Fujitsu Develops Secure USB Memory Device Featuring Automatic Data-Erase Function

April 17 2009

Prototype of newly-developed secure USB memory device

Fujitsu Laboratories today announced the development of two new technologies designed to prevent the unwanted disclosure of data from lost universal serial bus (USB) memory devices and prevent uploads to file-sharing networks: a USB memory device technology that after a fixed period of time automatically erases data stored on the USB memory, and a file redirect technology which ensures that the data from the USB memory device can only be stored on a specified server. This creates a secure environment that protects confidential information and

allows USB memory devices to be used as a convenient way to safely carry customer data back to one's own company to manage the data.

Leakage of personal or confidential information has grown to become an urgent problem that companies must address. In particular, portable storage medium devices such as USB memory devices are convenient for carrying information from the office to the home, but they can be lost or stolen during transit, or data stored on the devices can be leaked via a file-sharing network when viewed from personal PCs at home. Incidents involving this problem have affected a multitude of companies regardless of industry, and there is an urgent need for a practical way to resolve this problem.

Among the methods some corporations are using to address the problems of the loss or theft of portable storage devices - or the sharing of information stored on such devices - are forbidding employees from taking work-related notebook PCs home, or by insisting on thin clients that pass all traffic through controlled servers. However, any practical solution needs to function in real-world business environments where there will still be a need to physically transport confidential data. For example, when visiting a customer's office that lacks network access, a salesperson might bring a notebook PC, or the salesperson might temporarily store a confidential file from a customer on a USB memory device to carry back to the office.

In order to be able to securely transport and use confidential internal or customer data - not just to prevent data leakage, but also to ensure strict accountability in accordance with corporate compliance policies - two conditions must be met: 1) in the event that the USB memory device is lost or stolen, the data should not only be encrypted, but should automatically be deleted; and 2) confidential data should be prevented from being copied except on predefined USB memory devices or servers.

Fujitsu has developed an environment that enables data to be carried outside of a company safely and in compliance with the company's security policy. This environment consists of the following two technologies:

• **Secure USB memory device prototype**
The new and unique USB memory device prototype contains a processor and battery. After a fixed period of time, if the USB memory device is plugged into an unauthorized PC, the data can automatically be erased or the USB memory device can be rendered unusable. For example, the USB memory device can be set up with a policy whereby the data will be automatically deleted after 24 hours, or it will be deleted if the USB memory is plugged into an unregistered computer even once. By storing and carrying data on a USB memory device that allows for this type of security setting, in the event that the USB memory device is lost, the data stored on it will be automatically deleted and thus enable strict security.

• **File redirect technology**
Together with the self-erasing USB memory device, installing the file redirect software on a PC can be used to restrict the copying of data from the USB memory device, forcing it to reside only on the USB memory itself and a specific company server. This can also be used to prohibit confidential data from being sent as an e-mail attachment or from being printed. Since confidential data is prohibited from being written to the hard disk drive of the PC, it prevents data from being stored on PCs or USB memories and later transferred to file-sharing networks, whether by accident or intentionally.

The combination of the aforementioned two new technologies makes it possible for data to be carried inside or outside a company securely.

For example, if a company sets policies so that a self-erasing USB memory device is set up with an access period of 24 hours and sensitive

company data can only reside on a particular server and the USB memory, the data can be securely carried out of the company, and for example changes to client presentation materials can be made safely even on a customer's PC. In addition, confidential data can be stored on the USB memory device at the customer's location, carried back to the company, and then stored only on the company's server that is used for managing confidential data.

In both of these cases, even if the USB memory device is lost, the data on it would be automatically deleted after 24 hours. Thus, as confidential data would be stored only on the USB memory device and the confidential-data server, there would be no risk of accidentally leaking the data via a PC.

Currently, this technology is undergoing internal trials at Fujitsu in relation to project-management services. Following these internal trials, verification tests will be executed to target commercialization.

Source: Fujitsu