



The Five Failings of Password Security

Exploring the problems with weak static passwords, and how you can handle it.

White Paper

Password security is one of the weakest forms of user authentication in the industry. Yet businesses continue to use it to protect their most important corporate data. In this white paper we will demonstrate why this may be a large risk to your business, and show how two-factor authentication and identity assurance can help to protect your business against attacks to weak, shared or stolen passwords.



Copyright © 2012, Scorpion Software Corp.
All Rights Reserved

Table of Contents

| | |
|--|---|
| Introduction | 3 |
| The benefit and burden of passwords. | 3 |
| Are passwords safe? | 3 |
| Is password security really a problem? | 3 |
| Passwords can be shared. | 5 |
| Passwords can be stolen..... | 5 |
| Passwords can be easily guessed. | 6 |
| Passwords can be cracked. | 6 |
| Passwords can be hard to manage..... | 7 |
| So how can you handle it? | 7 |
| Understanding Identity Assurance | 7 |
| Understanding Two-Factor Authentication..... | 7 |
| Introducing AuthAnvil | 8 |
| Conclusion | 9 |
| About Scorpion Software | 9 |

Introduction

Password security is one of the weakest forms of user authentication in the industry. Yet businesses continue to use passwords to protect their most important corporate data. These passwords are the keys you use to access your personal and corporate data anywhere in the world. It might be for accounts local on your computer, or could be your confidential customer data that may be hosted with a provider online. They are used everywhere, which has been a great advantage to business productivity and access, while at the same time also becoming a great liability.

In this white paper we will demonstrate why passwords alone may be a large risk to your business, and show how two-factor authentication and identity assurance can help to protect your business against attacks to weak, shared or stolen passwords.

The benefit and burden of passwords.

Passwords have been around for a long time. People are accustomed to using passwords to access information, even when it seems like a burden at times. As more and more systems require passwords, it gets more difficult to manage and use effectively.

Passwords seem inexpensive. Most operating systems and applications include password security, and users are comfortable with the workflow required to use them. What's not taken into account for is how inadequate this form of security can be when used incorrectly, or with little due care and attention.

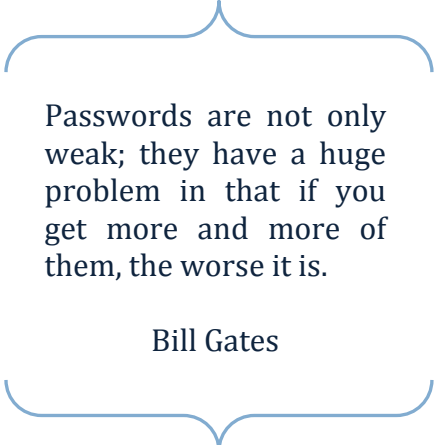
Are passwords safe?

Passwords are generally considered to be a weak form of user authentication. They can be difficult to manage and hard to remember. Worse yet, because they are so easy to pass around, you don't know if the person actually using the password is who they say they are. Add remote access for these users, and now you have a really BIG problem.

You can think of passwords as a shared secret. And much like any secret, if it gets out, the game is over. Attack vectors ranging from social engineering ("shoulder surfing") to more complex data sniffing ("key loggers") make it easy to capture and hold credentials without the user knowing. The victim typically doesn't even know they have been compromised; sophisticated adversaries will utilize their access without you even knowing it.

Is password security really a problem?

You bet! In a recent study², cases of cybercrime relating to network intrusion and data theft prosecuted and publicly disclosed by the United States *Department of Justice Computer Crime and Intellectual Property Section* that occurred between March 1999 and February 2006 were examined. The information collected and analyzed portrays a clearer picture of the attacks and real damages of computer security crimes than has previously been available.



Passwords are not only weak; they have a huge problem in that if you get more and more of them, the worse it is.

