Security

Black Hat TPM Hack and BitLocker [1]

Windows Security [2] - Wed, 02/10/2010 - 14:08

Last week at the Black Hat DC conference a presenter showed how one manufacturer's Trusted Platform Module (TPM) could be physically compromised to gain access to the secrets stored inside. Since that presentation, I have had plenty of questions from customers wanting to know how this might affect Windows. The answer? We believe that using a TPM is still an effective means to help protect sensitive information and accordingly take advantage of a TPM (if available) with our BitLocker Drive Encryption feature in Windows 7.

The attack shown requires physical possession of the PC and requires someone with specialized equipment, intimate knowledge of semiconductor design, and advanced skills. While this attack is certainly interesting, these methods are difficult to duplicate, and as such, pose a very low risk in practice. Furthermore, it is possible to configure BitLocker in a way that mitigates this unlikely attack.

With our design for BitLocker in Windows 7, we took into account the theoretical possibility that a TPM might become compromised due to advanced attacks like this one, or because of poor designs and implementations. The engineering team changed the cryptographic structure for BitLocker when configured to use ***enhanced pin*** technology, discussed in the BitLocker Drive Encryption in Windows 7: Frequently Asked Questions [3]. As a result, an attacker must not only be able to retrieve the appropriate secret from the TPM, they must also find the user-configured PIN. If the PIN is sufficiently complex, this poses a hard, if not infeasible, problem to solve in order to obtain the required key to unlock the BitLocker protected disk volume.

BitLocker remains an effective solution to help safeguard personal and private data on mobile computers. For more information on BitLocker best practices, we have published guidance in The Data Encryption Toolkit for Mobile PCs [4]. This toolkit discusses the balance of security and usability and details that the most secure method to use BitLocker in hibernate mode and a TPM+PIN configuration. With the advancements in Windows 7, users that are worries about potential attacks such as this one should also enable the ***Allow enhanced PINs for startup*** group policy setting for their environment.

Categories: Security [5]

Windows BitLocker Claims [6]

Windows Security [2] - Mon, 12/07/2009 - 11:00

Windows 7 is seeing success in the marketplace which I am very happy about from a security perspective.

The Microsoft Security Intelligence Report [7] has shown us again and again that the more up-to-date a PC is, the less likely it is to be infected by malware and other potentially dangerous software. So Windows 7 making strides is helpful to the ecosystem overall from a security standpoint. Success comes at a price though, through greater scrutiny and misinterpretation of some of the technologies. One of those technologies is BitLocker.

I've seen numerous claims the past few weeks about weaknesses in BitLocker and even claims of commercial software that "breaks" BitLocker. One claim is from a product that "allows bypassing BitLocker encryption for seized computers." This claim is for a forensics product and has legitimate uses; however, to say it "breaks" BitLocker is a bit of a misnomer. The tool "recovers encryption keys for hard drives" which relies on the assumption that a physical image of memory is accessible, which is not the case if you follow BitLocker's best practices guidance. The product, like others used legitimately for data recovery and digital forensics analysis, requires "a physical memory image file of the target computer" to extract the encryption keys for a BitLocker disk. Our discussions of Windows BitLocker have always been to communicate that it **is intended to help protect data at rest** (e.g. when the machine is powered off). If a forensics analyst or thief/adversary has physical access to a running system, it may be possible to make a copy of the computer's memory contents by using an administrative account on the system, or potentially through hardware-based methods such as direct memory access (DMA).

Another report discusses targeted attack vectors where the attacker must gain physical access to the computer, multiple times I might add. This research is similar to other published attacks where the owner leaves a computer unattended in a hotel room and anyone with access to the room could tamper with this computer. **This sort of targeted attack poses a relatively low risk to folks who use BitLocker in the real world.** Even with BitLocker's multi-authentication configurations, an attacker could spoof the pre-OS collection of the user's PIN, store this PIN for later retrieval, and then reboot into the authentic collection of the user's PIN. The attacker would then be required to gain physical access to the laptop for a second time in order to retrieve the user's PIN and complete the attack scheme. These sorts of targeted threats are not new and are something we've addressed in the past; in 2006 we discussed similar attacks, where we've been straightforward with customers and partners that BitLocker does not protect against these unlikely, targeted attacks.

Our customers are confronted with a wide spectrum of data security threats that are specific to their environment and we work hard to provide capabilities and information to help the customer achieve the right balance of security, manageability, and ease-of-use for their specific circumstances. BitLocker is an effective solution to help safeguard personal and private data on mobile PCs and provides a number of protection options that meet different end-user needs. Like most full volume encryption products on the market, BitLocker uses a key-in memory when the system is running in order to encrypt/decrypt data on the fly for the drives in use. Also like other encryption products, a determined adversary has significant advantages when they have physical access to a computer.

