The End of Passwords: Problems

by M. E. Kabay, PhD, CISSP-ISSMP
Professor, Computer Information Systems
Norwich University, Northfield VT

I detest passwords. Why do I loathe passwords as a method for authentication? Let me count the ways:

1. Most systems allow users to choose their own passwords. Most users have no clue how to choose passwords that will resist even the mildest guessing based on elementary research of their interests (family, hobbies, pets, favorite sports teams) or simple dictionary-based attacks (ordinary short words). Many users choose the word "password" or their own name as their password.
2. If the system applies filters to passwords to impose content and structure requirements (e.g., minimum length, inclusion of numbers or special characters, exclusion of words in a dictionary) then most users use the same password over and over and for every possible application requiring a password including their external e-mail, offshore gambling sites, auction sites, book clubs, and pornography vendors.
3. Reasonable system administrators require periodic changes of passwords; paranoid system administrators require changes of passwords so often that the users become desperate because they keep forgetting their passwords.
4. Users faced with demands for changes of passwords adopt a policy of using the same password all the time, or possibly changing a single number in the password; e.g., ramo1bilu, ramo2bilu, ramo3bilu and so on.
5. Some administrators make the mistake of having a single day (e.g., once a month) on which all passwords expire; they thus create a flurry of interventions as support staff help users who forgotten their new passwords.
6. If the system applies password histories to prevent reuse of passwords [* see note] on a particular system, users write to passwords down on scraps of paper and stick them to every available surface, often with helpful identifying notes such as, "Password for accounting system."
7. Most users share their passwords with anyone who asks; e.g., technical support staff, the guy in the next cubicle, and even complete strangers on the street who offer them a chocolate or nothing at all.
8. Some system administrators still leave their password files accessible to any eight-year-old who wants to run a password cracker for fun and profit. A very few still use unencrypted password files.
9. Many system administrators still receive no (or ignore any) real time alert when attackers try online password guessing, especially if the attacker uses slow scans that attack many different user IDs, but only one of the time, over many hours or days.
10. Some system administrators still believe that inactivation of user IDs under password-guessing attack is a reasonable response; they thus hand their system over to attackers for a simple denial of service: try every account with a dummy password. Admittedly, most system administrators understand that requiring manual intervention to reset a lost account is not the cleverest policy in the world; therefore, they configure their systems to have a

reasonable timeout (e.g., a few minutes).

11. Sometimes organizations send users both their user ID and their password in the same unencrypted message, making it too easy for accidental or deliberate interception to break security.
12. In environments where time pressure is extreme, such as medical facilities, many users bypass the nuisance of constant logon/logoff cycles by having workstations logged on every morning by whoever gets there first and then simply using that session all day.

In the next article, I'll review the usual options for replacing passwords; in the last couple of articles in a short series I will present what I think of as the Holy Grail of identification authentication -- and it's here at last.

[* Note: I cannot resist my favorite error message of all time: Jean-Jacques Quisquater reported this gem to RISKS 21(37):

"Q276304 - Error Message: Your Password Must Be at Least 18770 Characters and Cannot Repeat Any of Your Previous 30689 Passwords"

Commented the correspondent dryly, "New level of security at Microsoft."]

* * *

For Further Reading

Kessler, G. C. (1996). Passwords – strengths and weaknesses.
< http://www.garykessler.net/library/password.html >

Wagner, R. (2003). Windows password weaknesses could threaten your enterprise.
< http://www4.gartner.com/DisplayDocument?doc_cd=116510 >

Wagner, R. (2004). Will trade passwords for chocolate.
< http://www.securitypipeline.com/news/18902074 >

Quisquater, J-J (2001). Microsoft error message.
< ftp://ftp.sri.com/risks/21/risks-21.37 >
* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

The End of Passwords: Inadequate Solutions

by M. E. Kabay, PhD, CISSP-ISSMP
Professor, Computer Information Systems
Norwich University, Northfield VT

In my previous article on this subject, I ranted about how awful passwords are as a mechanism for authentication of identity. Practically everyone already knows that the for fundamental mechanisms for binding social identity to user ID -- that is, authentication – are

- What you know: passwords or passphrases such as nonsense strings or supposedly private information (e.g., your first love's pet name).
- What you are (static biometrics): characteristics of your body such as retinal patterns, iris patterns, hand geometry, fingerprints, face, height-to-weight ratio.
- What you do (dynamic biometrics): e.g., dynamics of voice, speech, signatures and typing.
- What you have (tokens); e.g., keys, passcards, badges, photo IDs, or anything unique or nearly unique that is difficult to obtain or counterfeit.

