Password Policy: The Good, The Bad, and The Ugly

Dr. Wayne C. Summers and Dr. Edward Bosworth
Columbus State University
4225 University Ave.
Columbus, GA 31907
summers_wayne@colstate.edu bosworth_edward@colstate.edu

Abstract

"We're secure! We use passwords!" How many of us have heard this claim? Or even – "We're secure! We have a password policy!" Using a password or having a password policy in today's world of computing is not enough. Passwords provide a first line of defense in most cases, but there is much more. "A recent survey by Rainbow Technologies Inc. indicates that the use of insecure passwords can be costly -- and potentially risky -- for corporate data."[Rosencrance] This paper focuses on the use of passwords and password policy and looks at the good, the bad and the ugly scenarios that arise.

Introduction

In today's world of increasing dependence on computers and computer systems, it is imperative that we be able to rely on secure and confidential connections to the computers. Traditionally, this has been by authentication with usernames and passwords. "A *password* is information associated with an entity that confirms the entity's identity." [Bishop] The password is a string of characters that can either be automatically generated by the system or selected by the entity or user. Passwords can range from a single character to passphrases, which can be hundreds of characters in length and be comprised of series of words and phrases. The goal of a password is to authenticate a user. It is a piece of information that the user knows. If someone can guess a user's password, she can impersonate the user.

"A recent survey by Rainbow Technologies Inc. indicates that the use of insecure passwords can be costly -- and potentially risky -- for corporate data."[Rosencrance] The survey results were based on responses from 3000 IT professionals and found that most users had insecure passwords. Many users create inherently weak usernames and passwords, while many others write their passwords down. Much of this is exacerbated by the constant need to change the passwords. In fact the study found that 55% of the end users reported that they wrote their passwords down at least once and that 9% of all users write every password down. In addition, 40% of the users reported that they share their passwords.

Nearly 50% of the users surveyed have at least five passwords for their business with over 24% having more than eight user names and passwords. 51% of the users surveyed reported that they require IT help to access their applications because they forgotten their passwords.

So what is the solution? 80% of those surveyed reported that their organizations have actually strengthened their password policies requiring "nonwords" for passwords, or combinations of numbers and letters. This has resulted in more users forgetting the passwords or writing down their passwords. The other extreme is that over 20% reported that they were not required to change their passwords on a regular basis.

The Bad

Passwords are often the first and only line of defense. Unfortunately, they are typically not used well. Many users choose trivial or the default passwords. Passwords are not frequently changed.

In 1977 and 1978, one of the authors worked for a company located in the northeast part of the U.S. as a system programmer. The computer was a PDP-11/45. Each account had to have a password and the company policy was that passwords should be the user's initials. This policy was well known, so when a senior vice-president left and had his account removed, they noticed a lot of suspicious activity on their modems one night and fairly soon thereafter the ex-employee's new company started producing products remarkably similar to those produced at the original company.

In early versions of UNIX, passwords were stored in a file /etc/passwd. This file was available to anyone who had an account on the computer. The passwords were stored in encrypted form as 11 characters with a 2-character salt. UNIX uses one-way hash algorithm (*Crypt*) to disguise the passwords. It was very easy to copy to a file and use a cracker program on a fast computer to discover the passwords. Some versions of UNIX now use the MD5 hash algorithm. Most versions today keep the passwords in a shadow file that is only accessible to the root account.

Early versions of Windows had no mechanism for maintaining secure passwords. Starting with Windows NT, attempts were made to secure the password of users. The password hashes are kept in a security database (SAM - security account manager) in \Windows-directory\system32\config\SAM. This file is locked when Windows is running. A copy of the password file is also copied into the Windows-directory\repair folder. Windows NT uses two hash algorithms to encrypt passwords. The first is the NT hash where the password is converted to Unicode and then run through MD4 hash algorithm to obtain a 16-byte value. The second is the LAN Manager hash where the password is padded with 0's up to length of 14 characters, converted to uppercase, split into two 7-character pieces. Each half is encrypted using 8-byte DES (data encryption standard) keys. The result is combined into a 16-byte, one-way hash value. The passwords are not randomized with a salt value (hence you only have to crack the same password for two users once).

It is relatively easy to obtain passwords in most Windows environments. This can be accomplished by sniffing the passwords off the network, booting the computer with another operating system (e.g. Linux or DOS) disk and copying the SAM file, using a program like LINNT to obtain administrator access (only works on a pre-sp3 computer WITHOUT syskey installed), obtain a copy of the SAM file from c:\winnt\repair or a backup directory, or obtain a copy from a tape or emergency repair disk.

There are many schemes for password cracking. Among the different types of password cracking attacks are:

- Dictionary Attack - uses a file that contains most of the words found in a dictionary
- Brute Force Attack - tries every possible combination of letters, numbers and special characters
- Hybrid Attack - concatenates extra characters to dictionary words and trying different combinations

“According to news reports published on 23 July 2003, Swiss technology researchers have issued a report that describes how Windows computers protected by alphanumeric passwords can be quickly and easily cracked – in less than 14 seconds – by using precalculated data stored in look-up tables.” [Wagner]

Many software products are distributed with default passwords that are never changed. For example, Oracle 8.1.7 comes with the following default usernames and passwords: SYS (*change_on_install*), SYSTEM (*manager*), and Sysman (*oem_temp*). There are a number of software products with default passwords *default* and *password*, that are never changed by the software installer.

“Security experts and overworked systems administrators for years have implored users to pick hard-to-guess passwords and to change them often. But many users persist in using their names or children's birthdays as log-on credentials, and two recent worm outbreaks have shown why that's such a risky practice.” [Fisher] The exploit of weak passwords being used by these worm outbreaks is not that much different from the exploit used by the Morris worm in 1988.

The Ugly

“Computer passwords are supposed to be secret. But psychologists say it is possible to predict a password based on the personalities of users or even what is on their desks…. According to a recent British study, passwords are often based on something obvious. Around 50 percent of computer users base them on the name of a family member, partner or a pet. Thirty percent look to a pop idol or sporting hero.”[Brown]

Eric Cole [Cole, 285] tells a wonderful story of a user who doesn’t take passwords seriously: “In the course of the conversation, he asked if I was going to check passwords and try to crack them. After I told him that I was, with all seriousness, he told me that I was going to have some difficulty trying to guess his password. He then turned around, stretched his arms over his head, took a practice golf swing, and said, ‘I think I am going to try to get in nine holes after work today.’ Do you want to try and guess what his password was? GOLF!” Cole reports that eighty percent of the salespeople he surveyed had a password of either golf or bogey.

One solution to overcome users that select easily guessed passwords is to randomly assign passwords. If you are lucky, you can keep select randomly generated passwords until there is one you like. Oftentimes, though the random password is not easily remembered. This encourages users to write down the password (and username!) and store the information in a “convenient” location. Often this is under keyboard or even on the monitor. More sophisticated users carry their list of passwords in a little black book while the more technically savvy users keep the passwords in their handheld computers.

This type of carelessness provides all types of opportunities for social engineering, where you try to convince someone to give you their user ID and password. The most obvious way is simply to ask the user for their password. Other techniques include shoulder surfing, where the “attacker” watches the user typing in the username and password, and dumpster diving, where the “attacker” looks through the trash for usernames and passwords.

The Good

So what is the solution? What are good passwords? What should be in a password policy?

It is imperative that organizations have and enforce a password policy. Policies explain what the rules are and what is expected of the computer users. Having a policy also provides a framework for enforcing password rules in a consistent fashion.

Every logon must have a strong password associated with the account. According to Vincent Weafer, senior director of Symantec Security Response, “It may be tempting to create password so they are easier to remember, but you are playing right into the hacker’s hands. The challenge is to make the password difficult to guess without making it impossible to remember.” [Armstrong].