We recognize users want advice with regards to BitLocker and have published best practice guidance in The Data Encryption Toolkit for Mobile PCs [4]. In the toolkit, we discuss the balance of security and usability and detail that the most secure method to use BitLocker in hibernate mode and a TPM+PIN configuration. Using this method, a machine that is powered off or hibernated will protect users from the ability to extract a physical memory image of the computer.

Windows 7 BitLocker continues to be a foundational component adding to any defense in depth strategy for securing systems, and specifically laptops. Even with the great enhancements made in Windows 7 such as BitLocker To Go, it still remains that BitLocker alone is not a complete security solution. IT professionals as well as users must be diligent when protecting IT resources and the best protection against these sorts of targeted attacks requires more than just technology: it requires end user education and physical security also play important roles.

Categories: Security [5]

Windows 7 Vulnerability Claims [8]

Windows Security [2] - Fri, 11/06/2009 - 19:56

Now that Windows 7 is available, a recent blog by Chester Wisnieski (who works at security vendor Sophos), entitled Windows 7 vulnerable to 8 out of 10 viruses [9], which has stirred some interest.

Here's a quick summary for those who missed Chester's blog. During a test SophosLabs conducted, they subjected Windows 7 to "10 unique [malware] samples that arrived in the SophosLabs feed." They utilized a clean install of Windows 7, using default settings (including the UAC defaults), but did not install any anti-virus software. The end result was 8 of the 10 malware samples successfully ran and the blog proclaims that "Windows 7 disappointed just like earlier versions of Windows." Chester's final conclusion? "You still need to run anti-virus on Windows 7." Well, we agree: users of any computer, on any platform, should run anti-virus software, including those running Windows 7.

Clearly, the findings of this unofficial test are by no means conclusive, and several members of the press have picked apart the findings, so I don't need to do that. I'm a firm believer that if you run unknown code on your machine, bad things can happen. This test shows just that; however, most people don't knowingly have and run known malware on their system. Malware typically makes it onto a system through other avenues like the browser or email program. So while I absolutely agree that anti-virus software is essential to protecting your PC, there are other defenses as well.

Let me recap some of the Windows 7 security basics. Windows 7 is built upon the security platform of Windows Vista, which included a defense-in-depth approach to help protect customers from malware. This includes features like User Account Control (UAC), Kernel Patch Protection, Windows Service Hardening, Address Space Layout Randomization (ASLR), and Data Execution Prevention (DEP) to name just a few. The result, Windows 7 retains and refines the development processes, including going through the Security Development Lifecycle, and technologies that made Windows Vista the most secure Windows operating system ever released.

Beyond the core security of Windows 7, we have also done a lot of work with Windows 7 to make it harder for malware to reach a user's PCs in the first place. One of my favorite new features is the SmartScreen Filter in Internet Explorer 8. The SmartScreen Filter was built upon the phishing protection in Internet Explorer 7 and (among other new benefits) adds protection from malware. The SmartScreen Filter will notify you when you attempt to download software that is unsafe - which the SophosLabs methodology totally bypassed in doing their test.

So while I'm not a fan of companies sensationalizing findings about Windows 7 in order to sell more of their own software, I nevertheless agree with them that you still need to run anti-virus software on Windows 7. This is why we've made our Microsoft Security Essentials [10] offering available for free to customers. But it's also equally important to keep all of your software up to date through automatic updates, such as through the Windows Update service. By configuring your computers to download and install updates automatically you will help ensure that you have the highest level of protection against malware and other vulnerabilities.

Categories: Security [5]

Copyright (C) Technique Microsystems Ltd. All rights reserved.

Source URL (retrieved on 11/22/2026 - 07:28): http://www.techniquemicro.com/aggregator/categories/1

Links:
[1] http://windowsteamblog.com/blogs/windowssecurity/archive/2010/02/10/black-hat-tpm-hack-and-bitlocker.aspx
[2] http://www.techniquemicro.com/aggregator/sources/2
[3] http://technet.microsoft.com/en-us/library/ee449438(WS.10).aspx
[4] http://technet.microsoft.com/en-us/library/cc500474.aspx
[5] http://www.techniquemicro.com/aggregator/categories/1
[6] http://windowsteamblog.com/blogs/windowssecurity/archive/2009/12/07/windows-bitlocker-claims.aspx
[7] http://www.microsoft.com/sir
[8] http://windowsteamblog.com/blogs/windowssecurity/archive/2009/11/06/windows-7-vulnerability-claims.aspx
[9] http://www.sophos.com/blogs/chetw/g/2009/11/03/windows-7-vulnerable-8-10-viruses
[10] http://www.microsoft.com/security_essentials/