I'm not going to go into the details of these systems in this essay. What I want to point out is that most of these systems are good for session initiation but not so great for automatic session termination. One can place one's finger on a fingerprint reader, insert a magnetic card into a reader, look into an iris scanner, speak into a microphone, type on a keyboard, sign one's name -- all of these methods can allow an authorized user to log on to a system.

The problem is that once the interaction is complete, there is usually no mechanism for automatically detecting the departure of the authorized user. Indeed, if one tries to use tokens such as magnetic cards to detect departure by forcing the user to leave the card in the reader while the session is in progress, one of two unpleasant consequences will result: either the user will leave the card in the reader and walk away or the user will walk away with the card attached to his or her wrist and either be yanked backward or pull the equipment onto the floor with a clatter.

One promising biometric technology to allow automatic session initiation and termination is face recognition. Theoretically, it ought to be possible to set up a camera-based facial recognition system that can correctly detect the departure of an authorized user. However, I don't know of such a system in use (let me know if you do).

Another technology that should allow the kind of automatic logon and logoff I've been dreaming of is proximity cards. We already have long-established access-control systems that use Wiegand cards, which have metal particles embedded in plastic so they produce a unique signature in response to radio waves. Proximity sensors can be placed in the wall to control door locks and allow people to go in and out without having to touch their cards.

For the last 20 years, I have wanted to see a proximity sensor used with workstations to control automatic logon and logoff. This week, I learned of the authentication equivalent of the Holy

Grail: we finally have a good method for fast, effective password-free access control using proximity badges and sensors. And the results are even better than I had imagined.

More in the next article.

* * *

For further reading:

Lynch, C. (1998). A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Networked Information Resources.
< http://www.cni.org/projects/authentication/authentication-wp.html >

Kabay, M. E. (2003). Identification and Authentication lecture, IS340 course.
< http://www.mekabay.com/courses/academic/norwich/is340/14_I&A.ppt >

What is a Wiegand card?
< http://whatis.techtarget.com/definition/0,,sid9_gci852292,00.html >

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Coping with Strong Passwords

By Charisse M. Sebastian, CNE

[M. E. Kabay comments: I was invited to speak at a meeting of the *New England Information Security Group* < http://www.neisug.com/ > in May 2004 and was delighted to meet Charisse Sebastian. We had such a great time exchanging stories and ideas about technical support and security that I invited her to write about her insights into the importance of good communications between the IT group and the user community. Here is her contribution to the *Network World Security Strategies* column with my thanks.]

* * *

In previous articles about passwords, Dr Kabay has expressed his distaste for this method of identification and authentication (I&A). But whether he likes them or not, most of us are stuck with passwords and the management problems they cause.

In an age of hackers, viruses, terrorism and malevolent employees, talking about security can make people either try to glamorize it, à la James Bond, or minimize it, as in, "It won't happen to me." Both attitudes are distractions that decrease security. Security is too often an afterthought, especially in the United States, where the American culture of openness can interfere with effective security. Openness is a valid and altruistic attitude for social interactions, but protecting networks from intrusion and accidents is crucial to long-term success in business. Unfortunately, efforts to make users more aware of security are often met with the attitude that IT must be paranoid or with silent resistance.

The most common sources of conflict where IT and users interact over security are password-protected logins and Internet communications. Until we see affordable improvements in I&A, strong passwords and good management remain essential.

In today's environment, everybody connected to the Internet is a potential target.

Some salient statistics – for what they're worth:

* Calls dealing with password resets are the #1 demand for help desk support. [1]

* Total annual cost of U.S. corporate online security breaches in 2000: $15 Billion [2]

* Percentage of U.S. companies not implementing "adequate" security: 30% [3]

* Percentage of U.S. companies that spend 5% or less of their IT budget on security for their networks: 50%. [4]

Strong passwords require 8-14 characters, minimum and a mix of case, numbers and symbols. But to a user, strong means more complicated. Users either simplify the password itself or help themselves remember it -- often with a Post-It (TM) note on the monitor bezel or under the mouse pad.

This issue requires human interaction to resolve. First, I cannot emphasize enough the importance for IT staff from the CIO on down to the lowliest help desk assistant to avoid condescending to users – as in, "We're IT and they're just users." Learn what the users are thinking. How do they view security? Why and how have they opposed security? Instead of dictating to users from IT, look at the issues from the users' point of view. Get them to buy into the policy willingly and enthusiastically as stakeholders, not as put-upon victims of an administrative dictatorship. As a suggestion, as part of new employee orientation (and an existing employee refresher too), have the IT instructor go to a criminal-hacker Web site to show users the kinds of threats that IT has to deal with every day and how such threats can harm the users directly and personally.

