

[www.securecomputing.com](http://www.securecomputing.com)

Secure Computing® has been solving the most difficult network and application security challenges for over 20 years. We help our customers create trusted environments both inside and outside their organizations.



**Secure Computing Corporation**

**Corporate Headquarters**

4810 Harwood Road  
San Jose, CA 95124 USA  
Tel +1.800.379.4944  
Tel +1.408.979.6100  
Fax +1.408.979.6501

**European Headquarters**

East Wing, Piper House  
Hatch Lane  
Windsor SL4 3QP UK  
Tel +44.1753.410900  
Fax +44.1753.410901

**Asia/Pac Headquarters**

1606-8 MLC Tower  
248 Queen's East Road  
Wan Chai Hong Kong  
Tel +852.2598.9280  
Fax +852.2587.1333

**Japan Headquarters**

Shinjuku Mitsui Bldg. 2, 7F  
Nishi-Shinjuku 3-2-11  
Shinjuku-ku, Tokyo, 160-0023  
Japan  
Tel +81.3.5339.6310  
Fax +81.3.4496.4537

**Weak passwords weaken networks.  
Is your network safe?**

Remote access has opened up a world of possibilities for everyone who uses a computer at home or work. Today, users can access their corporate network from a hotel room in Philadelphia. Network administrators can manage their company's systems from home, no longer needing to pull their clothes on and groggily drive to the office at 3 A.M. Web-based access systems, Citrix and other thin-client technologies, and Outlook Web Access have made it possible to access many corporate networks from anywhere at any time.

With this convenience, however, comes an enormous amount of risk. Keylogging software, surreptitiously installed at 14 public Internet terminals in the Manhattan area, allowed an attacker to compromise the personal information and network access of dozens of people and organizations. One company based in Silicon Valley endured months of unauthorized access by a competitor before they discovered the breach. Last year, an organized identity theft ring victimized over 300 customers of a well-known financial institution, costing over \$3 million.

The cause of all of these exploits—and indeed, the root cause of hundreds of corporate breaches, identity thefts, and millions of dollars lost every year—is the password.

The average computer user has dozens of accounts online and at their job. Access to nearly all of these systems requires a password. Most people can't memorize different passwords for all their accounts, particularly if they only access certain applications once a month. Here are some ways average users combat their memory problems:

1. They choose one password for everything. Of course, if their password for their personal Web mail is compromised, chances are good that their company network password is compromised as well.
2. They write their passwords down. One online study revealed that over 30% of people surveyed wrote their passwords down and "hid" them: under their keyboards, on their staplers, or in their desk drawers.
3. They choose information they can easily remember. Many people—up to 35%, according to some experts—choose some piece of personal information: a name of a family member or pet, or a birthdate. The problem is, everyone knows your daughter's name. A potential hacker can make small talk in the lobby with an employee—and come away with dozens of passwords to try.
4. They get clever. In one company's password audit, 10% of passwords were "stud," "goddess," "cutiepie," or some other vanity password. Even more disturbing, 12% of passwords were "password"—and most of the users who chose it thought that it was a clever choice.

The problem is that hackers know all of this. Before they attempt personal information to crack a password, the first thing they try is "password." Hackers will also pretend to work at a company, striding confidently into the front doors with a nod of the head to the security desk or the receptionist. Any passwords on monitors or under keyboards are fair game. Once a hacker has cracked a password, they can view confidential documents or e-mails without the organization ever knowing about it.

The answer to this huge problem is strong authentication. This refers to factors that work in combination to protect a resource. ATMs are the most common example of this: to access your checking account, customers must use two factors to be authorized. First, they must have their physical bank card (one factor: what you have), and second, they must know their personal identification number, or PIN (second factor: what you know). Most people would not want their checking account guarded with just a PIN or just the card—yet companies use password-only protection to guard resources that are many times more valuable than the average person's checking account.

Government standards are now making it imperative to protect consumer information. Health care agencies and financial institutions in particular are finding that implementing strong authentication is a step towards complying with recent legislation to protect patients and customers.

Without realizing it, many organizations had been using strong authentication for years: employees had to know passwords to access the company network (one factor: what you know), but also needed to be inside the building (second factor: where you are). But remote access has taken away the location requirement, as demanded by today's business environment, and authentication has become vulnerable as a result.

Today, there are several candidates for strong authentication solutions:

1. Tokens are small pieces of hardware, about half the size of a credit card (but a bit thicker), that often fit on a keychain. Like an ATM card, this factor is a "what you have." They often have LCD displays and give the user a one-time passcode for each login. Instead of logging in with a password, the user activates the token and types in the characters from the token display into the password field. Tokens usually require a piece of server software that allows or denies access to the user. The big plus for most IT departments is that token solutions don't require a piece of client software on the user's machine. Tokens, therefore, can be used anywhere: on public Internet terminals, on the Web, from any laptop, desktop, or palmtop. Some users resist tokens initially, and some companies are concerned about price: upwards of \$70 per user as an initial cost for many solutions. But the solution is cost-competitive, highly reliable, portable, and one of the simplest options available to deploy.

2. Smart cards look like credit cards with a computer chip inside, and is also considered to be the "what you have" factor. The user inserts the smart card into the smart card reader to access the requested resource. Many analysts have been saying for years that smart cards are going to make tokens obsolete. However, many smart cards require public key authentication, which is supported only by a small range of protocols. Smart cards are generally portable only to machines that also have smart card readers. Additionally, the hundreds of dollars per user to buy, deploy, and install smart card readers and software has scared away most customers. But many computer manufacturers are beginning to make smart card readers standard equipment on their high-end laptops, meaning that lower costs may not be far off. There are also high-profile customers, like the U.S. Government and Microsoft, who have already standardized on smart cards.

3. Biometrics gets a huge amount of press. This "what you are" technology could be a fingerprint scanner, a retina scanner, a signature reader, or some other piece of identifying information tied to each user's physical identity. Most experts agree that the technology isn't quite ready yet—for instance, many fingerprint scanners can be fooled by simple attacks. These solutions are also quite expensive, and not very portable—they're often tied to a single machine.

There are some "low-tech" solutions as well.

An online bank in Scandinavia issues cards with one-time passcodes printed on them; users simply cross each one off as they use them. Many organizations—particularly government agencies—refuse to allow remote access because of the security risks. Still others brave the password jungle, asking their users to create complex schemes to make their passwords strong enough to survive a determined hacker (or a security audit).

Still, the majority of commercial companies continue to allow remote access with nothing more than passwords. For these organizations, it may just be a matter of time before a hacker gains unauthorized access—if it hasn't happened already.

Secure Computing Corporation provides strong authentication solutions in its SafeWord product line, as well as other network and application security products designed to let your remote users in and keep hackers out.

For more information, please visit [www.safeword.com](http://www.safeword.com).