PASSWORDS - WHEN NEEDS MUST

Passwords, the concept is a much debated topic in information security. The debate covers everything from how inadequately they protect systems all the way to how to best choose one. But whatever you think, you cannot deny that passwords are still very much alive, and by all indications will probably still be around for a while, and so we need to know about them.

Why Passwords?
Well most the of the protections used in information security centre around the simple fact of authentication. The system must first know who a user is before it can know how it must deal with that user, and this is done through different authentication factors:

Authentication	*Description*
Type 1	This is when *something you know* is used
Type 2	This is when *something you have* is used
Type 3	This is when *something you are* is used
Type 4	This is when *something you do* is used
Type 5	This is when *somewhere you are* is used

Now of these different authentication classifications, the one which has been around the longest and which is the easiest to implement is *Type 1* authentication, the time-honored usage of a password. By giving a system the right username and password, you convince that system that you are that user and are thus granted all the rights and limitations relevant to that user. Unfortunately, passwords are also considered to be the weakest form of protection around.

Why Are Passwords Bad?
There are a couple of reasons as to why passwords have their bad reputation;

- Users tend to choose passwords that are easy to remember, this makes them easy to crack as well.
- Random passwords are difficult to remember and end up being written down.
- Passwords can be shared, passed on, or even forgotten.
- Passwords can be found out via a large number of ways.
- Passwords are stored in password databases which are prime targets
- Passwords can be compromised by the very protocol being used [1]

How Are Passwords Attacked?
There are more then a few ways in which an attacker can attempt to crack a password;

- Use *network sniffing* to attempt to find out what usernames and passwords are being used [1]
- Use *social engineering* to attempt to trick a legitimate user into giving out passwords
- Use *social engineering* to gain information in order to make educated guesses about the password
- Use *brute force* attacks to use all possible combinations of characters in attempting to crack passwords
- Use *dictionary* attacks to use commonly used words in attempting to crack passwords
- Trying *default* passwords in case of lazy administrators
- Gaining *access* to the password database

What To Do?
If you have to use a password then, you should follow some basic guidelines to ensure that you choose one which

is not going to make an attackers job any easier;

- Change passwords periodically as even if an attacker does have you password, it would make it invalid.
- Do not use any system's default passwords
- Do not use the same password across multiple systems as if an attacker compromises one he would automatically compromise the rest.
- Do not use any part of your name, email address, phone number, nick name, company, beliefs, etc.
- Do not think that bad passwords spelt backwards are secure
- Do not use dictionary words, slang, or industry acronyms
- Do not use common keyboard combinations like *qwerty*
- Use long and unlikely passwords
- Do not repeatedly use the same passwords, rather come up with new ones
- Do not tell anyone else your password
- Do not write your password down
- Use multiple character sets (A-Z, a-z, 1-0, !-*) and non-standard spelling
- Never use cleartext protocols [1]
- Never use protocols with weak encryption
- Try to crack your own password to see how secure it is.
- Use account lockouts to limit the number of times the system accepts an incorrect password
- Use auditing with system logs to track logon successes and failures.

What Else?
The are some novel ways in which passwords have been implemented which aim at making their use more secure;

- *One-Time* passwords are passwords which change each time they're used.
- *Pass-Phrase* passwords are where a phrase is used rather then a single word per say.
- *Cognitive* passwords use a set of questions whose answers only the legitimate user should know
- *Dual-Factor* authentication combines passwords with the use of something else, such as tokens, etc
- *Challenge-Response* systems ask the user something different each logon to which the correct response must be given

Well that the end of this article, remember passwords are not bad, people who choose weak passwords are bad. Seriously though, the use of passwords is not going to disappear any time soon and choosing and using passwords can be made much more secure of just following good password practices and not being lazy. Bear in mind that attackers will always choose an easy target over a difficult one, so make sure your passwords cause any attacker many headaches.

---

[1] : Protocols - The Problem with Cleartext