Features of a strong password include:

- Minimum length of six-ten characters. The longer the password, the longer it will take to crack.
- Must contain at least three of the following: lowercase alpha, uppercase alpha, digit, and special character. The more variety in the password, the longer it will take to crack.
- Alpha, number and special characters must be mixed up. Don’t just add digits to the end of the password.
- Do not use "dictionary" words. This includes dictionaries of common proper names and foreign language dictionaries. Also avoid “common words” with digits appended.
- Suggestions for good passwords might include using first letters of a phrase with appropriate substitutions for different letters. For example, “May the force be with you” becomes Mt4%wU where the F in force becomes 4 and the b in be becomes %. Another example might be “I teach 3 classes at Columbus State University” becomes It3c@cSu.

Other password policy features include:

- Do not reuse the previous five passwords. Some organizations suggest never reusing a password.
- Minimum password age of ten days. To keep users from going back to a previous password.
- Maximum password age of 45-60 days. This should be determined by how long it would take a hacker to crack the passwords
- Lock password after three-five failed logon attempts. This eliminates hackers from running a program to try different password combinations.
- Do not write any password down.
- Do not share your password.
- Users must immediately change their password if they suspect the password has been compromised.
- The user’s account must be disabled after a thirty-day period of inactivity.
- Password display must be masked when echoed on the computer screen.
- Vendor default passwords must be changed before the vendor’s products are used.
- Publish and EDUCATE the users of the password policy.

Passwords must be protected. This can be accomplished by the system using strong encryption and protected shadow files. Users have to be educated about the importance of keeping their passwords private. Users must be educated about the dangers of writing the password down, even in a "secret hiding" place.

Conclusions

Passwords are an important component of securing our computer systems, but they are not the entire solution. Their purpose has been and should continue to be a mechanism for determining what a user knows. We need to include more than that. In addition to what we know, we should be including one or more of the following: "what you have", "who you are", and "what you produce." What you have may include physical devices like smart cards and tokens. Who you are include physical features like fingerprints, hand topography and geometry, retinal and iris scans, and facial scans. What you produce may include voice and signature patterns.

One popular variation of this is to use one-time passwords. With a one-time password, the user is given a device that generates a new password at a fixed time interval. The device is synchronized to a server that generates the same password at the same time. When the user wants to log into the system, the user looks at the device and types in the password, which is authenticated by comparing with the password generated by the server. Each time, the user is assigned a unique password. If a password is compromised, it will only work the one time. The drawback to this system is that the user must have the device with them whenever the user wants to connect to the computer.

Whatever the password policy, it is imperative that all users be educated on the policy and that all users understand the importance of following the policy. All of these are part of the "Defense in Depth" posture that is so important in today's world where we rely on more than one indicator to authenticate a computer user. Security is no longer an option. It is a requirement.

References

Armstrong, I. (2003). "Passwords exposed users are the weakest link". *Scmagazine*. June 2003. http://www.scmagazine.com/scmagazine/2003_06/cover/index.html

Bishop, M. (2003). *Computer Security. Art and Science.* Addison Wesley.

Brenton, C. & Hunt, C. (2001). *Active Defense: A Comprehensive Guide to Network Security*. Sybex.

Brown, A. (2002). "UK study: Passwords often easy to crack". CNN.com. March 13, 2002. http://www.cnn.com/2002/TECH/ptech/03/13/dangerous.passwords/

Cole, E. (2002). *Hackers Beware*. New Riders Publishing.

Fisher, D. (2003). "*Worms Prove Passwords Do Matter*". eWeek. March 11, 2003.

Garfinkel, S. and Spafford, G. (2002). *Web Security, Privacy & Commerce*. O'Reilly & Associates, Inc.

McClure, S., Shah, S., & Shah, S. (2003). *Web Hacking*. Addison Wesley.

Rosencrance, L. (2003). "Survey: Insecure passwords can be costly for companies," ComputerWorld. August 8, 2003.

Wagner, R. (2003). "Windows Password Weaknesses Could Threaten Your Enterprise," Gartner FirstTake. July 25, 2003.
http://www.gartner.com/resources/116500/116510/116510.pdf

Whitman, M. and Mattord, H. (2003). *Principles of Information Security*. Thomson Course Technology.