**The Realities of Password Security**

By Felipe Guillen

January 2004

**INTRODUCTION.** One would assume that having to stress the importance and value of having an effective computer security password program (especially in the workplace), would today be quite an unnecessary undertaking. Unfortunately, this is not so. Even with all of the frequent and well publicized computer violations and unauthorized penetrations by all forms of diversely motivated individuals – there exists still today an incredible amount of naive and disbelieving individuals who scoff at the need for such precautions. What makes matters worse, is that many of these cynical types are actually the so called "professionals" – hired by companies to ensure that their in-house computers and networks are properly protected from illicit access and potentially damaging hacks.

Here then we have a scenario where on the one hand we have a certain segment of computer users who demonstrably care not for proper computer security routines and precautions – and on the other hand we have those whose job it is to secure computers and networks from hack attacks, but who far too many of which feel only basic, rudimentary precautions (if any) are needed! This is quite reminiscent of swimmers who ignore well posted warnings of "NO SWIMMING" due to shark infested waters, then are totally shocked when attacked after ignoring the warnings, and seek someone to sue because their own poor decisions. What a way to make these people into "believers"! **News Flash** – Many of these recalcitrant souls will STILL adhere to their well ingrained and careless former ways, as they apparently are unable or unwilling to learn from their mistakes. "You can lead a horse to water - ……....."

**THE PROBLEM.** Today's society has realigned itself heavily upon the side of technology – and all of its vulnerabilities. While rushing headlong into the embrace of the new and expansive power and potential of today's rapidly and continuously evolving technological advances, unacceptably far too little thought or effort is devoted to the **critical and equally essential** issues of protective protocols. Mesmerized by the new and heretofore unheard of capabilities and resources of today's electronic metamorphosed society, we have the equivalent of an adolescent who has just acquired it's first race car – before learning how to drive. Thus the resultant is inescapably predictable.

***If an equal amount of concern were expended on security as is expended on functionality, well over three quarters of today's well documented and wide spread computer compromises and hacks – would not have occurred.***

In this security advisory we will address just one of many vital protocols intended to improve the operational security of today's computer systems – Passwords. Properly used and maintained, a password based security program goes far as a first line defense against illicit computer accesses and data theft/destruction. Here we shall see how easy it can also be defeated by those "on the inside".

As simple as it is to institute and maintain a program where passwords are regularly used and changed as situations warrant (depending upon the business type and threat potentials, password changes may be required and range from only once per month – to daily), we find such excuses as "using passwords take too much time", "passwords are a hassle", "why use passwords, no one can get into our office/ building without ID", etc., for NOT using passwords. From some so called IT (Information Technology) "professionals" we get such excuses as "they (the computer users) won't listen to our directives", or "we have computer security well in hand (when in truth they do NOT)" - and a well worn favorite for justifying a weak, ineffective password program - "we would rather have them (computer users) using a simple easy to remember password even if they don't change it, than no password at all". By this faulty logic, one can then comfortably rely on the safety of an in-flight aircraft which while having one dead engine – the other of it's two engine set is currently doing is just fine! (In such a case WE will take a cab!)

Thankfully – not all IT professionals are members of this dubious society of pretenders to the critical position of IT Administration.

While in our 28 years of experience in the field of intelligence security we have indeed met far too many of these pretenders - many of which were seriously deficient in even a basic knowledge of systems operations and of the programs employed by their own firm (we wonder how they were ever hired for the position!), we **have** met TRUE professionals. When we are called in by a firm who is indeed served by a responsible IT Administrator, their trademark is quite evident. For example, the network and individual computers are all protected by layered security protocols, passwords are in use and their appropriate change cycles are enforced and continuously verified, systems are well protected against virus and other malicious programs, personnel take computer security seriously and in addition are kept informed of new threats and the appropriate countermeasures, critical files are compartmentalized and restricted to only those users with the authority to access them (and the computers containing especially critical files are further protected by hardware based security systems such as biometric access controls), etc.

It is crucial that management support their expert IT staff as well as their security departments. Understaffing or under funding these important departments will yield a firm protection that exists only on paper, as they lack the funding to actually implement the required programs. Management must further support the policies enacted by their security professionals, to insure that violators of established protective protocols and procedures will in fact be subject to corrective action. Lacking this support criteria, all but guarantees a large scale disregard for security dictates and directives by their employees.

Today's advanced technology reliant society **mandates** that appropriate, well qualified personnel be assigned the position of responsibility for operations security – if serious and malicious system compromises are to be averted. Gone are the days when casual levels of security would suffice in safeguarding systems and files. Today we see the rapid and widespread proliferation of two notable classes of transgressors; **[a]** the professional operative who makes use of every opportunity presented to him/her by either inherent system hardware or software vulnerabilities, and/or by personnel based failings, and **[b]** the amateur or opportunist class, which by has just enough knowledge to take advantage of vulnerabilities they become aware of casually – from either the "inside" (i.e., as employees or other personnel having regular access to the computers and networks) or "outside" (non-company personnel who are still able to gain access to targeted computers or networks). Both classes cause serious damage in their own right. Advancing technology merely magnifies existing weaknesses, while simultaneously creating yet more paths for compromise that must be promptly identified and addressed.

In a remarkable case in point display of the ineptitude of some of the more ill-suited and incompetent pretenders to the role of "professional" IT administrator (yet who HAVE been placed in just such a critical position), one such individual actually argued FOR the case of short, easily remembered and rarely changed passwords (a hallmark of a pretender!)! This individual who was in fact the system administrator for a major U.S. firm, argued that short easy to remember passwords that did not need to be changed often – would make both his and the computer users jobs easier! (I would add – the Hackers job will too be made easier!) Further, this individual insisted that "security types" stop causing added problems in the computer industry - by insisting on the use of unnecessary, more comprehensive security programs! Is it any wonder then, why so many American companies experience tremendous computer losses?