Second, help users to incorporate strong passwords in a way they can remember them, without writing them down. Suggestion; run together words in common phrases up to about 16 characters, mixing case and substituting/adding symbols and numbers for some letters.

Third, with user input, create a well-defined, solid foundation of company-wide policies and procedures. That means for everyone from the CEO on down, no exceptions. For end users to become stakeholders it's critical that they understand that everyone is involved and why. Why does IT need their help? Why do they need to be concerned? Why are IT in effect are an extension of their own departments?

In summary, computer security is an endless process. With continuing user investment and input in a real team effort with IT, security becomes manageable, effective and non-intrusive. Often, instead of purchasing some new piece of security technology, getting users actively involved in security could save further strain on already tight IT budgets. The process of finding or creating the mix of technology, procedure and policy involves analyzing the system including input from users to understand what is needed. Once new procedures are in place and policies established, they have to be maintained, monitored and tested on a regular basis. That includes feedback from the users, taken seriously, on a regular basis.

Computer security is a journey, not a destination.

* * *

References

[1] Courion Corp Password Management Overview
<
http://www.courion.com/products/pwc/index.asp?lid=PasswordCourier&lpos=orange_banner?Node=PWC >

[2 - 4] DataMonitor PLC, New York as reported in "Security Statistics" (July 9, 2001),
< http://www.computerworld.com/securitytopics/security/story/0,10801,62002,00.html >

* * *

Charisse Michelle Sebastian (mailto:char-sebastian@att.net) is an IT Support Evangelist and passionately loves IT, specializing in desktop/user support, troubleshooting, training, server

support, security, writing and mentoring. Right now, while working in a consulting practice and in transition, she is on an active job search and invites correspondence.

* * *

A Master's degree in the management of information assurance in 18 months of online study from Norwich University – see
< http://www3.norwich.edu/msia > for details.

M. E. Kabay, PhD, CISSP is Professor of Computer Information Systems in the School of Business and Management s at Norwich University in Northfield, VT. Mich can be reached by e-mail at <
mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Reward Smarter Password Choices

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
Norwich University, Northfield VT

Reader Andreas Englisch from Munich wrote to me with some interesting suggestions about improving password management. With his kind permission, here are some of his comments (by the way, readers are welcome to write to me in German and French as well as English; and with the help of my translation program I can also manage to muddle through Spanish, Italian and Portuguese).

* * *

If you force passwords to expire after a fixed interval, people tend to define passwords containing a number. When their passwords expire, they simply increase that number by one; e.g., password1, password2, password3, etc.

Most systems prevent reuse of a password for a set period; for example, "The last 15 passwords are saved and may not be re-used." This password-numbering habit prevents a new password from being rejected by the system, but if anybody gets hold of such a password by shoulder surfing, dumpster diving, finding the sticky-note under the keyboard and so on, it is not going to be very difficult to find the next password in the series.

Moreover, I do not like password expiry by fixed intervals from another perspective: It treats all passwords the same, no matter how "good" (i.e. complex) they are. But would it not be better to set the password expiry interval as a function of password complexity? For example, if I use a really complex string of alphanumerical characters, I would have to change my password much less frequently than if I chose a more guessable password. This strategy would encourage people to use and remember better passwords than they currently use; in addition, they might stop using the same-old-password-1, same-old-password-2 approach to new passwords. Using this kind of approach, perhaps a bad password would have to be replaced after 30 days but a good one after 90 days and a really tough one after 180 days.

* * *

Dear Herr Englisch,

Your analysis of passwords with numbers is correct: any password with a number in it suggests that the next one will have similar characteristics. Therefore, password-checking algorithms should compare new passwords against old ones not only by a simple lookup list but also by using wild-card matching algorithms to detect static passwords that change in only one number or character or which shift all characters by the same increment of the sort sequence (e.g., "alpha1" becomes "bmqib2" and then later "cnrjc3") (and no, these are not my password!).

However, I worry a bit about long password lifetimes. It seems to me that the primary reason for forcing password changes is that passwords can be compromised by inadequate security practices, as you yourself pointed out.

The cryptographic strength seems to be a lesser vulnerability. For example, an eight-character password with uppercase and lowercase letters and numbers available could take months to crack (see "Brute-Force Cracking Estimation" < http://www.mekabay.com/methodology/keyspace.xls >) depending on processing power, but a single instance of shoulder-surfing could compromise it within a day of its being changed.

So perhaps the reward for more complex passwords can be tempered by concern over possible compromise; 30-60-90 days, for example?

In any case, I appreciate your taking the time to write and thank you for letting me quote you. Danke sehr!

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Writing Down Passwords

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

I have long argued that passwords are a terrible way of authenticating identity:

- Many well-meaning but unaware people choose really stupid, easy-to-guess passwords such as the names of people important to them (or favorite sports teams, or the product whose billboard is visible from their office window, or the names of objects on their desk);
- Good passwords increase the keyspace not only by being longer but also by using upper- and lowercase letters, numbers and special characters – resulting in monstrosities such as "j3q(K8bX_*5" – and let's not even _think_ about allowing "O" and "0" in the character set;
- Some users generate their passwords using funny rules such as using particular letters from the words in phrases (e.g., using the third letter of each word in "Mary had a little lamb; its fleece was white as snow" produces "rdatmsesiso") – and then they forget the rules;
- People sometimes use numerical increments to get around rules preventing password reuse (e.g., fisu3nema, fisu4nema, fisu5nema. . .) thus compromising their _next_ password as soon as the _current_ password is discovered;
- Users often use exactly the same password for everything (their private Web e-mail, their corporate professional e-mail, their DVD-club login, their talking-slug club – everything) with the result that any single password compromise is a potentially complete security compromise;
- Making passwords hard to guess forces many people to write them down;
- Physically-recorded passwords get stored in the same places network security auditors have always found them: in desk drawers, under keyboards, under chair seats, in files labeled "C:\passwords.txt"and even in plain view on the back (or front!) of video screens;
- When people _do_ pick hard-to-guess passwords and _don't_ write them down, they often call the HelpDesk or security administrator to reset them because they _forget_ them, causing a great deal of irritation and wasted time for everyone concerned.

A study < http://www.nucleusresearch.com/press_releases/prpassword1006 > published last year by Nucleus Research reported findings on user behavior concerning passwords. To no one's surprise, the researchers found that "More than a third of employees write down or electronically record their passwords, creating significant vulnerabilities. Even worse, lowering the quantity of passwords, changing password complexity, or changing password change frequency had no impact on employee actions." They also found that "There was also no correlation between complexity, frequency, and quantity and how often users called the help desk with password-related issues. Seventy percent of enterprise users call the IT help desk once a year for help with a forgotten or missing password; 16 percent call two to three times a year; 9 percent call three to five times a year; and 5 percent call more than five times a year for password help."

The full report is usually available by subscription only, but the company has very kindly opened it temporarily for use by readers of this column < http://www.nucleusresearch.com/research/g68.pdf

>. Based on a survey with 325 respondents, efforts at improving password management by ordinary users generally fail. Specifically, the same proportion (1/3) of users keep a written record of their password regardless of the amount of

- user education,
- password complexity,
- security-policy restrictiveness.

In my next column, I'll look at how these findings relate to what cognitive psychologists know about our capacity to understand risk.

Nucleus Research is an IT-related research organization that takes a unique investigative approach to its research and helps end-user organizations assess the value realized from technology acquisitions. To learn more, please visit www.NucleusResearch.com . My thanks to the company for opening their proprietary research report to readers. [I have no financial relationship whatever with Nucleus Research.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Hidden Costs of Passwords

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Many users who focus on their individual experience and needs rather than on corporate security management think that passwords are free. Indeed, password functions come with our operating systems and much of our software; we don't have to pay anything extra to buy this form of authentication. However, both common sense and research findings support the view that authenticating identity using passwords is a significant expense for organizations.

The major issue is forgotten passwords. Users who lose track of their passwords may have access to an automated password-resetting process, in which case costs may be modest. For example, it is possible to set up a one-way encrypted database of personal information questions and answers and have the user answer a number of these to authenticate to the system. One example is the M-Tech Identity Management Suite™ < http://psynch.com/features/self-service-password-reset.html > which provides precisely this functionality (among others) to avoid Help Desk involvement in password resets.

Even this process has a modest cost that depends on the cost per minute of salary and extended costs (relating to costs of facilities, supplies, services and their financing) for the forgetful employee's time. I've always been told to estimate extended costs at around 50%, so someone earning $80,000 a year (for 2,000 hours of work) might be costing the employer around $1/minute. You can do the rest of the math.

The cost grows if the Help Desk gets involved, especially if there's a lag in responding to the emergency call. In addition to the cost of the Help Desk personnel's time (which one can either include or discount as being paid anyway, depending on the point of view), the big cost begins to be the ticking clock as the locked-out user waits for a reply. For the $1/minute employee mentioned above, a five-minute wait twiddling her fingers amounts to $5 of wasted costs – but a half-hour delay is $30. Do you ever have to wait half an hour for a callback from the Help Desk?

Multiply the lost passwords by the number of employees and the average number of times people forget their passwords and you can see that the costs begin to rise significantly. At some point, tokens and biometrics begin to seem less expensive, comparatively, than they seemed at first glance. In a 2005 article, Lisa Phifer writes, "According to Burton Group and Gartner studies, password resets represent 30 percent of all help desk calls. The META Group estimates that each help desk call costs $25."< http://www.isp-planet.com/technology/2005/beyond_passwords_1a.html > In a white paper by RSA (makers of cryptographic tokens, remember), the authors claim that for a 1,000-user organization, the total cost of ownership over the first three years is around $673,000 or $673 per user. About 98% of that depressing expense is due to management costs.

Similar calculations are shown in a Cost of Ownership (ROI) document from RoboForm.< http://www.roboform.com/enterprise/solutions/costofownership.html > The makers of this single-signon solution estimate cost savings of about $417 per user in the first three years for a 1,000-user organization through reduction of lost-password calls.

Avatier, makers of the Avatier Password Station, have placed an ROI Calculator for their product on the Web.< http://www.avatier.com/products/PasswordStation/ps_cost_analysis.html > It allows you to entire the number of employees, the number of Help Desk calls per user per month, the duration of Help Desk calls, the hourly costs of both Help Desk staff and callers, the percentage of Help Desk calls relating to password reset (30% on average according to Gartner Group) and the percentage of users who will use their product. The calculator shows the ROI in months, total cost savings in year one and total cost savings by the end of the third year.

I suggest that you take the time to examine the resources above and others you can find online. And the next time some innocent challenges you about how "free" passwords are, you can discuss the issue with a more realistic perspective than they bring to the table.

[MANDATORY DISCLAIMER: I have no financial relationships whatever with any of the companies mentioned in this article.]

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Generating Good Passwords (1):
PC Tools Secure Password Generator

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

What's a good password?

System and security administrators often have to explain to naïve users that "Betty4me", "myDog*Bowser" and "password6" are not good passwords. They are too easy to construct using dictionary-based attacks < http://www.tech-faq.com/dictionary-attack.shtml > that compare one-way hashes of combinations of real words mixed with numbers and symbols with the one-way hashes of user passwords stored in password files. Some of them are also too easy to guess if the attacker knows something about the private life or preferences of the user (like the name of the user's dog).

Some helpdesks suggest to their users that they try public password generators. I looked at a few and have the following comments on what I observed.

For purposes of comparison, I limited my search of passwords to 10 characters which had to include letters, did not use mixed case, included numbers, and included punctuation. I kept mixed-case out of the passwords because I think that remembering which letter is uppercase or lowercase in a more-or-less random string increases the difficulty of remembering the password and therefore the likelihood that a user will write it down. Where possible, I generated 10 suggested passwords at once.

My first test used PC Tools Software's "Secure Password Generator."< http://www.pctools.com/guides/password/ > The Web page allows selection of length, use letters, mixed-case, number, and symbols and also allows the user to exclude similar-looking characters (l, 1, I and o or 0). Here's a sample pass with 10 characters, lowercase only, including special characters and excluding the confusing characters:

drud8?a*et
=r8st8t7ud
!78etr9cr*
4e@ufrugac
8_sececexu
gath65*ke*
9#upura_r!
$estugeth!
*e_uka&ra3
6etr=xuspa

Hmm, I'm not sure that these are particularly easy to remember, although at least there seem to be nice alternations of one or more consonants with a vowel, making it possible to try pronouncing them. However, I think that the unconstrained gibberish is worse:

rle8le0le-
!leC2_+wri
Xoep9=Adr1
-oe!RL2cri
pHL6*H5uDl
p_lA3l4Gou
xlE*i61?Le
glaP2&wROu
Wl0F-ouchi
wLa=lAg2aD

Yechhh! This alphabetic farrago is asking for calls the HelpDesk for password resets – or sticky notes on the underside of the keyboard.

More next time.

* * *

A quick heads-up about the upcoming ISACA Security Management Conference (SMC2007) in Winnipeg, Canada Nov 6-7, 2007: program at < http://www.isaca-wpg.org/SMC2007/program.htm >.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Generating Good Passwords (2): Bytes Interactive Password Generator

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Last time I asked, "What's a good password?" and discussed a Web-based service for creating random passwords. This time I'm looking at the "Bytes Interactive Password Generators"< http://www.goodpassword.com/index.htm >.

