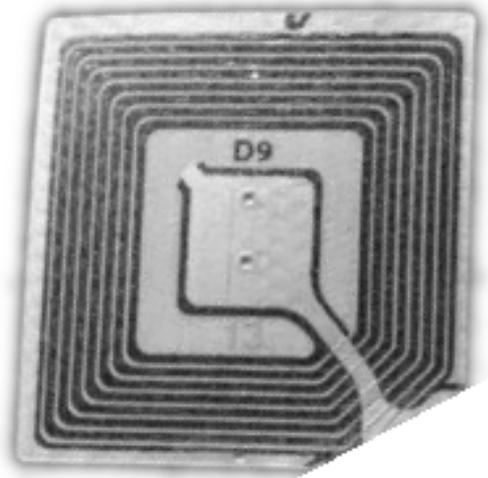
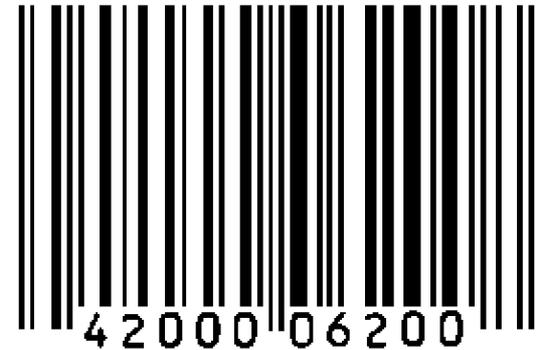


Soylent Badges: An Attack Surface Analysis of RFID

Dan Kaminsky



=



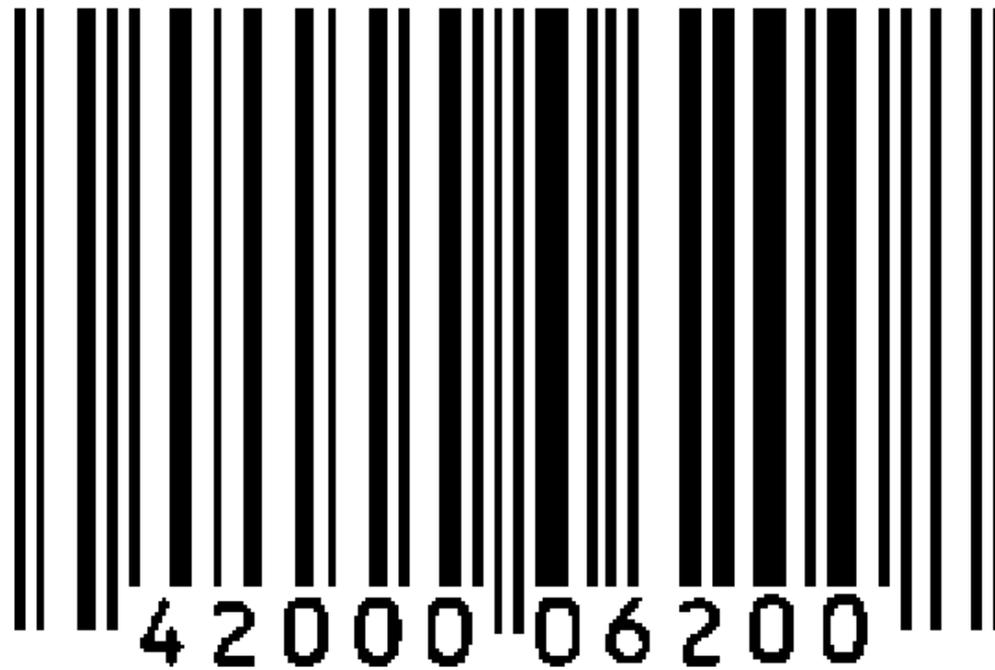
Introductions

- Well known speaker at network security conferences
 - Black Hat Briefings in Las Vegas
- Co-author of several books
 - Hack Proofing Your Network
 - Aggressive Network Self-Defense
- Spent most of my career working directly for Fortune 500's
 - Cisco
 - Avaya
 - Microsoft
 - MySpace
- Provide research and training to DoD
- So how'd I end up looking at this?

