# the LOOSE wire blog

technology: usage and abusage. By WSJ columnist Jeremy Wagstaff

ABOUT

SEARCH

Web loosewireblog

Google Search

ADBRITE



« Plaxo Moves Into Macland | Main | How To Build Your Own Airstrip »

March 16, 2006

## How To Infect An Airport

Could it be possible to use Radio Frequency ID tags, or RFID, to transmit viruses? Some researchers reckon so. Unstrung reports that a paper presented at the Pervasive Computing and Communications Conference in Pisa, Italy, the researchers from Vrije Universiteit in Amsterdam, led by Andrew Tanenbaum, show just how susceptible radio-frequency tags may be to malware. “Up until now, everyone working on RFID technology has tacitly assumed that the mere act of scanning an RFID tag cannot modify backend software, and certainly not in a malicious way,” the paper's authors write. “Unfortunately, they are wrong.”

According to The New Scientist the Vrije Universiteit team found that compact malicious code could be written to RFID tags by replacing a tag's normal identification code with a carefully written message. This could in turn exploit bugs in a computer connected to an RFID reader. This made it possible, the magazine says, to spread a self-replicating computer worm capable of infecting other compatible, and rewritable, RFID tags.

An RFID tag is small — roughly the size of a grain of rice, the New Scientist says, and contains a tiny chip and radio transmitter capable of sending a unique identification code over a short distance to a receiver and a connected computer. They are widely used in supermarkets, warehouses, pet tracking and toll collection. But it’s still in the early stages of development. Which leaves it vulnerable. Until now, however, it was thought the small internal memory would make it impossible to infect. Not so, say the researchers.

So what would happen, exactly? RFID virus would then find its

ADS

Subscribe to this blog's feed

Subscribe to my Podcast

way into the backend databases used by the RFID software. The paper, Unstrung says, outlines three scenarios: a prankster who replaces an RFID tag on a jar of peanut butter with an infected tag to infect a supermarket chain's database; a subdermal (i.e., under-the-skin) RFID tag on a pet used to upload a virus into a veterinarian or ASPCA computer system; and, most alarmingly, a radio-frequency bag tag used to infect an airport baggage-handling system. A virus in an airport database could re-infect other bags as they are scanned, which in turn could spread the virus to hub airports as the traveler changes planes.

So how likely is this? Not very, Unstrung quotes Dan Mullen, executive director of AIM Global, a trade association for the barcode and RFID industries, as saying. “If you're looking at an airport baggage system, for instance, you have to know what sort of tag's being used, the structure of the data being collected, and what the scanners are set up to gather,” he explains. Red Herring quotes Kevin Ashton, vice president of marketing for ThingMagic, a Cambridge, Massachusetts-based designer of reading devices for RFID systems, as saying the paper was highly theoretical and the theoretical RFID viruses could be damaging only to an “incredibly badly designed system.” Hey, that sounds a bit like a PC.

But he does make a good point: because RFID systems are custom designed, a hacker would have to know a lot about the system to be able to infect it. But that doesn’t mean it can’t be done, and it doesn’t mean it won’t get easier to infect. As RFID becomes more widespread, off-the-shelf solutions are going to become more common. And besides, what will stop a disgruntled worker from infecting a system he is using? Or an attacker obtaining some tags and stealing a reader, say, and then reverse engineering the RFID target?

My instinct would be to take these guys seriously. As with Bluetooth security issues such as Bluesnarfing, the tendency is for the industry itself not to take security seriously until someone smarter than them comes along and shows them why they should do.

Email this • Add to del.icio.us • Subscribe to this feed

March 16, 2006 in Security, Viruses | Permalink

TRACKBACK

TrackBack URL for this entry: