White Paper

Biometrics - How To Render Portable Data Security Convenient

Usage and Benefits of Biometric Authentication – A handy tool to increase security policies' efficiency in protecting endpoints

October 2007

COSOSYS

Table of Contents

Introduction 3

Making Use of Portability Benefits 3

UFD (USB Flash Drive) Security Caveats 3

What Can Really Happen? 4

How to Secure a UFD 4

Biometry - Viable Solution to all Possible Authentication Flaws 5

Why Should a Company Secure UFDs? 5

CoSoSys – Carry it Easy +Plus with Biometric Data Protection 6

Conclusion 6

About CoSoSys 7

References 7

Copyright Notice 8

Introduction

As storage technology breakthroughs become a day to day fact, the world shifts focus to smaller and smaller devices to store data. From laptops and notebooks to pocket PCs and external hard drives, the trend is easy to understand. This is why USB flash drives, also known as UFDs, are so popular these days: they are small enough to be placed in one’s tiniest pockets and carry large amounts of data.

But the features one is mostly looking for in such devices – their portability and convenience that entail enhanced mobility, also make them an easy target to theft and even easier to misplace. This is why UFDs are bringing an enhanced need for comprehensive security policies, from traditional authentication and encryption measures, to more refined features, such as biometric authentication, a method relying on unique physical and behavioral traits of human beings.

Making Use of Portability Benefits

Now at version 2.0, the USB standard is widespread and any PC or notebook allows for it to be plugged and played, with no additional installation needed. This turns UFDs into extremely easy to use devices. Files are transferred at high speed onto and from the flash drives over and over again.

Moreover, they are quite powerful in terms of storage capabilities, and represent the high-end of portability. Compared to other storage devices, such as CDs or DVDs, UFDs are by far less exposed to hard to control factors such as shocks, vibrations or high variations in temperature.

UFD (USB Flash Drive) Security Caveats

While carrying your files everywhere grants mobility options that could boost a company’s business activities, the embedded security threats posed by UFDs cast a shadow on their extensive corporate usage. While small and easy to carry, USB flash drives are also easy to loose, which would then lead to sensitive data leaks. Moreover, misuses of such devices can lead to taking private information home and sharing it by mistake from a PC, leading to the same result.

These facts are also proven by Gartner’s 2006 global study that showed 25 percent of information theft as being linked to network intrusion. The same study found that 60 percent of data breaches can be easily linked to lost or stolen mobile devices.

A 2007 Proofpoint survey reached similar troubling facts, as more than one quarter (26.3%) of the surveyed companies reported that their business was impacted by sensitive or embarrassing information exposures occurring in the last year.

Another similar study, conducted by Check Point Software 2006 among IT professionals from Belgium, Luxembourg, and the Netherlands showed that 76 percent of respondents never use any data security to protect information stored on USB devices. The great majority of respondents also said that they regularly use USB flash drives. If any of these devices were to be lost, the damages would be disturbingly significant.

Theft is another threat incurred by UFDs lacking any type of security. The 2005 Computer Security Institute FBI Computer Crime & Security Survey showed laptop and portable device theft to be the most commonly reported attack of the year, thus managing to surpass other attacks, such as denial of service, viruses or insider thefts. In other words, three quarters of responding companies reported such an incident in 2005.

What Can Really Happen?

Besides casting a doubtful image on a certain organization, losses of confidential data can lead to fines and other more severe consequences. In January 2006, the Federal Trade Commission charged US based commercial data broker ChoicePoint Inc. a settlement fee of 15 million dollars to compensate for the leak of consumer data and the violation of consumer privacy rights.

A well known incident involving private data loss occurred when sensitive payment details belonging to Perth and Kinross Council employees where found practically laying on the street, on a misplaced UFD. The USB key containing 59 documents, most of them belonging to the council's Environmental Services Department, was recovered near a bike shelter close to the council building. More extreme cases involve national security. Such an incident took place in 2006 when flash drives containing classified US military information were sold as used hardware in a marketplace from Bagram, Afghanistan.

How to Secure a UFD

While in the digital environment, a user employs a digital identity to prove they are who they say they are, also providing some form of authentication. Such identities are, however, hard to keep a secret. Authentication, thorough as it may be, is subject to leaks, especially when knowledge or possession is used.

Knowledge-based authenticating is mostly limited to passwords. Users set a password according to corporate security policies and then they are required to remember it. Policies might require complex combinations of letters, numbers and special characters. But such a password will never prevent the user from writing it down on a piece of paper that he/she will later loose. On the other hand, ways to break passwords are improved every day.

Possession implies a token used by the employee. A good example would be an identity badge granting access to enter a certain office or building area. In this case, theft and loss are also huge threats and if security relies on such tokens only, additional measures of verifying if the person using it is authorized to do so might lack.

Biometry - Viable Solution to all Possible Authentication Flaws

- Biometric authentication relies on a unique physical or behavioral trait of an individual which cannot be simulated. Biometrics is preferred to other authentication means because of three important reasons: biometric traits cannot be forgotten or mislaid and they can generally be lost only through severe traumas
- They are extremely difficult to copy, share and distribute
- They always require the physical presence of the person being authenticated at the time and point of authentication

The most common version is the usage of fingerprints to authenticate. Used to identify individuals for over one hundred years, fingerprints are preferred for biometric usage as they are readily accessible and require little physical space both for the needed reading sensor hardware or the stored data. Backed with secondary password protection systems, fingerprint based authentication can provide you and your employees with a safe usage of portable devices.

