Journal of International Information Management

Volume 10 | Issue 2 Article 4

2001

New concepts in password management

S. E. Kruck
James Madison University

John R. Sciandra
James Madison University

Karen A. Forcht
James Madison University

New concepts in password management

S. E. Kruck
John R. Sciandra
Karen A. Forcht
James Madison University

ABSTRACT

Passwords have been used for many years in the security of computer systems. The password mechanism has not changed in recent years and has several inherent security problems. This paper examines several password problems including sniffers, dictionary and brute force attacks. A specific Department of Defense incident is cited to illustrate a method to thwart sniffers followed by several suggestions intended to increase the security of the password process.

INTRODUCTION

Passwords are used throughout computing today as they provide a simple means of access control and authentication, thus helping to ensure that a person accessing a particular system is authorized to do so. As technology has advanced, increasingly more complicated computer systems contain more and more mission-critical information. Unfortunately the implementation of basic password control has not changed much over the last several years. Since it is still unlikely that the basic password mechanism can and will change very quickly across large corporations or other large entities such as the Department of Defense (DOD), it may be more useful to examine the way in which these large organizations manage those passwords and develop methodologies to work within existing structures. Hopefully, by using some techniques in which the DOD information specialists may already have expertise, new ways may be suggested to manage passwords and address a few of the problems.

First, we must examine the basic password mechanism and understand some of the problems associated with it. Second, the DOD specific problem will be evaluated. Human behavior is illustrated followed by suggested password authentication schemes and password protection techniques.

PASSWORD PROBLEMS

Passwords are generally a single group of characters that are used with a login name to allow access to computer resources. The password field is specially designed to hide the characters as they are typed. The computer screen typically displays asterisks in order to hide the

underlying text. This simple programming technique protects the password from casual observers. The computer system must have a stored version of the password in a file to compare with the password the user entered. There is a danger of the file being discovered. To protect passwords stored in a password file, they are encrypted using one of several common algorithms (Garfinkle & Spafford, 1996). When the computer receives the text version of the password, it is encrypted using this same algorithm and compared to the encrypted version in the password file. If the two versions match, access is granted.

In today's world of networking, we now have centralized servers that authenticate passwords. They are often called Authentication Servers or Domain Controllers. Once authenticated, the user has access to the network and its resources. To use an Authentication Server, the password is sent across the network in its unencrypted form and then the authentication server performs the steps of encrypting it and performing the comparison. By sending the password across the network in plain text, it is vulnerable to something called a Sniffer (Cahpman & Zwinky, 1995).

Sniffers

A sniffer is a program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information from a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal since passwords are sent across the network in plain text. A sniffer can collect the text file and display it to whoever is looking. Although sniffers are difficult to detect, there are a few products that have recently emerged that may aid in detection (Brucker, 2001).

There are several problems with detecting sniffers that go beyond the technological issues. First, many network protocols do not support the detection software. For example, a network running ATM protocols will not support antiSniffer software; however, the software will work on networks using the Rthernet protocol (McDysan & Spohn, 1998). Second, sniffer detection is a resource intensive process because personnel must constantly check the network for sniffers. The success of manual searches is dubious since a sniffer can be disguised to look like other software on the network (AntiOnline, 2001; Inficad Communications, 2001; Infowar.Com, 2001).

To make matters worse, many intruders will start the sniffer software and then delete the executable file from the system. This means the only evidence of the sniffer is found in memory. One way to stop the sniffer in this instance would be to reboot the entire system.

The most vexing problem is that once deleted and eradicated, the organization is still faced with an intruder who most likely has been collecting passwords for some time and now has a base of passwords for the system. They can simply use one of the captured passwords to log in and reinstall a new sniffer elsewhere on the network. It's akin to putting a fire out with your feet. As you stomp out one flame another one pops up next to you. Evidence of this has recently been published in an article regarding intrusions in the DOD. To address this problem, under the direction of the Secretary of Defense, an order was issued for a DOD department-wide password

change that was to happen all at once. Before looking at the success or failure of the DOD password change, there are a few other password problems to examine.

