Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Personal Media Devices: The Cool Threat Vector

This paper discusses the use of personal media devices as a potential threat vector for corporations. The author contends that personal media devices provide an ideal mechanism for smuggling information out of moderately secured business environments based on two observations: First, technological advances in this market sector have surpassed the effectiveness of security controls that are presently in place in most organizations. Second, these devices appear to have one clearly defined purpose; a music device is expec...

Copyright SANS Institute
Author Retains Full Rights

AD

ForeScout

Personal Media Devices: The Cool Threat Vector

Keith Daly
GSEC 1.4b – Option 1
7 November 2003

Abstract

This paper discusses the use of personal media devices as a potential threat vector towards corporations. In this work, the author contends that personal media devices provide an ideal mechanism for smuggling information out of moderately secured business environments. This assertion is based on two observations: First, technological advances in this market sector have surpassed the effectiveness of security controls that are presently in place in most organizations. Second, these devices appear to have one clearly defined purpose; a music device is expected to play music. Therefore, the most effective means to mitigate the risk that these devices introduce is shown to be the prohibition of these devices in the business environment and the implementation of effective security awareness programs in the corporation.

In the first section of this paper, the author examines common perceptions that people have of personal media devices in business environments. As the causes of these perceptions are examined in the following section, the case for considering these devices as effective threat vectors is established. This is followed by a technological overview of these devices. This information is later used to describe how these devices can be used in successful attacks. Finally, the author makes recommendations of how to mitigate the risks that are associated with these devices.

Perceptions

During the early stages of my research, I wanted to determine people's existing general perceptions, concerning the security implications of portable media devices used in the workplace. Strangely, I could not find reliable statistics on the matter from the standard sources on the internet, so I decided to do a bit of my own research. Feeling that a standard, corporate-style questionnaire, containing questions such as "Do you use personal electronic devices at work?" and "If so, do you use them for illegal activities?" would not give me a true indication of security awareness, I chose to use less scientific but, arguably, more accurate methods. I needed to talk to people in their office environment.

In order to carry out a "field study" efficiently, I told the following story to about 30 random people and afterwards asked them what they think may be wrong or dangerous. The individuals that I told this story to, work for several different

© SANS Institute 2003 As part of the Information Security Reading Room Author retains full rights
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

employers and have a diverse range of positions within those organizations (i.e. technical and non-technical, executive level to entry level, etc.) Security professionals were purposely excluded from this survey. The only other common factor between them is that they all knew that my job "has to do with security stuff" in some capacity. This, of course, made all the participants in my survey attempt to look for security violations that were occurring. However, even with this known bias, the results were interesting.

The Story:

> It's 10:00 p.m. on a Monday night. Except for a few system administrators that keep an eye on the production computer systems from a secure isolated room, two security guards that sit at the front desk of the office building, and a cleaning crew, the entire staff of the company has left for the night.
>
> The offices are cleaned in the evening, during non-business hours, so as not to disturb the staff that carries out the core business activities of the organization during the day. Since the desks are empty at night, nobody is there to get in the way of the cleaning tasks. This also means that there is nobody to interact with while completing these tasks. As a result, some of the cleaners listen to music on portable music devices while they do their work.
>
> The supervisors and a few members of the cleaning crew work for the company on a permanent basis. The remaining cleaning staff works on a temporary basis through a reputable agency. Most non-supervisor members of the team consider this work to be a second job that they decided to take on a temporary basis, in order to supplement their income.
>
> The only entrance to the building, apart from a locked loading dock in the back of the building, is the hallway that passes in front of the security desk. All permanent cleaning crew members are issued entrance badges, complete with picture, which must be used to enter the building via an automatic badge reader system. All temporary staff must sign their names in the presence of a security guard, in an entrance log each day before entering the building and must wear temporary identification tags while on the premises.

The question asked:

> What, if anything, do you notice that is wrong or dangerous in this scenario?

