Secure USB

The threat and the opportunity

By Jon Collins, July 2008

This article originally appeared in Infosecurity Magazine India

In a nutshell:

USB-based devices such as memory sticks are often seen as a risk to information security. However, a number of such devices can not only protect against such risks, they can also help to provide a more secure desktop IT environment.

Key points:

- USB devices have had a profound effect on how we share information. However they are easy to lose, and are most frequently configured without any security protection.
- More recently, a number of devices are becoming available with more advanced security features, right up to being capable of supporting a comprehensive, locked down set of security measures.
- Organisations should of course review their policies concerning the use of USB-based devices, particularly the use of unprotected devices for data transfer
- However, organisations should also recognise that certain devices can offer a much higher level of information security protection.

When the USB standard was first launched, few would have imagined the profound effect it would have on how we use computers and share information. Today however, we see a plethora of new, different kinds of device that benefit from the USB specification – not least flash memory storage, which has obsolete the floppy and all but replaced the CDROM as a way of transferring files, but also such esoteric uses as using the powered USB port to charge mobile phones and other handheld devices.

The simplicity of USB storage belies a number of quite serious security threats, however. Not least of course, that it is possible to shovel quite a load of corporate data onto such devices – which today can reach a size of 16GB plus. This may be done for malicious reasons, but more often it could be quite innocuous – an employee who doesn't know which files he might need to work on over the weekend, may just dump the entire directory structure onto a USB stick. Woe betide, then, should he or she lose it on the way back home.

Risks such as these have led some organisations to take quite drastic measures to prevent the use of USB storage in particular, from disabling the device drivers, to (so the anecdotes go) super-gluing the USB ports on desktop computers. While such stories may be apocryphal, they reinforce

the belief that USB is in some way a bad thing, and access should be prevented. This thinking leads to a dilemma in many IT shops – not least because USB storage has become an essential element of collaboration and file sharing, but also because USB has such a wide variety of other functions.

Despite being tarred with the brush of insecurity, the fact is that USB-connected devices offer opportunities to reduce a number of security risks. To catalyse acceptance of more advanced devices, we need to simultaneously quell the quite genuine concerns about the risks associated with USB storage. Let's look at this first.

The ability to encrypt data on a USB device has been available for a number of years, pioneered by companies like M-Systems (Now part of SanDisk) and licensed via the brand DiskOnKey to the likes of HP and Apple. Essentially, such devices can be partitioned into insecure and secure areas, and an encryption chip on the device ensures that data stored on the secure area can only be accessed via a valid username and password combination. Such devices are almost impossible to hack: indeed, the circuitry is designed to burn out should attempts be made to break the encryption codes. Meanwhile there are endpoint security companies such as DeviceWall whose technologies support the encryption of data onto any device. In both cases, the result is that employees can have a single, locked down storage device both for passing of non-sensitive data, and for transport and backup of sensitive files.

There are several security benefits to such an arrangement. Of course data is protected against theft or loss (unless the thief has the password, of course!); also, it provides the basis of secure offsite backups, for example if an employee spends a lot of time outside the office it is good policy to recommend backing up data at suitable intervals. If there are concerns about the security of the computer being used (for example if working on a client site or in Internet cafes), then data can be accessed directly from the device. For further protection, some device manufacturers such as MXI are incorporating fingerprint readers directly on the device. A swipe of a finger replaces the need for a username/password, which is not only more convenient, but reduces the risk of theft even further.

Some devices can store not just data, but applications. The U3 initiative for example (www.u3.com) provides an application framework for Microsoft Windows computers so that U3-enabled applications can be executed directly from the USB stick; furthermore, when the device is removed, so are any traces of the applications and data involved. A wide variety of software is available, from apps such as OpenOffice, the Firefox web browser and Thunderbird email client, to network diagnostics tools so (say) an engineer can arrive at a client site with his toolbox on a single thumbdrive which can be plugged directly – and securely – into a client computer.

As well as features to help us work more securely with USB devices, there are also devices that exclusively provide security functionality. As a simple example, think of token-based USB plugs: these tend to be tight on storage capacity (running into the kilobytes rather than the megabytes), as their function is to manage encryption keys rather than data. There is the Aladdin eToken for example, or indeed, the RSA 6100 chipcard in its USB form factor (check now). While both come with handy tools to manage online usernames/passwords (or Web Sign On, in Aladdin's parlance), the real strength of such devices is in the corporate environment, when they can be used to support two-factor authentication for logging on to the corporate IT environment.

Other vendors are loading different kinds of security functionality onto the USB device. Accario for example has combined application wrapping, strong authentication, virtual private network termination and a fingerprint reader onto its AccessStick product. As an interesting example of a use case, AccessStick is targeted at Citrix environments: put simply, you can go onto any computer anywhere in the world, and access your corporate IT environment, remotely and securely. A similar idea is behind the MobiKey product from Route1.

The logical next step is for the device itself to run security applications. One company, Yoggie, has launched a firewall appliance (the Pico) on a USB stick, which is in fact a Linux-based, Pentium-class computer running a range of end point protection applications. We expect to see a number of such devices appear over the next couple of years, potentially combining capabilities such as those sported by the AccessStick and the Pico, and making use of virtualisation to enable an entire, secured compute environment that can run on a single drive. While attractive, such ideas are yet to reach the mainstream as there remain technical issues, for example around the portability of the virtualisation platform.

There are clearly plenty of benefits to be had from security-enabled and security-enabling USB devices. We know however, that one of main challenges associated with security is its management. Many of the devices mentioned here can operate in a stand-alone mode, that is, they can be configured and secured by the user. However, certain features require a level of centralised management – not just to administer such things as encryption keys and the like, but to control the devices themselves.

This is an area in which we are currently seeing a great deal of activity. SanDisk's Cruzer Enterprise device for example offers a range of management features, including Active Directory integration, remote password administration and centralised updates. Not only this but, if lost or stolen, the device can be configured to "ping" its presence to a central management console, from where it can be disabled remotely. A number of the companies mentioned above, including MXI and DeviceWall, offer similar capabilities. While beneficial, it would be fair to say that this is an evolving market and there are still some challenges to be overcome – for example, agreement of a common standard such that all manufacturers can be singing off the same hymn sheet.

What can we conclude? In the future, USB devices will continue to add new features and find new applications (the recent release of the TrackStick USB-based GPS module offers a whole new set of possibilities, for example). With all their potential however, the one challenge USB devices can never overcome alone is down to their small size: we need to take it as inevitable that the little blighters will be lost, misplaced, dropped down the backs of sofas, accidentally crushed underfoot or otherwise rendered inaccessible. Any security policies need to build in criteria not only for their appropriate use, but also the consequences of such loss. Perhaps they will become like car keys: while we have learned to treat them carefully, equally, we should know where we keep the spare.

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream business and IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.