

RFIDIots!!!

*Hacking RFID Without A Soldering Iron
(or a Patent Attorney)*

Adam Laurie

adam@algroup.co.uk

<http://trifinite.org>

<http://rfidiot.org>

BlackHat Briefings

Las Vegas, 2007

Who Am I?

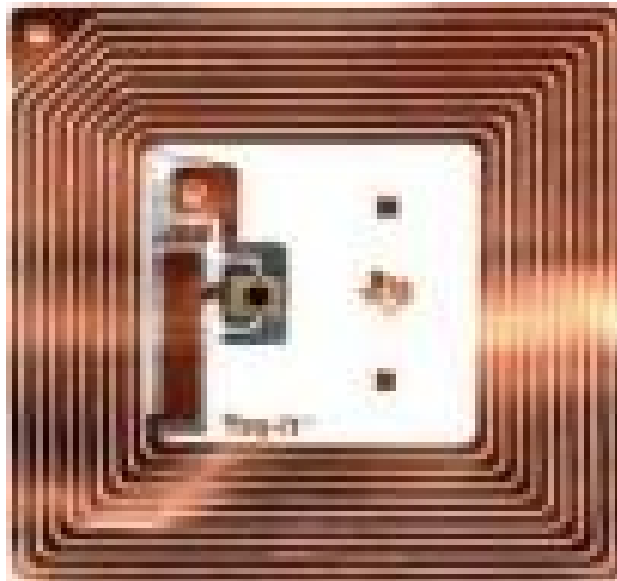
- The Bunker non-exec
- Co-Publisher APACHE-SSL
- DEFCON 'goon'
- Open Source developer / researcher
 - Bluetooth
 - RFID
 - Full Disclosure / White Hat!
- Freelance research / training / lecturing

What do I do?



What is RFID?

- Radio Frequency IDentification
 - Radio Frequency or Magnetically Coupled chip
 - Chip is passive
 - Energy from reader activates the chip



'Dumb' vs 'Smart'

- Dumb: Simple ID/Data only
 - Door Entry Systems
 - e.g. HID
- Smart: Smartcards
 - Payment Cards
 - e.g. London Transport Oyster
 - Biometrics
 - Passports



'Dumb' RFID – Moo am I?

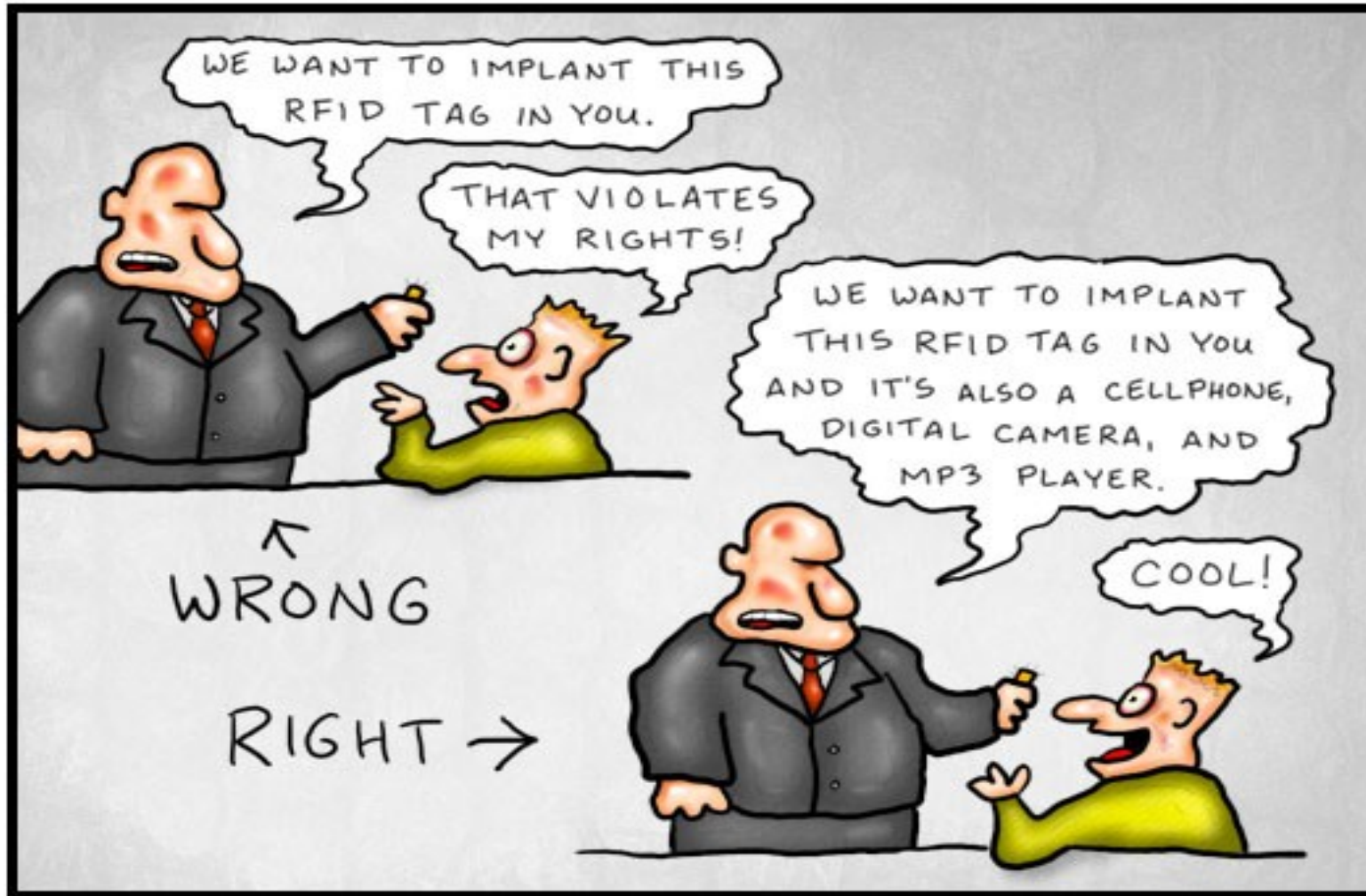


- Animal ID
- Hotel Keys
- Car Immobilisers
- Ski Passes
- Goods Labels
- Luggage Handling
- Vending
- Human Implants

Selling the idea of Human Implants

DOCTOR FUN

16 Jan 2006



Copyright © 2006 David Farley, d-farley@ibiblio.org
<http://ibiblio.org/Dave/drfun.html>

This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

Human Implants



- Military
 - Access Control
- Mental Patients
 - Tracking
- Beach Bars
 - Digital Wallets

Unique ID?



- DIY Cloning Units
 - <http://cq.cx/vchdiy.pl>

Spot the original?



Unique ID?



- DIY Cloning Units
 - <http://cq.cx/vchdiy.pl>

Spot the original?

- Industry Defence:



Unique ID?



- DIY Cloning Units
 - <http://cq.cx/vchdiy.pl>

Spot the original?



- Industry Defence:

“These 'clones' do not have the same form factor and are therefore not true clones”

2nd Line of Defence

2nd Line of Defence

- Security by Patent Attorney?

2nd Line of Defence

- Security by Patent Attorney?
 - HID vs IOActive

2nd Line of Defence

- Security by Patent Attorney?
 - HID vs IOActive
 - “HID Responds to Staged Proximity Card Cloning”
 - http://www.hidcorp.com/page.php?page_id=147
 - “IOActive Provides Clarification on HID Dispute”
 - <http://www.ioactive.com/pressreleases.html>

Unique ID?



- Readers cannot 'see'
so form factor
irrelevant

Unique ID?



=



- Readers cannot 'see' so form factor irrelevant

Cloning Devices



Cloning Devices



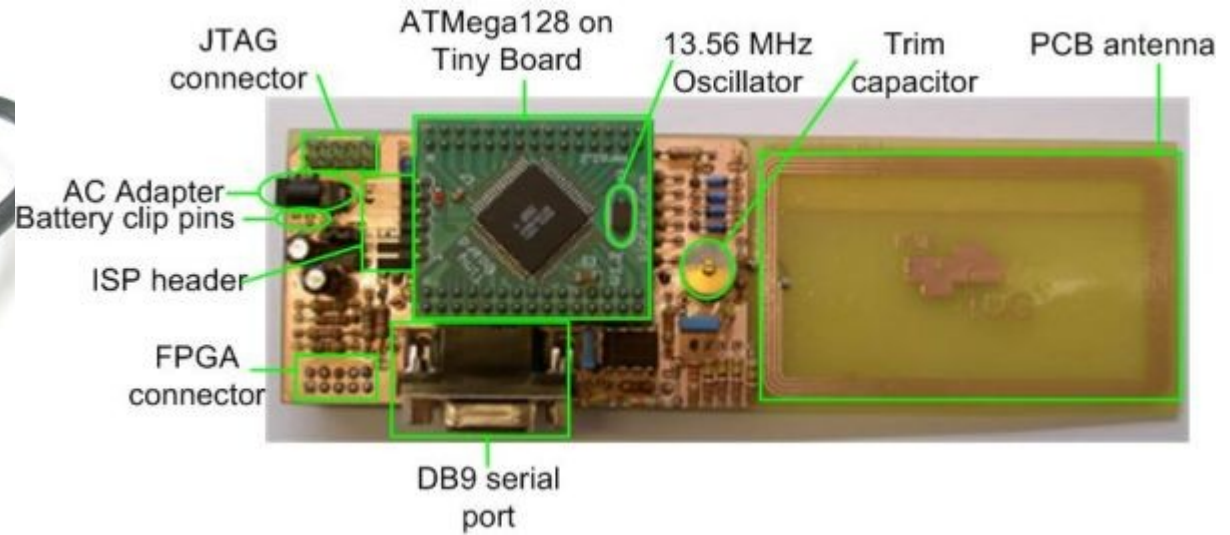
Cloning Devices



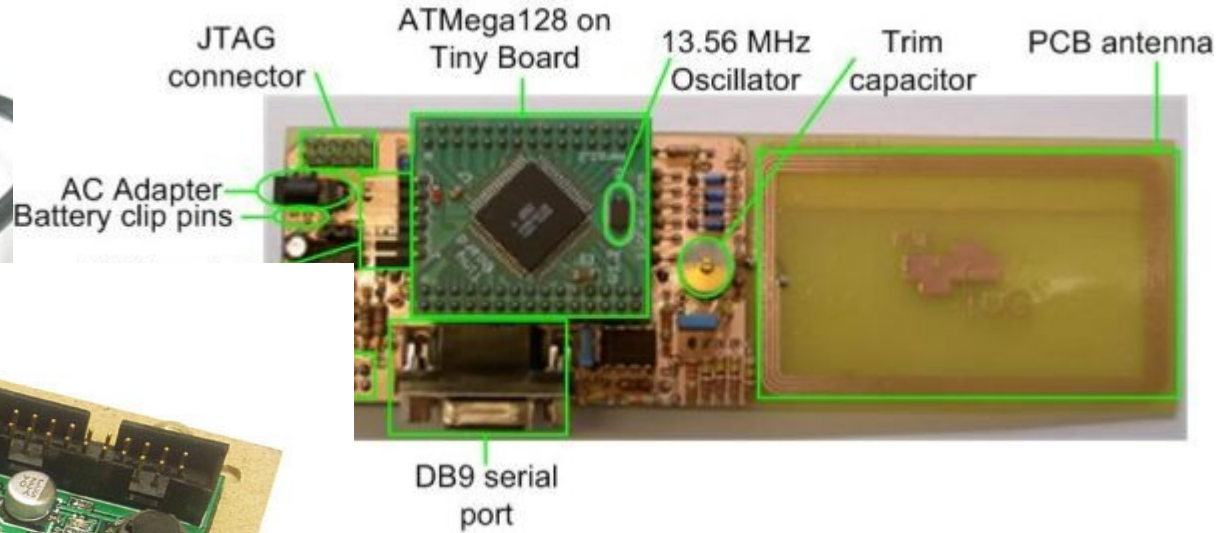
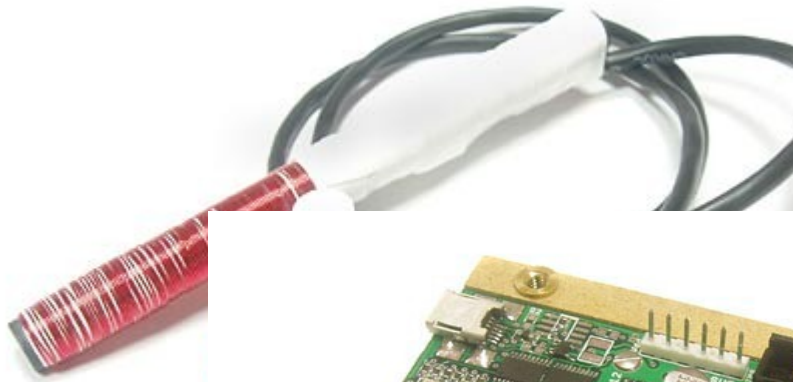
Cloning Devices



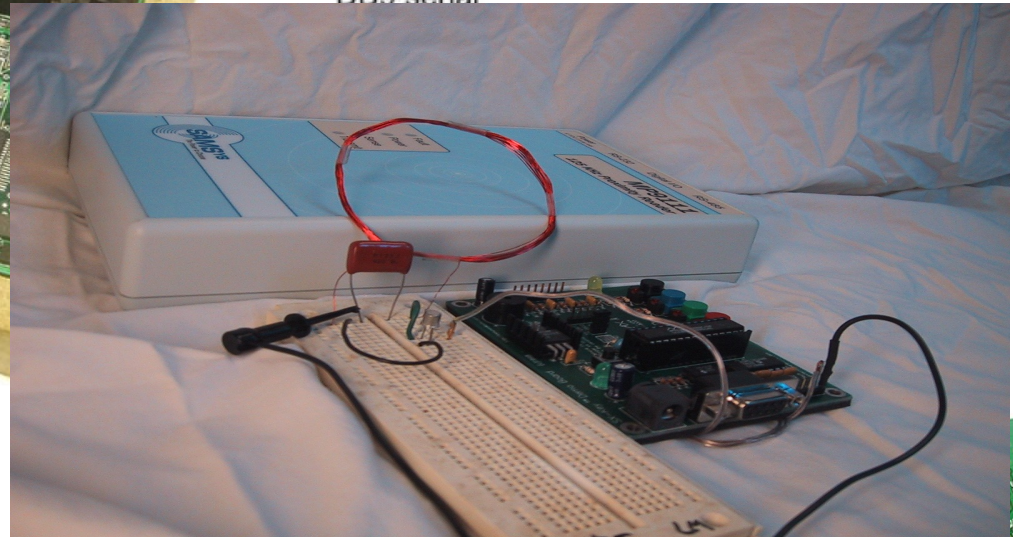
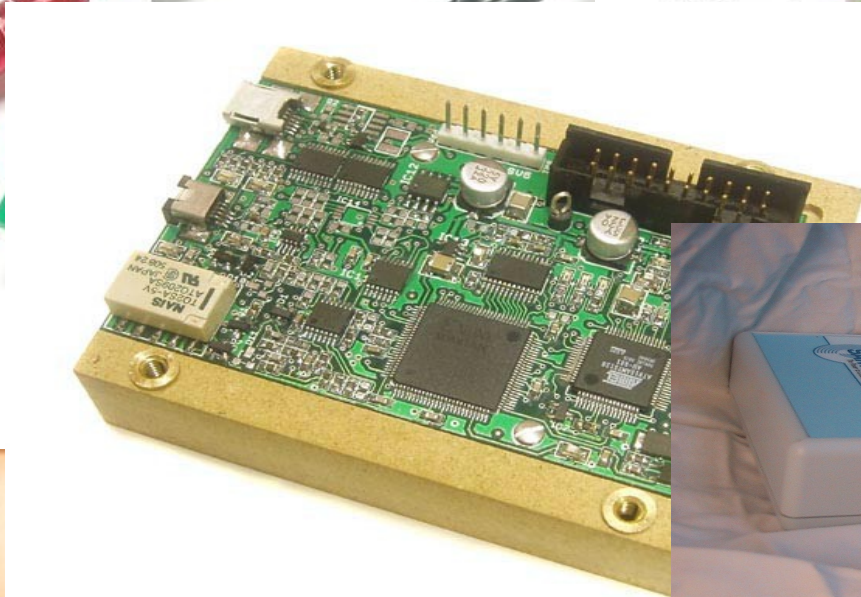
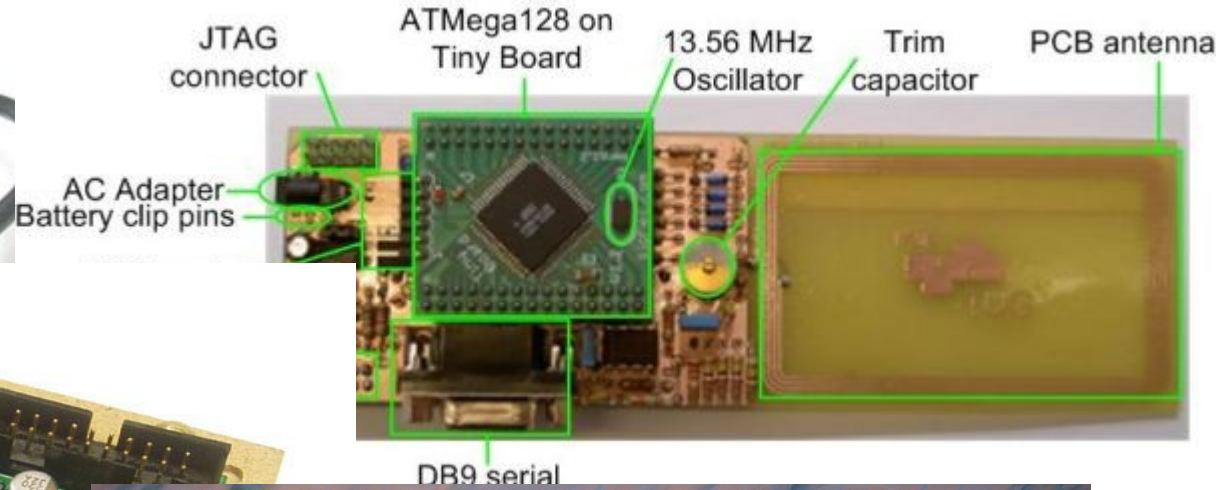
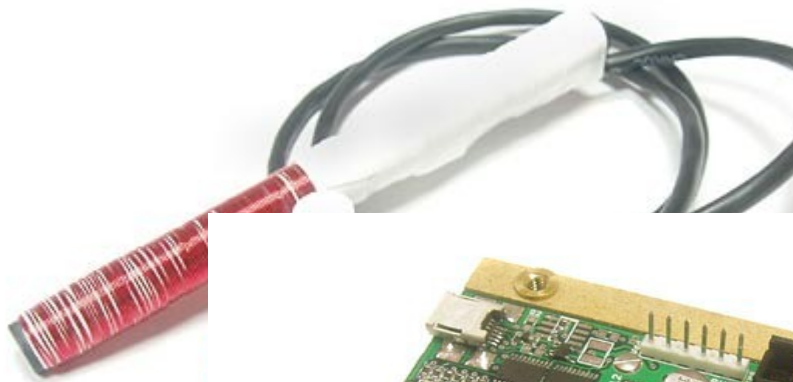
Cloning Devices



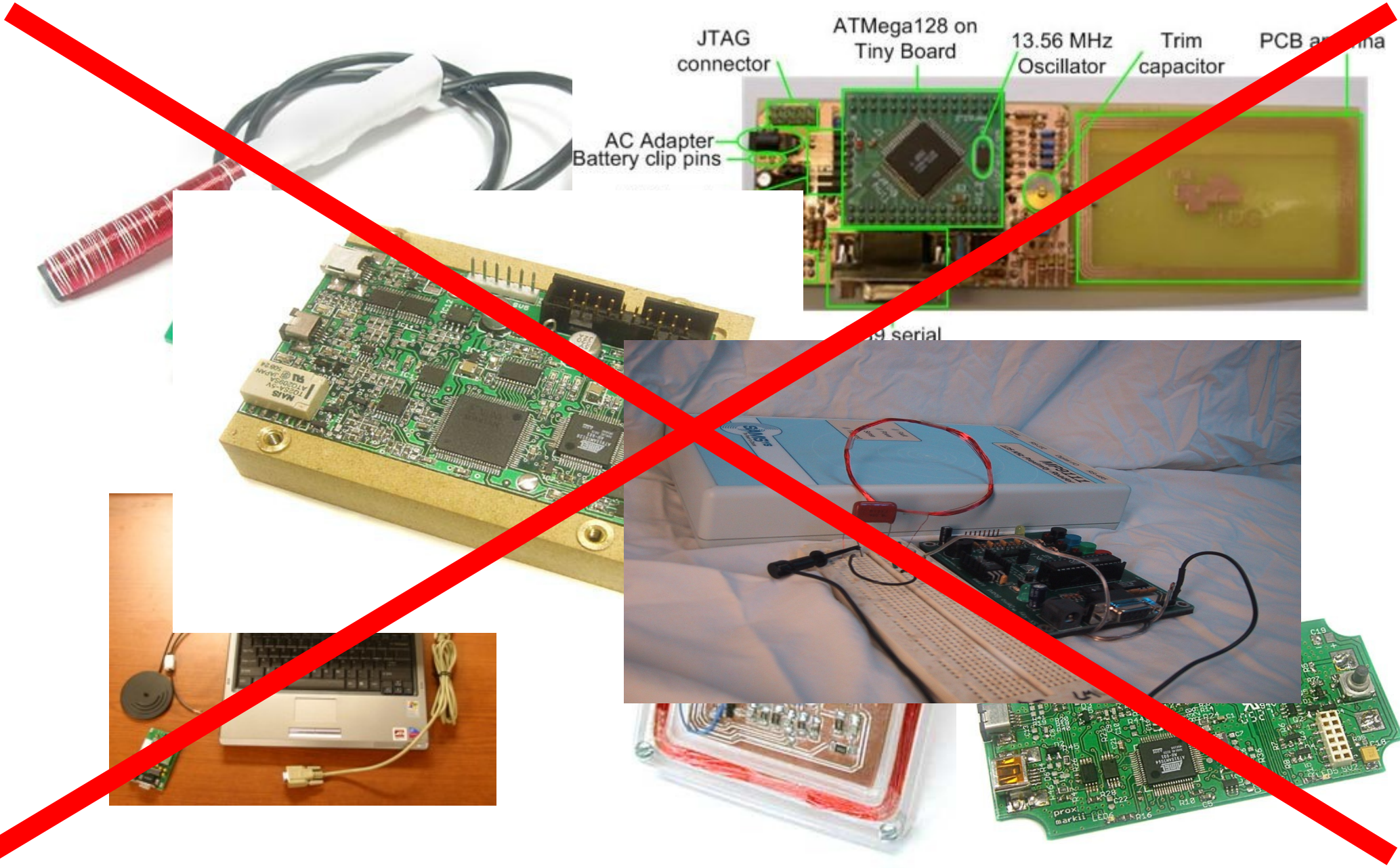
Cloning Devices



Cloning Devices



Cloning Devices



The Challenge

- Create a 'true' clone
 - Same ID
 - Same Form Factor

Understanding the ID

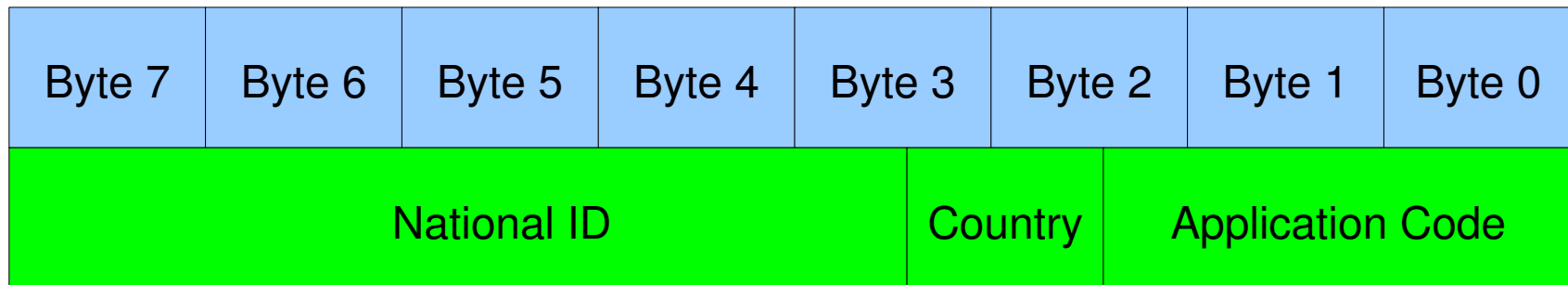
- Industry standard example
 - Animal Tagging
 - ISO-11784/5 FDX-B
 - Application flag (Animal/Non-Animal)
 - 3 Digit Country or Manufacturer code
 - National ID

Sending the ID

- Reader and TAG will communicate with
 - Specific frequency
 - 125/134.2 kHz - 'dumb'
 - 13.56 Mhz - 'smart'
 - Specific data bitrate
 - RF/2 - RF/128
 - Specific encoding (modulation) scheme
 - FSK, Manchester, BiPhase, PSK, NRZ
 - Specific bit patterns
 - Header / Data / CRC

Decoding the ID

- 8 Byte raw ID from 'dumb' reader



- Reverse MSB/LSB
- Reverse each Nibble
- Right shift (x2)
- Convert to Decimal

Decoding the ID

- 8 Byte raw ID

70	91	53	12	EA	6F	00	01
----	----	----	----	----	----	----	----

- Reverse MSB/LSB

10	00	F6	AE	21	35	19	07
----	----	----	----	----	----	----	----

- Reverse each Nibble

80	00	F6	57	48	CA	89	0E
----	----	----	----	----	----	----	----

Decoding the ID

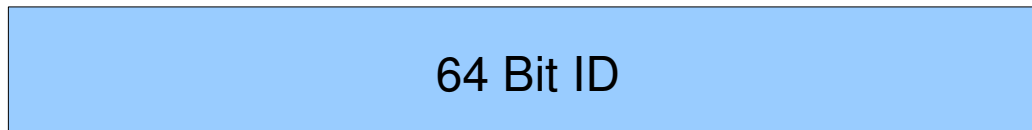
- 8 Byte raw ID

80	00	F6	57	48	CA	89	0E
Application ID 8000		Country F65	National ID 748CA890E				

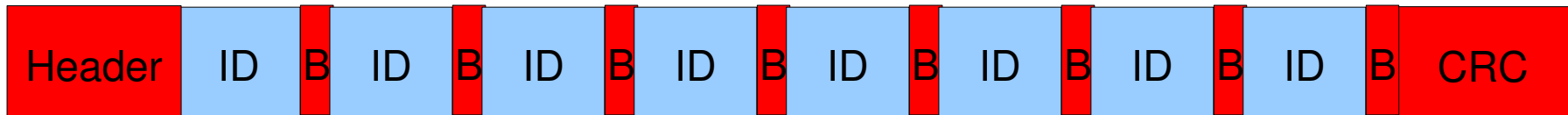
- Country F65 rightshifted: 3D9 == '985' decimal
 - icar.org: 'Destron Fearing / Digital Angel Corporation'
- National ID 748CA890E == '31286003982'

Encoding the ID

- Reverse the decoding process



- Add Header / CRC to raw binary ID



- Fixed bits embedded in ID prevent header being duplicated in datastream
- Now we have 128 bits of raw bit-level ID
 - How do we deliver it?

Multi-Format Transponders

- Why make 10 transponder types when you can make 1?
 - Lower manufacturing costs
 - Lower stocking/distribution costs
 - Convenience

Multi-Format Transponders

- Independently configurable parameters
 - Q5
 - Configuration for Bit Rate, Modulation etc.
 - 224 Bits user programmable memory
 - Dump <n> data blocks on wakeup
- Multiple 'personalities'
 - Hitag2
 - Configuration for 'Public Modes'
 - 256 Bit user programmable memory
 - Dump <n> data blocks on wakeup as per Mode setting

Sending the ID

- Take a redundant Door Entry tag
 - Re-Set configuration as appropriate
 - Bit Rate
 - Modulation
 - Inversion
 - Number of blocks to dump on 'wakeup'
 - Program data blocks with raw ID

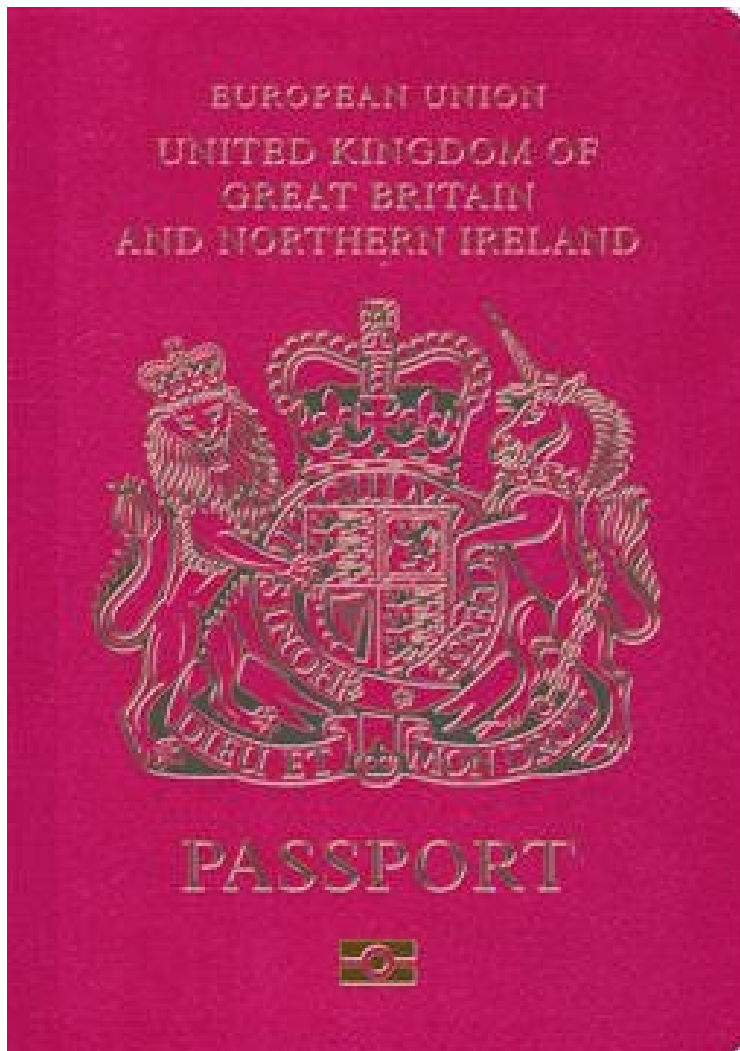
Demonstration

- Clone Trovan 'Unique' TAG
 - Access Control System
- Clone ISO 11784 'Animal' TAG (FDX-B)
 - Cow Implant
 - VeriChip paperweight

RFID implanted chip threats

- Track individuals
- Target individuals
- Impersonate individuals
 - Gain access to restricted areas
 - Provide alibi for accomplice!
- 'Smart' Bombs
 - Device only goes off if target of sufficient rank is in range.

'Smart': Encryption is your friend



- RFID Enabled
'Biometric' passports
- 48 Items of Data
 - Fingerprint
 - Facial Image
 - Birth Certificate
 - Home Address
 - Phone Numbers
 - Profession

Keys to your kingdom



- Pseudo random UID
 - Cannot determine presence of specific passport without authentication
- Strong Authentication
 - Basic Access Control
 - 3DES
- Content Encryption
 - Extended Access Control

ePassport Modification

- “Not Possible” due to cryptographic signatures
 - Certificate Authority (CA) not verifiable
 - Signatures provided by document
 - CA Key provided by same document
 - Public Key Directory (PKD) not available
- Self-Signed Forgery may not be detected!

ePassport Certificates

New Zealand genuine:

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1122333666 (0x42e573e2)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=NZ, O=Government of New Zealand, OU=Passports, OU=Identity Services Passport CA
Validity

Not Before: Jan 23 21:46:58 2007 GMT

Not After : May 18 12:00:00 2012 GMT

Subject: C=NZ, O=Government of New Zealand, OU=Passports, OU=MRTD, CN=Document Signer
200701241034

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (2048 bit)

Modulus (2048 bit):

00:a8:bf:fb:c0:ae:f4:c7:fe:ec:19:71:b6:25:e9:

...

ePassport Certificates

New Zealand forgery:

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1122333666 (0x42e573e2)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=NZ, O=Government of New Zealand, OU=Passports, OU=Identity Services Passport CA
Validity

Not Before: Jan 23 21:46:58 2007 GMT

Not After : May 18 12:00:00 2012 GMT

Subject: C=NZ, O=Government of New Zealand, OU=Passports, OU=MRTD, CN=Document Signer
200701241034

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (2048 bit)

Modulus (2048 bit):

00:dc:19:33:f3:11:86:a4:82:b9:c7:21:45:ca:81:

...

Other ePassport threats

- Key data may be obtained through other channels
- Passport profiling
 - Determine country of origin without logging in
 - Implementation errors:
 - Australian passport does not start with '08' on select
 - Australian passport does not require Basic Auth on 'File Select', only on 'File Read'.
- Target specific passport holders
 - Bomb that works for Australians only...

RFIDIOT

- Open Source Python library
- Hardware independent
 - ACG
 - Frosch
 - PCSC-Lite
 - OpenPCD coming soon

<http://rfidiot.org>

Questions?

<http://rfidiot.org>

adam@algroup.co.uk