Network Security Depends On Physical Security

- I noticed every site I was working at used these badges to control access to the servers
- It doesn't matter how much you lock down a network – if someone can just walk in through the front door (literally), you lose
- So thus the question: What would it take to break the RFID-based badges that controlled physical access to the networks I was charged with protecting?

What is RFID?



RFID: It's Made of Barcode.

| <u>Barcode</u> | <u>Passive RFID</u> |
|--|---|
| Attaches data to things | Attaches data to things |
| Not self-powered – requires someone to shine a light on it | Not self-powered – requires someone to emit radio waves at it |
| Returns data by absorbing or not absorbing light | Returns data by absorbing or not absorbing radio waves |

- Radio is just low frequency light
- Variant: “Active RFID”, has a battery in it
 - “Glow in the dark barcode”
 - Can “encrypt”

That's not necessarily a bad thing: Barcodes Were Revolutionary

- One of the most significant technologies for commercial processes in the last hundred years
 - Production lines
 - Transport and shipment
 - Retail
- **Barcodes improved commercial efficiency by several orders of magnitude**
 - Can we do better?



RFID: Building A Better Barcode

Advantages Of RFID

Can read more data

Can read through dirt, shelves,
and pockets

Can read many at once

Can read quickly

Can read reliably – small false
negative, no false positive

Cannot copy with office
electronics



Introduction to Attack Surface Analysis

- OK, so RFID is a (much!) better barcode.
 - “What could possibly go wrong?”
- Attack Surface Analysis steps:
 - 1) Identify what the system is doing, and *why*
 - If you don’t know what the system is *supposed* to do, you’ll never understand what it’s *allowing* you to do.
 - 2) Interpret what the system provides, not from the perspective of a legitimate user, but that of an attacker
 - A door with no possible attacker might as well not be locked
 - A road that nobody might not pay for has no need for RFID to track drivers
 - **“Secure unless there’s a bad guy”** is useless

Through The Looking Glass

| <u>Trusted User</u> | <u>Attacker</u> |
|---|---|
| Can read more data | Can read more data |
| Can read through dirt, shelves, and pockets | Can read through dirt, shelves, and pockets |
| Can read many at once | Can read many at once |
| Can read quickly | Can read quickly |
| Can read reliably – small false negative, no false positive | Can read reliably – small false negative, no false positive |
| Cannot copy with office electronics | Can copy with radio shack electronics |

Immediate Conclusion

- **RFID's enhanced accessibility is as nice for attackers as it is for legitimate users**
 - But what would an attacker acquire?
 - If you don't know *why* people would deploy this technology, you don't know *what* it would mean for an attacker to steal from the system
- Three major classes of RFID deployments
 - Inventory: "What is here?"
 - Attendance: "Who is here?"
 - Access Control: "Who isn't here?"

Inventory Control

- Inventory Control: Use of RFID to do continuous or intermittent identification of physical objects at a location
 - Shrinkage Management: Attacker can make a store screw up its purchasing schedule, not recognize theft as its happening.
 - Cargo Ship Manifest Auditing: Attacker can add or remove items from the scanner manifest, facilitating smuggling.
 - Competitive Analysis (Commercial and Military): Attacker can monitor inventory levels of competitor, determining when to strike.
- **While there are scenarios in which inventory tracking issues become interesting, they're a stretch – RFID is really well suited to be the “barcode of the future”**
 - You just need to keep them off people...
 - ...which nobody ever does.

Attendance Monitoring

- Inventory Control: Use of RFID to do continuous or intermittent identification of individuals at a location
 - Tradeshow Monitoring: An attacker could make an event think a particular speaker was popular, or not.
 - Classroom Monitoring: An attacker could make a student appear to be present or absent, potentially triggering harassment.
 - Protest Monitoring: An attacker could query the RFID tags within government-issued identification, acquiring a list of all individuals at an event
 - Not necessarily LEO doing the scanning
 - Non-LEO could transmit false names to LEO, potentially implicating innocents
 - Nationality Targeting: An attacker could use the RFID on a passport to target Americans for attack.
 - We'll return to this.

Risk Analysis from Attendance Monitoring

- Original reaction: So?
 - People are carrying around high-powered transceivers and (from the attacker's perspective) charging them up for you every day so you can keep track of them
 - Cell phones
- Upon further investigation...
 - People put stranger and stranger things in the RFID
 - You can't ask a cell phone for a list of recently visited train stations.
 - It's...problematic to go anywhere without Government-issued ID.
 - Nobody got arrested for not having a cell.
 - Normal ID checks require asking for ID – RFID has no request
 - This gets **especially** tricky if non-LEO ever get access to the content of the chip

Access Management: Where the real problems begin

- Access Control: Use of RFID to selectively allow some users, and not others to access a resource
 - Credit Cards: An attacker can spend someone else's money.
 - Corporate Badges: An attacker can achieve physical access to corporate facilities and labs, potentially committing espionage.
 - Military Badges: An attacker can achieve physical access to military facilities and storage depots, potentially destroying assets and killing people.

Out of sight, out of mind

- Nobody would suggest using barcodes to protect anything, let alone corporate resources, let alone lives
 - Radio barcodes are invisible.
 - Therefore, they're "OK".
- There are more secure RFID technologies
 - "Part of a two factor authentication system"
 - "Encrypted" (meaning it doesn't return the same "barcode" each time)
 - **Secure variants are almost never deployed in the field.**
 - The problem: Nobody knows what they are or aren't disclosing. They just hear a scan beep.
 - Perception is driving false reality.
 - It's just really easy to break into a lot of places that spent a lot of money for it to not be so easy.

So why aren't Physical Security people all over this?

- Very few physical attackers in the real world
 - Breaking into buildings is risky to the attacker – you're physically throwable into a jail cell.
 - Almost unstoppable success rate if an attacker is determined enough
 - An attacker can always drive a car into an office wall.
 - This leaves a car-shaped hole.
 - **Physical Security has not realized RFID attacks fail to leave car-shaped holes.**
 - Attackers thus have much less risk of triggering a manhunt

Would “Unclonable Badges” fix the problem?

- They would help.
 - The idea is you don't return the same code each time – the badge calculates a new barcode and sends that.
 - Only a real reader can make a badge respond
 - Only a real reader can understand the code returned
 - Hard to do this securely on limited electrical resources, but possible.
- Why does this only partially solve the problem?
 - Who said the badge was anywhere near the reader?

The Buddy System (“Ghost/Leech”)

- You park your RFID-keyed car and go to a restaurant.
- One car thief tails you in and sits at the table next to you.
- The other walks up to your car.
- When the car sends a request for its key, the request is copied over a cell phone link to the thief at the table next to you.
- The thief next to you sends a copy of the car’s request.
- Your car keys reply – “Sure! Unlock the door, I’m coming in.”
- **The attack above works with arbitrarily good cryptography. There is only one way to mitigate.**
 - You can’t give away your credentials to just anyone who asks
 - We need RFID badges to not be “always-on”, at least in all scenarios.

So What Should We Do?

- Start working on these problems. The equipment to complete these attacks is about to get much more common.
- Anti-Privacy Markets are **common**
 - DoubleClick's entire business model was tracking people moving around the net
 - \$100 for your cell phone records, still
 - Verizon just required an opt-out to keep them from selling 'em themselves
 - Serious rumors that ISPs will sell your entire HTTP clickstream
 - **Prediction: RFID movement data will get commoditized with revenue sharing**

The Model

- It's completely reasonable to build a door frame that will read all RFID badges that walk through it.
- A private firm pays stores to put RFID monitors in doorways that are capable of reading the loyalty cards as people walk through
- Said private firm resells demographic and PII data regarding who's going where at what time
 - Cell phone can't provide the "door check" of RFID
 - Cell phone carriers couldn't risk the business hit
- **The above scenario is pretty likely in the next few years.**
 - Might use government issued ID
 - Might use Supermarket loyalty cards
 - Might use ambient tags from clothing sales
 - This will at least get funded, as peer markets already exist in my world.

Conclusion

- RFID is just a barcode.
 - It's a lot easier to read, but it's still just a code.
 - There are somewhat more secure exceptions. Nobody uses them.
- This is really cool technology for inventory control.
- This is really creepy technology for population monitoring.
 - This monitoring will be massively privatized and will leak data nobody knows how to read
- This is really broken technology for access control.
 - We should start using “unclonable” badges.
 - We should start using badges that require user activation to leak credentials
 - We should start looking into what to do now, because a real storm of bad things is coming our way.