Windows® 8 and Windows RT

NEW BEGINNINGS

By: Douglas Otis
Forward-Looking Threat Research Team

Contents

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Introduction

This research paper provides an overview of the changes Microsoft introduced in Windows® 8 and Windows RT. It explores the changes Microsoft made upfront and "under the hood" to improve the security architecture of Windows 8 and Windows RT.

Windows 8 represents a new Microsoft strategy to meet users' desktop, tablet, and smartphone solution needs, as corporations recognize the synergy and productivity obtained through allowing and closely integrating employee use of mobile devices. After all, mobility dramatically changes how services and interactions are best achieved, supplanting the need for the traditional keyboard and mouse. Mobility interaction is further augmented by multi-touch orchestrated through a rich set of gestures, on-screen keyboards, and voice dictation.

Microsoft's new strategy represents significant changes made to the OS's user interface (UI), among others. While the UI enhancements can lead to improved productivity and user satisfaction, the learning curve involved in using it can represent a set of security concerns. This paper looks specifically at some of those concerns.

Windows 8 and Windows RT also represent the latest version in Microsoft's ongoing work to improve the security of its platform. Beginning with Windows XP SP2 in 2004, each version of Windows has seen significant architectural improvements to reduce the attack surface and mitigate the impact of successful attacks. This paper also looks at some of these improvements as well.

Enhanced Security

UEFI

Windows 7's 64-bit version supports Unified Extensible Firmware Interface (UEFI), which Windows 8 extended with Early Launch Anti-Malware (ELAM) to ensure that the first OS drivers loaded are offered by the users' anti-malware solution vendor.[1]

Driver Policies

Windows 8's driver policies are located in the **HKLM\System\CurrentControlSet\Control\EarlyLaunch\DriverLoadPolicy** registry. These policies can be configured through Group Policy on a domain-joined client. Anti-malware solutions may even expose these policies to end users in nonmanaged scenarios.

[1] http://msdn.microsoft.com/en-us/library/windows/desktop/hh848061(v=vs.85).aspx

Windows To Go

To support bring-your-own-device (BYOD) strategies, Microsoft announced the launch of Windows To Go—a fully manageable Windows 8 corporate image on a USB drive.[2] Administrators can, according to Microsoft, safely provision systems using Windows To Go booted from any 64-bit machine anywhere, regardless of connectivity. As a fully manageable corporate PC image, it includes management features like Windows Update policies, corporate anti-malware solutions, and BitLocker.

ASLR

Windows 8 has had a few security improvements, including Address Space Layout Randomization (ASLR), which was introduced in Windows Vista® and enhanced with better randomization to foil known bypass techniques.[3] ASLR involves randomly arranging the positions of key data areas, usually including the base of the executable and position of libraries, heap, and stack, in a process's address space. This hinders some types of security attacks by making it more difficult for an attacker to predict target addresses. Some changes to the Windows kernel and heap with integrity checks and randomization similar to ASLR were made as well. These make it harder for malware to find the hooks they need into the OS.

Safer Browsing

Internet Explorer® (IE) 10 offers the Enhanced Protected Mode sandbox. It works by extending the existing Protected Mode functionality to help prevent attackers from installing software, accessing personal information, accessing information from corporate intranets, and modifying system settings.[4]

[2] http://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/devices/windowstogo.aspx and http://technet.microsoft.com/en-us/windows/jj874386.aspx?ocid=wc-mscom-ent

[3] http://www.digitalbond.com/scadapedia/security-controls/address-space-layout-randomization-aslr/

[4] http://technet.microsoft.com/en-us/library/jj128101.aspx

Picture Password Use

Windows 8 and Windows RT now offer graphical means to enter sign-on passwords, which provides additional security. Because you can use a picture password, signing in to your PC is more personal. This feature lets you choose your picture password and use up to three gestures on it. A picture password is more secure from hackers than a traditional easy-to-remember password. You can draw any three-element sequence of lines, circles, or point gestures on a picture using the touch screen with your finger or a mouse.[5]

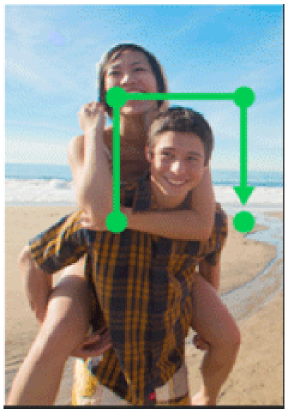

Figure 1: **Sample picture password**

DirectAccess

Microsoft also introduced DirectAccess as an alternative to VPNs for securely connecting PCs to corporate networks.[6] Windows 8 does not require IPv6 for DirectAccess, which operates before a user even signs in. This immediately connects computers to corporate networks, helping organizations maintain compliance on remote or mobile computers and seamlessly apply policies and patches. This feature was introduced in Windows 7 and was slightly improved for Windows 8.

What Could Have Been Done Better?

Thousands of dedicated and specialized applications that offer highly intuitive interaction are now available. Human interface engineering represents the future of software development, as shown by other OSs. It seems Windows 8 and Windows RT may have made too many trade-offs to avoid reengineering bundled applications and many of the unwieldy ribbon-style menus. Applications that are poorly integrated with new hardware interfaces may have held back the OS's evolution.

Key Combinations

A lot of Windows 8 and Windows RT features are accessed using key combinations that act as hidden "shortcut" keys. These combinations are not always accessible using the touch interface and may depend upon problematic gestures for nontouch displays. Note, too, that some windows may appear on the desktop that will remain hidden while using applications running in the "modern UI" mode.

[5] http://windows.microsoft.com/en-us/windows-8/picture-passwords#1TC=t1

[6] http://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/windows-7/features.aspx

BYOD

Making provisions for BYOD strategies via Windows To Go overstate inherent security possible with USB devices. Windows To Go currently requires USB drives with at least 32GB booted by a 64-bit machine. Ideally, users can bring their own laptops to work. To access the corporate network, all they need is a USB stick that has been configured by their organization's IT administrator to run all of the applications, including security software and policies, and access the office files they need. Although offering a simpler solution, bootkits or compromised subsystems are not made safe by booting from a clean USB device, nor is the personal device likely to be Trusted Platform Module (TPM) enabled. Once a preboot environment is infected, this is beyond the OS on a USB device to remedy. See more details in the Security section below.

Security

ELAM requires anti-malware vendors to decide within 50 milliseconds whether a particular driver should be permitted to run or not. Unfortunately, based on an ITSEC analysis of the Windows 8 UEFI platform, Andrea Allievi—a senior security researcher—was able to thwart its UEFI protection with what has been dubbed the "first UEFI bootkit" for Windows 8.[7] His proof-of-concept (PoC) malware defeated Windows 8's Kernel Patch Protection and Driver Signature Enforcement policies.

UI Changes

One of the most tangible changes to Windows 8 was made to the Start screen. It is now accessed via an icon that looks like an angled four-pane window. From the Start screen, you can access IE from the modern UI wherein the location bar and padlock icon quickly hide to give the browser "immersive" access to the entire display. This approach, unfortunately, leaves users less aware of their destination and which application currently controls the display. This creates an endless number of opportunities for deception as a means to sidestep security.

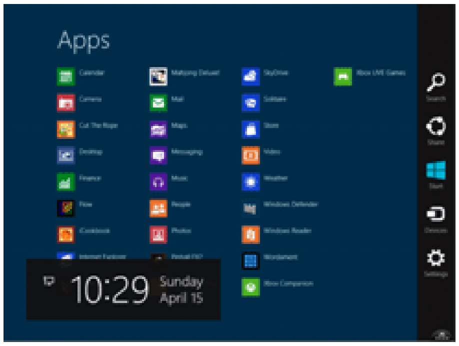

Figure 2: **Display showing the result when** Win + Z **(All Apps) or** Win + Q **(Search Apps) is pressed**

[7] http://www.theregister.co.uk/2012/09/19/win8_rootkit/

Flash Drive Capacity

Windows RT's OS image is 6.7GB with other system support functions taking about 16GB of a device's flash drive. This means that other devices with 16GB flash drive capacity offers roughly the same user storage as that offered by a 32GB Windows RT device.

