

John Edwards

Why Windows Will Always Be High-Risk



John Edwards, Technology Journalist, 8/21/2013

[Bio](#) [Email This](#) [Print](#) [Comment](#) 16 comments

Rate It



50% 50%
[Save It](#)

Year after year, new Windows versions and upgrades arrive, and mobile PC users dutifully use the enhanced operating system (OS) on their systems. Just as reliably, Microsoft representatives assure customers that the latest Windows edition is the most secure version ever.

There's no doubt that Windows has become much safer over the years, but few would say it is even close to being secure. Microsoft's OS is like a house where the owner gradually adds locks to more doors and windows over the years, yet many entryways remain wide open.

Despite Microsoft's repeated promises and best intentions, malware continues to plague enterprise Windows users. Even businesses that are fastidious about installing and maintaining anti-malware tools face the threat of a zero-day attack that will immediately render their Windows-based systems insecure.

Windows' soft underbelly is its registry. A key feature of Microsoft's flagship OS since the days of Windows 95, the registry is essentially a hierarchical database where configuration settings and preferences for applications, various hardware devices, and the OS itself are stored. As a centralized entity, it's a big, fat, juicy target for all types of attackers. The database is a veritable sitting duck packed full of information ready for manipulation and exploitation.

Microsoft has struggled over the years to make the registry more secure, manageable, and self-repairing, yet hackers continue to find ways to bypass and defeat these changes. It doesn't have to be this way. Despite persistent predictions of imminent doom, the Mac OS X operating system remains far more secure than Windows. It works differently. It stores application settings separately in files (called preferences) using the XML format. The benefit is that corruption of one preference file usually will affect only a single application. Corruption within the Windows registry can have wide-reaching effects -- up to and including total system failure.

On a Mac, even if a preference file does become corrupted (by an attack or internal error, for example), the user can easily delete it. Relaunching the program will automatically create a like-new preference file, and things immediately go back to normal. With Windows, altered registry keys have to be fixed or cleaned, and more often than not, this a complex process doesn't turn out right.

Windows, sadly, is hobbled by its own legacy. Microsoft can't get rid of the registry because it's required by a huge stockpile of legacy applications -- virtually every Windows application created to date.

To help loyal users worldwide, Microsoft needs to offer a version of Windows that sheds the registry in favor of a decentralized configuration and preferences model. As soon as the new OS is introduced, Microsoft should encourage its application software partners to create new programs and major updates only for the new OS. The old registry-inflicted version of Windows will eventually (and thankfully) die off.

To allow an organized transition away from the registry, the new Windows should include a compatibility mode for users who opt to run their legacy apps in an unsecured environment. Everybody else will be able to enjoy working in comparative safety, perhaps even without the need for add-on malware protection (as most Mac users already do).

More Blogs from John Edwards

Painlessly Secure Mobile Content

30 comments

As devices proliferate, content security is growing more complex. Here are some simple ways to gain the upper hand on content thieves.

BYOD Users Fear & Loathe IT

25 comments

A growing number of employees fear that IT will steal personal data from their devices.

Ensuring Encryption Really Works

10 comments

Encrypting data stored on notebooks and other mobile devices is a great idea, as long as you do it the right way.

Develop an Ironclad Mobile Payment Strategy

10 comments

Crafting a secure mobile payment strategy is a multistep process that requires careful planning. Here's where to begin.

MORE FROM JOHN EDWARDS



flash poll

What are the primary reasons you would attend a live IT trade event, such as Interop or Mobile World Congress? (Select all that apply.)

- To attend educational sessions
- To learn about new products
- To meet industry experts
- To network with peers
- To network with vendors
- To collect conference swag
- To take certification exams or classes
- I would not attend a live IT event

Submit

All polls

information resources

content provided by Good Technology

- [Mobile App Management: 10 Real-World Requirements](#)
- [Data Loss Prevention: When MDM Isn't Enough](#)

Will Windows always be a high-risk operating system, particularly for mobile users, who tend to be less fastidious about malware protection than their desktop counterparts? Yes, unless Microsoft finally does the right thing and sends its aged and inherently insecure Windows registry into history.

Related posts:

- [Windows Mobile Gains Ground](#)
- [Active Directory Integration Simplifies BYOD](#)
- [Microsoft's 'One Platform' Includes New MDM](#)

[Email This](#) [Print](#) [Comment](#)

comments

[NEWEST FIRST](#) | [OLDEST FIRST](#) | [THREADED VIEW](#)

PAGE 1 / 2 > >>



Horizon777
9/23/2013 12:51:14 PM
User Rank **ONE BAR**

Re: No such thing as 100% secure
Netcrawl, first the OS developer needs to realize that investing in security features will not go wasted as the large class of customers that carries confidential data will switch on to your platform. If those customers find that the homework done by developer means that no security compromise will take place, a lot of high revenue sales can be secured.

Rate It

 50% 50%
[Save It](#)

[Reply](#) [Post Message](#) [Messages List](#) [Start a Board](#)



Anand
9/19/2013 6:35:49 AM
User Rank **ONE BAR**

RE: Why Windows Will Always Be High-Risk
One thing that Windows always goes ahead to guarantee the users is security with the latest versions but the users still face constant attacks. This brings the questions just how safe is Windows? It is important to know that as it revises the latest versions so are the people who come up with the malwares. This therefore ensures that they can always find a way through which they attack the system. But I also admit that the latest versions have been quite efficient and face very minimal attacks. I hope that the next versions will be able to stay ahead so that security is actually said and guaranteed. People are tired of always walking on eggshells just wondering when the next attack is going to come.

Rate It

 50% 50%
[Save It](#)

[Reply](#) [Post Message](#) [Messages List](#) [Start a Board](#)



Mobile
8/29/2013 2:58:33 AM
User Rank **FIVE BARS**

Re: No such thing as 100% secure
@Horizon77 Agreed, there is no way to ever claim 100% secure, I wonder who even fancies the notion ?

Rate It

 50% 50%
[Save It](#)

[Reply](#) [Post Message](#) [Messages List](#) [Start a Board](#)



Mobile
8/29/2013 2:56:15 AM
User Rank **FIVE BARS**

Registry MakeOver ?
....." Microsoft needs to offer a version of Windows that sheds the registry in favor of a decentralized configuration and preferences model."

Rate It

 50% 50%
[Save It](#)

I agree John, but enticing developers to change course will be no easy task, it seems as though if they threw more resources towards security - MS might be able to improve their record, but this is an expense to date - MS does not seem to want to incur.

[Reply](#) [Post Message](#) [Messages List](#) [Start a Board](#)



Mobile
8/29/2013 2:44:25 AM
User Rank **FIVE BARS**

Re: No such thing as 100% secure
John, you have really done an excellent job of exposing the shortcomings of the Windows OS. I am surprised to learn MS would used this structure in their mobile devices. One would think they would use this opportunity to change course. Windows Mobile users, can you say "antivirus" ?

Rate It

 50% 50%
[Save It](#)

[Reply](#) [Post Message](#) [Messages List](#) [Start a Board](#)



Horizon777
8/25/2013 10:24:52 PM
User Rank **ONE BAR**

Re: No such thing as 100% secure
Netcrawl, the best strategy would be to hire some hackers who can understand the way of operating of hackers and what makes their task difficult. I am sure organisations will be doing that currently as security experts may be good in theory but practically only a hacker can be perfect.

Rate It

 50% 50%
[Save It](#)

[Reply](#) [Post Message](#) [Messages List](#) [Start a Board](#)

- Data Loss Prevention: When MDM Isn't Enough

- [CSO Brief: Embracing Mobility From BYOD to Business Enablement](#)
- [Balancing Mobile Productivity and Risk](#)
- [Five Mobile Collaboration Threats Facing All Enterprises Today](#)
- [Mobile Platforms: Driving Productivity and Business Transformation in Lean Manufacturing Firms](#)
- [10 Essential Questions to Ask about Mobile Security and Containerization](#)
- [Gartner Research: Enterprise App Stores Can Increase the ROI of the App Portfolio](#)
- [Enterprise Mobility: A Three-Step Approach to Winning Technology Strategies for CIOs](#)
- [Easily and Securely Mobilize Your Business Apps](#)

All resources

follow us on twitter

Follow us



Mobility Hub @Mobility_Hub 9 Oct

Getting Up to Speed on Mobile App Dev ow.ly/pEmtY

Retweeted by Jessica Mcmillan

[Expand](#)

philip ramsey @spyc1 8h

Safety & Security is out!
paper.li/spyc1/13284769... ▶ Top stories today via @AnesthesiaLLC @TPSChrisBoddy @Mobility_Hub

Mobility Hub @Mobility_Hub 9 Oct

Getting Up to Speed on Mobile App Dev ow.ly/pEmtY

Retweeted by Durwin Keys

[Expand](#)

Mobility Hub @Mobility_Hub 9 Oct

Getting Up to Speed on Mobile App

like us on facebook

The Mobility Hub

Like You like this.

You and 15,966 others like [The Mobility Hub](#).



Toby
8/25/2013 6:55:41 PM
User Rank **FIVE BARS**

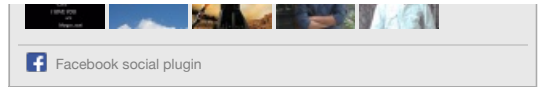
Re: Securing the registry

@MKudla: You make some good points an make them well. I can certinly see how this is not an apples to apples discussion as you point out.

[Reply](#) [Post Message](#) [Messages List](#) [Start a Board](#)

Rate It

50% 50%
[Save It](#)



Netcrawl
8/25/2013 3:42:09 AM
User Rank **FIVE BARS**

Re: No such thing as 100% secure

@Horizon777 I agree with you I believe its impossible to have 100% secure, it won't happen. They are getting much creative and smarter every day, catching them would be an uphill battle. How can you secure your PC? These guys are getting better everyday learn quickly from our mistakes. I think the best things to do right now is to find those vulnerabilities first, we need to outrace them in tracing bugs especially in the Windows platform.

[Reply](#) [Post Message](#) [Messages List](#) [Start a Board](#)

Rate It

50% 50%
[Save It](#)



Horizon777
8/25/2013 3:42:21 AM
User Rank **ONE BAR**

No such thing as 100% secure

Expecting 100% security is not realistic because intruders will always be powerful as well because of the financial incentive involved in gaining access to sensitive data. All Microsoft and other OS developers can do is make improvements. Being secure if is a relative term then comparison is ok however being 100 % secure is not possible.

[Reply](#) [Post Message](#) [Messages List](#) [Start a Board](#)

Rate It

50% 50%
[Save It](#)



M.Kudla
8/24/2013 6:26:34 PM
User Rank **ONE BAR**

Re: Securing the registry

While the registry is often a target I don't think you're realizing all the benefits that come with the structure. It's an intentional decision to use the registry and one that they will continue to make.

It's a boon for enterprise management... there's a reason that they don't use the .nix structure and it's not just because apple does. User and file management are inehrently different for a reason... have you seen enterprise desktop environments built on apple operating systems ever?

This article over-exaggerates the vulnerabilities for windows. "Zero day exploits" are mainly something that affects software platforms these days and not OSs, the phrase came to widespread popularity with the recent java security problems... a multi-architecture platform whose vulnerabilities affected ALL operating systems. Almost every OS these days is so solid that hackers go after software vulnerabilities as hooks into the kernel, not after "windows vulnerabilities." I'm not the biggest Windows fan but I think you're confusing the fact that it's the most prevalent and popular operating system with the most externally developed apps with the idea of an OS like Apple's (an operating system that runs apps almost exclusively designed by the people that designed the OS). I find this kind of half-accurate reporting to be a problem when I talk to people honestly trying to decide on the most practical and usefull secure environment, they're often misinformed.

[Reply](#) [Post Message](#) [Messages List](#) [Start a Board](#)

Rate It

50% 50%
[Save It](#)



UBM TECH

OUR MARKETS: **Business Technology** | **Channel** | **Electronics** | **Game & App Development**

Working With Us: Advertising Contacts | Event Calendar | Tech Marketing Solutions | Corporate Site | Contact Us / Feedback

[Terms of Service](#) | [Privacy Statement](#) | Copyright © 2013 UBM Tech, All rights reserved