GFI WHITE PAPER

Pod Slurping – An easy technique for stealing data

The problem with uncontrolled use of iPods, USB sticks and flash drives on your network

A common misconception is that perimeter security measures such as firewalls and anti-virus software are enough to secure corporate data residing on the corporate network. In this white paper, we explore how the uncontrolled use of portable storage devices such as iPods, USB sticks, flash drives and PDAs, coupled with data theft techniques such as 'pod slurping', can lead to major security breaches.

Introduction

Our dependency on technology has never ceased to grow. Increased portability, ease of use, stylish looks and a good dose of marketing hype are the perfect cocktail to entice the population at large! Suppliers of consumer electronics are registering an ever increasing demand for portable consumer electronics. Apple's iPod for example, is one of the most successful electronic gadgets in the world. Since the iPod launch in 2001, Apple have sold almost 60 million units (CNNMoney.com, 2006). iPod has become a universally appealing source of audio entertainment – the eponym for MP3 players. Projections show that the demand for iPods and other MP3 flash-memory music players will continue on a positive trend and will surge to nearly 124 million units in 2009 (Kevorkian, 2005).

> ■ **IDC Market Analysis**
> "Shipments of iPods and other MP3 flash memory music players will surge nearly 124 million units in 2009."

As the popularity of iPods continues to grow, an alarming army of white earphones is slowly taking over the workplace. In fact, these MP3 players have become as common in any workplace as they are on public transport. But what is so alarming about having iPods and MP3 players at work?

Pod slurping: How can insiders steal your data?

Developments in portable device and data storage technology are escalating. The latest versions of MP3 players and flash memory devices have huge storage capabilities; yet these gadgets are small enough to easily conceal and sneak in behind the corporate line of defence. Further to this, easy connectivity and high speed data transfer has become increasingly more widespread – a user may simply plug the device into a USB or FireWire port and they are up and running – no drivers or configuration required! In practice, this means that a data thief can get away with even more precious data, and a negligent employee can dump more viruses onto the corporate network even when connecting for only a short time.

iPod is just one example of such portable contraptions. At a glance it is an innocent-looking portable audio device. However under the hood it boasts up to 60 GB of portable storage space; practically large enough to store all the data found in a typical workstation. This means that a malicious insider can use an iPod to covertly take out (i.e. 'steal') proprietary data and millions of financial, consumer or otherwise sensitive corporate records at one go!

■ **2006 Identity Fraud Survey**

"In 2005, the costs and damages caused by identity theft reached $56.6 billion."

Gartner analysts Contu and Girard (2004) warned of the security risks associated with the uncontrolled use of portable storage devices within corporations. Today, information theft has become a plague on modern society; data leakage, data ciphering, and data disclosure incidents are all but some of the terms used by security experts to refer to information theft. However, the most original term so far is probably the term 'pod slurping' that was coined by US security expert Abe Usher (2005).

Pod slurping: An easy technique for stealing data

Usher uses the term 'pod slurping' to describe how MP3 players such as iPods and other USB mass storage devices can be easily used to steal sensitive corporate data. "There are dishonest people in the world", says Usher, "many of them work at many companies - and these USB devices make it rather trivial to steal huge amounts of data" (Schick, 2006).

To demonstrate the vulnerability of corporate security, Usher developed a "proof of concept" software application that can automatically search corporate networks and copy (or "slurp") business critical data on to an iPod. This software application runs directly from an iPod and when connected to a computer it can slurp (copy) large volumes of corporate data on to an iPod within minutes. What's more is that slurping is not limited to iPods and MP3 players alone. All portable storage devices can be used to slurp information; digital cameras, PDAs, thumb drives, mobile phones and any other plug-and-play devices which have storage capabilities!

Data slurping is a very simple automated process and does not require any technical expertise; a user may plug in the portable storage device to a corporate workstation and by the time it takes to listen to an MP3, all the sensitive corporate data on that workstation is copied to the portable storage device.

■ **Pod Slurping Blog**

"…in 2 minutes, it's possible to extract about 100 MB of Word, Excel, PDF files -basically anything which might contain business data…"

Insider information theft is a real problem

Information theft has now become a major concern for every organization and thus data leakage prevention is slowly taking up a bigger portion of the IT budget. This drive is attributed to two factors: The wave of malevolent threats that is hitting every industry and the increase in regulatory requirements which demand more protection and tighter controls over client records and other confidential information. More stringent controls and severe penalties are forcing organizations to address regulatory compliance more seriously. In January 2006, the Federal Trade Commission charged commercial data broker ChoicePoint Inc. a settlement fee of 15 million dollars for leaking consumer data and violating consumer privacy rights (Federal Trade Commission, 2006).

A misconception shared by many organizations is that security threats mostly originate from outside the corporation. In fact, countless dollars are being spent every year on firewalls and other solutions that secure the corporate perimeter from external threats. However statistics show that internal security breaches are growing faster than external attacks and at least half of security breaches originate from behind the corporate firewall. Unfortunately, corporate insiders are the first and easiest route to evade perimeter security. The trusted position of corporate employees and their constant exposure to corporate data makes detecting and stopping of data theft an enormous challenge – especially in environments where corporate data is largely distributed!

> **Gartner Group**
> “70% of unauthorized access to information systems is committed by employees.”

Why would insiders want to slurp information?

Corporate data can be profitable in various ways; blueprints, engineering plans, tenders, pricelists, source code, database schemas, sound files, lyrics and much more – all this valuable intellectual property may be exploited by individuals or corporations to gain economical and business advantage over their competitors. The 2006 CSI/FBI survey indicates theft of intellectual property as having the fourth highest economical effect over organizations (Gordon et al., 2006). Malicious perpetrators may also steal sensitive consumer information such as medical and financial records from a company and divulge it to the public. This would damage the company’s reputation as well as make it liable to legal prosecution for violating consumer privacy rights.

In a nutshell, malicious intent, monetary gain and curiosity are probably the major motives behind information theft. Anyone is an enemy for a price and thus perpetrators can be various. Disgruntled employees that believe they are disrespected or exploited by their employers may take advantage of their trusted position and sell corporate plans and other sensitive information to direct competitors. Former employees who feel they have been unfairly dismissed may use their inside knowledge or exploit internal relationships to access, steal and publicly expose consumer information and damage the company. Trusted insiders can also turn into paid informers and engage in industrial espionage, data warfare or other extensive fraudulent activities such as 'identity theft'. The term 'identity theft' refers to crimes in which someone obtains and uses the personal details of another person (e.g. social security or credit card number) to commit criminal acts, usually for financial gain. To date it is the fastest growing crime in the United States. It was estimated that identity theft victims amounted to around nine million adults in the U.S. in 2005 (Johannes, 2006).

2005 Identity Theft Summit

"In Sacramento a perpetrator managed to buy $17,000 worth of goods using the name and social security number of celebrity golf player Tiger Woods!"

How can corporations mitigate the risks of information theft?

The key advantage of iPods and similar portable storage devices is easy access. In theory, this may be of great advantage for corporations. However, it is a well-reported fact that access and security are at opposite ends of the security continuum. The reason is that you never know what users may be doing with their portable devices. An employee might appear to be listening to music on his iPod, but actually he or she might be uploading malicious files or slurping gigabytes of valuable corporate data.

A possible solution to avoid information theft is to implement a corporate-wide portable storage control policy. To mitigate the security risks, some experts and researchers suggest conventional courses of action such as the physical blocking of ports, stringent supervision as well as drastic actions such as the total ban of iPods and similar devices from the workplace. However, this is not the best practical approach. Portable storage devices can be beneficial tools for the corporate workforce and a blanket ban would be counter-productive. In addition good practice dictates that you must never rely on voluntary compliance.

Pod Slurping Blog

"The cost of being proactive is less than the cost of reacting to an incident!"

The ideal way to ensure complete control over portable storage devices is by introducing technological barriers such as GFI EndPointSecurity. GFI EndPointSecurity is a software solution that allows total control over data transfers, to and from portable storage devices on a user by user basis throughout the network.

Conclusion

Companies are constantly at risk of losing sensitive corporate data. In this whitepaper we have explored how the uncontrolled use of portable storage devices within corporations poses major security risks including information theft. This is mostly attributed to the fact that firms tend to focus more on perimeter security and widely ignore the 'enemy within', making it easier for trusted insiders to steal valuable corporate data.

In order to secure corporate data and prevent data slurping, administrators must have a way to technologically control the use of portable storage devices, solutions such as GFI EndPointSecurity give administrators the power to control and report on such device usage throughout their network.

About GFI EndPointSecurity

GFI EndPointSecurity allows you control entry and exit of data via portable storage devices, allowing you to prevent users from taking confidential data or introducing viruses and trojans to your network. GFI EndPointSecurity allows you to actively manage user access to media players (including iPod and Creative Zen), USB sticks, CompactFlash, memory cards, PDAs, Blackberries, mobile phones, CDs, floppies and more. To read more and download a trial version, visit http://www.gfi.com/endpointsecurity/.

About GFI

GFI is a leading software developer that provides a single source for network administrators to address their network security, content security and messaging needs. With award-winning technology, an aggressive pricing strategy and a strong focus on small-to-medium sized businesses, GFI is able to satisfy the need for business continuity and productivity encountered by organizations on a global scale. Founded in 1992, GFI has offices in Malta, London, Raleigh, Hong Kong, Adelaide, Hamburg and Cyprus which support more than 160,000 installations worldwide. GFI is a channel-focused company with over 10,000 partners throughout the world. GFI is also a Microsoft Gold Certified Partner. More information about GFI can be found at http://www.gfi.com.

References

CNNMoney.com (2006) *iPod, Mac Sales Boost Apple Profit Almost 48%* available from: http://money.cnn.com/services/tickerheadlines/for5/200607191714DOWJONESDJONLINE001233_FORTUNE5.htm (last cited 27 July 2006).

Contu R. and Girard J. (2004) *Put Security Policies in Place for Portable Storage Devices*, Gartner.

Federal Trade Commission (2006) *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* available from http://www.ftc.gov/opa/2006/01/choicepoint.htm (last cited 27 July 2006).

Gordon L.A., Loeb M.P., Lucyshyn W. and Richardson R. (2006) *2006 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute.

Hunter R. (2003) *Enterprises and Employees: The Growth of Distrust*, Gartner available from: http://www.csoonline.com/analyst/report3317.html (last cited 27 July 2006).

Johannes R. (2006) *2006 Identity Fraud Survey Report*, Javelin Strategy & Research.

Kevorkian S. (2005) *Worldwide and U.S. Compressed Audio Player 2005-2009 Forecast and Analysis: MP3 All Over the Place*, IDC.

Schick S. (2006) *Be afraid of the file-slurping iPod*, globeandmail.com available from: http://www.theglobeandmail.com/servlet/story/RTGAM.20060209.wpodslurping09/BNStory/ (last cited 27 July 2006).

Scully J. (2005) *Summit on Identity Theft Solutions: Locking Up the Evil Twin* available from: http://www.da.saccounty.net/main/idtheft2005.htm (last cited 27 July 2006).

Usher A. (2005) *Pod slurping*, Sharp Ideas LLC available from: http://www.sharp-ideas.net/pod_slurping.php (last cited 27 July 2006).