Dictionary and Brute Force Attacks

Another problem with passwords is the use of words or names as passwords. These passwords are naturally easy to remember and unfortunately susceptible to a different kind of attack called a dictionary attack. Dictionary attacks read a dictionary file and as each word is read, it is used as the password for a particular account and an attempt to log in is made. For accounts that use real words or names, it is then only a matter of time before they fall victim to such an attack. There are many types of dictionaries freely available on the web. Many are centered on themes such as female names, male names, English words, rock bands, and so on. In order to circumvent such attacks, users must select passwords that are not found in any such dictionary.

The next type of attack is called a brute force attack where the intruder simply tires to sequentially go through combinations of letters and numbers that do not acctually form words. This type of attack can be very time consuming and although computer systems may be vulverable, there is a line of defense. If it would take an intruder with an average level of computing power *n* months to go through an untold number of permutations in a brute force attack, then we simply set a policy that says every *n* months the passwords must be changed. By the time the password falls victim to a brute force attack, it may be useless.

Other Options

This paper is focused only on password management but there are other technologies that can be used in place of passwords. Many of these are based on smart cards and other hardware devices that never send out plaintext versions of the passwords (AMERKORE International, 2001). In fact, the passwords themselves are actually encryption ciphers[1], thus making them very secure. There are also biometric devices being considered that can be implemented; however, they are currently cost prohibitive.

DOD SPECIFIC PROBLEMS

The DOD has specific problems in password management that are similar to other large corporations. The first is size. It becomes very difficult to manage such a large entity at the technical level. To compound the problem, each branch has its own set of guidelines and policies, making coordination on this level nearly impossible. Recently, the DOD required an across-the-board password change.

The system administrators were told to change all user's passwords. They were further instructed to power cycle the systems. They were instructed not to send out messages about these

[1] A cipher is encrypted text. Therefore, the password is encrypted twice with smart cards.

changes with the word password in them, which indicated the need for stealth. Below is an excerpt from an article posted to the *Risk Digest* by an anonymous System Administrator for unexplained reasons (Neumann, 2001):

> In the last few days I have received the most ludicrous requirement yet. It applies to every part of DOD. It requires us to change every password on the system and then power down and power up the system. I have been told this was signed off by the Secretary of Defense upon urging by his Joint Task Force for computer security.
>
> Shortly thereafter, we received another report that tell us (1) not to use the word "password" when directing our users to do this, (2) to use verbiage to our users explaining the need for the password change that is untrue, (3) to have the users change their passwords themselves rather than have the system force them to do it. On (2), I don't think they intentionally wanted us to lie; just obscure the reasons.

The fact that this article was even published indicates a failure of the necessary command and control systems and the inability to react effectively to the needs of enterprise-wide coordination. This was personnel failure that resulted in a breach of trust during the operation.

Furthermore, the tools necessary to verify compliance were not available to the system administrators to confirm that users did, in fact, change their password. The Army CERT (Computer Emergency Response Team), in an effort to rise to the challenge created a rudimentary tool that would poll domain controllers on NT systems and indicate if the password had not been changed. This was not effective for the untold numbers of UNIX systems that had to be manually verified. By reaching out to various vendors, some tools began to filter in that helped, but with great delays.

PASSWORD AUTHENTICATION SCHEMES

Passwords are used because they provide a simple means of access control and authentication to computer resources. The above discussion illustrated some of the problems with passwords. The DOD example further shows that password security may fail due to command and control issues. The following techniques are different methods to help alleviate or eliminate these password problems.

The ComSec Example

A closely related cousin to password authentication schemes is found in the Communications Security (Com Sec) arena. Most governments around the world run enterprise-wide communications networks that must be secure. This mechanism typically involves the use of communication ciphers that all nodes in the system must share. The coordination of such an undertaking must be regular, scheduled, and precise. It involves the secret distribution of all the ciphers to all nodes, which can then be implemented in a choreographed fashion. This is important since it would be a major problem if the various nodes were even temporarily cut out of the network. The scheduling of this activity is done by counting down the days since the current cipher was imple-

nented, each day known as a "ray day." This helps indicate the age of the cipher and serves as the countdown clock until the precise moment when the cipher changes.