**THE SOLUTION.** Maintaining an effective and on-going computer password program is not only a valuable and well proven method of reducing computer file violations, but is also one of the more cost effective and easily implemented routines in a company's security arsenal (incompetence and lassitude as in the above example, not withstanding). There are however certain pitfalls which you should be aware of and avoid. Below is a general ten point check chart of some of the more common and often introduced errors which would seriously compromise an otherwise effective program.

Review this basic check chart against your own current security program:

1. Never use such easily guessed and commonly used passwords as; “Love”, “Password”, “Hate”, “Me”, “911”, “Open”, “abcdef”, “NCC1701”, “Abra-Cadabra”, “007”, “xxxxx”, “4wheeler”, “12345”, “fun”, etc., to name just a few - or any of their numerous variations. There are whole lists of popular passwords (and obscenities!) which are well known and used by even amateur hackers to break in.

2. Never use phone, social security or license plate numbers, or addresses, pets names, dates, nicknames, boy/girl friends names, etc., for your passwords, as these too are often exploited.

3. Use at least eight character passwords. Longer passwords greatly increase the level of security, whereas short passwords increase the likelyhood of their being cracked or more readily guessed.

4. Never leave your password “hidden” under your keyboard, rolodex file, written on a “sticky note” and taped to your monitor (yes, we even see this done quite often!), taped inside a desk drawer, under the mousepad (or mouse), under a desk pad, written somewhere in your desk calendar, written under a desk curio or figurine, etc. You are only kidding yourself – they WILL be found!

5. Never use a “universal” password! Each person should have their own unique password, which will restrict them to only those computer areas necessary for the execution of their particular job.

6. Do not use words which relate to your favorite brand of music, bands, movies, favorite books, hobbies, cars, CD’s, favorite actors, former schools, your job title, employers name, etc.

7. Use passwords which require both upper and lower case characters. Never use a password that consists of all lower or all upper case letters or all numbers, characters, etc. Mix them up!

8. Supplement passwords with effective encryption programs which scramble critical files - turning them into “Digital Confetti”, and making them unusable without entering the proper second password. Thus one password restricts access to the computer system, while the second restricts access to the individual file or document which is securely encrypted. This is an ideal combination.

9. Ensure that you are not being watched when you type in your passwords. Though a simple procedure, watching as one types is an effective manner with which to compromise any password.

10. Use passwords which do not duplicate any of the characters. The more often a character is repeated in a word, the easier the password is to crack or guess. Use numbers and non-letter characters (i.e., #,@,^,=,%, etc.), as part of the body of your passwords to improve their security.

Retain the services a competent intelligence security agency to run an assessment of your firms particular threat exposures and required levels of security precautions. Password programs are only a small part of an overall business security package – not a stand alone cure-all! A risk assessment will provide a detailed listing of other program requirements. Supplemental analysis will insure that existing “Hazards in Place” will not negate the benefit of your newly implemented security program.

For an example of what could happen to an improperly planned and executed security effort (and of undetected examples of “Hazards in Place”), take the lessons learned from a client which thought that their self designed and implemented password program was the sole precaution needed to properly protect their computer files from compromise.

After experiencing repeated violations of some of their most sensitive and confidential computer files, the client called for expert assistance. Several serious deficiencies were promptly identified, and explained why they were having ongoing problems that they just could not seem to solve.

The more notable problems found included; [a] The passwords were never changed. Their risk exposures required no less than a WEEKLY password change, [b] Each password was assigned to a department, and all of the employees of that department used the same password, [c] The system administrator casually gave out his universal master access code to employees who forgot their passwords, so they may log back into the system – rather than doing the work himself and retrieving their forgotten password from the system, and the most serious issue of all - [d] several of their computers were found to have Logger systems in place, which recorded every keystroke typed on the computer. This made it easy for unknown individuals to later obtain a complete download of everything that was typed into the computer – including the passwords!

Note: The logger system that was used on their computers cost only about $50 each, but cost them tens of thousands of dollars in sustained losses before they decided to call for expert help.

Many factors must be considered before effective solutions and protective protocols can be selected and implemented. Further, any security program including password systems – must be periodically audited to insure that they are still effective and updated, and that all employees are complying fully in the programs use and procedures. These programs cannot be simply installed and forgotten.

Start with having an initial risk assessment performed of your business and offices. These cost effective first steps will provide you with a "map" of your current exposure risks, along with recommendations for properly addressing the identified open avenues of compromise. Risk assessments provide a detailed report of identified operational hazards and security deficiencies, along with recommendations for threat specific corrective countermeasures and follow-up.

The post assessment reports are prepared so as to address each firms individual hazards and threat potentials, as identified during the initial review. This is an inexpensive and worthwhile precaution when one considers the serious losses that can be avoided by securing against them before the fact. Once losses occur, recovery can be difficult and expensive - or even impossible. Many excellent business plans have been lost to acts of theft and undetected espionage. These crimes are rapidly increasing.

Don't be the next addition to the growing list of victims, many of which never even knew that their failure was attributable to the underhanded works of unethical individuals. Be pro-active and install protective programs and protocols designed to detect and counter any such affronts – before they are allowed to occur. Like car alarms – while not stopping all acts of business espionage or theft, a good security system may make a thief decide instead - to target the unprotected vehicle parked next to yours!

**FOR ADDITIONAL INFORMATION**. The author can be contacted at:

Mr. Felipe (Phil) Guillen, President
OMEGA, Inc.
P.O. Box 964
Tinley Park, IL 60477
708-429-1563

OMEGA is a Minority-Owned Business