

This copy is for your personal, non-commercial use only.

JULY 03, 2014

*Another Shareholder Performance*

## Microsoft's Gestures of Transparency

by BILL BLUNDEN

A Vice President from Microsoft has announced that the company's webmail services are now protected by an advanced encryption suite known as TLS, or Transport Layer Security, and also that Microsoft has launched a "Transparency Center" on its Redmond campus so that governments can inspect the company's *source code* (i.e. the blueprints to its software) [1]. Earlier this year, in January, Microsoft's Chief Privacy Officer publicized a similar Transparency initiative in Brussels [2].

As I've discussed in a prior Counterpunch essay [3] ("Google's Shareholder Theater"), encryption schemes like TLS falter as an alleged panacea to society's cyber-security problems. Hi-tech subversion, the practice of leveraging flaws to covertly gain access, is a trump card as anyone who has investigated the Heartbleed bug understands [4]. So let's examine the reality behind Microsoft's Transparency Centers because they're obviously an attempt to downplay the threat of subversion.

### **[Not So] Accidental Bugs**

History has shown that in a large system like Windows there will be a plethora of subtle bugs that observers will fail to catch. Defects of this nature will even evade professional quality assurance experts despite the fact that they're staring straight at them for hours on end.

Some bugs will be accidental, the result of sloppy software engineering. Thanks to Ed Snowden we know that there will also be other bugs that are not accidents; that were embedded in the source code to provide back doors to spies. This is a convenient ploy because "accidental" bugs offer the additional benefit of plausible deniability. Intentional back doors disguised in this manner can be explained away as absent-minded mistakes.

Microsoft's Windows code base currently spans millions of lines (Windows XP alone contained 45 million lines of code [5]). There is an endless supply of inconspicuous little hidey-holes where spies can be granted camouflaged access. Recall that Stuxnet, a malicious computer worm created by the American and Israeli spies, leveraged not just one but multiple unpatched Windows bugs [6].

Once spies gain a foothold on a machine they install "implants" (also known as rootkits) to maintain access and steal data [7]. U.S. intelligence has a veritable catalogue of such implants that they can draw on [8]. System administrators, the people who manage servers and routers, will likely view this catalogue and experience growing pangs of dread. This is the ugly truth: almost nothing is safe. Our

collective security and liberty have been undermined on an industry-wide basis at the behest of the American Deep State. Hi-tech companies dutifully cooperated. Behind this cooperation is the shadow cast by the neoliberal mindset, such that there are discreet undercurrents of shared class interest.

### **We've Seen This Before**

Building hi-tech trap doors for spies is hardly a recent phenomenon. Well over 15 years ago there was a guy from the NSA named Lew Giles who went around getting companies in Silicon Valley to play ball. Bruce Schneier describes how Giles operated [9]:

“The deal went something like this: Giles offered you preferential treatment for export if you would add a back door. The back door could be subtle enough that it wouldn't show up in the design, and only be obvious if someone analyzed the binary code. It could be something that would easily be viewed as a mistake if someone learned about it. Maybe you could weaken your random number generator, or leak a few key bits in a header. Anything that would let the NSA decrypt the ciphertext without it looking like the crypto was broken.”

“In return you would be able to export your products. But you and he would have to come up with some kind of cover story as to why you could export what was normally unexportable encryption, something that would allay any suspicion.”

Then there's also the strange affair involving a software company named Inslaw which sold a legal case-tracking solution called PROMIS (Prosecutor's Management Information System) to the federal government. Uncle Sam refused to pay Inslaw and pushed the company into bankruptcy. This did little to stop American and Israeli intelligence agencies from selling roughly \$500 million in pirated copies of PROMIS to other intelligence agencies. As you might have guessed the pirated copy of PROMIS had a back door installed that enabled remote monitoring [10]. Greeks bearing gifts and all that.

On a side note, there was an investigative journalist looking into the Inslaw case, Danny Casolaro, who died mysteriously just as he was about to make a big break. The death was ruled a suicide though Casolaro had received a number of death threats and he warned his brother shortly before he died that if anything happened to him it wasn't an accident [11]. Readers familiar with the CIA's links to the drug underworld will note general similarities to the death of another journalist named Gary Webb [12]. He allegedly committed suicide by shooting himself in the head. Twice [13]. Ed Snowden was justified in fearing for his safety before meeting reporters in Hong Kong.

### **Listen To Ken Thompson**

Ultimately Trust Centers are elaborate security theater. Microsoft sells compiled executable programs not source code and there's no telling if some special sauce hasn't been added surreptitiously. Never mind that, as mentioned earlier, an outwardly accidental bug which is completely visible in the code base (but extremely difficult to detect as a flaw in practice) might be intentional.

Consider Ken Thompson's canonical essay on Trusting Trust [14].

*“The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code. In demonstrating the possibility of this kind of attack, I picked on the C compiler. I could have picked on any program-handling program such as an assembler, a loader, or even hardware microcode. As the level of program gets lower, these bugs will be harder and harder to detect. A well installed microcode bug will be almost impossible to detect.”*

Thompson, the founding father of the UNIX operating system who is now in his 70s, is the epitome of a credible source. He has no reason to lie in his essay, no conflicts of interest, no financial incentive to pull the wool over your eyes.

### **Ulterior Motives**

The same cannot be said for the executives at hi-tech behemoths like Microsoft. Ed Snowden's revelations have put them in an awkward position. They were caught red-handed, having silently clambered into bed with the Deep State and the powerful private-sector interests that drive it [15]. It's part of the public record that Microsoft was the original entrant into the NSA's PRISM program back in 2007 [16], that the company gives U.S. intelligence early access to information on zero-day bugs [17], and that the company is almost certainly a participant in the NSA's ongoing subversion ops (e.g. BULLRUN and the SIGNINT Enabling Programs [18]).

When confronted with this duplicity company spokesmen initially denied involvement [19]. With their lies exposed the execs in Redmond are scrambling desperately to manage public outcry, to provide the perception of opposition so that onlookers are led to believe that Microsoft is fighting for user's rights rather than the bottom line.

Companies that take a genuine stance against the Deep State, like Lavabit, are the exception to the rule and they are quickly dispatched. For multinational companies like Microsoft, which recently signed a \$617 million deal with the Pentagon, there's too much money at stake to not collaborate with intelligence services [20]. And Microsoft continues to do so, both here in the United States and in countries like Russia [21].

**Bill Blunden** is an independent investigator whose current areas of inquiry include information security, anti-forensics, and institutional analysis. He is the author of several books, including “The Rootkit Arsenal” and “Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware-Industrial Complex.” Bill is the lead investigator at Below Gotham Labs.

### **End Notes**

[1] Matt Thomlinson, “Advancing our encryption and transparency efforts,” *Technet*, July 1, 2014, [http://blogs.technet.com/b/microsoft\\_on\\_the\\_issues/archive/2014/06/30/advancing-our-encryption-and-transparency-efforts.aspx](http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/06/30/advancing-our-encryption-and-transparency-efforts.aspx)

[2] Brendon Lynch, “Microsoft announces Brussels Transparency Center at Munich Security Conference,” *Technet*, January 31, 2014,

<http://blogs.technet.com/b/trustworthycomputing/archive/2014/01/31/placeholder-brussels-transparency-center.aspx>

[3] Bill Blunden, "Google's Shareholder Theater," *Counterpunch*, June 10, 2014, <http://www.counterpunch.org/2014/06/10/googles-shareholder-theater/>

[4] Alex Hern, "Heartbleed: Hundreds of thousands of servers at risk from catastrophic bug," *Guardian*, April 9, 2014, <http://www.theguardian.com/technology/2014/apr/08/heartbleed-bug-puts-encryption-at-risk-for-hundreds-of-thousands-of-servers/print>

[5] <http://windows.microsoft.com/en-US/windows/history#T1=era6>

[6] Liam O Murchu, "Stuxnet Using Three Additional Zero-Day Vulnerabilities," *Symantec*, September 14, 2010, <http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities>

[7] Bill Blunden, *The Rootkit Arsenal: Escape and Evasion In the Dark Corners of The System*, Jones & Bartlett Learning; 2 edition, March 16, 2012, ISBN-13: 978-1449626365

[8] Jacob Applebaum, "Shopping for Spy Gear: Catalog Advertises NSA Toolbox," *Der Spiegel*, December 29, 2013, <http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html>

[9] Bruce Schneier, "Back Doors, Export, and the NSA," *Crypto-Gram*, February 15, 1999, <https://www.schneier.com/crypto-gram-9902.html>

[10] Thomas, Gordon, *Gideon's Spies: The Secret History of the Mossad*, St. Martin's Press, 1999, ISBN 0-312-25284-6.

[11] Cheri Seymour, *The Last Circle: Danny Casolaro's Investigation into the Octopus and the PROMIS Software Scandal*, Trine Days, 2010, ISBN: 9781936296002

[12] "Gary Webb, 49, Journalist Who Wrote Disputed Articles, Is Dead," *Reuters*, December 13, 2004, <http://www.nytimes.com/2004/12/13/obituaries/13webb.html>

[13] Sam Stanton, "Reporter's suicide confirmed by coroner," *Sacramento Bee*, December 15, 2004, <http://web.archive.org/web/20080507054818/http://dwb.sacbee.com/content/news/story/11772749p-12657577c.html>

[14] Ken Thompson, "Reflections on Trusting Trust," *Communication of the ACM*, Vol. 27, No. 8, August 1984, pp. 761-763, <http://cm.bell-labs.com/who/ken/trust.html>

[15] Beatrice Edwards, "The Powerful Forces Shredding Our Constitution: Preface to 'The Rise of the American Corporate Security State'," *TruthOut*, May 20, 2014, <http://www.truth->

out.org/progressivepicks/item/23805-the-powerful-forces-shredding-our-constitution-preface-to-the-rise-of-the-american-corporate-security-state

[16] Glenn Greenwald and Ewen MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," *Guardian*, June 6, 2013, <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

[17] Michael Riley, "U.S. Agencies Said to Swap Data With Thousands of Firms," *Bloomberg*, June 15, 2013, <http://www.bloomberg.com/news/print/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html>

[18] James Ball, Julian Borger, and Glenn Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security," *Guardian*, September 5, 2013, <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>

[19] Joanna Stern, "Dissecting Big Tech's Denial of Involvement in NSA's PRISM Spying Program," *ABC News*, June 7, 2013, <http://abcnews.go.com/Technology/nsa-prism-dissecting-technology-companies-adamant-denial-involvement/story?id=19350095>

[20] Nick Taborek, "Microsoft's Windows 8 Lifted by \$617 Million Defense Deal," *Bloomberg*, January 5, 2014, <http://www.bloomberg.com/news/print/2013-01-04/microsoft-s-windows-8-lifted-by-617-million-defense-deal.html>

[21] Tim Cushing, "Microsoft Agrees To Hand Over Skype User Data To Russian Police," *TechDirt*, January 16, 2014, <https://www.techdirt.com/articles/20140116/12454325906/microsoft-agrees-to-hand-over-skype-user-data-to-russian-police.shtml>