Default scheme

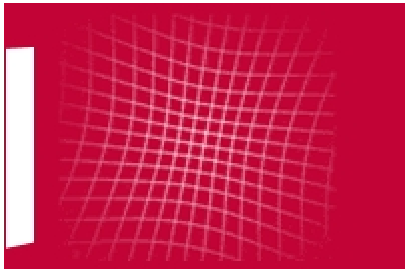
OUT-LAW.COM

UK Home > OUT-LAW News > This month's news > March 2006 > RFID chips can carry a virus, warn experts

RFID chips can carry a virus, warn experts

OUT-LAW News, 16/03/2006

Radio Frequency Identification (RFID) tags could be vulnerable to computer viruses, experts from Amsterdam's Free University warned yesterday. It had previously been thought that the limited memory available in the tiny chips made them safe from attack.



Not so, according to Melanie Rieback, Bruno Crispo and Andrew Tanenbaum, who authored the report. They reveal that they have found a way of placing a computer virus onto an RIFD tag – and demonstrated the discovery yesterday at the annual IEEE Conference on Pervasive Computing and Communications in Pisa.

RFID (Radio Frequency Identification) is a generic term for technologies that use radio waves to automatically identify objects.

An RFID chip comprises a microchip and a tiny antenna that transmits data from the chip to a reader. The reader is activated whenever the antenna comes into range and the data can be used to trigger an event – such as raising an alarm or signalling that a pallet of goods has arrived in a warehouse. Usually the range is no more than a few feet.

The chips can be incorporated into a range of products and have an advantage over barcodes in not requiring a line of sight between the chip and the reader. They offer a means of navigating complex global supply chains, allowing companies to track their products from factory to distribution centre, from warehouse to sales floor.

But the ability of the tags to report their location, identity and history raises concerns about personal privacy and security, as well as problems with technical interoperability and international compatibility. This latest warning adds a further concern.

According to the report, entitled Is Your Cat Infected with a Computer Virus? just one infected RFID tag is capable of disrupting an entire system with disastrous consequences.

The researchers have found that the tags can be made to perform buffer overflows – where too much data is put into the tag causing it to overwrite what was there originally – and can be subject to a malicious code insertion.

It gives the example of RFID tags attached to cases in an international airport, warning that if one infected RFID tag is scanned by a reader, the entire baggage handling system could be thrown into disarray as the database upstream of the reader becomes infected.

The researchers advise that simple countermeasures should prevent such attacks. According to Rieback, developers must check their RFID systems, and implement safety procedures and secure programme technology now, before the systems are put to large-scale use.

"This is intended as a wake-up call," Andrew Tanenbaum, told the BBC. "We ask the RFID industry to design systems that are secure".

Red Herring quotes Kevin Ashton, vice president of marketing for ThingMagic, a designer of reading devices for RFID systems, who scoffed the level of threat. The RFID viruses could be damaging only to an “incredibly badly designed system,” he said.

See:

- The research paper (10-pages / 194KB PDF)
- Red Herring's coverage

See also:

- European Commission consults on RFID, OUT-LAW News, 10/03/2006
- Growth of RFID must respect privacy, says EIU, OUT-LAW News, 09/03/2006
- Ofcom deregulates RFID in the UK, OUT-LAW News, 10/08/2005
- US watchdog approves RFID chip for human use, OUT-LAW News, 14/10/2004
- Ontario Privacy Commissioner publishes RFID guidelines, OUT-LAW News, 30/06/2004
- Wal-Mart accused of unethical RFID trial, OUT-LAW News, 13/05/2004