Herding Cats:
A Curmudgeon's Party Line

April 2012

BrandenWilliams
SECURE BUSINESS GROWTH

Sometimes it baffles me that the systems that control our most critical infrastructure lag far behind the rest of the information security world. It's easy to understand WHY it happened, but that doesn't make it any easier for a guy like me to be at peace with the situation. Even when ignoring the patch problem, there are many, many other issues with control systems that our industry must solve over the next several years.

How did we get here? Large industrial systems are built to have long lifespans—as in thirty to fifty years. Compare that with your mobile phone, tablet, server, or laptop which barely lasts more than three and you can start to see where the issue is. By themselves, each sector of device's respective useful lifespan is just fine in its own right. The economic models for computer or industrial systems are built around these periods and we plan our investments accordingly. But what happens when you want to control these big industrial systems remotely by giving them an IP address and allowing them to participate in an IPv4 or IPv6 network? Instead of an operator physically "Pushing the green button," it's just a few clicks of the keyboard to get things rolling.

Once this happens, we have two different systems with different expected lifespans and payback periods working together to do something. That "something" could be building cardboard boxes, milling grain, brewing beer, or controlling power generation. There are huge engineering and automation advantages to marrying these two paradigms, but security is not really thought through.

If you have been around infosec for a while, you may have heard the term Supervisory Control And Data Acquisition (SCADA) or a Programmable Logic Controller (PLC) in reference to serious security vulnerabilities that could threaten to take down factories or even stop the supply of clean water to large municipal areas. Some of these are simply fear mongers spreading FUD throughout the land, but others are critical vulnerabilities that need to be addressed.

Typically the first solution is to "air-gap" the SCADA or industrial networks from our normal PCs. That is not a total solution as Stuxnet showed us how malware can jump air-gapped networks by spreading through USB devices. All of these control systems should be air-gapped, but operators cannot ignore the rest of the issues in these systems. Could you pour epoxy into all of the USB ports on these devices? Probably, but what about upgrades and maintenance? We are better served by tackling these vulnerabilities head-on and applying agile software techniques to the parts of the system that are only designed to last a few years instead of fifty.

Smart grid can be another nightmare entirely as these systems may take on various wireless communication techniques such as IEEE 802.14.5 (a common implementation is called ZigBee) or other common wireless data interchange techniques. How are these devices protected? How will utility companies change their business to detect and respond to the new kind of fraud they will see? What if you could alter your meter to save money? Maybe you mess with your neighbor's meter as an act of revenge for leaving his barking dog outside all day or because he lacks basic residential horticulture skills. In the "old days," you needed physical access to the meters and quite a bit of knowledge of the inner hardware workings. Today you just need a laptop and some cheap hardware to start having fun.

Control systems married with IP and smart grid bring some really cool ideas and concepts to the table. We need this technology to continue to improve and new applications to surface such that we can scale our resources as a society to keep up with demand. Imagine

how these technologies can help improve the standard of living around the globe! Don't take this column as an anti-technology rant from an old curmudgeon wishing for the days of a party line and computer-free cars. Instead, take this as a challenge to learn more about these systems and engage the right engineers such that the products that end up in production are reliable and safer to use.

About the Author:

Branden R. Williams, CISSP, CISM, 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 the 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