

White Paper

**Two Factor Authentication  
Meets the Password**

Authors: Andrew Kemshall  
Phil Underwood

Date January 2006

Each of us routinely enters passwords, in some cases, many times a day! What is the point of this? It burdens us with the pain of trying to remember them and adds significant costs to the business to reset them. We do this with the misguided belief that the password is necessary to protect us and the business from other people trying to impersonate us. However the truth is that almost all the passwords that we use can easily be cracked, by even the most basic computer user with tools such as L0phtCrack, readily available from the Internet. The undeniable fact is that the human brain struggles to remember a password that is sufficiently strong enough to prevent modern computers cracking it in a short time period.

So if these passwords are essentially pointless, why even have them in the first place, after all don't we trust our work colleagues? Well, it's not just about trusting the internal employee, companies have to deal with extended enterprise users such as web portal partners, outsourced management companies and online e-purchasing users.

Who do you really trust? Contemplating not using a password would lead to anarchy and chaos, as e-purchasers could deny their transactions, competitive partners could invade other partner's information and employees could gain access to sensitive information such as staff salaries etc. Clearly a password is required; the dilemma is how to use a strong password within the limited memory capability of the human brain.

Using a password constructed from just lower case letters gives only 26 variations per entered character. However if upper case, lower case, numbers and symbols are used this leads to a much stronger password as each entered character has around 64 variations.

Using brute force techniques, modern PC's can reach up to 10 million tries per second. The table below outlines how long the password can resist this sort of attack before it is compromised. It is assumed that strong passwords with 64 variations for each entered character are used.

Password length	Tries per second	Time to break
4	10 million	1.6 seconds
6	10 million	1.9 hours
8	10 million	326 days
10	10 million	3600 years

We can see from this example that a password length of 8 can last for 326 days however, if 10 computers are used in parallel this time is reduce to 32 days, which is unacceptable.

It is also good practise to plan for the future. In 5 years time advances in computer power is predicted to increase this rate to in excess of 100 million per second, the following table shows an update based on 100 million tries per second instead of 10 million.

Password length	Tries per second	Time to break
4	100 million	0.16 seconds
6	100 million	11.4 Minutes
8	100 million	32 Days
10	100 million	365 years

Clearly the only viable password length has to be 10 characters or greater, which will allow reasonable security now and in the future.

A typical example of a 10 character complex password is listed below:

```
vLy47S=&>@  
yGJNKw06%e  
":)~">p8H"
```

Research has shown that most users can remember 4 characters of a complex password very easily, but when this is extended to 5 and above, it dramatically falls off, with little to no users being able to remember a 6 character complex password or greater. The password seems unusable and does not provide a viable solution for user authentication.

One approach by leading Two-Factor token vendors is to replace the logon components within the desktop with one that supports the use of a token. This essentially rips out the existing password mechanism for a proprietary one.

The drawback of this approach is the deployment of software on every desktop, in the case of Microsoft the GINA interface is modified which leads to problematic or no support for services such as terminal services, remote desktop and Dialup / VPN connections. For remote users that work offline, excessive delays are experienced whilst the token system attempts to communicate with its central server before timing out and allowing the user to logon offline.

Most companies concerned about strong authentication find this type of solution cost prohibitive and unmanageable in terms of both token and software deployment.

A more effective approach is a revolutionary patented solution by SecurEnvoy called "Password Automation" which utilises the existing operating system password mechanism. This tackles the real issues of managing 10 character complex passwords head on.

The solution splits the 10 character password into two portions, a 4 character password that is secret to the user and can be easily remembered and a 6 character part that is sent to the user's Mobile phone via SMS. The portion stored upon the user's mobile phone is further secured by the fact that it is dynamically updated periodically, typically every 7 days. The new password automatically overwrites the last password used, so there is no confusion as to which is the current password.

The user, when prompted for their password, would simply enter their 4 character password (something they know) appended by the 6 character password stored upon their mobile phone (something they have). By utilising something the user knows and something they have brings the strength of Two-Factor authentication to the password.

The SecurEnvoy Password Automation Server ties into the existing password sub-system rather than replacing it. By setting each user's password with the two factors re-combined, allows the operating system to directly understand the current two factor authentication codes.

So in conclusion, the future is bright for the passwords providing you can store at least a part of it in a device such as your mobile phone.