



news | reviews | digital life | internet | how-to | community | publications | download

search articles

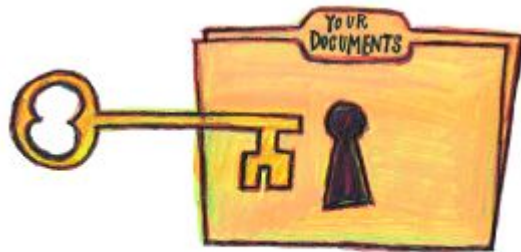
go

[home](#) > [Member Login](#)

Member Login ~ *story*

TCP Test Lab: Hardware security

By Dave Chappelle, posted 4/21/2002 6:27:26 PM



Computer security is a hot topic today, covering everything from authentication to data storage security, data transfer security, privacy, identity protection, physical asset protection, theft prevention, and loss recovery.

When you purchase a mouse, or other peripheral, you generally begin using it once connected, and forget about it. Not so with security products. Effective security requires maintenance. At the very least, passwords should be updated.

However, few of us change passwords regularly unless required to by network administrators. Fewer still are aware that most logins and passwords are sent over the Internet using "clear text"--which is not encrypted and can easily be read. If someone has placed a keylogger or other spyware program on your system, or intercepted your clear text, the new passwords will be instantly apparent. How would you know? Most likely, you wouldn't.

Hardware to the rescue

And that is the single biggest problem with computer security: it's never enough. Security is a process, not an event. With software solutions, it's not as simple as turning a key in a lock and forgetting about it. You must always be on guard.

No wonder so many users play ostrich, sticking their heads in the sand. Computers already require effort. Properly securing a computer requires more, and continuous, effort.

Generally, hardware security devices require less maintenance than software security programs. In an effort to increase the level of security knowledge and practices of our readers, we've examined a few security products covering different aspects of computer security.

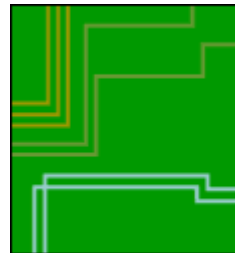
[email this story](#)

[printer friendly version](#)

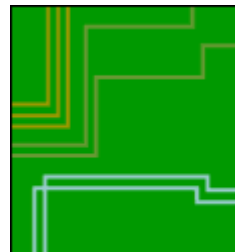
[post comment to this story](#)

6/20/2002

canadacomputes.com
Domain Registration
 Click here



Visit our merchant directory to see our Advertisers
 Click here.



AlphaShield: Address unknown

www.alphashield.com

Suggested retail price: \$269.99

Warranty: one year

Almost everybody knows the Internet isn't anonymous, as IP addresses are traceable. Theoretically, if your IP address is not visible, it can't be used for nefarious purposes. To keep your IP address safe, Burnaby B.C.-based Saafnet has released the AlphaShield IP address hider.



Its Stealth IP feature hides your computer's IP address. As an IP address is visible to any site a user requests to visit, it is difficult, if not impossible, to completely hide it. Corporations use NAT (network address translation) to display a different address. For small networks and home users, AlphaShield hides the IP address from unrequested sites and from any port scans attempted by hackers randomly scanning blocks of IP addresses.

The RPA (real-time packet authorization) feature inspects inbound and outbound data, permitting only authorized packets through. What's the significance of this? Some Web sites try to piggyback additional information into your computer along with your legitimate request. AlphaShield allows only requested information to pass, and rejects data that has not been requested.

The AlphaShield disconnects the computer from the Internet during periods of inactivity in two ways.

First, two buttons on the top serve as off and on switches, allowing for instant connection and disconnection to the Internet. The idea is that if you leave your computer for a while, you hit the disconnect button and upon returning, press the connect button to reestablish your Internet link.

Second, a three-position switch on the back of the unit controls connection modes. Manual and Locked modes automatically disconnect after 15 minutes of inactivity. In Manual mode, the disconnection is logical, while in Locked mode, the connection is physically broken and the assigned IP address released. In Auto mode there is no disconnection until the user hits the disconnect button.

The AlphaShield unit measures 13.4x7.8x2.6cm (5.2x3x1 in.), and comes with an AC adapter, a 2 m (6.5 ft.) length of Category-5 network cable, a quick installation guide, and user manual. AlphaShield plugs in externally, without requiring changes to a system--an advantage over software solutions.

The Alpha Shield works with external cable and DSL modems. It will work between a network and a modem, provided the network cards can operate at 10 Mbps (100 Mbps not supported).