Multitasking

Multitasking in Windows 8 depends on clicking the Windows icon and application tiles. Doing so also relies on screen corners and swipes through the top or bottom of an application display to access various menus. Hovering over display corners can be fairly problematic when run in a virtual environment using a scaled-down window.

Dynamic Information Updates

Dynamic information conveyed in application tiles is likely updated every 30 minutes. This rate is not practical for most notifications. The use of a split screen would be less essential if there was a comprehensive and effective notification scheme in place. Tiles rather than icons are not as friendly as many hoped.

"Chatty" IE Browser

Windows RT only permits the use of the "chatty" IE browser. As such, IE reports the position of your mouse over the entire display even while minimized. This poses a significant security concern for on-screen inputs and browser-accessible applications. While this reduces risks related to keylogging, reporting the location of the mouse even when the browser window is minimized may also leak vital information. Instead of counting clicks, cybercriminals can now measure mouse locations.

Reverting to Windows 7

Reports of being unable to uninstall Windows 8 due to UEFI restrictions from unhappy users have also surfaced.[8] This was likely due to their unfamiliarity with UEFI BIOS and accessing its settings. The speed at which the BIOS begins loading the OS is impressive but requires a different strategy for accessing BIOS settings. Though Windows 8 offers utilities to handle such an issue, not all users can learn to do so.

Even worse, it seems unlikely that the BIOS settings of a Windows RT device will ever allow any other OS to be installed on it.

[8] http://www.infoworld.com/t/microsoft-windows/unhappy-windows-8-here-are-your-options-210192

What Are Users Likely to Miss?

All Programs Menu

The absence of the All Programs menu requires users to search for installed programs that lack tiles through more tedious means. While they're given the option to place shortcuts on their Desktop, not all users will follow this option, which can lead to frustration in trying to locate installed programs.

Unlike in the All Programs menu though, the arrangement of icons does not adjust according to what's most frequently used. In some cases, the square icons can be rather sizable as well.

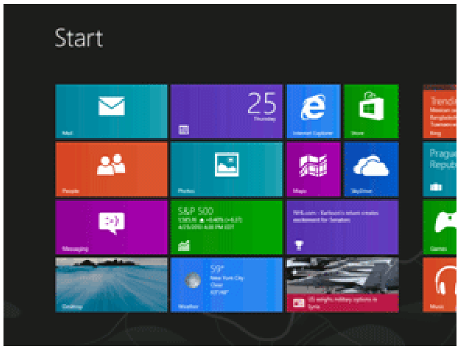

Figure 3: **Tiles of commonly installed apps on a user's desktop**

System Notifications

In previous versions, notifications indicated when updates were pending.

Notifications let users control when OS updates were installed because these had the tendency to disrupt workflow. Windows also often required system reboots, which may leave applications in an unstable state.

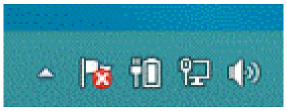

Figure 4: **System notifications on previous Windows versions**

Beyond startup, Windows 8 lacks either a bubble or system tray notification offered in prior versions. It instead recommends automatically installing updates that starts a timer, which determines when reboots are forced. Accordingly, users have less control over when their OS updates are installed should they forgo automatic installation. They would not know what needs to be updated as well since many adopted the practice of not shutting down their OS on a daily basis.

Windows Media Center

Windows Media Center is only available in the Pro version. Even in that version though, DVD Maker has been removed. Users who want to watch DVDs without purchasing the Pro version will need to install third-party codec software. This exposes them to malicious code posing as missing codecs that should have been included with the OS for security reasons alone.[9]

[9] http://blog.trendmicro.com/trendlabs-security-intelligence/zaccesssirefef-arrives-with-new-infection-technique/

Desktop Gadgets and Other Features

Gone are the desktop gadgets, the Windows Classic theme, or enabling one's status at the bottom edge of a window. Technical information once shown on the Blue Screen of Death (BSOD) has been replaced with a **: (**, which is unlikely to offer any clue when looking for a solution via a search engine.