The top 6 responses (listed in descending order of frequency):

1. The cleaning staff may be listening to illegally copied music on their portable music devices.
2. The cleaning staff may be able to get into the desks of the workers if they are not locked.

© SANS Institute 2003 As part of the Information Security Reading Room Author retains full rights
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

3. The security guards should look through the building (i.e. spy on the cleaning staff) instead of sitting at a front desk.
4. The temporary staff will not be as loyal to the company as permanent staff.
5. The agency may not have done proper background checks on the temporary cleaning staff.
6. The cleaning staff will not be as productive or safe while using the portable music devices. This may lead to liability suits for the organization.

As mentioned earlier, the intent when conducting this "research" was to determine the validity of my assumption, that personal media devices were dangerous to organizations; largely due to people's misperceptions of what these devices can do. Since this paper is not intended to be a case study, I will leave comprehensive research on the topic to statisticians.

However, this simple exercise proved my point. The fact that nearly everyone in my survey mentioned the legitimacy of the music content, while not one person mentioned possible alternate uses of the music player, confirmed my assumption that most people do not perceive these entertainment devices as a threat to businesses.

Explanation of Perceptions

Before examining the underlying technologies in detail and formulating effective countermeasures in order to offset the risks that these devices have introduced to the corporate world, I wanted to understand why these perceptions existed. For this activity, I enhanced my pseudo-scientific method, of talking to a random population of office workers, by finding support for their statements in the press. I wanted some assurance that their views were common to the corporate world.

1. Music personal media devices, such as the Apple iPod and Creative Nomad, are perceived to be single use, dedicated devices (i.e. used to play music).

   This perception is also reinforced in the media; mainly through advertising. While the media devices' technical information boasts that the device can be used as an additional hard drive, most people will not read this information; especially those people who do not own the device. According to the advertisements that everyone sees, the device plays music.

   In Salesforce.com's recent Dreamforce user and developer wireless technology conference, Microsoft's Senior Vice President and Chief Technical Officer, David Vaskevitch, "remarked on how useful it is to have devices with specific functionality. According to Vaskevitch, he carries an Apple iPod, Research in Motion's BlackBerry device and a digital camera when traveling, because each device is tailored to a specific job and does that job very well." [Kot03] While there is room for interpretation with this statement, many of the computer industry's leaders believe that this is an indication that Microsoft

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

may move into this area. If so, it does not appear that security will be put high on the list of Microsoft priorities; apart from digital rights management.

2. The Recording Industry Association of America (RIAA) has led a very successful global anti-piracy campaign. This has changed both the perception of these devices and the priorities of the security issues surrounding them.

   According to Lawrence Lessing, Professor of Law at Stanford Law School and founder of the Stanford Center for Internet and Society (CIS), "online copyrights come at the top [of the list of important internet security issues] because of the powerful lobbying of music companies, which are better described as firms faced with a rapidly eroding business model than as victims of crime." [Econ03]

   In the Economist article, Lessing goes on to blame the "stupidity and bribability" of policy makers for this ranking of priorities. Although I do not personally have enough information to either refute or support Lessing's comment, it is apparent to me that people's perceptions and priorities have at least changed due to the lobbying efforts of this group.

3. People generally think of computer security as a technical solution to a technical problem. For example, most people consider their computers to be secure, since the only way that they can get into their computers requires them to enter a user id and password that only they know.

   As explained later in this paper, any effective security solution must address people, processes, and technology. On a technological level, authentication mechanisms that are enforced on the local PC can always be broken, if the attacker has physical access to the PC; albeit with varying degrees of difficulty. From the process side, computers may be left unlocked overnight, thereby bypassing the technical controls. This oversight, which may be caused by a lack of security awareness training (people), makes the theft of locally stored information trivial and may lead to a compromise of the entire network.

4. Media attention and management level marketing brochures focus on securing mobile business assets rather than detecting and preventing intrusions which use them in an attack.

   Nearly everyone that either reads a newspaper, watches television, reads magazines, or reads news on the internet, has heard stories of Personal Digital Assistants (PDAs) being sold on internet auction sites, complete with confidential information. Invariably, the person selling the device thought that he had destroyed all the information that was contained on the device.

   I have never followed up any of these stories personally, so I cannot attest to their accuracy. However, even if the stories appear to be nothing more than urban legend, their publication will spawn discussions of how to improve security on mobile devices, at the management level of many large corporations. While this effectively increases the overall level of security

© SANS Institute 2003 As part of the Information Security Reading Room Author retains full rights
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

awareness in the organization, the focus of the effort is on the user of the PDA. Security discussions shift from protecting the corporation to protecting the executives from making the same stupid mistake as the guy in the story.

5. The cleaning staff is considered to be non-technical and largely temporary. Therefore, training for the cleaning staff, if it exists, will usually consist of the cleaning crew manager instructing the individual of how to efficiently clean the offices and how to use cleaning machines, such as floor polishers.

   While some computer training may exist for the cleaning crew in some organizations, I have never seen this in practice. I have yet to see a member of the cleaning staff be required to read a computer security policy or sign an end user computing agreement. The organizations generally assume that these people will not touch the computers. However this is never formally stated to the employee.

Technology Overview

The previous two sections of this paper provided insight into the perceived risk (or lack thereof) that personal music devices impose on corporations, while only alluding to some of the real risks that these devices produce. The remainder of this paper will describe how these devices can be used as an effective attack vector against a business and will recommend methods to reduce or eliminate the vulnerabilities that devices introduce.

This purpose of this section is to describe the technical aspects of currently available personal media devices and to look at the probable evolution of these devices in the near future. This section will focus on the technical aspects of these devices and their standard use (i.e. primary use). How to use them to exploit a system or network will be covered in the following section.

Manufacturers:

Currently, the market segment for these devices is rapidly expanding and new manufacturers are appearing on a regular basis. As a result, the competition between these manufacturers is fierce.

While the list of manufacturers that produce mp3-compatible personal music devices is quite large, Apple clearly stands out with a unit market share of 31% with its iPod (50% revenue market share) [IPL03]. This high market share is attributed mainly to Apple's early entry in the market and a superior overall design; in terms of both the unit design and software. However, for the purposes of this paper, the manufacturer of the device is not important. What is important is the specification of the device, the potential secondary uses of the device, and the market forces that are driving innovation in this market.

Innovation will be discussed later under the title "Evolutionary Trends". The important thing to keep in mind during this discussion is that Apple has a significant lead on the competitors (the closest competitor has a 10% share in unit sales). Combining this fact with rapidly expanding technological

© SANS Institute 2003 As part of the Information Security Reading Room Author retains full rights
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

capabilities, most manufacturers are attempting to add functionality as a means to gain market share.

Storage Capacity:

Storage capacity, one of the main distinguishing factors between hard drive based personal media devices such as the Apple iPod or Creative Labs Jukebox Zen Xtra and previous flash memory-based products such as USB drives and PDAs, is one of the main reasons that these devices should be considered to be a significant threat to any organization.

Currently, storage capacities on these devices range from 5 GB to 60 GB. Since most people would have difficulties filling a 5 GB hard drive with music, it should be obvious that the huge increase of storage space on these devices will be used for more than coercing the most avid "audiophiles" to use their particular device. This conclusion is also enforced by Toshiba's planned production levels of 1.8 inch drives in 2010 of 70 million units per year in contrast to its production of 1.8 million units this year[1] [Fra03]. Considering that price / performance of storage capacity doubles every nine months (variation of Moore's law) [GBGMPQS03], the hard drives should be much larger in terms of storage capacity and considerably cheaper in 7 years time. I am confident that the manufacturers will be able to put this additional cheap storage capacity to good use.

Also important for the purposes of this paper, the iPod has a built-in disk mode which allows the device to function as an external USB or FireWire hard disk. Most other manufacturers have similar modes of operation.

Interfaces:

The interfaces of the device will be a critical factor when using the device as a threat vector. Earlier versions of the iPod were only equipped with a FireWire port (IEEE 1394). While this provided a fast, 400 Mb/s transfer rate to the device, it meant that it could not interoperate with the majority of Windows machines. More importantly for this paper, it meant that the device could not communicate with most PC deployed in corporate environments.

The USB 2.0 standard has been integrated into the more recent releases of the Apple iPod, as well as nearly all competitors. While USB 2.0 was added to the iPod in order to capture the PC user market and it provided even faster transfer speeds to the device than IEE1394 (480 Mb/s)[2], the main impact for security was that it provided a means to connect this device to most computers that have been manufactured recently. Further, since the USB 2.0 implementation is downward compatible with USB 1.1, corporate consumers replace computers at a conservative estimate of every four years (calculation

[1] Toshiba is the manufacturer of 1.8 inch hard drives for both the Apple iPod and the Dell DJ.
[2] USB 2.0 transmits at a maximum speed to 480 Mb/s. FireWire transmits at a maximum speed of 400 Mb/s. Since the hard drive of the device stores data at a considerably slower speed than 400 Mb/s, this difference is negligible for large files and data streams that are larger than the SDRAM pre-fetch buffer on the device (32 MB on the iPod).

© SANS Institute 2003 As part of the Information Security Reading Room Author retains full rights
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

based on Moore's Law) [GBGMPQS03], and USB ports have been installed on nearly every computer manufactured in the past four years, this means that these devices are compatible with nearly every computer used in corporate environments; albeit possibly at a slower rate of 12 Mb/s on the older machines.

Size:

The size of personal music devices vary. The largest iPod device that is in production is 4.1 inches * 2.4 inches * 0.73 inches and weighs 6.2 oz. Other manufacturers have similar sized units.

For the purposes of this paper, the exact measurements are not important. What is significant is that the device is small enough to avoid attention while used in an attack.

Programmable Firmware:

Nearly all devices on the market boast programmable or upgradeable firmware. The marketing reason that is given for the existence of this feature is so that the device can be upgraded to handle future music formats and additional functionality, such as the incorporation of personal organizer software.

Of course, this feature allows the firmware, and therefore the operating system, to be easily replaced; for both good and evil purposes. In the case of the iPod, this feature has lead to the creation of iPod hacker groups and the porting of Linux to the iPod.

While I have not seen any evidence of this to date, it is conceivable that someone will create a complete exploitation toolkit for these devices that would essentially configure the devices to perform system exploits in an automated manner against a connected machine. This scenario is similar to the "root kits that are currently available for the "script kiddies".

Evolutionary Trends:

Evolution of the personal music devices into personal media devices will be driven by the intense competition that is present in the market segment. For several years, the Apple iPod has been the clear market leader because of its early entry into the market and its outstanding design. As more manufacturers enter the market, they will be forced to differentiate themselves from their competitors. This will obviously lead to an expansion of functionality on the devices. While some analysts think that these battles may be decided based on design, size, battery life, larger storage, price, or the introduction of wireless technologies [TIW03], the real competition is to introduce video capabilities to these devices.

Of course, this also implies that this will also cause increased demand on hard drive storage capability. However this will be more of a side effect of video than a simple increased demand of storage capacity by the consumers.

© SANS Institute 2003 As part of the Information Security Reading Room Author retains full rights
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

To support this statement, Archos already features video playing and recording features in its AV320. Sony and Phillips are expected to follow with their own personal media devices next year. Microsoft is expected to follow thereafter. However Microsoft's Media2Go format has been pushed back to Q3 2004. It is also rumored that Apple will launch its video iPod at its San Francisco exhibition in January 2004 [TIW03].

Threat Description

This section will describe several possible ways that personal music devices can be used successfully as a threat vector and identify the main critical success factors of each variation discussed. Since at least 92% of the worlds' desktop computers currently run some form of Windows (the figure is estimated to be as high as 97% in the corporate world by some analysts), this discussion will assume that Windows 2000 Professional is running on the target machine.

Step 1: Prepare the personal music device

Since you may need to prove that you are using the personal music for its primary purpose (to listen to music) at some point, load the device with several songs. I would suggest keeping at least 10 songs on the system, as it is more impressive if you can scroll through the items when demonstrating your device.

Step 2: Enter the Building

For this discussion, we will assume that the attacker has physical access to the office building and the office containing the target computer. While passing any security checkpoints, make no obvious attempt to conceal your personal music device. If security personnel comment on your "cool toy", commend them on their eye for detail and their good taste.

Step 3: Acquire Access to the Target Computer

If the computer has been left on and abandoned in an unlocked state, merely attach the personal music device by USB and proceed to step 3. Similarly, if this is your computer and you are committing industrial espionage, or if this is not your computer and you have obtained the correct user id and password, simply enter the appropriate credentials, attach the personal music device by USB, and continue to step 3.

If you are performing the attack during office hours, it is also advisable to place the personal music device out sight; either in the desk or under a stack of papers.

Gain access to the computer. To do so, check for temporary storage media drives. If these drives are available, use a password recovery utility, such as LinNT to gain local access to the machine. Alternatively, the machine can be started from the CD with another operating system, such as Knoppix. Once Knoppix is started, the personal music device should be recognized mounted

© SANS Institute 2003 As part of the Information Security Reading Room Author retains full rights
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

automatically as a USB drive; the NTFS drives may have to be mounted separately[3].

In any case, the exact method used to gain access to the computer is beyond the scope of this paper. The important thing to understand is that once the attacker gains physical access to the machine and the machine has bootable temporary storage drives and USB ports attached, the attacker will eventually get through the security boundaries. In this case, the use of multiple deterrence methods, such as encrypted volumes and boot restrictions is the best defense. This will be covered in detail in the following section.

Step 4: Download the information

Once access has been gained to the local machine, the personal music device should appear as an external USB hard drive; even under Linux. Copy the information as you would with any network file share.

When accessing network drives, I would suggest erring on the side of caution. As explained later, one important aspect of attacking via the system via the USB port is that access is the anonymity that this attack provides; the USB port is a trusted connection. Network access may tip off any network administrators that are on duty. It is much safer to use information that has been cached on the local PC.

When done, be sure to set the device back to its normal mode of operation.

Step 5: Leave the Building

This is the opposite of step 2. Again, if you are questioned about the personal media device, offer to play one of the songs that you downloaded in step 1 for the guard. If the security personnel comment on your “cool toy”, commend them on their eye for detail and their good taste.

Summary:

This section was written as a “how-to” to indicate the simplicity of using personal music devices to launch an attack against a business and to interject a little humor in the process. For the record, I do not condone this type of activity and its effects are very serious to the target organization.

The reasons why this attack is so effective are as follows:

- Secondary usage is well concealed. The personal music device appears to be a single, dedicated use item. Traces of secondary usage can easily be hidden while the primary use can still be easily demonstrated.
- Fast transfer rates. Reducing the amount of time to download the information reduces the exposure of the attacker and limits the chance that the attacker will be caught.
- Large storage capacity. The large hard drives that are supplied with personal music devices means that more information can be stolen at one

[3] See [Sch03] for full details on how to use Knoppix to “recover” the system.

© SANS Institute 2003 As part of the Information Security Reading Room Author retains full rights
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

time; reducing the number of times the attacker must expose himself to discovery.

- Anonymous connection. Since the device is connected directly to the target computer, the connection is assumed to be trusted; at least in a Windows environment. Any activities will be traced back to the target machine, but normally not to the personal music device, due to insufficient control of the port and insufficient activity logging.

Recommended Countermeasures

By this point, the reader should agree that portable music devices can be very effective potential threat vectors to any corporation. Strangely, I have never seen security policies that address this issue, from any organization. Obviously, there is an informational gap that must be closed.

As mentioned in previous sections of this paper, any effective security controls are not purely technical; they must address people, processes, and technology. The suggested countermeasures

Security Policy (Process):

The first step to changing any procedure or behavioral pattern of employees based on security concerns is to define a formal system-specific policy that addresses the subject. The policy must be clear and concise, explain the reasoning for the policy statement, and identify sanctions that may be taken if a user violates the policy. At a minimum, the policy should identify the use of personal media devices in the workplace as a serious violation.

Once the security policy has been added to the general security, everyone in the organization must reread and re-sign the policy. This includes personnel with positions that may not have anything to do with computers (e.g. the cleaning staff).

Security Awareness Training (People):

Security awareness training must be provided to everyone in the organization at a level that is appropriate to their position within the company. Items that strictly forbid action, such as a corporate-wide ban on personal media devices must be presented to everyone employed by the company; even temporary staff.

Technical Controls (Technology):

As mentioned earlier in this paper, once an experienced attacker has physical access to a target machine, it is just a matter of time before the system is compromised. The best thing that can be done is to increase the difficulty of breaking the security system, increasing the probability that the attacker will be caught.

© SANS Institute 2003 As part of the Information Security Reading Room Author retains full rights
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Encrypt Local Volumes:

All local volumes should be encrypted. Ideally, this encrypted should be integrated with strong authentication methods.

Disable Alternate Boot Methods:

Disable alternate boot devices, especially drives that hold temporary media. These settings must be password protected.

Remove USB and FireWire ports from all computers:

Since upper management are often the portion of the population that have the most use for attaching devices to the USB ports, any restriction that affects this functionality will not be accepted by the user population. However, this would still be a very effective countermeasure.

Avoid Data Remanence on Local PC

Data remanence refers to information that remaining on a computer system after the data should no longer be available. Examples of this are files that are scheduled for deletion, but have not been completely deleted from the system (i.e. files in the recycle bin or e-mail pending deletion in Outlook or Notes), and files that have been cached on the local system from a file server.

Deletion of cached files will help to reduce the information assets that are stored on the local PC, and will therefore reduce the machine's value to an attacker [MHNsa01].

To bypass the recycle bin:

- Set the Recycle Bin to delete files immediately in the Recycle Bin properties settings

To clear the page file (local cache) at system shutdown:

- For local machine \\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown to 1 (true)
  - If security templates are used for automated To change the security policy templates, located in %SYSTEM ROOT%\security\templates, change the following line:
    [Registry Values] section:
    machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown=4,1
  - Alternately, the Microsoft Management Console (mmc.exe) can be used, with the "Security Policy" snap-in, to edit the template files,

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

the following modification is equivalent to the manual method that is indicated above:
<template> → "Local Policies" → "Security Options" → "Shutdown: Clear virtual memory pagefile": Set to Enabled (default is disabled)

Conclusion

Personal media devices can be used as a highly effective threat vector in nearly all corporations, when the use of these devices is combined with rudimentary social engineering tactics. Unfortunately, due to user requirements and market pressure, there is very little that can be done to mitigate this risk on a technological level alone. Users will probably not be willing to give up their CD ROMs or USB ports, nor will they be willing to undergo physical searches every time they enter their office building.

Therefore, the most effective defense against this threat must incorporate people, processes, and technology; users should not expect a purely technical solution to this problem. The starting point to any effective countermeasure begins with defining a security policy. This policy must clearly enunciate the threat that these devices pose to the organization and detail the countermeasure that is put in place (i.e. the prohibition of these devices in the corporate environment).