The unit is as simple to set up as just plugging in the appropriate cables. We encountered one initial computer freeze-up, but after a reboot there were no further problems.

An auxiliary pass-through Ethernet port is for connecting other devices, or running tests, without providing stealth capability.

EToken: For your eyes only

www.alphashield.com

www.aladdin.com

Price: \$37 (R2 16 KB), \$39 (R2 32 KB), \$47 (Pro 16 KB), price to be set (Pro 32 KB)

Warranty: one year

From Aladdin Knowledge Systems, the eToken encrypts and stores private keys, passwords, and digital certificates--authentication methods used in e-commerce and secure data transfer.



Physically, the eToken resembles a USB memory device, and is roughly the size of a house key and can be easily attached to a key ring. Because it uses a USB interface, the eToken works with a standard USB port rather than requiring a dedicated reader.

For hard to reach spots, an extension cable is included that connects to a USB port on one end and the eToken on the other. A suction cup at the eToken end of the cable allows a user to attach it to a convenient place, such as the side of the system case or monitor.

The eToken works with numerous encryption and security (authentication) systems, including CheckPoint, VeriSign, Baltimore, Entrust, RSA, and Microsoft. Aladdin offers a developer's kit for tailoring the device to specific applications.

The eToken comes with software that allows you to change the eToken name and password. The eToken type, version, and available memory can also be checked and the device lights up when the software is installed and working.

To access eToken-protected data, a user has to provide both the eToken and a password. This is known as "two-factor" authentication. Even if the password is discovered, without the eToken being physically plugged into the USB port, the computer cannot be accessed. On the other hand, if you were to forget your password, the eToken would also become useless--plus you would not be able to reset it since you would also need the password to access the software.

ETokens are available in green, red, blue, purple, and in personalized versions. The R2 model uses 120-bit encryption. The Pro version is a 1,024-bit RSA smart card. Data is stored in EEPROM (electrically erasable programmable read-only memory). Aladdin assured us that the eToken will retain data for a minimum of 10 years, with at least 100,000 memory cell rewrites.

PC Pal: Remove at your own risk

www.palscomputers.com

Price: \$79.95

Warranty: two years

The PC Pal is a theft-prevention alarm--and it's a loud one. The factory default setting is 90 dB, the loudest alarm volume allowed in public places. You can order a 130 dB model, if you intend to use the device outdoors.

A lockset controls the alarm, with a turn of the key arming and disarming it. For locations with multiple systems, locksets can be ordered that use the same key.

The alarm is triggered by motion sensors, which can be adjusted for sensitivity. At low sensitivity, the PC case must be physically moved for the alarm to sound. At high setting, the alarm can be set off when someone

with a heavy footfall walks by.

In our tests, no one could carry a system more than a few steps before the alarm sounded even at the least-sensitive setting. If the alarm is unintentionally tripped, it can be deactivated using a push-button reset switch and a technique explained only to alarm purchasers.

A nine-volt battery powers the alarm for up to nine hours. A lithium battery version is available. Both battery power sources are separate from the system power supply and motherboard BIOS battery.

Versions are available to fit into 5.5-inch and 3.5-inch drive bays, or a PCI slot. A laptop version is in development. Custom installations are also available.

The PC Pal comes with warning stickers for additional deterrence.

SecuGen peripherals:

Are you really you?

www.secugen.com

Prices: \$249 (OptiMouse), \$229 (Hamster),
\$279 (Keyboard)

Warranty: one year

Tired of other people accessing and changing your system settings? Concerned that a roommate, sibling, child, or spouse might delete something important? Would you like to be the only person able to access your computer? If this describes you, you may want to consider biometric authentication. The SecuGen system, with I/O SecureSuite, including SecuDesktop 2000 software, uses fingerprint identification to authenticate users.



Measuring fingerprint details in three dimensions, SecuGen devices record the data. When activated, a number of the details must match the stored fingerprint record before a file is opened, a user is logged on, or a user can proceed further.

The OptiMouse sample we tested used an optical sensor. It connects via USB, but parallel and standard rolling ball versions are also available.

At 12x6x3.5 cm (4.6x2.34x1.36 in.), it is the size of an average mouse, with two buttons and a scroll wheel on top. Fingerprint data is captured through a small scratchproof polycarbonate window on the left side.

How secure is the fingerprint authentication? We tried using a two-dimensional fingerprint captured on clear tape with no success. We also attempted to use a finger cast made from common household silicone.

