Beyond the Beyond

Monday, 20 March 2006

Meanwhile, back in Arphidland

Mood: chatty

Now Playing: just back that shipping truck over here by the money laundry

From RFID UPDATE:

The Industry Reacts to RFID Virus Research

Last week's proclamation by a group of computer scientists that RFID tags represent a vehicle for the transmission of computer viruses precipitated a frenzy of headlines from both within and without the RFID industry. Executives at leading RFID companies were bombarded with calls from journalists, and industry association AIM Global was compelled to release a statement addressing the issue. Even the New York Times reported the story. Below are summarized the key takeaways of the whole episode.

First, and most important, the scenarios presented by the researchers were widely considered so contrived as to be unfeasible. A key premise of the researchers' assertions is that the bits and bytes stored on RFID tags would be interpreted by readers as executable instructions. The reality is that tag contents are never interpreted as executable code; they are interpreted only as simple raw data, like numbers. For an RFID system to interpret tag data otherwise would require a poor, insecure design that breaks the most basic and obvious rules of system engineering.

Which raises another point. The potential vulnerability is in the system design; there is nothing inherent to RFID tag technology that makes it vulnerable. As Julie England, Texas Instruments' general manager of RFID, said, "This is the kind of issue the software industry has seen for years." She continued, "Pointing out that poorly written backend software could weaken the RFID application as a whole ... is stating the obvious." As this recommended explanation by Ben Giddings, an engineer at RFID reader manufacturer ThingMagic reads, "RFID tags, just like barcodes, are just data. Nothing more than data. If you intentionally design a system to be vulnerable to certain data, then intentionally expose the system to that data, then yup, you'll have a problem."

Even if the particular scenarios outlined by the researchers are dismissed as academic, they raise the question of whether the eventual ubiquity of RFID tags will represent fertile ground for technological sabotage. (((Yeah. Obviously. Just not the old-fashioned kind of technological sabotage. You sic the NSA on this without any Congressional oversight, you bet they'll come up with something lively. Why would math spooks be stupider than Wal-Mart grocers?)))

While it is too early to draw definitive conclusions around this prospect, certain fundamental characteristics of RFID suggest that it will not be a very attractive target. Its capabilities for the transmission of data are not as advanced as, say, email. Noted Impinj CEO William Colleran, "In email, I can embed things that include scripts and application code. In RFID, everything on the tag is by definition data and not instructions."

Furthermore, email is already widespread to an extent RFID might never be. ((("Might never."))) Even assuming the boldest projections for RFID tag growth, the number of emails sent daily in 2006 is vaster than the number of tags that will be in production five years from now. (((Paging Julian Bleecker: the tags send the email.)))) "I don't see it," said Colleran. ((("I don't dare look."))) Why would hackers focus on RFID "when they have a much more powerful mechanism through the web and email?" (((Because thieves want to steal real stuff instead of virtual stuff, that's why.))) Ron O'Brien, senior analyst with security firm Sophos, pointed to evidence validating that logic: "We're starting to see a little more interest in instant messaging and mobile phones, but RFID doesn't appear to be the next frontier for virus writers to pursue." ((("Doesn't appear"? Absence of evidence as evidence of absence, eh?)))

Another question indirectly raised by last week's developments is how attentive to security the industry has been to date. (((Enough not to run the whole works on Windows, anyhow.))) With price reductions a leading, collective goal of all RFID

stakeholders, one might wonder if the industry has skimped on security features whose inclusion adds to cost. Not so, says those closely involved. The Gen2 standard is a prime example. "The standards bodies, EPCglobal in particular, have actually taken a particularly conservative approach to security," said Colleran. "Going from Gen1 to Gen2, we actually saw a significant increase in security." Sue Hutchinson, EPCglobal director of product management, was clear: "We've been very proactive in addressing security for our membership... Security has been paramount in all of our considerations." She noted that "the experiment they staged in the lab didn't involve EPC technologies at all."

So if the researchers' conclusions are so flimsy, why all the attention? Why, hype, of course. (((That's entirely true -- but it's still much better to fight it out in hype before you start fighting off the Russian mafia.))) The inclusion of two technology buzzwords -- "RFID" and "security" -- in one headline is eye-catching. Despite all that, most acknowledged that the paper served a good purpose. As Hutchinson said, "It's a reminder about how vigilant we need to continue to be in addressing security."

Posted by Wiredblogs at 12:57 PM CST | link to this post

Newer | Latest | Older