Herding Cats:
Alice, Bob, and Chuck

February 2011

BrandenWilliams
SECURE BUSINESS GROWTH

To an outsider, information security tends to focus completely on the Confidentiality leg of the C-I-A Tripod[1]. If I'm trying to secure information, I'm trying to keep it secret, right? That's fine and dandy for information that needs to be kept both secret, and largely inaccessible. If I don't need to share the information, I'm probably less worried about its authenticity and integrity. But what if I am using it in a regular business process that demands accuracy?

Imagine for a second that Coca Cola wrote the complete formula for its legendary drink down in one location for safe keeping. They would want to protect it with every resource they have to keep it secret and safe. Now imagine that the formula is now being loaded into a new system on the production line and the formula was changed while it was kept secure. The quality assurance group might be chasing their tails for days or months trying to figure out why Coke doesn't taste like Coke. They might be running around screaming "BAD! BAD MACHINE!" on the production floor, but the machine is just doing what it is told to do. If there was no way to validate the integrity and authenticity of the formula, who is really to blame? A machine, or Captain Mis-information[2]?

What if there is no way to get back to the original, or figure out what changed? How much money would that cost Coca Cola to fix?

Now let's take the concept and apply it to the world of software and trust. Hackers count on users only thinking about confidentiality with respect to information security[3]. They embed malware in websites and software downloads hoping that you don't pay attention to a signature validation failure on an SSL site. They bet on a code-signing authority to sign their malware to make it look like official software. Users are typically not in tune to the authenticity or integrity facets of information security which makes it easier to play on their trusting nature.

Users are not completely ignorant to integrity, however, their knowledge of the concept presents itself in a different way. For example, they do seem to care if a family member takes advantage of a Facebook account of which you forgot to log out[4]. "Hey, I didn't type that status message!" They also will notice if large sums of money are missing from their bank account or if someone forges their signature on a line of credit application. Imagine if banking institutions didn't have integrity checks when restoring from a backup. I'd be hoping for a bank error in MY favor!

Integrity and authenticity play a big role in our society's drive to do more with less and automate certain tasks to create scale. Instead of manually turning on every machine in a factory, we can send an instruction to wake them all up at once and get to work. What if the device is out of regular human contact like a remote research station or a satellite? Imagine if an un-authenticated, malicious instruction was sent to a satellite in orbit commanding it to alter its trajectory? How much damage could that cause? Quite a bit if it runs into something else or loses enough speed to de-orbit into a populated metropolitan area.

FOOTNOTES

[1] Apologies to our esteemed board member and InfoSec legend Donn Parker who introduced the Six Atomic Elements of Information Security which also includes possession, authenticity, and utility. Regardless, my point is just as valid—if not more so—when looking at it from that angle.

[2] I think Captain Mis-information would be a really fun superhero to write about. Swooping into a crisis shouting the wrong thing! Calling Taxis "fancy horseless horse carriage thingies!" Ruining your day's work by flipping a single bit! And, so on.

[3] Well, maybe they count on users not thinking at all, but you get the picture.

[4] Sorry, Dad.

In the world of cryptography, integrity and authenticity are two elements that are used to prevent man-in-the-middle attacks whereby a third party, Chuck, can intercept and alter communication between two individuals, Alice and Bob. If Bob has the ability to check the authenticity and integrity of a message, he will know instantly if it has been tampered with without reading the contents.

As we celebrate twenty years of the RSA Conference (The Adventures of Alice & Bob), hopefully we remember that keeping data a secret is just as important as validating its authenticity and integrity. I hope to see you at the show this year!

Contact information for requests for permission to reproduce or distribute materials available through this course are listed below.

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/.