Another technique seen in movies, of cutting off someone's thumb, won't work either, since a thermal register (body heat) is required. (Rather than test this method, we accepted the word of SecuGen reps.)

Most users will be prevented from accessing your files by the fingerprint window that appears in where you would normally see a password screen--as soon as the system is booted, a key is pressed, or the mouse moved to bring the computer out of standby mode.

However, design flaws in Windows 9x can let a determined person physically access your system. Booting into safe mode, booting into DOS, or booting from a floppy disk can bypass all third-party security software.

Even Windows 2000 security can be bypassed with third-party boot software designed for that purpose. For added protection, SecuDesktop can be used to encrypt individual files and folders.

On the plus side, once biometric authentication is installed, users don't have to remember their passwords. IT support professionals won't have to answer any more calls from users who have forgotten their passwords.

The Hamster is a standalone fingerprint reader, about the same size as a paper clip dispenser, that offers all the biometric security features. The keyboard will soon be available with a biometric sensor plus SmartCard reader.

Siemens ID Mouse Professional: Capacitive resistance reader

From: Siemens Biometrics (PSE TechLab in U.S.)

www.siemensidmouse.com

Price: US\$119

Siemens claims its original ID Mouse, introduced in 1999, is the best-selling standalone biometric device in Europe. It announced the ID Mouse Professional at Las Vegas Comdex in November, and we've been using our test sample off and on since then. As a mouse, this USB device is very comfortable to use. It has a scroll wheel and optical tracking rather than a physical ball, so it requires little maintenance.



The biometrics portion of the ID Mouse Professional is a fingerprint sensor. Like other biometric devices, it records a unique biological characteristic (in this case, a person's fingerprint) into its database, then uses it for authentication instead of a password. The software allows the user to register fingerprints from all digits.

The fingerprint reader is based on capacitive resistance rather than optical scanning, which Siemens says is a more rugged technology, that requires less space to implement--so the mouse is smaller and more durable.

We could find no product information about the ID Mouse Professional on Siemens' Canadian site, but there is information about it on its San Jose Calif.-based Siemens PSE TechLab site (www.psetechlab.com). It is currently available online for US\$119.

Valt.X: Safe behind a wall

www.valtx.com

Price: \$130 (single disk), \$250 (double disk)

Warranty: one year

There are plenty of software and hardware firewalls on the market--most of which prevent unauthorized access to systems or networks. Valt.X storage firewall is slightly different. It places a copy of selected data or the entire contents of a hard drive behind impenetrable and invisible protection.



Valt.X has its own built-in processor and memory. A 3.5-inch hard drive is attached and connected to the Valt.X device, which is then mounted in a 5.5-inch drive bay. An LCD on the front panel indicates the activity or mode selection of the drive. Another version provides two sensors to store an

selection of the drive. Another version provides two separate storage firewalls. Yet another will mount in a PCI slot.

We witnessed a single version in action. The Valt.X rep deleted an entire program from a test system. The system was rebooted, and the program was obviously missing. By rebooting again and accessing the Valt.X menu, the original configuration, including the missing program, was completely restored.

Restoring one program was impressive, but what happens when a malicious agent deletes an entire hard disk partition? We watched as the entire C: drive partition was deleted. The system was restarted and nothing was on the drive. It appeared totally new and unpartitioned. From an option in the Valt.X menu, the operating system was restored in seconds. The original system was intact, as if nothing had happened. And nothing had happened to the version behind the storage firewall.

Valt.X works with hard disks of any capacity, with any operating system, in any PC using ATA/EIDE drives. All speeds of hard drive are mountable, including ATA (UDMA) 100.

You can choose between live and protected modes. In the latter, any changes made to the computer during a session are lost when you shut down, so you are always rebooting to the same, fixed configuration.

Sometimes new software can render a perfectly good computer useless. How many times have you installed new software, only to completely ruin your system? Had you first backed it up with Valt.X, your old system could be restored in seconds.

It's better than those "restore disks" included with name brand computers, which only restore the original factory software and settings. Anything installed or configured between the day the system was unpacked and the fatal crash, is gone forever.

The only downside to Valt.X is that if an entire drive is to be protected, its capacity is cut in half. Our example was a 10 GB hard drive. To protect the entire drive, we were allowed no more than 5 GB of storage. At current low prices for data storage, that is a small price to pay for complete protection and virtually instant restoration.