The Iversen Principle

How can we relate the ComSec method of enterprise management of authentication to passwords? An innovative idea, which we call the Iversen Principle of Password Management, requires users to change their passwords on a set and scheduled basis. This would happen in very near synchronicity. The goal is to strive for the effect created by a DOD directive, but without the problems of coordination, without resistance by both users and system administrators and without all the requisite tools and procedures to successfully implement and verify it.

In effect, DOD would treat the management of passwords the same way it treats ComSec with regard to scheduling. There are, of course, many problems to overcome. Critics will immediately point out that this does little to solve the problem of sniffers and may actually compound the problem by providing a rich harvest of passwords to capture at once. Therefore, an effective way to minimize or eliminate the password change window and make it less vulnerable to a sniffer attack must be developed. Procedurally, the same actions can be performed as before, whereby the System Administrators would reboot systems shortly before the password change window. This is an attempt at stopping any sniffer processes currently running. Another method of eliminating this password change signature across the DOD enterprise is to not implement it enterprise-wide at the same time, but rather at the enclave level. Each enclave is responsible for setting up a random schedule of password change. Since most sniffers only work at the enclave level, this would create a very low password change window and minimize the potential exposure for the entire enterprise. By randomizing the schedule, there would be less chance of an intruder guessing when to set up and monitor the sniffer.

There would be a requirement for tools that will allow system administrators to manage scheduling, handling users who become locked out, password generators and other tools. Tools would also need to provide positive compliance verification for System Administrators.

Passphrases

The Iverson Principle does not provide a complete set of management objectives and only addresses the need for scheduled changes. There are other aspects of password management that need to be considered that will aid in the overall password management and provide another level of security. One problem with passwords is they must be remembered in order to use them. Users make several common mistakes to help remember all their various passwords, such as taping a note to the computer screen, taping it under the desk or in a desk drawer, scribbling on the desktop planner, and other places. This makes the capture of passwords to someone who is physically present very easy. In one respect, this can be considered a form of social engineering, which is a common method of reconnaissance used by potential intruders. Remembering passwords adds to the problem of how we retain information. Harold Goodglass has conducted research into how we retain information in long-term memory (McConnell, 1986). He suggests that

Journal of International Information Management, Vol. 10 [2001], Iss. 2, Art. 4

remembering and retrieving information is done by categorizing the information. The following is an example of how to file away the word "chair" in long-term memory in eight categories:

1. Identity - remember the "chair" in and of itself, often splitting it into other categories
2. Class - a "chair" is a piece of furniture
3. Attributes - a "chair" is soft or hard, large or small
4. Context - expecting to see a "chair" in a living room, not in a bathtub
5. Function - associating "chair" with the verbs like 'sit' or 'recline'
6. Sensory associations - "chair" will be paired with the sensory of typical chairs, e.g., touch and smell
7. Clangs and visual patterns - filing the concept of a "chair" away in memory and certain salient features of the word itself such as sight and sound
8. Reproductive information - includes information on the muscle movement needed to say or type the word chair

McConnell goes on to state that these are not the only means of categories we use to store the information and how the use of familiar words to form passwords, provides a mechanism for remembering them. On the other hand, the use of terse, computer generated mnemonic style passwords leaves us with no real basis for remembering them other than rote memorization. It is this reason and the inconvenience associated with forgetting the password that leads us to write them down which places them in a compromising situation.

Given the problems cited above regarding both users remembering passwords and the guessing of passwords by potential intruders, consider ways to minimize the intruder's ability to attack passwords. This is where passphrases come in. A passphrase is more like an actual sentence than a single password. Passphrases themselves are still vulnerable to modified dictionary attacks and brute force attacks and, therefore, we should not use them directly. Instead a passphrase is morphed using an easily remembered rule to create a password that is not susceptible to dictionary attacks. Tools must be developed that would aid in generating passphrases instead of random character sequences so that they are easily remembered. The way this works is that a set of rules which is unique to the site and easily remembered by users, such as "the first letter of every word," could be used to morph a phrase like, "this is how to remember a passphrase" to create a password "tihtrap." Users can easily remember a phrase and a rule. This is better than a random sequence such as r5Qtu4i, which has the same number of characters as "tihtrap." Passphrase schemes would need to be further enhanced by the addition of numbers or special characters according to a rule. By adding a random number somewhere in the password example, the morphed password becomes tih3trap, which is still easier to remember than r5Qtu4i.