Bill Gates

Some of the key findings in this study¹ showed that:

- Most crimes, eighty-four percent (84%), could have been prevented if the identity of the users connecting were checked in addition to user IDs and passwords
- Losses from stolen IDs and passwords far exceeded damages from worms, viruses, and other attack methods not utilizing logon accounts
- Vast majority of attackers, seventy-eight percent (78%), committed crimes from their home computers; most often using unsanctioned computers with no relationship to the penetrated organization

Based on the responses from over 600 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, the findings of the “CSI/FBI Computer Crime and Security Survey” (<http://www.gocsi.com>) confirm that the threat from computer crime and other information security breaches continue unabated and that the financial toll is mounting. Patrice Rapalus, former CSI Director explains this best when he says “There is much more illegal and unauthorized activity going on in cyberspace than corporations admits to their clients, stockholders and business partners or report to law enforcement. Incidents are widespread, costly and commonplace.” This has significant implications for businesses in a whole variety of ways:

- The cost associated with loss of data and information. This includes everything from the cost to recover lost data or information to the more extreme example of having to completely rebuild a data or information set from scratch. This might also include the loss of competitive advantage to others who come to access this lost data.
- The cost associated with lost reputation for breaches of confidentiality. Many, many businesses would suffer huge losses if their customers thought that their confidential data has been accessed – financial institutions and any institution maintaining financial records, and any business that collects credit card numbers are just a few examples.
- The cost associated with a breach of laws, rules or regulations. Many businesses are obliged by law to maintain confidentiality – medical, hospital, legal etc. A breach of their information might also result in legal or regulatory sanctions over and above loss of reputation and customer confidence.

Because of the extremely embarrassing and costly nature of such a breach, these businesses work hard to keep these examples quiet. However, they do happen and happen frequently. Highlights from the “Computer Crime and Security Survey” survey include:

- 52% of respondents detected computer security breaches within the last twelve months.
- 98% of respondents had firewalls installed when they were breached.
- 97% of respondents had anti-virus installed when they were breached.
- 74% of the financial losses were due to viruses, unauthorized access and theft of proprietary information.

Clearly it’s not safe out there. Attackers today are highly sophisticated, well organized and are relentlessly probing weaknesses in network and application security with a specific intent to steal, spy or cause damage. Existing firewall and anti-virus software cannot keep up with the attack of new blended threats taking place in

¹ “Network Attacks: Analysis of Department of Justice Prosecutions 1999 – 2006”

the growing hostile world of the Internet. Insider threats to proprietary information and critical business resources lead to large risks of financial loss, and weak static passwords make it easier for attackers to get in.

As companies extend access to their business online, they need enhanced password security, better identity management, and improved remote access control.

So let's explore the five failings of password security, and then discuss what you can do to handle these risks.

Passwords can be shared.

The very nature of passwords makes it easy to share. There is no way to tie the user to the password, which means anyone can use that credential and pretend to be someone they are not. And there are literally thousands of news stories about how this is taken advantage of to provide incentive and financial gains to users.

One such example is in the scandal that rocked the banking world in January of 2008. French bank "Societe Generale" revealed that a single insider had produced losses in excess of \$7.2 billion through fraudulent trades. He was able to use passwords² belonging to colleagues³ to hide transactions and create false accounts to bypass monitoring safeguards that the bank had in place.

Another example of just how easy it is to share passwords comes from a survey⁴ by Infosecurity Europe (www.infosec.co.uk) who found over 70% of the office workers were prepared to give away their password to strangers masquerading as market researchers with the lure of a chocolate bar as an incentive for filling in the survey. Another slightly worrying fact discovered by researchers is that over half of people questioned use the same password for everything (e.g. work, banking, web, etc.)

There was something more worrisome found through previous⁵ Infosecurity surveys though... two thirds of workers admitted to have given their password to a colleague and three quarters said they knew their co-workers passwords!

Passwords can be stolen.