Although unlikely, if drive space is limited, the entire drive need not be backed up to Valt.X. Specific files, groups of important data, and possibly an operating system can be placed behind the storage firewall.

This solution protects server hard disks as well as those in standalone computers. It's a versatile product, and one that users of any experience will consider long overdue.

Security glossary

Authentication: Determination of a user's identity. Performed three ways: what you have (key or token), what you know (password), or who you are (biometrics).

Biometric: Organic measurement. Evaluating one or more distinguishing biological attributes: finger and palm prints, voice, eye, ear, gait, and facial features.

biological traits: finger a d palm prints, voice wave patterns, a d retina a d iris patterns, for example.

bps: Bits per second--a measure of data transfer. A bit is the smallest portion of digital data. Other common data rate measures are kilobit (1,000 bits) and megabit (one million bits).

CA: Certificate authority--a network authority that issues and manages security credentials like public keys. Part of a PKI, a CA checks with the RA to verify information provided by the requestor of a digital certificate. Once confirmed, the CA issues a certificate.

Decryption: Restoring encrypted, and therefore unreadable, data into readable form.

Digital certificate: Issued by a CA to establish credentials when conducting Web transactions. Contains your name, a serial number, expiration dates, a copy of the certificate holder's public key, and the issuing authority's digital signature. Kept in registries so authenticating users can look up other users' public keys.

Digital signature: An electronic signature used to authenticate the identity of the sender of a message or the signer of a document.

DSL: Digital subscriber line--high-speed Internet service carried over the same telephone line that carries voice calls.

Encryption: Transforming readable data into unreadable form.

Firewall: Hardware or software that controls information flow between computers.

IP: Internet protocol. Messages are divided into individual units of data, known as packets. IP ensures each packet arrives at its required destination, or address.

IP address: A unique number consisting of four groups of three numbers, each from 0 to 255. Every computer on the Internet has one.

Keylogger: A type of spyware that records keystrokes of a computer, and either sends the recorded keystrokes to another party or stores them for later retrieval and use.

Logical disconnect: Allowing a system to remain physically connected, but not allowing data to be received or transmitted. IP addresses can then be maintained and the system used, but it can't communicate with other computers.

NAT: Network address translation--translating an IP address of one network to a different IP address, which is known to another network, often the Internet. The translation process increases security by allowing for authentication of each request. A company conserves global IP addresses by using a single IP address for all communications.

Partition: An area of a hard drive designated for storing data, the size of which must be set by the user prior to formatting.

Packet: A byte plus one parity bit that is for error checking.

Physical disconnect: A physically open circuit--unplugging the cable.

PKI: Public Key Infrastructure--a system enabling user to transfer money and information securely. Often used in e-commerce transactions. User has two mathematically related keys: one private, one public. She retains the private key, using it to encrypt sensitive data. She distributes the public key to those who must view the data. Recipient uses the public key to decrypt the message and read it.

Port: A passageway for different services, each using TCP to transfer data. TCP maintains order by assigning a unique port to each service. Port identifiers number from 0 through 65,535. Firewall security involves closing all ports except those required for essential services.

Port scan: A hacker technique for finding undefended computers. Messages are sent to each port, one at a time. The response received indicates if the port is in use. It can then be probed for weaknesses and exploited.

RA: Registration authority--a network authority that verifies requests for digital certificates.

Spyware: Software installed on an unsuspecting user's computer for the purpose of spying. Some spyware programs record keystrokes. Others capture and store images from the monitor at preset intervals so another party can see everything the unsuspecting user saw. Advanced spyware programs can email the captured data to the spy. Spyware is invisible to the user.

TCP: Transport control protocol. Messages are divided into individual units of data known as packets. TCP maintains control of these data packets so they can be routed efficiently around the Internet.

TCP/IP: Transport control protocol/Internet protocol.

VPN: Virtual private network. Using encryption technology on two computers to send and receive private information over a public network, such as the Internet. Often referred to as a "VPN tunnel."

By Dave Chappelle

 [email this story](#)

 [printer friendly version](#)

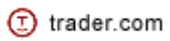
 [post a comment](#)

Comments

No comments have been posted yet.

□

[advertising](#) : [newsletter](#) : [product alert](#) : [have your say](#) : [about us](#)
[merchant program](#) : [merchant directory](#) :



CanadaComputes.com is operated by Gadekin, a Trader.com member company.
Copyright ©2000 Canada Computer Paper Inc., All Rights Reserved
[privacy policy](#) : [legal information](#)