Logons

There is one last idea which may be the most controversial of all. A recent penetration testing exercise team was able to successfully install a sniffer on the particular network and

capture user ID's, passwords, and other information that helped map out the network. During the course of the test, the team was able to compromise most of the systems. One system was of particular interest because a continuously maintained vigilance of the sniffer over the course of the entire exercise never captured a single login account for this system. This was truly amazing because the system was in heavy use by many different people. In post analysis, it was discovered that the system, once logged into, was never logged out for the duration of the exercise. At first glance, this seemed a horrible disregard for good security practices, but the fact that the system was never compromised has led to some interesting thoughts.

Given that users who have access to a system are to be considered "trusted," such as system administrators, we could make an assumption that sharing a single logon account is not any more dangerous than the very access which is granted. With root or administrative access to a computer system, it is easy for rogue system administrators to hide their tracks, so the sharing of a single logon account may not be any more dangerous. The advantage naturally gained is in the low password transmission across the network to verify with the encrypted password file, which minimizes vulnerability to sniffers.

The next problem is of course, how, in this environment, can be secure the system from users who are not authorized to access it? Under this scenario, a casual passer-by may simply access the system and compromise it. The answer is to supplant logical access controls with the physical ones by securing the system in an area where only those who are authorized to access it are physically able to do so. This would not work well for normal user systems that need to be made available to the public base of users, yet, it would work very well for those systems that make up the network infrastructure. This would work well for network servers by placing them in a physically secure area, modifying the current policies to give the authority to the system administrators to keep the system logged on in a nearly permanent fashion. The use of screen saver passwords that are not transmitted across the network could be used to secure the system and further reduce the danger. Keeping a system logged on in a permanent fashion is generally considered a bad practice and often not allowed by policy. Therefore, a policy change to leave the systems logged in would be required to protect the system from unauthorized use.

CONCLUSION

This article proposed several new concepts in password management to thwart password sniffers, dictionary and brute force attacks. One method is the Iverson Principle, which would stop any sniffers running on a regular basis. A second method: creation of passphrases which would add another level of security by providing a memory aid for passwords that would not be found in any dictionary. The final method increases password protection but requires that computer systems and servers that can be physically secured to be left logged in.

As with any new idea, it will take discussion in the community to help facilitate the effectiveness of any of the ideas put forth. Some may think these ideas may sound illogical or absurd and there may be problems with the ideas, both technologically and policy wise. The first step though, is to foster new ideas.

REFERENCES

AMERKORE international. (2001, June). The SmartCard resource center. Available at http://www.smartcard.com/.

AntiOnline -- Computer Security Hacking & Hackers. (2001, June). Available at http://www.antionline.com/.

Brucker, J. (2001, June). Computer security web sites and resources. Available at http://www.compsci.buu,ac.th/~jim/security/resources.html.

Chapman, D. B. & Zwicky, E. D. (1995). *Building internet firewalls.* O'Reilly & Associates Inc.

Garfinkle, S. & Spafford, G. (1996). *Practical unix & internet security* (2nd ed.), O'Reilly & Associates Inc.

Inficad Communications. (2001, June). attrition.org. Available at http://www.attrition.org.

Infowar.Com. (2001, June). Infowar, InfoSec Portal, Information Warfare, Security, Cybercrime. Available at http://www.infowar.com.

Lorenz, K. (1974). *On aggression.* A Harvest Book (HB 291).

McConnell, J. V. (1986). *Understanding human behavior* (5th ed.) (pp. 399-400). Holt Rinehart Winston.

McDysan, D. & Spohn, D. (1998). *ATM theory and applications* (Signature Edition). McGraw-Hill.

Neumann, P. G. (moderator). (2001, June). Forum on Risks. Available at http://catless.ncl.ac.uk/Risks.