Why Should a Company Secure UFDs?

Other than the obvious and immediate effect of using biometrics on an UFD, which is protecting the stored data, such a security policy has a subsequent objective. Using fingerprint authentication turns the respective authentication mechanism into a gateway, allowing or denying access to certain sensitive applications such as online banking services, internal databases and so on. The use of the fingerprint validation system is therefore expanded to monitor users when running any of the existing software applications.

While it can appear to be a large investment, securing the UFDs a company's employees use is necessary to ensures compliance to current standards. Regulations currently being legislated in the US and internationally, such as Sarbanes-Oxley, HIPAA and Gramm-Leach Bliley, focus on increasing the accountability of individuals and organizations for their actions regarding access and use of sensitive information. This accountability further implies a strong binding of individuals to their digital identity.

HIPAA (US)

The Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996. A key goal of HIPAA is to protect medical records by establishing transaction standards for the exchange of health information, security standards, and privacy standards for the use and disclosure of individually identifiable health information.

SOX (US)

The Sarbanes-Oxley (SOX) Act of 2002 - developed to protect investors by improving the accuracy and reliability of corporate disclosure. According to Section 404 of the Act, all public companies to assess and report on the effectiveness of internal controls and procedures for financial reporting, including access and dissemination of sensitive financial information.

GLBA (US)

The Gramm-Leach-Bliley Act (also knows as GLBA) aims to protect the personal information of consumers stored in financial institutions. The Act requires all financial institutions to implement and maintain security measures to protect customer information and prevent unauthorized access and use of customer records.

CoSoSys – Carry it Easy +Plus with Biometric Data Protection

CoSoSys' Carry it Easy +Plus Bio software offers fingerprint protection for sensitive portable data while having it transferred to and updated on different PCs or notebooks.

When using Carry it Easy +Plus Bio, data stored on biometric storage devices can only be accessed based on a unique fingerprint. The application also provides a backup password authentication method, thus enhancing the protection it offers. As theft and loss are common in the world of UFD users, Carry it Easy +Plus Bio has a smart system that allows those finding a lost UFD to access the owner's contact details, while denying them access to private data stored on the device.

As an additional security tool, Carry it Easy +Plus Bio comes with a Password Manager providing safe login for Internet Explorer. User Names and Passwords are saved on the portable storage device and are automatically completed when visiting the registered websites. The solution also has privacy needs in mind: it allows users to browse the Internet from different PCs without leaving traces that could lead back to what sites have been viewed.

To increase usability and mobility of traditional storage devices, Carry it Easy +Plus Bio comes with portable Outlook and Outlook Express / Windows Mail and synchronization options for both Outlook and your documents.

Conclusion

UFDs are the highlight of a fast growing portable storage device market which is now making its way into the business sector. Keeping them secure helps all types of companies comply with legal standards and avoid negative consequences, while fully benefiting from the portability and mobility such devices entail.

Carry it Easy +Plus Bio offers an easy and cost saving way to enhanced security policy, as it works on already available hardware. Apart from protecting day to day business from the cruel reality of proprietary data leakage and theft, the CoSoSys software applications addresses mobility needs of the current corporate environment.

Biometric Flash Drives with Carry it Easy +Plus Bio allow for a seamless integration within the corporate IT environment. The safe functioning of Carry it Easy +Plus Bio is fully integrated with the CoSoSys Endpoint Security solutions that safeguard data on notebooks and PCs by controlling the use of portable storage devices on protected computers. This helps generate a comprehensive and adaptable security policy, perfectly fit for companies operating in all activity fields.

About CoSoSys

CoSoSys SRL is specialized in the development of software for portable storage device enhancement and network endpoint security. The application portfolio includes functions from password security, data synchronization and network security. CoSoSys distributes its products globally through world's leading hardware manufacturers, software Distributors, Resellers and directly to users at www.cososys.com. CoSoSys enjoys a continuously growing installation base of users worldwide. The company is headquartered in Cluj-Napoca, Romania and has sales representatives in the United States and Germany.

References

Check Point, The Need for Encryption: Keeping Lost, Stolen Data Protected
http://www.checkpoint.com/securitycafe/readingroom/datasecurity/need_for_encryption.html

Federal Trade Commission (2006) ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress
http://www.ftc.gov/opa/2006/01/choicepoint.htm

Federal Trade Commission, the "Gramm-Leach-Bliley Act" or GLB Act,
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Gordon L.A., Loeb M.P., Lucyshyn W. and Richardson R. (2005) 2005 CSI/FBI Computer Crime and Security Survey, Computer Security Institute.
John Leyden / The Registrar, March 2007, Security flap as Scottish council loses USB key,
http://www.theregister.co.uk/2007/03/21/perth_council_usb_loss/

John Leyden / The Registrar, April 2006, Afghan market sells US military flash drives.
http://www.theregister.co.uk/2006/04/18/afghan_market_security_breach/

Office for Civil Rights - Health Insurance Portability and Accountability Act (HIPAA),
http://www.hhs.gov/ocr/hipaa/

ProofPoint (2007), 2007 ProofPoint Survey Finds that 32% of Large U.S. Companies Employ Personnel to Read Employee Email,
http://www.proofpoint.com/news-and-events/press-releases/pressdetail.php?PressReleaseID=165

Sarbanes-Oxley (SOX) Act of 2002,
http://www.sec.gov/about/laws/soa2002.pdf

Copyright Notice

CoSoSys cannot be held responsible for any special, collateral or accidental damages, related in any way to the use of this document.