Since the security policy will be difficult to enforce in practice, punishment for any violations must be clearly stated and must be severe enough to deter attackers. Finally, as with any corporate security policy, this policy directive must be supported by all levels of management and the information must be communicated effectively to everyone in the organization.

© SANS Institute 2003 As part of the Information Security Reading Room Author retains full rights
© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References:

[Econ03] "Fighting the Worms of Mass Destruction". The Economist. 27 November 2003 (print edition).[4]

[Fra03] Frauenheim, E. "Toshiba Has Bigger Plans For Small Drives". CNET News.com. 11 November 2003. URL: http://news.com.com/2102-1041_3-5105989.html

[GBGMPQS03] Geer, D., Bace, R., Gutmann, P., Metzger, P., Pfleeger, C. P., Quarterman, J.S., Schneider, B. "Cyber InSecurity: The Cost of Monopoly". 24 September 2003. URL: http://www.ccianet.org/papers/cyberinsecurity.pdf (6 December 2003).

[IPL03] "Live Coverage of the Apple Music Event". iPodLounge. 17 October 2003. URL: http://ipodlounge.com/apple_announce.html (6 December 2003).

[Kah02a] Kahney, L. "Have iPod, Will Secretly Bootleg". Wired News. 28 February 2002. URL: http://www.wired.com/news/mac/0,2125,50688,00.html (6 December 2003).

[Kah02b] Kahney, L. "IPod: Music to Hackers' Ears". Wired News. 8 April 2002. URL: http://www.wired.com/news/print/0,1294,51586,00.html (6 December 2003).

[Kot03] Kotadia, M. "Microsoft CTO Touts Blackberry, iPod". CNET News.com. 17 November 2003. URL: http://news.com.com/2100-1041-5108040.html (6 December 2003).

[MHNsa01] McGovern, O.R., Haney, J.M. "Guide to Securing Windows 2000 File and Disk Resources". National Security Agency Report Number: C4-009R-01. 19 April 2001. URL: http://nsa2.www.conxion.com/win2k/guides/w2k-8.pdf (6 December 2003).

[4] This article is also available on the internet at http://www.economist.co.uk/science/displayStory.cfm?story_id=2246018

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

[MS03] Security at Microsoft. November 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/msit/security/mssecbp.asp (6 December 2003)[5].

[Ram02] Ramachandran, J. Designing Security Architecture Solutions. New York, NY: John Wiley & Sons, Inc, 2002.

[Roj03] Rojas, P. "Note to Sony: Skip iPod Knockoff". Wired News. 11 October 2003. URL: http://www.wired.com/news/business/0,1367,60767,00.html (6 December 2003).

[Sch03] Schroder, C. "System Recovery With Knoppix". IBM Developer Works. 23 October 2003. URL: http://www-106.ibm.com/developerworks/linux/library/l-knopx.html?ca=dgr-lnxw06KnoppixRecovery (6 December 2003).

[Shi03] Shimpi, A.L. "Apple's New iPod – Evolutionary, Not Revolutionary". 3 June 2003. URL: http://www.anandtech.com/audio/showdoc.html?i=1827 (6 December 2003).

[TIW03] "The iPod Wars". Guardian Unlimited Online. 1 November 2003. URL: http://www.guardian.co.uk/online/comment/story/0,12449,1075300,00.html (6 December 2003).

[XB02] Xydis Ph.D., T.G., Blake-Wilson, S. "Security Comparison: Bluetooth™ Communications vs. 802.11". Bluetooth Security Experts Group. 1 February 2002. URL: http://www.bluetooth.com/upload/14Bluetooth_Wifi_Security.pdf (6 December 2003).

[5] Complete "Security at Microsoft" document in MS Word format can be found at http://download.microsoft.com/download/0/8/b/08b37d71-6ecd-4f7f-bd2a-d68038953de5/SecurityatMicrosoftWhitePaper.doc

© SANS Institute 2003 As part of the Information Security Reading Room Author retains full rights

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced