your staff to use the full range of keyboard characters for their passwords. This means there are 96 possible combinations for each character position and even an 8 character password will take months to brute force.

At this stage you also have to decide if you are going to enforce complexity. This is the difference between saying to your users "you can choose any character" and saying "you must have one upper case, one lower case, one number and a special character."

The best option is to properly educate your users and let them select their own passwords rather than mandate rules – by doing so you actually reduce the difficulty an attacker faces. However, if you are concerned your staff will resort to simplistic passwords which will undermine your security model, then set constraints.

Password Age & Expiry

Nothing lasts forever and this is especially true of passwords.

Passwords must always be set up in a manner that you can cancel them as soon as a user no longer needs access or when set periods of time elapse. This is the password ageing process.

Rather than decide on an arbitrary period of time (frequently 30, 60 or 90 days), you should work out what best suits your security model and design the ageing rules to fit your business needs.

The way to calculate this is to estimate how long it would take a dedicated attacker to compromise your passwords with a brute force attack. Half of this time period should be the maximum password age you allow.

By doing this you ensure that even if your password files are somehow compromised, by the time an attacker has broken them, it will not matter because the passwords will have changed.

Using a general rule of thumb, if you allow all 96 keyboard characters and mandate passwords be 10 characters long, then it is likely that it will take under 90 days for a brute force attack to work. This means the password age should be set to expire every 45 days.

Password Sharing & Writing Down

The optional part of your password standard is deciding if you will allow users to share passwords and / or write them down.

It is traditional for people to immediately ban all users from these acts, but you should always consider the reasons in light of your overall security posture first.

Password sharing is bad practice because it means you can no longer be sure that the user logged in is the person you think it is – which undermines the authentication process – but there may be a legitimate business reason. It is also worth bearing in mind that is it hard to stop users sharing passwords and, if you want to, then you need to make it easier for them to share resources with their own ID.

When it comes to writing down passwords, things are less clear cut, but everything still hinges on your threat analysis and security design. If you have a largely internet-based threat and believe there is a risk attackers will get access to your password file, you may want to have password rules that are very long and very complex and then allow your users to write these down to aid memory.

However, if your office areas are open to the public and there is a genuine risk that people can easily walk around unchallenged, you may want to prohibit the practice. Again, it is worth bearing in mind how difficult it is to prevent users writing down passwords if they struggle to remember them.

Benefits of good password security planning

As you can see, there is a fairly straightforward process to follow when it comes to planning your passwords. By working through each stage, the decisions become easier and you have the significant advantage of knowing that your decisions are sensible, rational and most importantly applicable to your business.

The direct benefits of following this process are:

- **Direct Value**. By using password authentication properly you can save yourself having to spend large sums of money on multi-factor systems.
- **Improved Security**. Your security is built around how you do things, not some other company elsewhere in the world.
- **Reduced Operating Costs**. Well implemented passwords are easy for the users to remember and simple for administrators to control.
- **Enhanced Training**. Knowing why you have made decisions about passwords will make it easier to work authentication into your security awareness programmes.

Summary

Passwords authenticate users to systems. They are a crucial first line of defence. However, they may be vulnerable to attack. Potential attacks include "brute force" (trying many combinations of possible characters) and "social engineering" (obtaining password details from people). If compromised, a password can provide the attacker with full access to your information systems.

To ensure that an organisation gets the best value from passwords, it should adopt an approach that integrates password use into its general security plan.

This plan must start from an identification of potential threats and a realistic evaluation of the risks that might result from a breach. Appropriate and proportionate security measures should be designed, with a focus on establishing standards for creating, managing and using passwords. All password holders should be made aware of their roles and responsibilities for implementation.

Taking this approach will bring a range of benefits to your organisation, including financial savings and an improvement in general security levels.

About Halkyn Consulting

Halkyn Consulting Ltd is a specialist security consultancy based in North Wales, experienced in providing security advice to local, national and international clients including government agencies, multinational corporations, small businesses and homeowners.

For more advice on how to properly use passwords or any other questions you may have related to security and protecting your home, business or other assets, you can reach Halkyn Consulting at www.halkynconsulting.co.uk or info@halkynconsulting.co.uk.