Herding Cats:
Trusting Trust

September 2010

BrandenWilliams
SECURE BUSINESS GROWTH

The business of information security simply does not work without trust. Trust in systems, trust in data, and trust in third parties are critical to making the entire information security ecosystem function well.

Truly secure systems are not always functionally effective. For example, one old information security adage is the only secure computer is the one that doesn't exist, or is encased in tons of concrete, or whatever you want to throw in there. Essentially, a computer that is totally secure won't be very functional (if functional at all). Introduce the concept of trust, and while we cannot 100% eliminate a security threat, we can certainly get most of the way there and allow the machine to function.

The concept of trust allows the entire computing ecosystem to create centers of excellence around discrete areas of information security. For example, millions of people use one of the most visible signs of trust virtually every time they go online--the SSL-enabled web browsing session. As a user, I trust that when I go to my favorite website and enter in data like my payment card to purchase goods and services, that the website on the other end is actually who I think it is. Of course, we also use the session to encrypt and protect the data in transit, but one of the basic functions of SSL is to authenticate the site name as valid. A trusted third party, a Certificate Authority that is implicitly trusted by users, creates and signs a certificate that is loaded into the web server and matched with a key. If everything checks out, users can trust that the server is who you say it is[1].

The system works well when everyone plays their part well.

What if we didn't have trust? Imagine if you as a user had to somehow validate that the online store you were browsing actually belonged to the store at which you were shopping. Depending on the server's or store's location, I am sure some kind of travel would be required. Instead, you trust that a closed lock or green bar in your browser means you are safe[2].

Diving deeper, we arrive at the concept of trusted computing. While largely developed by the Trusted Computing Group[3], the concept itself could take certain elements that are considered open today, and close them down in a manner that would do more to eliminate viruses and malware than any anti-virus vendor ever could. Imagine you could provide electronic copies of documents, and through a trusted computing infrastructure, demonstrate the non-repudiation required to prove without a shadow of a doubt that a certain person viewed, edited, accepted, and signed said documents--all electronically. Definitely sounds a little Big Brother to me, but depending on how it was implemented, it could be quite functional and efficient.

We can take certain elements of security for granted with trust. Provided we can demonstrate that the systems are operating within their limits and as predicted, we can assume that certain functions are handled for us.

Trust can also be used to protect intellectual property. With fully functional Digital Rights Management (DRM), it is conceivable that electronic information theft could be reduced or completely eliminated. Instead of remote hacking, we might see a resurgence of studies

FOOTNOTES

[1] Before someone emails me about device vs. user vs. process authentication, I understand this is an oversimplification of a complex process that relies on several perfectly executed human interactions to work. Keys can be compromised and browsers can be hacked.

[2] Which depending on the scenario is not always true, but for the vast majority of the time, it is.

[3] http://www.trustedcomputinggroup.org.

on compromising emissions, or TEMPEST. That would certainly change the landscape a bit to reinforce physical security and the use of Faraday cages to protect our information versus firewalls and anti-virus. Granted, I am painting an extremist view of what the world could look like, but the reality is that the amount of investment and environmental change required to execute that vision is not practical for most businesses. It would need to be built into the systems we use today and in the future to be something we leverage as part of our overall IT strategy.

None of this, of course, would be possible without our little friend, trust.

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog, buy his book, or reach him directly at http://www.brandenwilliams.com/.

TEL 214 727 8227
FAX 214 432 6174
BLOG brandenwilliams.com
EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH