Autopope! - Excuse me, I'm having an Accelerando moment ...

Mar. 15th, 2006

05:38 pm - Excuse me, I'm having an Accelerando moment ...

In between hacking on the latest Merchant Princes novel ("Three coaches full of mediaeval weekend warriors drove in convoy through the Massachusetts countryside ...") I decided to take a moment off to check slashdot. And what did I see?

Is your cat infected with a computer virus?

> RFID systems as a whole are often treated with suspicion, but the input data received from individual RFID tags is implicitly trusted. RFID attacks are currently conceived as properly formatted but fake RFID data; however no one expects an RFID tag to send a SQL injection attack or a buffer overflow. This paper is meant to serve as a warning that data from RFID tags can be used to exploit back-end software systems. RFID middleware writers must therefore build appropriate checks (bounds checking, special character filtering, etc) to prevent RFID middleware from suffering all of the well-known vulnerabilities experienced by the Internet. Furthermore, as a proof of concept, this paper presents the first self-replicating RFID virus. This virus uses RFID tags as a vector to compromise backend RFID middleware systems via a SQL injection attack.

Oh, and one of the co-authors is Andrew S. Tanenbaum. Yes, that Andrew Tanenbaum. (So I'd say it's serious even before I read past the abstract.)

It's one of those moments when someone whacks you on the side of the head and tells you something that should have been blindingly obvious, but wasn't -- and which simultaneously tickles your sense-of-wonder gland. (Not to mention being the most kick-ass attention

grabber of a title for a comp. sci. paper I've seen in ages.) Yes, this is going to happen. And the implications are mind-numbingly larger than they look at first sight.

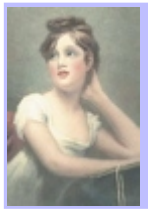
I can see I'm going to have to re-think large chunks of the background to "Halting State" ...

Current Mood:  contemplative

Current Music: Wonderland - Xymox

(16 comments | Leave a comment)

Comments:



From: kaygo

Date: March 15th, 2006 - 05:57 pm

(Link)

Is there a journal reference, or is this a draft?

(Reply to this) (Thread)

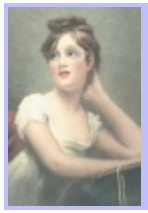
From: autopope

Date: March 15th, 2006 - 06:01 pm

(Link)

I suspect it's a draft (there are no references in sight), but it looks fairly interesting all the same ...

(Reply to this) (Parent) (Thread)



From: kaygo

Date: March 15th, 2006 - 06:08 pm

(Link)

Oh, it's interesting.

Go to any warehouse and access corporate systems via the tags in the stock, if I'm reading it right.

(Reply to this) (Parent)

From: autopope

Date: March 15th, 2006 - 05:59 pm

(Link)

More here: RFID viruses and worms.

Tech query: on a 12-year timescale, are we likely to see current RFID standards augmented by a somewhat smarter, more data-rich device with, say, up to 16Kb of storage and netowrking via ZigBee? Power from micromechanical actuators or photovoltaic cells, price around the $0.5-5.0 mark in bulk (rather than the $0.05 target of RFID tags), that sort of thing. (I'm now cursing myself for having chucked out the complementary intro copy of "RFID World" that flopped through the letter box a couple of months ago ...)

(Reply to this) (Thread)

From: nojay

Date: March 15th, 2006 - 06:34 pm

RFID

(Link)

There's a tendency for pundits to throw the kitchen sink into any speculation of future trends in a given technology -- you ought to see what features car designers were thinking about thirty years ago that would be part of the Car of Tomorrow that most of us are driving around in today.

RFID tags are not going to be rewriteable in-situ for the same reason the barcode on a box of cornflakes isn't rewritable. They are a primary key identifier for whatever they're fitted to, like your cat. There might be rewriteable devices similar to RFIDs used for other things but they're not going to be used for stock control. The fraud possibilities alone are mindboggling (a pallet-load of twenty high-end server boxes getting reprogrammed to present itself to the dispatch dock as soap powder, frex).

What this journal article says is that RFIDs are a data source for stock control systems (well duh!) and a maliciously-programmed RFID could cause buffer overflows in stock control software for nefarious purposes; given the very small payload in an RFID this

would probably be meant to open a portal for another attack via a higher-bandwidth connection. Good software design will prevent this from ever happening in the real world.

You could say barcodes are a threat too since they are scanned automatically the same way RFID tags are. It's just that RFID tags hold much more data and don't have to be visible to be "read", the big bonus which is making them so tempting for producers and retailers. Panic over, you can take the tinfoil off the cat now.

(Reply to this) (Parent) (Thread)

From: autopope

Date: March 15th, 2006 - 06:44 pm

Re: RFID **(Link)**

I believe some (fairly sophisticated) criminal gangs have on occasion taken WalMart and their ilk to the cleaners, with the aid of some sticky labels and a bar code printer. But the bar code system is supposed to be a universal identifier. The RFID system is begging to be used more flexibly, and sooner or later some folks who value convenience over security are going to be bitten by it. Probably only really feasible for an inside job, but it's thought-provoking.

What I'm thinking about is the next generation. (Assets labelled with anti-theft chips that talk via ZigBee, track their position relative to one another, broadcast their state -- e.g. if they need a new battery charge or are nearing their sell-by date -- and start screaming if they're tampered with or removed, for example.)

(Reply to this) (Parent)

From: bellinghman

Date: March 15th, 2006 - 06:54 pm

Re: RFID **(Link)**

The 'no rewrite because of fraud' wouldn't be a very good solution. If you can get close enough to a tag to rewrite it to emulate some soap powder, you're close enough to blow it and stick the tag you just swiped from the soap powder on it instead.

(Currently, barcodes do get rewritten. Or rather, overwritten: someone sticks a barcode for something cheap over the real barcode for an expensive item. This is a large part of the reason why the display at the till should be showing a description as

well as a price - the till monkey should be there as a sanity check.

Whether they actualy pay much attention is another matter. When 99.9% of items that successfully scan are correct, the 0.1% will tend to slip through.)

A large chunk of today's reasoning about RFID is that it makes a good end-to-end stock tracing system. This is why there are RFID tags that are rewritable in situ - you want to add information over time.

Hundreds of thousands of Londoners are carrying rewritable RFID tags already ... beause that's what Oyster cards are. So you don't need a cat.

(Reply to this) (Parent) (Thread)

From: nojay

Date: March 15th, 2006 - 07:34 pm

Re: RFID **(Link)**

But the rewriteable tags aren't totally rewriteable -- there will be a R/W area and a ROM area and never the twain shall meet. The write-once ROM has a unique identifier, with checksums and crypto etc. The updatable area isn't used to ID stuff.

Right now RFID tags with rewritable capabilities need near-contact with the rewriter since it's the only way to get enough juice into it to flip the bits -- that's why you can't just walk past the driver with your Oyster card in your pocket and have it clocked. Real RFID can do stock control from a feet or more away, through packaging. This might change in the future, but the article referenced is more about the stock control middleware getting corrupted by evil tags rather than an criminal enterprise going after the tags themselves for the purposes of theft.

It's quite difficult to disable a tag and they can be made to be effectively incorruptible without physical contact unless you lug a small microwave oven around the supermarket with you. I can also think of other solutions to the tag replacement scam; crypto every tag and record them in the shop's back office system. If a product is presented at the till with an invalid tag or a tag that was already marked as sold (crook buys soap powder, goes out, rips RFID tag off the box, goes back into store, picks up box of expensive wine, blows the wine's RFID tag, presents it at the till with soap powder tag attached) then the alarms go off.

(Reply to this) (Parent) (Thread)

From: hattifattener
Date: March 16th, 2006 - 04:43 am
Re: RFID (Link)

For the virus idea to work, it doesn't matter if the tag isn't completely rewritable; it only matters that there's enough rewritable space on the tag to fit an exploit and a replicating payload into. Maybe that space is supposed to be holding a log of the package's exposure to heat or vibration, or something like that.

As palfrey points out, this isn't fundamentally new in any way. It's an Apple-][disk virus in a new medium, and it's only news because RFIDs are getting a lot of attention lately. But it's quite probable that the people writing the tag reader software aren't thinking of tag data as possibly hostile, and might not be paranoid enough about it.

(Reply to this) (Parent) (Thread)

[User Picture]

From: rpresser
Date: March 16th, 2006 - 08:47 pm
Re: RFID (Link)

The original article wasn't concerned with rewritable tags at all. The original idea was:
1. Take malicious tag past reader attached to insecure system.
2. Malicous tag infects total RFID solution system, which was already being used to create more tags frequently as part of its design function. (The nightmare example was baggage tagging in airports.)
3. Infected RFID solution sytem now writes new tags with virus in them, too.
4. Wherever the new tags go, they can infect more (insecure) systems in the same way.

It reminds me of dog heartworms. A non-infectable carrier (airline passenger / mosquito) is required to transport the infectious agent (RFID tag / heartworm larva) from one infectable host (baggage system / dog) to another.

(Reply to this) (Parent)

From: redbird
Date: March 15th, 2006 - 07:47 pm

Re: RFID **(Link)**

The article notes that if an attacker wants to infect someone's database, they aren't necessarily limited to the tiny space in RFIDs--they could use devices with larger payloads. The solutions suggested in the article will help. Without them, an attacker could just drop one of those things in a backpack, and stroll past the RFID reader to install a backdoor.

(Reply to this) (Parent)

From: seawasp

Date: March 16th, 2006 - 04:02 pm

RFID? **(Link)**

If you're ONLY talking about RFID, maybe not. But that's a narrow field. If you mean microtagging in general, on a 12 year timescale you could get into manufacturing devices about 3x3 millimeters which would include sensors, power harvesting, some computational ability, and an RF transciever, which could be placed just about anywhere to monitor just about anything. If you look at the "Faerie Dust" technology in "Boundary", that's about where I expect the technology to go in 20 - 30 years.

(Reply to this) (Parent)

From: meico

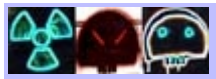
Date: March 15th, 2006 - 06:45 pm

(Link)

I think it's important to note that this sort of attack applies to the venerable bar-code as well... (albeit it would be a bit more difficult).

Imagine a DNA scanner (a la Gattacca) being hacked by someone introducing a drop of blood with DNA specially designed to exploit bugs in the sequence analysis system... Ack!

(Reply to this)



From: hirez

Date: March 15th, 2006 - 08:52 pm

(Link)

Coo-er.

I was in the audience for Ms. Rieback's talk on fun with RFID at WhatTheHack last year. At the time it seemed to be more concerned with random pranks, rather than anything 'useful' like that. I'm happy to be wrong there.

Meanwhile, there's this: https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN)

I must admit I rather care for the idea of the RFID-Guardian.

(Reply to this)

From: palfrey

Date: March 15th, 2006 - 11:15 pm

(Link)

Had a glance over it, and it looks like it could be shortened to "treat RFID tags as you would any other user input data (i.e. assume it's malicious and check for nasty things) and everything's fine". Achieving self-replication using SQL (which *may* work if the system designers are dumb) in minimal space is kinda cool, but only as hack value.

(Reply to this) (Thread)

From: antonia_tiger

Date: March 16th, 2006 - 11:36 pm

(Link)

Never underestimate the criminal stupidity of either users or management.

(Reply to this) (Parent)