Thursday, March 16, 2006

HOWTO make an RFID virus

Computer scientists from Vrije Universiteit Amsterdam developed the first "self-replicating RFID virus." The idea is that the radio frequency identification tag acts as a "vector" to infect the RFID middleware software that companies, for example, may be running as part of a system to track inventory of products. From the Web site outlining their work:

> In our research, we have discovered that if certain vulnerabilities exist in the RFID software, an RFID tag can be (intentionall) infected with a virus and this virus can infect the backend database used by the RFID software. From there it can be easily spread to other RFID tags. No one thought this possible until now. Later in this website we provide all the details on how to do this and how to defend against it in order to warn the designers of RFID systems not to deploy vulnerable systems.
>
> While we have some hesitation in giving the "bad guys" precise information on how to infect RFID tags, it has been our experience that when talking to people in charge of RFID systems, they often dismiss security concerns as academic, unrealistic, and unworthy of spending any money on countering, as these threats are merely "theoretical." By making code for RFID "malware" publicly available, we hope to convince them that the problem is serious and had better be dealt with, and fast. It is a lot better to lock the barn door while the prize race horse is still inside than to deal with the consequences of not doing so afterwards.

Link to RFID Viruses and Worms page, Link to BBC News report *(Thanks, KVH!)*

UPDATE: Ben Giddings of ThingMagic, who is only speaking as an "annoyed engineer" not a ThingMagic representative, says this is all a bunch of hooey:

> The "RFID Virus" is absolutely laughable.
>
> If you read the "paper", here's what they do:

1. Construct an RFID middleware system, intentionally design it to have some really obvious security flaws, ones that even most basic web developers know to avoid, namely the two security no-nos of implicitly trusting external data, and treating data as code.

2. Knowing the exact nature of those two obvious security flaws, including the exact implementation of the flaws, send malicious data that exploits those flaws.

This is so laughably stupid, but somehow it got picked up by the news outlets because it contains buzzwords: "RFID" and "Virus".

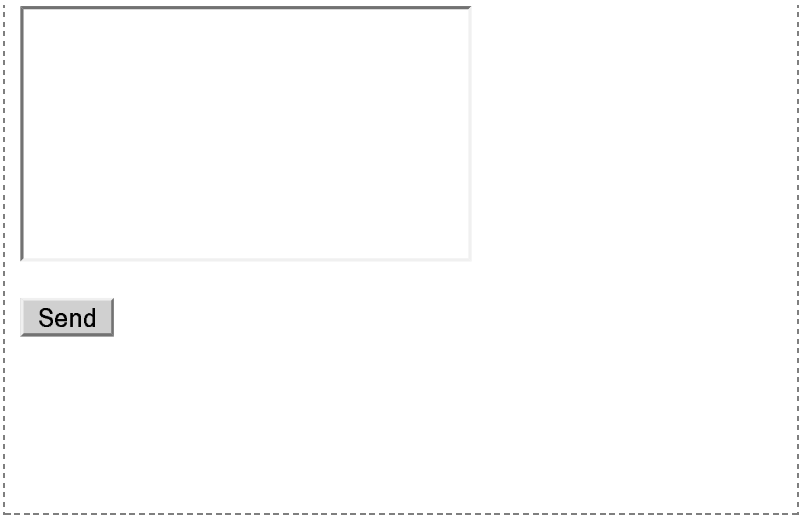
Really, what they're doing is the equivalent of:

1. Designing a barcode system to automatically self-destruct if it ever reads a barcode of 1337 1337, for no reason other than to prove it's dangerous.
2. Broadcasting to the world that the barcode system will self-destruct if it ever reads a barcode of 1337 1337.
3. Intentionally reading a barcode of 1337 1337.
4. Claiming that barcodes are dangerous.

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.

I'm surprised the music industry hasn't tried this with MP3s. Design a MP3 player that will format your hard drive if it sees a certain often-downloaded song, download that song, show the drive getting formatted, then claim that MP3s are dangerous because they might format your hard drive.

posted by David Pescovitz at 10:27:22 AM permalink | Other blogs' comments


Send