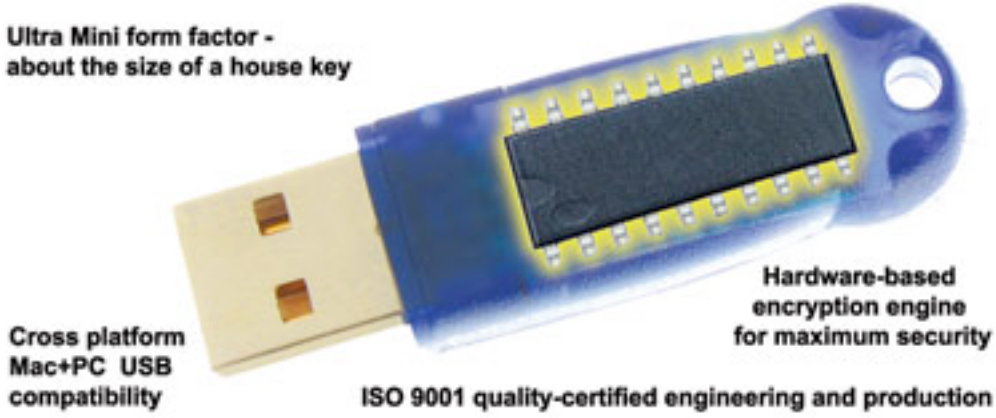
SecuriKey's technology

Two-factor authentication

It is as simple as two pieces of evidence. Password technology is something that most everyone is familiar with. Combining that password with a one of a kind object… that only you would have… significantly increases security. Any security expert will tell you that a second factor of user authentication increases security by an order of magnitude. That is exactly why your bank uses it at the ATM. Your card… and a PIN (password.)



What's in the SecuriKey Token?

To most people it is magic. In reality, it is a custom designed ASIC chip that makes the token a security encryption engine. It encodes and encrypts the login sequence. Without it plugged into the USB port, there is no login. When you remove it… SecuriKey locks out any input or computer use. Only when the correct password is entered while the token is in place, will the computer be unlocked.

What else does it do?

The SecuriKey software and hardware (the token) supply the security you need to protect your data. But SecuriKey can also help with some other measures to increase security. The software allows you to coordinate with data encryption software… another level of defense. You can then lock down your hard drive as the only allowable boot device for your computer. You can also access Safe Mode Blocker. Enlisting all of these measures essentially makes your computer impenetrable by anyone but you.

Why don't passwords work?

Weak passwords can be easily guessed

One reseller estimated that 80% of his clients used the word "password" as their Windows® logon password. Weak passwords that take only seconds to compromise include names of close relatives, pet names, anniversary or birth dates, maiden names, common English words or combinations of the above. Passwords are an easily bypassed, single point of failure.

Most strong passwords get written down

Strong passwords contain at least eight alpha-numeric characters mixed in such a way that no English words are created. One network administrator was appalled to find post-it notes containing logon passwords stuck to the computer monitors of his users after issuing "strong passwords".

Strong password policies require passwords to be changed frequently (every 30-90 days). Users simply cannot remember long strings of meaningless text, especially if that string changes every 30 days. They think their only hope for logging on, is to write down the string and hide it from the network administrator somewhere in their cubicle or work-space.

Even strong passwords can be cracked

The CERT® Coordination Center, a security clearing house and part of the Carnegie Mellon Institute, commissioned and then published research by Dr John D Howard. The following is taken from his paper entitled, "An analysis of Security Incidents".

"8.1.3.1 Password Vulnerabilities - The most frequently recorded vulnerability involved various problems with passwords, which were mentioned in 938 incidents (21.8%, column 18, Figure 8.3). There were 16 different combinations of keywords that indicated password problems. Most of the password vulnerabilities were in three categories: password files, generally indicating that a password file had been copied (592 incidents, 13.8%, 63.1% of password vulnerabilities), password cracking, which indicated that passwords had been determined by the operation of a password cracking tool (448 incidents, 10.4%, 47.8% of password vulnerabilities), and weak passwords, which could be easily guessed (156

incidents, 3.6%, 16.6% of password vulnerabilities). It is interesting to note that password cracking was recorded as an exploited vulnerability in nearly an order of magnitude more incidents than the tools used for the cracking (448 incidents mentioning password cracking, compared to 52 incidents mentioning password cracking tools)."

Why doesn't data encryption work on its own?

Good encryption programs assume that once a user is granted access to the computer, then decryption of data will take place automatically behind the scenes so as not to interfere with the user's work flow. By simply guessing or finding the logon password, someone will always have access to encrypted data, unless time is taken to create a unique encryption key for each data file. Creating these individual encryption keys can be more costly than the creation of the data, and in general is so time consuming and confusing that it simply isn't done. What's more, not all encryption systems are created equal. Bad encryption programs provide encryption that can be easily decrypted with utilities found all over the Internet. So, the result is that data encryption - even good encryption - doesn't protect you within the context of the security problems of password-based access control.