Hardware-Related Issues

For this paper, Windows 8 for 64-bit machines was tested on an Intel® Core™ 2 Duo P7550 processor with the NVIDIA® GeForce® 9400M video adapter. The computer froze to the point of displaying a message that warned against powering off following a system update. After waiting an hour, the computer refused to respond to any input, leaving only the option of shutting down. Fortunately, the computer recovered and noted the event in the log.

Similar problems were encountered when Windows 8 was run on an Intel Core i7 processor within a virtual environment provided by VirtualBox. Unlike Windows 7, Windows 8 is also susceptible to an unlikely flood of IPv6 router advertisements.

When using Windows 8 on a 64-bit machine, IE 10 had a tendency to crash and require another sign-on that did not return to the page that crashed. This is likely due to some video driver issue, which will take time to resolve. Clearly, the touch application programming interfaces (APIs) have set back driver stability compared with Windows 7.

Windows RT also takes a fair amount of time to launch or close applications compared with other OSs. The overarching concern regarding lethargic response is whether this apparent excess retains future vulnerabilities. This is not surprising, judging by the number of crashes and system hangs seen during testing. Sometimes, not properly shutting down may explain a power drain issue.

Issues concerning the Windows on Windows (WoW) software that establishes a separate 32-bit environment have also been raised.[10] Windows 8 64-bit no longer supports the 16-bit environment, a necessary exclusion to better ensure the success of ASLR. As such, organizations that still use legacy 16-bit applications cannot run these on Windows 8. Also, as with Windows 7, WoW retains a bug offering partially compatible libraries that inhibit garbage collection for some 32-bit applications.

The speed at which Windows 8 shuts down is impressive, especially for systems that use flash drives. Perhaps shortcuts taken to gain this speed may have caused some of the malfunctions and system hangs noticed.

[10] http://en.wikipedia.org/wiki/WoW64

Conclusion

Windows 8 and Windows RT come at a time of great change in the industry and challenge for Microsoft. The growth of the iOS and Android OS user bases has created a shift, prompting Microsoft to respond with the radical UI changes in Windows 8 and Windows RT.

While the changes to the UI may have been the right thing to do from a marketing point of view, it also introduced new risks, as people have to learn a new, “right” way to do things.

Not all changes are bad. Things like the new picture password feature definitely represent a step forward. And Microsoft continues the solid, steady progress it is making with architectural improvements in features like ASLR for years now.

Overall, Windows 8 and Windows RT definitely represent a mixed bag of good and bad. Intel’s release of a dual-core Atom™ processor provides similar battery life to that found in Microsoft’s RT Surface™. Now, lower-priced systems with greater storage question the viability of Windows RT since it also lacks support for Active Directory and Cisco or Juniper VPN solutions.

Microsoft has announced an update this summer with Windows 8.1; maybe we’ll see some of the rough edges I’ve outlined smoothened out in that update.

References

- http://blog.trendmicro.com/trendlabs-security-intelligence/zaccesssirefef-arrives-with-new-infection-technique/
- http://msdn.microsoft.com/en-us/library/windows/desktop/hh848061(v=vs.85).aspx
- http://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/devices/windowstogo.aspx
- http://technet.microsoft.com/en-us/windows/jj874386.aspx?ocid=wc-mscom-ent
- http://www.digitalbond.com/scadapedia/security-controls/address-space-layout-randomization-aslr/
- http://technet.microsoft.com/en-us/library/jj128101.aspx
- http://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/windows-7/features.aspx
- http://windows.microsoft.com/en-us/windows-8/picture-passwords#1TC=t1
- http://www.theregister.co.uk/2012/09/19/win8_rootkit/
- http://www.infoworld.com/t/microsoft-windows/unhappy-windows-8-here-are-your-options-210192

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO INCORPORATED

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

www.trendmicro.com

TREND MICRO™

Securing Your Journey
to the Cloud

©2013 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.