"Trust THIS!"

By Branden R. Williams – ISSA member, North Texas, USA chapter

Whenever someone throws out the term "Trusted Computing" or "Trusted Systems," some of us think back to our information security training and groan. Not the *Rainbow Series*[1] again!? I thought we killed centralized computing and dumb terminals years ago! Stop talking to me about relics from the past and instead work on implementing the Copy/Paste function on my iPhone!

The world of computing was much different before most of the U.S. population carried devices containing microprocessors. Cell phones, iPods, laptops, and even digital watches contain computers inside them – many of them more powerful than the systems that were designed in the days of Trusted Computing.

What would our world look like if we all used trusted systems? Would the effects of data breaches be reduced? Would we see fewer viruses in the wild? Would botnets exist?

One thing I've learned through my many years as a security professional is that when someone shows you some neat, new software package, it is probably full of security holes. Sometimes new features rely on vulnerabilities in the underlying operating system in order to function. Many software vendors have released emergency patches to their own products which stopped working after security vulnerabilities in the underlying operating system had been closed.

Does anyone remember when PDFs were safe? And why, oh why, did we decide to enable JavaScript inside them? To extend its functionality and enhance its features, of course!

Machines that could be certified as trusted systems don't have to fill small rooms with noisy equipment. In fact, some systems are now shipping with a Trusted Platform Module which can enable many of the features of a trusted system. So while appearances may not differ, the challenges of using a system like this would.

For example, you know the music you love listening to on your computer? Digital Rights Management (DRM) would work in a trusted system so well that corporations and individuals could rely on it being nearly 100% effective. Today we have the ability to work around some of the DRM controls that publishers have added to their content, but in a trusted computing world, these methods would not work. The licensed content that you receive would be encrypted such that only the specific system it is licensed for could actually view it. Decryption or removal would be virtually infeasible.

What about all these data breaches? The ability to exploit software would be greatly reduced. While a hacker may be able to see the potential for a buffer overflow, the internal workings of a trusted system will prevent dreaded buffer-overflows from occurring.[2] Instead of easy exploits allowing hackers to take over thousands of computers with ease, hackers would have to know more about the system – specifically how it is architected, the access model, and in most cases a valid set of access credentials. It does not make exploiting systems impossible; it just makes it much more difficult.

Not only is the risk of a data breach on a trusted system greatly reduced, a breach may not even yield anything useful, depending on how the data is stored. If protected properly, data on a trusted system would not be viewable unless it was on that specific piece of hardware. Even altering the hardware would produce a different cryptographic check, thus preventing someone from replacing parts of the hardware to subvert the system controls.

So if it is so great, why not implement it? Strategy and innovation in business run at light speed. Without flexible computing resources available,[3] the capability of innovation slows. IT infrastructures must adapt to emerging business needs, otherwise it becomes a strain on business instead of an enabler. In order to be able to adapt with any speed, the infrastructure would need to be well thought out. Nearly every company I have visited over the years could not definitively say that all of their laptops were of identical hardware and software specifications. There are always one-offs, making trusted computing an oasis for the general user population.

There is clearly a role for trusted computing in the IT environment regardless of the underlying operating systems you run. Any centralized computing resources that handle regulated data or elevated permissions could be further protected with trusted computing, making the threat of the big breach that much lower.

About the Author

Branden R. Williams, CISSP, CISM is currently the Director of the PCI Consulting Practice at VeriSign and regularly consults with top global retailers, financial institutions, and multinationals. He can be reached at bwilliams@verisign.com or at http://www.brandenwilliams.com.

1 Which was actually only released 25 years ago (1983).

2 I'm referring to the basic "gotcha" of the Von Neumann architecture here, so if you were to take a standard PC and try to apply a trusted system model on it, this may not apply.

3 Such as powerful laptops that drive business through the kludging of Access & Excel.