



## Pass the Word on Passwords

By Ed Morales

Consultant, Risk & Compliance Group  
Compushare, Inc.

Financial institutions today often overlook a critical security control for the protection and integrity of their data and systems – password policy enforcement. A single, compromised password can result in an onset of attacks, the costliest of which is financial fraud according to CSI's recently published "12th Annual 2007 Computer Crime and Security Survey". The passwords we use are as valuable as the information we work to protect and the creation of strong and complex passwords is critical to the safety of the institution. However, most institutions rely on network policy settings that are based on best practice minimums for policy recommendations. As a result, institutions – and their employees' passwords – often fall short during security assessments and find themselves vulnerable to attacks.

Most institutions might be surprised at just how easily a password can be cracked, even when the minimum best practice policy settings are enabled. To understand this concern, we must first clarify Microsoft's password complexity requirements, which are often misunderstood. Meeting Microsoft's minimum requirements unfortunately does not automatically translate into a strong and effective password. Take, for example, the password 'Password123'. You would not dream (I hope) of using such a weak password nor would you suspect that your Windows system would even allow for the creation of such a generic password. Microsoft's complexity requirements call for three of the four following criteria to be met:

- Must use an upper case alpha letter
- Must use a lower case alpha letter
- Must use a number
- Must use a special character

As you see, 'Password123' does in fact

meet the minimum password complexity requirements in a Microsoft environment. Believe it or not, 'password' or any variation of 'password' is very commonly used today.

Complexity can somewhat be circumvented as the above example demonstrates. Therefore it is not a failsafe measure and should be supplemented. To stress this point, most standard 8-character passwords with enforced complexity can be easily cracked. Password cracking tools, easily available and accessible over the Internet, have advanced greatly and will continue to advance over time. Precompiled data tables, called 'rainbow tables', compile every possible



word combination and are commonly used by hackers. In most cases, 8-character passwords can be cracked in literally a few minutes by the use of these tables.

So how can a financial institution strengthen its frontline and help its employees to create stronger passwords?

The main reason why most people struggle in creating effective passwords is really quite simple; they are trying to create pass 'words'. The term itself suggests that a person use a password that, might be hard to guess, but is essentially a word. With this subconscious restriction, most people will add a number to the end of a word in an effort to adhere with password complexity requirements. Reversing this misconception and training users to create stronger passwords can be easy. Take, for example, the password '45String'. While complexity requirements are met, the word 'String' would be quickly picked up by cracking software. The password '45Str!ng' would be harder to crack, but not necessarily harder to remember. Even better, would be '45Str45!ng45'. What was once

the word 'String' is now bifurcated into two sets of random alpha characters separated by numbers. Rainbow tables can no longer easier hack this code.

You might notice the final example above is 12-characters long, opposed to the standard 8-characters. Most security specialists today recommend adopting a 12-character minimum password policy for simple reason – the longer the password, the harder to crack. We effectively created a strong password by increasing the character length and embedding numbers into a standard word. The new pass-code is much harder to crack but not necessarily difficult to remember.

Institutions can also benefit by using a 15-character minimum for network accounts with elevated privileges. According to Microsoft experts, "A 15-character password composed only of random letters and numbers is about 33,000 times stronger than an 8-character password composed of characters from the entire keyboard."

Another countermeasure that can be taken to help mitigate risks is to disable the LAN Manager hash (LM hash). By default, Windows environment network passwords are stored in an encrypted database referred to as a 'hash file'. Any hacker with access to rainbow tables can crack most passwords stored in the LM hash format. With simple group policy setting changes, LM hash files can be eliminated from being stored on your network. Windows will then revert to storing all network passwords in the newer, stronger NTLMv2 hash format.

Combining an increase to the minimum password length policy along with proper training on the creation of strong passcodes can result in a secure network were passwords cannot be easily cracked. Teaching employees to utilize strong passcodes can be effective when the issue is demonstrated as one of overall security to the institution. Ineffective passwords are often the weakest link in a security chain and each and every user should be made aware that they are a key frontline factor for the protection of data at the institution... so pass on the word.