Freedom to Tinker

… is your freedom to understand, discuss, repair, and modify the technological devices you own.

« Discrimination, Congestion, and Cooperation

RFID Virus Predicted

Wednesday March 15, 2006 by Ed Felten

Melanie Rieback, Bruno Crispo, and Andy Tanenbaum have a new paper describing how RFID tags might be used to propagate computer viruses. This has garnered press coverage, including a John Markoff story in today’s New York Times.

The underlying technical argument is pretty simple. An RFID tag is a tiny device, often affixed to a product of some sort, that carries a relatively small amount of data. An RFID reader is a larger device, often stationary, that can use radio signals to read and/or modify the contents of RFID tags. In a retail application, a store might affix an RFID tag to each item in stock, and have an RFID reader at each checkout stand. A customer could wheel a shopping cart full of items up to the checkout stand, and the RFID reader would determine which items were in the cart and would charge the customer and adjust the store’s inventory database accordingly.

Simple RFID tags are quite simple and only carry data that can be read or modified by readers. Tags cannot themselves be infected by viruses. But they can act as carriers, as I’ll describe below.

RFID readers, on the other hand, are often quite complicated and interact with networked databases. In our retail example, each RFID reader can connect to the store’s backend databases, in order to update the store’s inventory records. If RFID readers run complicated software, then they will inevitably have bugs.

One common class of bugs involves bad handling of unexpected or diabolical input values. For example, web browsers have had bugs in their URL-handling code, which caused the browsers to either crash or be hijacked when they encountered diabolically constructed URLs. When such a bug existed, an attacker who could present an evil URL to the browser (for example, by getting the user to navigate to it) could seize control of the browser.

Suppose that some subset of the world’s RFID readers had an input-processing bug of this general type, so that whenever one of these readers scanned an RFID tag containing diabolically constructed input, the reader would be hijacked and would execute some command contained in that input. If this were the case, an RFID-carried virus would be possible.

A virus attack might start with a single RFID tag carrying evil data. When a vulnerable reader scanned that tag, the reader's bug would be triggered, causing the reader to execute a command specified by that tag. The command would reconfigure the reader to make it write copies of the evil data onto tags that it saw in the future. This would spread the evil data onto more tags. When any of those tags came in contact with a vulnerable reader, that reader would be infected, turning it into a factory for making more infected tags. The infection would spread from readers to new tags, and from tags to new readers. Before long many tags and readers would be infected.

To demonstrate the plausibility of this scenario, the researchers wrote their own RFID reader, giving it a common type of bug called an SQL injection vulnerability. They then constructed the precise diabolical data needed to exploit that vulnerability, and demonstrated that it would spread automatically as described. In light of this demo, it's clear that RFID viruses can exist, if RFID readers have certain types of bugs.

Do such bugs exist in real RFID readers? We don't know — the researchers don't point to any — but it is at least plausible that such bugs will exist. Our experience with Web and Internet software is not encouraging in this regard. Bugs can be avoided by very careful engineering. But will engineers be so careful? Not always. We don't know how common RFID viruses will be, but it seems likely they will exist in the wild, eventually.

Designers of RFID-based systems will have to engineer their systems much more carefully than we had previously thought necessary.

This entry was posted on Wednesday March 15, 2006 at 7:05 am and is filed under Security, Privacy. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.

5 Responses to "RFID Virus Predicted"

1. Wikilab » Un motivo nuovo per diffidare dell'RFID Says:
   March 15th, 2006 at 8:40 am

   […] [Via Freedom to Tinker] […]

2. Brian Clark Says:
   March 15th, 2006 at 12:21 pm

   An interesting idea. However, I think it presumes a level of flexibility more applicable to general purpose computers than might be built into a retail inventory system. Where are the UPC viruses?

Using read-only RFID tags would prevent wide spread propagation. While there may be advantages to read-write tags, most retail stores would have a vested interesting in preventing write access to the tags. Once propagation is limited so is the majority of the threat.

If you posit the need for read-only tags, the system begins to look more like a sophisticated UPC system that adds serial number to the vendor and part number information currently scanned. Limiting the input variable variables make an attack more difficult. For instance, if the tag data is all numberic then is no need to assign values for alpha characters in the scanner (as is done in some barcodes).

Another problem I see is that there would be a lot less information available on the back end systems. The readers themselves might be a fairly known quantity, but the inventory database and related systems would be harder to determine.

Barcode scanners can be programed by scanning barcodes, so one would assume that the same feature is available in RFID scanners. However, having to physically enable the programming/modifcation mode is likely to a feature as well.

I am not saying an RFID virus won't ever show up, just that I have my doubts about the size of the risk. A virus problem with RFID would need an application using a large number of low value tags (ie. payment cards would be high value and theoretically more strictly designed).

My assumptions are: 1)that RFID will be deployed more as an engineered business system (think retail cash register/checkout scanner) and not as a fancy frontend to a PC in retail environments, and 2) that the retail environment will be largest area of risk due to the number of 'untrusted' users interactions. Should a use arise where a large number of writeable RFID tags available to the public - say, on cars in a parking lot then maybe there's potential.

Where damage and propagation is limited so is fame and fortune. Where fame and fortune is limited so is incentive, and writing a RFID viruses will take incentive at some level.

3. paul Says:
March 15th, 2006 at 3:25 pm

If current retail is any indicator, some large number of RFID systems will be cobbled on top of otherwise ordinary PCs, with (if anything) less-well-maintained OS and application patching than desktops. I agree that classic viral propagation is probably unlikely, but that's far from the only attack one might worry about. If malicious code propagates on the reader/PC side of the system, perhaps with the help of social-engineering attacks to get readers in the right mode, that would be sufficient for many purposes. Furthermore, as long as the attacker controls the reading order, the diabolical bits don't have to be limited to a single RFID tag.

(I'm now wondering about the utility of this kind of thing from the other side of the fence — should, say, passport RFIDs be primed with data strings believed bollix readers of kinds not authorized to read passports?)

4. RFID chip as virus vector at Security Says:
   March 16th, 2006 at 4:57 am

   […] Ed Felten has written up a great, less technical roundup of the points raised in the paper. From it A virus attack might start with a single RFID tag carrying evil data. When a vulnerable reader scanned that tag, the reader's bug would be triggered, causing the reader to execute a command specified by that tag. The command would reconfigure the reader to make it write copies of the evil data onto tags that it saw in the future. This would spread the evil data onto more tags. When any of those tags came in contact with a vulnerable reader, that reader would be infected, turning it into a factory for making more infected tags. The infection would spread from readers to new tags, and from tags to new readers. Before long many tags and readers would be infected. […]

5. Computerworld Blogs Says:
   March 16th, 2006 at 8:13 am

   RFID malware demonstrated (and DIY axis of crypto)…

   Welcome to today's IT Blogwatch, in which RFID tags can infect your back end — sounds nasty [You're fired -Ed.] Not to mention a DIY Enigma cypher machine …
   …

Leave a Reply

Name

Mail (will not be published)

Website

Submit Comment

Powered by WordPress.
Entries (RSS) | Comments (RSS).