Global Information Assurance Certification Paper

Passwords: Is there a better way?
Richard Turcotte
Version 1.2c

There is a sentimental poem written during the U.S. Civil War about a woman who wanders through the lines of the Federal army looking for her wounded husband. Everywhere she goes, she is challenged by sentries who ask her: “Who goes there?” And she truthfully answers: “Mary.” She is never stopped and eventually finds her wounded soldier. The name of the poem? “The Password Was Mary.”

From our dim history we have learned that passwords began as battlefield necessities and that perimeter defense consisted of pickets and sentries. We latched onto the simple password premise – random words, easily remembered – and have never let go.

We still see “Mary” and its derivatives as passwords today. To show just how popular Mary still is, a recent search through www.google.com for “password and mary” yielded 119 replies. Of these, 26 were password-setting scenarios using “Mary” as an example. Of the rest, 32 were for password acquisitions, with the contact’s first name as Mary.

While the password is still considered the back line in a strategy of defense in depth, it has become more of a delayer than a deterrent. It is undoubtedly the most ubiquitous terminal-based response to challenge. The question is: How long before technology completely defeats the password and other technology replaces it?

Security normally uses three different types of authentication:

- Something you know — a password, PIN, or piece of personal information (such as your mother's maiden name);
- Something you have — a card key, smart card, or token (like a SecurID card);
- Something you are — a biometric.

Let us consider these individually and see what their status is today.

Passwords

Password security, as it is disseminated today, usually consists of these four items:

1. Don't tell anyone your password.
2. Don't write your password down anywhere.
3. When you decide on a password, make sure it can't be guessed.
4. If you think there's even a chance someone else might know your password,

change it.

That puts the onus squarely on the computer user. The larger the organization of which this user is a part, the more complex life with passwords can become. The U.S. Department of Defense Password Management Guideline is 30 pages long. The section on password length is worth quoting if only to show how deeply in mathematical computations some organizations will go to secure these passwords:

> The security afforded by passwords is determined by the probability that a password can be guessed during its lifetime. The smaller that probability, the greater the security provided by the password. All else being equal, the longer the password, the greater the security it provides. This appendix reviews the mathematics involved in establishing how long a password should be.
> The basic parameters that affect the length of the password needed to provide a given degree of security are:
> L = maximum lifetime that a password can be used to log into the system.
> P = probability that a password can be guessed within its lifetime, assuming continuous guesses for this period.
> R = number of guesses per unit of time that it is possible to make.
> S = password space, i.e., the total number of unique passwords that the password generation algorithm can generate.
> **C.1 Relationship**
> Considering only the cases where S is greater than L x R and therefore P is less than 1, the relationship between these parameters is expressed by the equation:
> P = L x R
> A detailed explanation of the derivation of this basic equation is given in Appendix F.

It is wordy, but it is trustworthy? Not entirely. Having strong passwords and a strong password policy like DoD's will only carry so far in the face of startling technological advances made by those whose mission it is to break passwords.

The two most advanced developments in this area are L0phtcrack and Pwdump2. L0phtcrack, which began as a Unix password cracking program called Crack, has advanced so far as to have won the Inforworld Golden Guardian Award in 1999 and has been recommended by no less than the Microsoft Corporation.

These stars from the Dark Side have come into the light and now are exemplary "White Hats". L0phtcrack (that's a zero) is from L0pht Heavy Industries (www.lopht.com) and is considered the ultimate Windows NT password security tool. Ironically, because it can crack just about any password, it should also be considered the ultimate password security threat. L0phtcrack has been downloaded an amazing half-million times.

Somehow, it is difficult to believe that all these downloads were for the purpose of

securing passwords.

The bottom line is that L0phtcrack will break the computer password. It may take time, but it will do it. There is practically no defense. Microsoft believed that it had effectively stopped L0phtcrack when it released the Syskey utility as part of Windows NT Service Pack 3. But along came a program named Pwdump2.

Both L0phtcrack and Pwdump2 operate against password encryption. Encryption – scrambling passwords into code – works well against password guessers and keeps passwords from appearing in their native state as they are stored in databases or sent across networks. But the encryption itself has a flaw: It must be stored somewhere. It is this file or database that password crackers use to break the code.

Encryption creates a hash, a string of characters that is the result of the scramble done by the encryption algorithm. The complicated math has changed the password into something quite unrecognizable. Often added to the algorithm is a salt – a set of random characters added to the original password before it is encrypted. A common salt is a time-of-day string. This changes the hash every time a user logs into his system.

Hashes are a one-way proposition, which makes them so valuable. Applying the same algorithm to the hash will not produce the original password, just more scrambled hash.

Here comes the advantage of the password-cracking program. It does not merely guess at the password the way the average office hacker would. The cracker has something against which to compare. It uses its own encryption to create its own hash. By comparing its hash with the database hash it can tell it if cracked the password or not. If the hash is the same, that's assumed to be the password.

Microsoft's Syskey further encrypted the hashes stored in a Windows NT computer database, defeating the L0phtcrack program. But Pwdump2 uses sophisticated techniques to get the unencrypted password hashes from the operating system's memory. Instead of going after the database, L0phtcrack uses the results of Pwdump2 (username and password hashes dumped to a .txt file) to run its crack successfully.

Password advantages: It is a mature technology. Just about everybody has one.

Disadvantages: Just about anybody can crack it.

Smart Cards

Smart cards -- credit-card sized plastic cards with an embedded computer chip – are much newer, entering only their second generation. Because of this, smart card technology is still too diverse to accept universal systems, and much too disparate to handle universal applications.

Despite this, there are more than 300 million mobile telephones containing smart cards, and more than 4 million TV satellite receivers similarly equipped. Smart cards

are very popular in Europe, where they are found in about 64 million EuroPay, MasterCard and Visa cards. Everyone in the German and Austrian national health care program (80 million clients) has a smart card.

Experiments are being carried out at airports with smart cards for frequent flyers and in other loyalty programs handled by banks and other commerce. And in many data centers, the smart card has replaced the entry/swipe card for admittance to the center, as well as admittance to the network.

The smart card of today carries around 32 kilobytes of data in 8- to 16-bit architecture. It can download data and applications. Current average cost of a card with Multos or Java OS technology is about $15, compared to 25 cents for a bank-issued magnetic-stripe credit card.

Its security advantage is that there is yet no widespread method of stealing data from the card without stealing the card. Its security advantage is in its possession. On the software side, smart cards still must deal with challenge/response. They have to ensure both authentication and authorization. The card user must be authenticated; at present the most prevalent method is through a personal identification number (PIN) – just another password.

Further, the card's strictly pre-approved activities must be authorized. The card can produce a digital certificate that authorizes use by authenticating the user.

Most of the smart card's value lies in its future. With larger storage capacity envisioned soon, multiple applications on a single card promise to let the user access control to buildings, data centers, computer networks; allow the user to cache cash and take over the bank-issued magnetic-stripe card functions; carry software and software development tools; and be delivered at a more attractive price, in the $2 to $4 range.

Smart card advantages: Better than passwords; much more versatile and portable.

Disadvantages: Still tied to a PIN mechanism for secure access. And, of course, the card can be stolen.

Biometrics

The most forward-looking security encompassed in the field of biometrics (bio=living, metric=measure).

This technology is considered by its adherents to be the most secure and convenient authentication tool because it can't be borrowed, stolen, forgotten or forged. In this, they are nearly correct.

Biometrics measures individual physical or behavioral characteristics to authenticate identities. Physical biometrics includes fingerprints, hand- or palm-prints, retina/iris, and facial characteristics. Behavioral biometrics includes signatures, voice recognition, typing patterns and even the walking gait.

Of these, fingerprints and signatures are getting the most recognition. Fingerprinting has a sacred-cow history in the U.S., with a huge database already established by federal law enforcement agencies, notably the FBI.

Let us examine the most common technologies:

Fingerprints

A larger variety of fingerprint security devices are available than for any other biometrics. Fingerprint security can be found by frequent visitors to Disney World, computer users at several West Coast high-tech companies, in the computers at MasterCard International and the city of Oceanside, Calif. Computer giant Compaq is embedding fingerprint scanners into keyboards and laptops. Prices for the device have dropped 80 to 90 percent in the last three years. Standalone fingerprint readers can be had for less than $100. If it's embedded in a computer keyboard, the extra cost is about $10.

Fingerprint scanning is so popular that it already has a cracker. A computer company analyst created duplicates of his fingerprints on thin media. He succeeded in tricking a scanner. Then he created rubber fingers to hold his molded prints. He is now working on a rubber hand to defeat hand-scanning and on a full face mask to fool face scanners. This may not be as impressive as it first sounds. The tools and technology to create three-dimensional latex fingerprints are not standard items in a hacker's toolkit. And this cracker did not have to deal with theft of the fingerprints.

