RFID viruses

p2p news view / p2pnet: Ubiquitous RFID (Radio Frequency IDentification) technology is here to stay, like it or not. And many civil liberties organizations definitely don't like it, saying the tags, often called spy chips, are wide open to abuse.

Here, Princeton professor Ed Felten discusses something new – RFID viruses.>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

RFID Virus Predicted
By Ed Felten – Freedom to Tinker

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.

(Wednesday 15th March 2006)

[POST A COMMENT TO THIS STORY]

Other stories on p2pnet.net:

3D firm Sketchup Googled
'We've strapped on a rocket'

Pork chops, the MPAA and movies
China Dan's words of wisdom

UK court on ISP liability
Sympathetic ruling

UK broadband - slooooow
Most uses at 2Mbps

Dutchnova.com bites the dust

Poodles Good. Cell phones Bad.

Brein intimidation

Jam cell phones in cinemas
New stop-gab measure?

Top 10 Security Live CD distros
BackTrack - No 1

Oz court decision

DRM delays PlayStation 3 launch
Hollywood vs manufacturers

Bush, Google and online porn
A lot? Or a hell of a lot?

archives 2006 : march | february | january
2005 : december | november | october | september | august | july | june
may | april | march | february | january
2004 : december | november | october | september | august | july | june
may | april | march | february | january
2003 : december | november | october | older

mission | privacy | contact: jon[at]p2pnet.net