This site provided two types of password: the random and the "Leet."

The Leet password generator asked for a phrase of eight or more words. I gave it the classic "The quick brown fox jumped over the lazy dogs" and it created "+q8Fjo+1d" with a "Password Pattern" of "LclCclLlc." The symbols in the password pattern are supposed to help the user remember how to transform the first letter of the passphrase into the password. The meaning of the symbols is as follows:

C	Upper Case Character
c	Lower Case Character
l	1st Leet Character Equivalent
L	2nd Leet Character Equivalent

The "l" and "L" symbols refer to certain letters that have two different substitution codes for the "elite" (leet) alphabet; thus the first Leet character in this transposition cipher for A is @ and the second is 4.

A	@ 4
B	8
C	[(
D	D
E	3
F	F
G	6 9
H	#
I	! 1
J	J
K	K
L	1
M	M
N	N
O	0
P	P
Q	Q
R	R
S	5 $
T	7 +

U	U
V	V
W	W
X	X
Y	Y
Z	2

The Web site authors state, “To remember your 1337 Password you need two keys, first the pass phrase and second the password pattern. This pattern will indicate whether the password characters are either upper or lower case, or a Leet Equivalent. The pass phrase one should try to memorize or at least know what book, page and location on the page the phrase was taken from[.] The password pattern is harder to remember so we recommend writing it down or using our Password Recovery Feature.[sic]by creating a cookie from our web site to remember the pattern for you. Try the Password Recovery Feature.”

As you may imagine, I am not keen on the generated passwords, since they do not strike me as particularly easy to remember unless the user knows the hacker alphabet by heart. Perhaps this generator is intended for people who are or have been script kiddies, hacker wannabees or otherwise involved in the criminal hacker subculture.

However, the idea of writing down the password _pattern_ (not the password or the passphrase) or of storing the pattern in a cleartext cookie on an unencrypted drive does _not_ strike me as a significant security risk in the absence of the original passphrase. The pattern alone is useless without the passphrase.

Next time (the last in this short series), I’ll introduce a random-password generator based on a classic paper in the computing literature.

* * *

A quick heads-up about the upcoming ISACA Security Management Conference (SMC2007) in Winnipeg, Canada Nov 6-7, 2007: program at < http://www.isaca-wpg.org/SMC2007/program.htm >.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Generating Good Passwords (3):
xyzzy

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the first two of this three-part series, I've been asking, "What's a good password?" and looking at password generators available free on the Web.

A couple of password generators based on the classic paper by Morrie Gasser, "A Random Word Generator for Pronounceable Passwords" published by MITRE Corporation in 1975 are available online. The "Java Password Generator" < http://www.multicians.org/thvv/gpw.html > by Tom Van Vleck is programmed in Java (with source code available). The demonstration version doesn't offer any parameters for controlling the output, but it produces random pronounceable passwords with alternating consonant groups and vowels. Here's a sample:

tickmeni
diarrati
ospussit
sivestat
fetiplea
catontan
atuorthw
ustempre
bleinian
gnappism

The author recommends, "The best way to use this generator is to take its output it in ways known only to you. Make some letters capital, or insert punctuation and numbers." He also points out, "Steve Weintraub has written a nice pre-packaged version called XYZZY < http://haxial.com/products/xyzzy/ > for Mac and Windows."

Mr Weintraub's freeware program is 183 KB and uses digram frequencies (see < http://dynamicnetservices.com/~will/academic/bit95.tables.html >) to optimize the readability of the random strings: "The algorithm used to create the passwords is based on work of several people. In simple terms, it uses the statistics of how often one letter appears next to another and generates passwords based on these trends. For example, if a password contains the letter 'Q', then it is very likely that it will also contain a 'U' right beside it, because this is almost always the case in real words." This utility let's you choose the number of characters, the number of passwords to create and whether to include numbers. Here are some examples from a run of the program using 10 characters including numbers:

garmatta63
emidaener1
melizedo83
ramenejor9
dacealarp7

condeded86
micadend76
lichoozo01
untratlyk1
tizemish97

The author writes, “For added fun, try to think of definitions for the words that xyzzy generates.” I would say, “for added security” because such mnemonics make it easier to remember the password without writing it down.

I like this program so much that I am now using it to help generate my own passwords with the addition of a few strategically-placed special characters (which I’m not going to tell you)<grin>.

[My thanks to the crew of the Norwich University HelpDesk for drawing my attention to xyzzy and thus suggesting the topic of this column and the preceding two.]

* * *

A quick heads-up about the upcoming ISACA Security Management Conference (SMC2007) in Winnipeg, Canada Nov 6-7, 2007: program at < http://www.isaca-wpg.org/SMC2007/program.htm >.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Managing Lost Passwords:
How Not to Do It

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

Dear Bob,

I am writing to you formally in your capacity as CEO of the Metaphoronic Corporation, makers of the bioport< http://www.imdb.com/title/tt0120907/ > that I had installed in my lower spinal column last year for direct neural connectivity< http://brainwaves.corante.com/archives/2008/07/02/webcast_of_entire_neural_interface_conference_in_june.php > to my Windows 2010 < http://blogs.zdnet.com/microsoft/?p=592 > operating environment. It's been great, by the way: I love the way I can simply _*think*_ what I want to make the system perform properly. The only problem I've had is what happens when I daydream, but let's not go there.

Today I could not sign into the Web page for the SpinalTap< http://www.imdb.com/title/tt0088258/ > application that makes adjustments to the interface and could not find instructions on getting the password e-mailed to my e-mail account or on how to reset it to a temporary password and get _*that*_ by e-mail, so I called your HelpDesk to find out what to do.

The very nice agent cheerfully demonstrated that your HelpDesk has no clue how to deal with lost passwords for SpinalTap: she

1) Asked me for my user ID: unacceptable because it began a phone-based process for resetting a password;

2) Asked me one of my verification questions ("What was the last name of the girl who arranged for me to step on her foot on a ski trip in 1963?"): UNACCEPTABLE because it means the authentication data are not one-way encrypted;

3) Read me my old password: UNACCEPTABLE because it means the password file is not one-way encrypted!

Normally, passwords and other authentication data are one-way encrypted: the responses to questions are encrypted and the ciphertext of the response is compared to the stored ciphertext of the correct answer; however, it is difficult (expensive, slow) in practice to regenerate the original cleartext data unambiguously from the stored ciphertext. (See my lecture on cryptography fundamentals if you like < http://www.mekabay.com/courses/academic/norwich/is340/20_Cryptography_1.ppt >.)

Access to the authentication questions, to their answers, and to the passwords implies that the HelpDesk agent(s) can impersonate customers at any time by logging into SpinalTap using their purloined IDs. The damage caused to your Company's reputation if one of your employees were to sabotage a customer's settings and cause serious damage – psychotic breakdown, for example,

due to the impression that two-headed lizards were chewing on his left hallux – could be disastrous.

To put the problem in perspective, it would be the same kind of problem of impersonation as if a member of your staff were falsely accused of damaging Company records, sending inappropriate e-mail within the Company or to external recipients or posting inappropriate materials on a Company Web page. Not only would the victim of the impersonation suffer – so would the Company.

Although I realize you probably know this perfectly well, for the record, I will assert that

1) The problem is not the individual HelpDesk agent's: she was courteous and professional and doing her job as she was instructed to do it. She deserves no blame.

2) IMNHO,* The SpinalTap system, not the HelpDesk, should have a mechanism for resetting the password by ASKING THE USER the authentication questions on screen before e-mailing a one-time password to the officially registered e-mail account for recovery.

3) The idea that a phone call supposedly from a user (but potentially from a social engineer) is an acceptable basis for resetting has been discounted decades ago. In the absence of automated password resets, the only acceptable mechanism for secure re-authentication of an employee is to have the user physically come to the HelpDesk or to a proxy for recognition or for documentary identification and authentication using a Company-issued photo ID. Possibly you can get around this requirement in a distributed environment by using Webcams, but there are security issues there too because of the uncertain integrity of digital imagery. However, for an external customer who cannot reasonably show up at your offices, you _*must*_ develop a social-engineering-resistant methodology like the simple approach using pre-established e-mail addresses which is already implemented by uncounted numbers of Web sites.

I recommend that the written procedures for coping with loss of a password on the SpinalTap system be analyzed by the Company HelpDesk managers and corrected. If there are no written procedures, I will help write some for you that conform to industry best practices at my usual consulting rates.

Best wishes,

Mich

=>o ASCII ribbon campaign against HTML e-mail o<=

_____

* IMNHO = in my never-humble opinion <g>

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance < http://www.graduate.norwich.edu/infoassurance/ > and CTO of the School of

Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mekabay@gmail.com >; Web site at < http://www.mekabay.com/index.htm >.