Hand geometry

This measures and analyzes the shape of the entire hand. It's as easy to use as fingerprint scanning, but if offers a larger area from which to authenticate results. It is considered exceptionally accurate.

Retina

This analyzes the layer of blood vessels in the back of the eye. It uses a low-intensity light source to scan unique patterns. It is considering quite accurate but involves users having to look into a binocular-type device; awkward for those who wear glasses and irritating for those who do not enjoy close contact with public devices.

Iris

This analyzes features found in the colored ring of tissue that surrounds the pupil of the eye. It is less intrusive than retina scanning and works well without contact with the scanning device, so it does not bother eyeglass wearers. Ease-of-use issues and lack of systems integration are its common drawbacks.

Facial

This currently requires a digital camera to develop the facial image for authentication. Its major drawback in computer networks is the extra peripheral needed to compose and develop the image. Its major use seems to be in the casino industry, which keeps facial recognition records of patrons it considers undesirable.

Signature

Since this is the most popular paper-based authentication method, it has good user acceptance. This method analyzes attributes that paper signatures cannot record: speed, velocity and pen pressure.

Voice

This method is not based on voice recognition but the creation of voice-prints, which are transformed into text. Its potential is enlarged because it needs no new hardware; voice recording already exists on computers. That is balanced by the possibility of ambient noise distorting the recording. It lags behind other biometrics because it is more complicated.

Advantages of biometrics: No passwords, ease of use.

Disadvantages of biometrics: Lack of standards, immature technology, cost.

Conclusions

We are in the midst of three kinds of security technology: passwords, smart cards and biometrics.

We have seen that passwords alone are no longer secure; it is time to retire Mary. Smart cards, despite their prevalence, are today only a transition step to free us of the password and stop the hackers. These cards still rely on an extrinsic source for authentication. Some users will not believe that a four-number PIN can be more secure than a seven-number, alpha-numeric encrypted password. But that password already has been broken. Why should we be more optimistic about the PIN?

Because biometrics does not involve an extrinsic source for authentication, it seems to offer the best security solution. The U.S. Department of Defense has gone on record that it is investigating the most mature biometrics technologies: fingerprints, signatures and facial recognition, in that order. But adding biometric devices involves a big change and some cost.

From a real-world view, smart card and biometrics technology will continue to flourish inside and outside the computer industry. It remains to be seen which one, or which combination of these, will be the common authentication tool of the future.

The password, unfortunately, will be used until it is outlawed by all operating systems.

References

Moore, Frank, Ed., The Civil War in Song and Story, New York: P.F. Collier, 1889.

Liu, Simon and Silverman, Mark. "A Practical Guide to Biometric Security Technology." IEEE Computer Society. Jan-Feb., 2000. URL: http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm (19 April 2001).

"A guide to Unix account passwords and password security." 11 Aug. 1999. http://www.acs.calpoly.edu/policies/passwords.html (19 April 2001).

"Department of Defense Password Management Guideline." 12 April 1985. http://packetstorm.securify.com/papers/password/dodpwman.txt (19 April 2001).

Savill, John. "How can I check the security of my passwords?" 22 Dec. 1999. http://www.windows2000faq.com/Articles/Print.cfm?ArticleID=14774 (19 April 2001).

Machrone, Bill. "How Do I Hack Thee?" PC Magazine. 15 Nov. 1999. http://www.zdnet.com/filters/printerfriendly/0,6061,2385238-50,00.html (19 April 2001).

Lavigne, Dru. "Cracking Passwords to Enhance Security." The O'Reilly Network. 24 Jan. 2001. http://www.oreillynet.com/pub/a/bsd/2001/01/24/FreeBSD_Basics.html (22 April 2001).

"The Smart Card Market Opportunity." Smart Card Industry Association. 4 Feb. 2000. http://www.scia.org/knowledgebase/default.htm (22 April 2001).

Cagliostro, Charles. "Primer on Smart Cards." Smart Card Industry Association. Dec. 1999. http://www.scia.org/knowledgebase/default.htm (22 April 2001).

Gaudin, Sharon. "Biometrics Eyes the Enterprise." Network World. 8 May 2000. http://www.nwfusion.com/research/2000/0508feat2.html (19 April 2001).