In this day and age, the threat landscape that makes up the Internet shows us that it is hard to defend against the villainy of the unknown. The viruses, vandals and thieves that now exist make it extremely difficult to trust websites, applications and even email, whether you believe it comes from a trusted source or not. The number of hostile systems and programs continues to grow as cyber-criminals and pranksters deliver more intelligent malware to attack systems and steal valuable information.

It's easy to dismiss this kind of threat as more imagined than real, but consider that in April of 2008, around 20,000 corporate executives received phishing emails that purported to be a subpoena. The emails seemed authentic because they addressed the execs by name and included their phone numbers, as reported⁶ by the Washington Post. By clicking on the link in the email and following the directions supposedly required to view

² http://www.infosectoday.com/Articles/Privileged_Password_Management.htm

³ <http://www.iht.com/articles/2008/02/04/business/socgen.php>

⁴ <http://news.bbc.co.uk/2/hi/technology/3639679.stm>

⁵ http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/

⁶ http://blog.washingtonpost.com/securityfix/2008/04/identity_theft_smash_grab_ceo.html

the subpoena, the executives installed software on their computers that could then steal usernames and passwords. So far, the scam has netted over 2,000 victims, according to the Post.

Passwords can be easily guessed.

On average, the human brain can hold only four to nine "random bits of information" in short-term memory⁷. Considering this and the sheer number of secrets a person needs to remember in this password-protected age, it is not surprising that the most common password is simply "password."

Besides serving as an easy-to-remember code for less-creative computer users, "password" is often used as the default password for many web sites and software applications, making it extremely common and not at all secure. In other words, "password" is a bad password. With more complex password policies now being enforced, the most popular password as of late is "password1". Doesn't seem that we learn much.

Other perennial favourites include "God," "sex," "money," and "love." Passwords based on the names or birthdays of partners, children, or pets are also quite common. And so are passwords that refer to the system or website in question. As an example, in a recent analysis of 34,000 real passwords stolen from Myspace.com⁸ users in a phishing attack, two of the most popular passwords used were "myspace1" and "password1".

As we use more online services and access more privileged systems that require passwords, the worse it becomes. It turns out to be much easier to use a common password across multiple systems, or use passwords that may be easy for an attacker (or computer) to guess, knowing only a small amount of information about the target.

Passwords can be cracked.

If there is one thing that computers do well, it is completing mundane tasks over and over again without complaint, or tire. Computers can complete millions of computations a second, making it straightforward to process information in way we humans can't. In its common form, "password cracking" is done when a computer tries to repeatedly guess a password. Over the years, there has been plenty of software applications released that you can download for free that allow you to "brute force" your way to get someone else's account.

As passwords become more complex, the task to attack them does also. To keep up with this trend, attackers have come out with methods to pre-compute the values to compare against, speeding up the time to break weaker passwords if they can get access to the password information on a system. Famed security expert Bruce Schneier revealed⁸ that in the Myspace attack previously discussed, more than 55% of the passwords would have been cracked in less than 8 hours. Yet that particular demographic shows to have a majority of younger computer savvy users. In another study, it was found in an analysis of 200 corporate accounts that the passwords were even worse, with an average length of less than 8 characters with only alpha-numeric representation. This means it would take even LESS time to attack these corporate passwords than many of the ones found on Myspace.

⁷ http://en.wikipedia.org/wiki/Short-term_memory

⁸ http://www.schneier.com/blog/archives/2006/12/realworld_passw.html

Passwords can be hard to manage.

The difficulty for users to manage password credentials as businesses become more connected has caused the introduction of weaker passwords that are easy to collect or circumvent. Industry studies⁹ show that the average user has to remember 20 or more different passwords for the various systems and applications that they use each day.

Typically these users will try to keep the same easy to remember password across multiple systems. When that is not possible, many times they write their passwords down where they are easy to find, such as on yellow sticky notes which they leave near their computer. Further to this, the usage of hostile malware such as keystroke loggers and other data mining applications allow adversaries to easily collect these passwords to gain remote access to multiple systems in the business and ultimately gain access to protected resources and privileged information.

So how can you handle these failings?

The biggest problems with passwords are that they can be shared, stolen or easily guessed. Once that occurs, someone else can take on the identity of the user that credential belongs to, effectively gaining access to all information that account is authorized to view. There is no way for you to determine if it was the actual user or not, and in many cases you won't even know the account is breached.

The way to address that is through Identity Assurance.

Understanding Identity Assurance

Identity is the foundation of trust. Without the confidence in knowing who is using a particular credential, you simply cannot rely on passwords to access confidential information if you need to be sure who is viewing and updating the data. Being able to prove the identity of someone when they try to login to access information reduces this risk and provides greater assurance that they are indeed the intended party.

There are many different ways to attain identity assurance, with varying levels of trust. One of the most efficient and cost-effective ways is to provide another factor of authentication that binds the transaction together with the user. This is more commonly called two-factor authentication.

Understanding Two-Factor Authentication

Two-Factor Authentication (2FA) is the process where an identity is validated with two distinct and different pieces of information in the form of:

1. **Something you have** – a physical device of some kind. This could be a security token, a smartcard or even a simple key.
2. **Something you know** – a secret that only the user knows, such as a personal PIN

⁹ "Identity Management: Consumer's Habits & the Potential Backlash Faced by Business" published by Winmark Research <http://www.rsasecurity.com/go/ntk/idmreport/IDManagement.pdf>

We can see 2FA used all around us. Some examples include long distance phone cards and physical door access systems to financial transactions completed at an ATM at our local bank.

The fact you have something (like a bank card), and know something (like your 4 digit PIN), gives enough assurance that the person using the credential is indeed the intended party.

One such 2FA system comes from Scorpion Software, with a product called AuthAnvil.

Introducing AuthAnvil Two Factor Auth

AuthAnvil Two Factor Auth is the first strong two-factor authentication system designed for small business. It helps to reduce the risks of remote access to corporate systems and data, and adds a way to positively identify that users who connect to the office are who they say they are, and are authorized to do so.



Remote access points to a business such as those from Terminal Services, Outlook Web Access, Remote Web Workplace, VPN and even Sharepoint can now be strengthened with two-factor authentication with just a few clicks. Simple and easy. At a price small businesses can afford.

Two Factor Auth provides the physical hardware tokens (something you have) which you carry around with you, along with a personal PIN (something you know) which you use during login. When you need to connect to privileged company resources like your email, computer systems or databases you are challenged to include your *AuthAnvil Passcode* along with your normal login credentials. An AuthAnvil Passcode is a combination of your personal 4 to 8 digit PIN along with a one-time password (OTP) generated with your token. Combined, it produces a complex credential that cannot be guessed, forged or ever used twice.

More importantly, it provides an identity assurance validation that the person accessing your company assets not only knows the appropriate password, but also has the right PIN and hardware token when they attempt to log on. In other words, even if an adversary was able to obtain, steal or guess a password, it will be useless to them, reducing the risk exposed by weak password security.

More information about Two Factor Auth can be found at www.authanvil.com.

Conclusion

For organizations that allow remote access from untrusted locations, meeting the security objectives of identity assurance is highly important to reduce the risk of business interruption and the costly financial burden that may be placed if unauthorized access to company information assets is ever realized. Proprietary information loss, bad publicity and possible legal actions can be detrimental to the growth of your business on top of the business interruption that is sure to occur in the face of a breach.

Implementing strong two-factor authentication to provide the technical safeguards as required to provide identity assurance is important to your business, and will go a long way towards helping you achieve a safer computing environment. Scorpion Software's AuthAnvil Strong Authentication System can help reduce the risk of such business threats and provide assurance levels that only *identified* and *authorized* personnel gain access to such sensitive information.

About Scorpion Software

Scorpion Software Corp. designs and delivers strong authentication solutions for small business. Headquartered in British Columbia, Canada, Scorpion Software helps small businesses manage online risk while offering unprecedented password protection. More information about the company is available at www.scorpionsoft.com.