InfoSecDaily™ /Security blogs
Updated @ 17:00 UTC, Monday, 20 March, 2006.

Rfid Transponders
Evaluation and Development Kits Get Specs & Prices. Ship Same Day!

Supply Chain Management
The time is now to get your products implemented into the GDSN.

AntiVirus & Spyware Virus
Free AntiVirus trial & AntiSpyware remover. Download rated 5 Stars.

RFID Solutions
For all indoor/outdoor applications See our Custom Smart Mark line!

Ads by Goooooogle

Advertise on this site

March 19, 2006

RFID VIRUSES - AND OTHER UNINTENDED CONSEQUENCES

Kim Cameron's Identity Weblog [2006/03/15]

The world's first virally infected RFID tag.

A friend sent me recently to a web site that I think has many lessons to teach.

These lessons are layered like the skin of an onion, starting with a threat analysis of RFID. The authors (Melanie R. Rieback, Bruno Crispo and Andrew S. Tanenbaum) do a great job not only of thinking through and prototyping threats, but of explaining themselves in a paper called "Is Your Cat Infected Wiith An RFID Virus?" Reading it you'll see this is not a rhetorical question.

Recieve email updates

b News é Blogs é Alerts
Subscribe

Search this site

Go ›

March 2006 »

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

The site has many other treats as well. For example:

> To make clear what kinds of problems might arise from RFID hacking by amateurs or criminals, let us consider three possible and all-too-realistic scenarios.
>
> - A prankster goes to a supermarket that scans the purchases in its customers' shopping carts using the RFID chips affixed to the products instead of their bar codes. Many supermarkets have plans in this direction because RFID scans are faster (and in some cases can be done by the customers, eliminating the expense of having cashiers). The prankster selects, scans, and pays for a nice jar of chunk-style peanut butter that has an RFID tag attached to it. Upon getting it home, he removes or destroys the RFID tag. Then he takes a blank RFID tag he has purchased and writes a exploit on it using his home computer and commercially available equipment for writing RFID tags. He then attaches the infected tag to the jar of peanut butter, brings it back to the supermarket, heads directly for the checkout counter, and pays for it again. Unfortunately, this time when the jar is scanned, the virus on its tag infects the supermarket's product database, potentially wreaking all kinds of havoc such as changing prices.
> - Emboldened by his success at the supermarket, the prankster decides to unwittingly enlist his cat in the fun. The cat has a subdermal pet ID tag, which the attacker rewrites with a virus using commercially available equipment. He then goes to a veterinarian (or the ASPCA), claims it is stray cat and asks for a cat scan. Bingo! The database is infected. Since the vet (or ASPCA) uses this database when creating tags for newly-tagged animals, these new tags can also be infected. When they are later scanned for whatever reason, that database is infected, and so on. Unlike a biological virus, which jumps from animal to animal, an RFID virus spread this way jumps from animal to database to animal. The same transmission mechanism that applies to pets also applies to RFID-tagged livestock.
> - Now we get to the scary part. Some airports are planning to expedite baggage handling by attaching RFID-augmented labels to the suitcases as they are checked in.

Ads by Gooooooogle

Printronix Printers
Printronix Authorized Distributor Online Quotes and Ordering Site
www.printersandsupplies

SRS International Group
Corporate and domestic asset protection and tracking
www.srsinternationalgrou

Exact Indoor Positioning
Indoor tracking using ultrasound 100% accurate and safer than RFID
www.sonitor.com

Gen 2 & ISO RFID
RFID Systems & Implementation. RFID Tags, Readers & Printers.
www.intermec.com

Advertise on this site

> This makes the labels easier to read at greater distances than the current bar-coded baggage labels. Now consider a malicious traveler who attaches a tiny RFID tag, pre-initialized with a virus, to a random person's suitcase before he checks it in. When the baggage-handling system's RFID reader scans the suitcase at a Y-junction in the conveyor-belt system to determine where to route it, the tag responds with the RFID virus, which could infect the airport's baggage database. Then, all RFID tags produced as new passengers check in later in the day may also be infected. If any of these infected bags transit a hub, they will be rescanned there, thus infecting a different airport. Within a day, hundreds of airport databases all over the world could be infected. Merely infecting other tags is the most benign case. An RFID virus could also carry a payload that did other damage to the database, for example, helping drug smugglers or terrorists hide their baggage from airline and government officials, or intentionally sending baggage destined for Alaska to Argentina to create chaos (e.g., as revenge for a recently fired airline employee).

he links below give more technical detail about possible attacks nd how to prevent them. The authors suggest that you read them ı order.

- RFID Middleware
- Classes of RFID Malware
- The Architecture of RFID Systems
- Vulnerabilities that Can Be Exploited
- How to Write an RFID Virus
- How to Write an RFID Worm
- How to Defend against RFID Malware

MORE HARDY PIONEERS TRY OUT IN

LONG TAILED MOUSE JUMPS ON BOA »