Guide to Enterprise Password Management: NIST Needs Your Comments

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

I hate passwords. I think passwords are a dreadful way of authenticating identity: they cost a lot < http://www.mandylionlabs.com/PRCCalc/PRCCalc.htm >, they change too often (and so users write them down), the rules for preventing dictionary and brute-force attacks are generally easy for users to circumvent (da3isy*doggie, da4isy*doggie, da5isy*doggie…), there are too many of them (and so users write them… oh never mind), and nothing can stop users from writing them down (and sticking them in their wallets, under their keyboards, behind their screens, in their desk drawers….). And yet we constantly hear non-technical managers resisting smart-token-based authentication or proximity cards because they are supposedly too expensive.< http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=17144&TEMPLATE=/ContentManagement/ContentDisplay.cfm >

Growl.

Well, given that we are still stuck with this wretched authentication method, National Institute of Standards and Technology< http://www.nist.gov/index.html > Computer Security Division < http://csrc.nist.gov/ > of the Information Technology Laboratory< http://itl.nist.gov/ > Computer Scientists Karen Scarfone< http://csrc.nist.gov/staff/rolodex/scarfone_karen.html > and Murugiah Souppaya < http://csrc.nist.gov/staff/rolodex/souppaya_murugiah.html > have prepared SP 800-118, "DRAFT Guide to Enterprise Password Management"< http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf > and await your comments for improvement.

The blurb reads, "SP 800-118 is intended to help organizations understand and mitigate common threats against their character-based passwords. The guide focuses on topics such as defining password policy requirements and selecting centralized and local password management solutions."

As always, this Special Publication is complete and thorough. After the usual introduction to the scope and structure of the document, the authors present a brief overview of passwords (section 2) followed by two major sections and their subsections:

The document ends with appendices containing special considerations for firmware and hardware passwords, a glossary, and a list of common acronyms and abbreviations.

NIST requests comments on draft SP 800-118 by May 29, 2009. Please submit comments by e-mail < mailto:800-118comments@nist.gov > with "Comments SP 800-118" in the subject line.

I submitted six pages of comments and will inflict, er share, one of them in my next column.

* * *

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

IMPERVAious to Common Sense: The Awful Truth about Passwords

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

One of my favorite correspondents is Nahum Goldmann< http://www.cytrap.eu/files/ReguStand/2007/pdf/2007-05-About-NahumGoldmann-NO-picture.pdf > of Array Development< http://www.arraydev.com > in Ottawa, Canada and publisher of the *Journal of Internet Banking and Commerce*< http://www.arraydev.com/publishing.asp > and other peer-reviewed publications. Nahum never fails to send out interesting links and commentary, and recently he pointed to a valuable research study that I think will significantly help system administrators in reaching users on the perennial battle over passwords.

In December 2009, 32 million passwords stored without encryption on the Rockyou.com Website were stolen and published on the Web for anyone to see.< http://www.computerworld.com/s/article/9142327/RockYou_hack_exposes_names_passwords_of_30M_accounts > The security firm IMPERVA< http://www.imperva.com > published a thorough analysis< of these passwords to see how a large sample of users – not just those responding to a survey< http://www.imperva.com/ld/password_report.asp > – actually manage their personal authentication.

The results were not good.

The five-page report is confirmation that passwords are a terrible way to authenticate people.< http://www.mekabay.com/infosecmgmt/end_pw.pdf > Users chose short, simple passwords that would be easy to crack using brute force; nearly half "used names, slang words, dictionary words or trivial passwords (consecutive digits, adjacent keyboard keys, and so on). The most common password among Rockyou.com account owners is '123456'."

The authors provide clear pie-charts and bar graphs to make their point in a way that anyone can understand, including scoffers who consistently sneer at the security team's attempts to improve password complexity.

The last page has simple, clear advice that may reach at least some of your users:

1. Choose a strong password for sites you care for the privacy of the information you store. Bruce Schneier's advice is useful: "take a sentence and turn it into a password. Something like "This little piggy went to market" might become "tlpWENT2m". That nine-character password won't be in anyone's dictionary."
2. Use a different password for all sites – even for the ones where privacy isn't an issue. To help remember the passwords, again, following Bruce Schneier's advice is recommended: "If you can't remember your passwords, write them down and put the paper in your wallet. But just write the sentence – or better yet – a hint that will help you remember your sentence."
3. Never trust a 3rd party with your important passwords (webmail, banking, medical etc.)

The advice for administrators is also worth discussing at your next security group meeting.

The PDF file is free, simple to distribute, and attractive. What have you got to lose?

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Computer Information Systems < http://norwich.edu/academics/business/infoAssurance/index.html > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >