Exhibit 7
what this talk is:
Pen-testing a subway system
what this talk is not:
evidence in court
(hopefully)
You’ll learn how to

- Generate stored-value fare cards
- Reverse engineer magstripes
- Hack RFID cards
- Use software radio to sniff
- Use FPGAs to brute force
- Tap into the fare vending network
- Social engineer
- WARCART!
AND THIS IS VERY ILLEGAL!

So the following material is for educational use only.
ATTACK

PHYSICAL SECURITY
there is almost always a free way to get in
turnstile control boxes open...
almost everywhere
computer screens visible through windows
door keys left in open boxes
state-of-the-art surveillance... often unattended
documents left in the open
Fargo DTC515 Thermal Card Printer

Bidder or seller of this item? Sign in for your status

Current bid: US $79.99

Your maximum bid: US $________
(Enter US $60.99 or more)

End time: Jun-29-08 19:43:35 PDT (2 days 1 hour)
Shipping costs: US $30.12
UPS Ground
Service to 02142, United States

Ships to: United States
Item location: Minneapolis, Minnesota, United States
History: 1 bid
High bidder: 1***o (804 🌟)

You can also: Watch This Item
Get SMS or IM alerts | Email to a friend

View larger picture
ATTACK THE MAGCARD
pick the hardware
$5<
Homebrew reader
With inserts, can read 3-tracks
stripesnoop.sourceforge.net

$139.95
Spark Fun Electronics
3-Track Lo-Co
Includes source code

$300
MSR206 or MAKStripe
3-Track Hi/Lo-Co
Works with our GPL’d software
is value stored on the card?

**try a cloning attack**
If yes, then

you now have free subway rides for life
Oh, but you want more than that, eh?
reverse engineering

The Charlie Ticket
Reverse engineering

Everybody talks about it,
But where do you start?

1) Make a guess about what's in the data
2) Change a single variable; see what changes
3) Repeat many times with varying data
4) Compare similar and dissimilar data
5) Ignore constant regions
6) Build/use tools
reverse engineering

Isolate Variables method

To locate a single variable:

- Group data by that variable
- Ignore global similarities (between different groups)
- Ignore differences within groups

Resulting locations are probably where the data is stored
<table>
<thead>
<tr>
<th>ticket type (ticket / pass)</th>
<th>value (in cents)</th>
<th>ticket #</th>
<th>const</th>
<th>time</th>
<th>last const</th>
<th>last trans</th>
<th># of uses (in nickels)</th>
<th>checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC901 0402AC9D 000000005B8 00C8</td>
<td>0150342 248 A84EBD 132 BE</td>
<td>1</td>
<td>const</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Charlie Ticket
 Forgiving
<table>
<thead>
<tr>
<th>ticket type</th>
<th>value (in cents)</th>
<th>ticket #</th>
<th>time</th>
<th>const</th>
<th>last reader station used (approx)</th>
<th>checksum</th>
<th># of last trans uses (in nickels)</th>
</tr>
</thead>
<tbody>
<tr>
<td>const</td>
<td>0000000005B8 00C8</td>
<td>0150342 248 A84EBD 132 BE</td>
<td>028 0002 0000002025D0000 E0D60</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ticket Type Value (in cents)</td>
<td>Const</td>
<td>Ticket #</td>
<td>Time</td>
<td>Last Reader Station Used</td>
<td>Last Trans (in nickels)</td>
<td>Const (approx)</td>
<td>Checksum</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------</td>
<td>----------</td>
<td>------</td>
<td>--------------------------</td>
<td>------------------------</td>
<td>---------------</td>
<td>-----------</td>
</tr>
<tr>
<td>000000005B8 FE4C</td>
<td></td>
<td>0150342 248 A84EFD 1.32 BE</td>
<td>1</td>
<td></td>
<td>028</td>
<td>000000002025D0000 FC90</td>
<td></td>
</tr>
</tbody>
</table>
MagCard Reverse-Engineering Framework

Bitstir
Reverse Engineering GUI

MSR206
read()
write()
erase()
...

MagCard

Utilities
conversions
comparisons
checksums
time stamps
...

CharlieTicket
Boston, MA

MetroCard
New York City, NY

...
Demo: MagCard and Reverse Engineering Toolkit

- wrote Python libraries for analyzing magcards
- integrated with the MSR206 reader/writer
- GUI helps visualize and organize data
what about other subways?

- Most subway fare collection systems in US are made by two major integrators
  - Scheidt & Bachmann made Boston T, San Francisco Bart, Long Island Railroad, Seattle Sound Transit, London Silverlink, etc. systems
  - Cubic Transportation made NYC MTA, Washington DC WMATA, Chicago CTA, Shanghai Metro, etc. systems

Are they hackable? Yes!
Learn about your RFID card
MIFARE Classic

- 13.56MHz RFID smartcard
- End-to-end proprietary "crypto" (Crypto-1)
- 1K memory & unique identifier on card
- Over 500 million tags in use
Crypto-1 Cryptanalysis

Crypto-1 reverse engineered by Karsten Nohr, University of Virginia, 2007:
- Etched and inspected silicon wafer using high-powered imagery.
- Found and reconstructed crypto portions from over 10k gates.
- Found vulnerabilities in the cipher and implementation
security of the MIFARE card

Mutual 3-pass authentication

sector? key A or B?

read key

random-challenge

answer, random-challenge

verify answer

Each sector two keys

answer

verify answer

Non-linear filter functions
security of the MIFARE card

Mutual 3-pass authentication

sector? key A or B?

random-challenge

answer, random-challenge

answer

verify answer

Non-linear filter functions
security of the MIFARE card

Non-linear filter functions
security of the MIFARE card
to execute these attacks we need to interact with the card

choose your hardware
$50
MiFare RFID Reader/Writer
Comes with source code
Hard to hack, but doable

$220
OpenPCD + OpenPICC
Open design 13.56MHz RFID reader + emulator
Free schematics (www.openpcd.org)

$700
USRP
Full control over signal input/output
Works with GNU Radio + our plugin
card/reader communication

CharlieCard

13.56MHz
ASK modulation
Modified miller encoding

13.56MHz
+- 847kHz
OOK modulation
Manchester encoding
charlie card + reader FFT

carrier

subcarrier

subcarrier
GNU radio RFID toolchain

Tune Radios

subcarrier (card-> reader)

Band-Pass Filter
GNU radio RFID toolchain

Tune Radios

Band-Pass Filter

Demodulate

Demodulate

subcarrier (card -> reader)

carrier (reader -> card)
GNU radio RFID toolchain

Tune Radios

Band-Pass Filter

Demodulate

Demodulate

Modified Miller Decoder

to file

subcarrier (card -> reader)
carrier (reader -> card)
challenge/response pairs

sniffing the turnstile
attacks on the MIFARE card

Goal: get secret key (can clone card with it)

Brute Force
attacks on the MIFARE card

Goal: get secret key (can clone card with it)

- Brute Force
- Manipulate PRG Timing
attacks on the MIFARE card

Goal: get secret key (can clone card with it)

Brute Force

Manipulate PRG Timing

Algebraic Attacks
when all else fails

brute force it
Why Brute Force with an FPGA?

Because it's fast!

- General purpose device
- Finite instruction set
  (Uh, oh. Sounds RISCy)
- 1-8 parallelizations

FPGA

- Dedicated logic
- Hardware description language defines hardware
- Hundreds of parallelizations
KwickBreak FPGA Brute-Forcer
Executes known plaintext attack to recover key

Code Generator

KwickBreak GUI
interfaces w/

FPGA Brute Forcing Platform

-- generates

uses

FPGA
Hardware Used
Opal Kelly
XEM3001
www.opalkelly.com

Crypto-1
DES
...

14
writing a (trivial) XOR module

module xorPlugin(
    input wire clk,
    input wire [47:0] key,
    input wire [47:0] plaintext,
    output reg [47:0] encrypted,
    output reg ready);

    always @(posedge clk) begin
        ready <= 1;
        encrypted <= key ^ plaintext;
    end
endmodule
writing a (trivial) XOR module (cont)

./kwickbreakGenerator.py

>>> Please enter your plugin module name, as written.
xorPlugin
Output filename (and path)
xorBruteForceUtil.v
How many cores would you like on the chip?
50
If you have a pipelined design, how many clock delays for valid data?
0
xorBruteForceUtil.v successfully written!

Now just create a new project in Xilinx ISE, load the files, and synthesize

Done!
Subways using MiFare Classic

- Boston (CharlieCard)
- London (Oyster Card)
- Netherlands (OV-Chipkaart)
- Minneapolis
- South Korea (Upass)
- Hong Kong
- Beijing
- Madrid (Sube-T)
- Rio de Janeiro (RioCard)
- New Delhi
- Bangkok

and more
network security

- Performed site surveys of T stations and offices (no WiFi found)
- Performed wireless device audit
- Found unguarded network switches
fiber switches in unlocked room
connect fare vending machines to the internal network
fiber switches in unlocked room
connect fare vending machines to the internal network
Social Engineering

Executed the "PHANTOM MEETING" attack

Gained access to internal network drops and computers

Nobody suspected a thing as we walked into offices and conference rooms...

So we took it up a notch.
First there was wardialing
then there was wardriving

then there was warwalking

then there was warflying and warboating

then there was war-rocketing

then there was warballooning

and now... warcarting

**WarCart**

- **Pan/Tilt Mechanism**
  - Attachments include antennas or a smoke grenade launcher

- **Two Laptops**
  - For control and data logging

- **Scanner**
  - To pick up various communications

- **Control Box**
  - W/ key switch for activation

- **Antenna Switch Box**
  - To toggle between antennas and radios

- **Flash Drive Dropper**
  - For U3 hacksaws

- **900 MHz Antenna**
  - Directional, great for cordless phones

- **19dBi WiFi Antenna**
  - Directional

- **12dBi WiFi Antenna**
  - Omnidirectional

- **25-1300 MHz Antenna**
  - General coverage, great for picking up the police

- **CCD Camera**
  - Trip documentation

- **Lights**
  - 2M candlepower for night operations

- **PA Speaker**
  - For announcements and intimidating music
We decided to take it to the MBTA headquarters!
And then we ran into some problems with the police.

That's one of the WarCart's smoke grenades, by the way.
So to avoid ending up like this

We turned back
contributions
contributions

1) Exploited physical security holes
2) Reverse engineered the CharlieTicket
3) Wrote code to analyze & generate magcards
4) Wrote a toolchain for analyzing 13.56MHz RFID transactions using the USRP+GNUradio
5) Attacked problems with the MIFARE Classic cards
6) Wrote brute forcer-generator to crack keys on an FPGA
7) Developed software to reduce MQ to SAT, allowing key recovery
8) Wrote code to read and clone MIFARE cards (given the key)
Exhibit 8
Dear Ieuan:

Attached please find the presentation slides that our clients submitted to DEFCON.

As we discussed on the phone earlier today, the tone of this presentation is geared toward the DEFCON audience. To be clear, our clients do not intend to disclose information that would enable the audience to duplicate the research, and the presentation will omit key details to ensure responsible disclosure.

While we remain open to discussing the content of the presentation, please note that these slides have been included in a CD distributed to DEFCON attendees.

We will try to give you a call as early as possible tomorrow in light of the time difference. We will aim for 9:00 ET/6:00 PT.

Best regards,

Marcia

Marcia Hofmann, Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

tel: (415) 436-9333 x. 116 | fax: (415) 436-9933 marcia@eff.org | http://www.eff.org

Join EFF today! http://www.eff.org/support

ieuan.mahony@hklaw.com wrote:
> Kurt, Marcia, and Jennifer:
> Per our 11:30 call, I will be available for another hour or so
> tonight. I have not circulated your inquiry about possible
> willingness to postpone the hearing. Please let me know if you wish
> us formally to consider this as a request.
> > I note that we still do not have your clients' presentation materials.
> > I am inclined to object to any discussion of a postponement, as the
> > decision to continue to withhold these materials makes me concerned.
> > As I stated during our 9:00, and 11:30 calls this evening, I see no
> > basis for continuing to withhold this information.
> > > With that said, we remain interested in discussing an amicable
> > resolution. Once I have finished the Supplemental Declaration I
> > discussed, I will begin work on a proposed Consent Judgment and format
> > for your review.
> >
> > Ieuan
Case 1:08-cv-11364-GAO   Document 9-8   Filed 08/09/08   Page 91 of 97

*Holland + Knight*

*Ieuan G. Mahony*

Partner
Holland & Knight LLP
10 St. James Avenue
Boston, MA 02116
Main 617 523 2700
Direct 617 573 5835

Cell 791-789-4230
Fax 617 523 6850
Email ieuang.mahony@hklaw.com
www.hklaw.com

*NOTICE: * This e-mail is from a law firm, Holland & Knight LLP
(*H&K*), and is intended solely for the use of the individual(s) to
whom it is addressed. If you believe you received this e-mail in
error, please notify the sender immediately, delete the e-mail from
your computer and do not copy or disclose it to anyone else. If you
are not an existing client of H&K, do not construe anything in this
e-mail to make you a client unless it contains a specific statement to
that effect and do not disclose anything to H&K in reply that you
expect it to hold in confidence. If you properly received this e-mail
as a client, co-counsel or retained expert of H&K, you should maintain
its contents in confidence in order to preserve the attorney-client or
work product privilege that may be available to protect confidentiality.

>
Exhibit 9
Marcia:
I am circulating this now. Given the time, and Scott's flight, I am not sure how close a review of the substance we will have by the hearing.

I have the following two requests, and would appreciate a response as far in advance of the hearing as you are able:

1. Please let me know the time at which the slide deck was first distributed to DEFCON attendees.

2. Please let me know the relationship, if any, between (a) the point in time the MIT Undergrads understood the MBTA wanted an opportunity to view these materials; and (b) the point in time when the materials were distributed at DEFCON.

I will wait for your call, and would appreciate a response to the above two questions.

Ieuan

-----Original Message-----
From: Marcia Hofmann [mailto:marcia@eff.org]
Sent: Saturday, August 09, 2008 4:38 AM
To: Mahony, Ieuan (BOS - X75835)
Cc: kurt@eff.org; jennifer@eff.org; jaren@mit.edu
Subject: Re: MBTA v Anderson et al

Dear Ieuan:

Attached please find the presentation slides that our clients submitted to DEFCON.

As we discussed on the phone earlier today, the tone of this presentation is geared toward the DEFCON audience. To be clear, our clients do not intend to disclose information that would enable the audience to duplicate the research, and the presentation will omit key details to ensure responsible disclosure.

While we remain open to discussing the content of the presentation, please note that these slides have been included in a CD distributed to DEFCON attendees.

We will try to give you a call as early as possible tomorrow in light of the time difference. We will aim for 9:00 ET/6:00 PT.

Best regards,

Marcia

--
Marcia Hofmann, Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
tel: (415) 436-9333 x. 116 | fax: (415) 436-9993 marcia@eff.org | http://www.eff.org

Join EFF today! http://www.eff.org/support
ieu.an.mahony@hklaw.com wrote:
> Kurt, Marcia, and Jennifer:
> Per our 11:30 call, I will be available for another hour or so
> tonight. I have not circulated your inquiry about possible
> willingness to postpone the hearing. Please let me know if you wish
> us formally to consider this as a request.
> 
> I note that we still do not have your clients' presentation materials.
> I am inclined to object to any discussion of a postponement, as the
> decision to continue to withhold these materials makes me concerned.
> As I stated during our 9:00, and 11:30 calls this evening, I see no
> basis for continuing to withhold this information.
> 
> With that said, we remain interested in discussing an amicable
> resolution. Once I have finished the Supplemental Declaration I
> discussed, I will begin work on a proposed Consent Judgment and format
> for your review.
> 
> Ieuan
>
> *Holland + Knight*
> *Ieuan C. Mahony*
> Partner
> Holland & Knight LLP
> 10 St. James Avenue
> Boston, MA 02118
> Main 617 523 2700
> Direct 617 573 5835
> 
> Cell 781-789-4230
> Fax 617 523 6850
> Email ieuan.mahony@hklaw.com
>
> www.hklaw.com
> 
> *NOTICE: This e-mail is from a law firm, Holland & Knight LLP
> ("H&K"), and is intended solely for the use of the individual(s) to
> whom it is addressed. If you believe you received this e-mail in
> error, please notify the sender immediately, delete the e-mail from
> your computer and do not copy or disclose it to anyone else. If you
> are not an existing client of H&K, do not construe anything in this
> e-mail to make you a client unless it contains a specific statement to
> that effect and do not disclose anything to H&K in reply that you
> expect it to hold in confidence. If you properly received this e-mail
> as a client, co-counsel or retained expert of H&K, you should maintain
> its contents in confidence in order to preserve the attorney-client or
> work product privilege that may be available to protect confidentiality.
Mahony, Ieuan (BOS - X75835)

From: Mahony, Ieuan (BOS - X75835)
Sent: Saturday, August 09, 2008 5:26 AM
To: 'Swope, Jeffrey'
Cc: 'Marcia Hofmann'; kun@eff.org; jennifer@eff.org; jaren@mit.edu; William Mitchell; Scott Darling; Mahony, Ieuan (BOS - X75835)
Subject: RE: MBTA v Anderson et al

Jeffrey:
I make the following request of you, again, as far in advance of the hearing as you are able:

(1) Please state when MIT first became aware of this slide deck?

(2) Please state whether MIT at any point had access to a copy of this slide deck? If so, when?

Thank you

Ieuan

-----Original Message-----
From: Mahony, Ieuan (BOS - X75835)
Sent: Saturday, August 09, 2008 5:15 AM
To: 'Marcia Hofmann'
Cc: kurt@eff.org; jennifer@eff.org; jaren@mit.edu; 'Swope, Jeffrey'; William Mitchell; Scott Darling; Mahony, Ieuan (BOS - X75835)
Subject: RE: MBTA v Anderson et al

Marcia:
I am circulating this now. Given the time, and Scott's flight, I am not sure how close a review of the substance we will have by the hearing.

I have the following two requests, and would appreciate a response as far in advance of the hearing as you are able:

(1) Please let me know the time at which the slide deck was first distributed to DEFCON attendees.

(2) Please let me know the relationship, if any, between (a) the point in time the MIT Undergrads understood the MBTA wanted an opportunity to view these materials; and (b) the point in time when the materials were distributed at DEFCON.

I will wait for your call, and would appreciate a response to the above two questions.

Ieuan

-----Original Message-----
From: Marcia Hofmann [mailto:marcia@eff.org]
Sent: Saturday, August 09, 2008 4:38 AM
To: Mahony, Ieuan (BOS - X75835)
Cc: Kurt@eff.org; jennifer@eff.org; jaren@mit.edu
Subject: Re: MBTA v Anderson et al

Dear Ieuan:

Attached please find the presentation slides that our clients submitted to DEFCON.

As we discussed on the phone earlier today, the tone of this presentation is geared toward the DEFCON audience. To be clear, our clients do not intend to disclose information that would enable the audience to duplicate the research, and the presentation will omit key details to ensure responsible disclosure.

While we remain open to discussing the content of the presentation, please note that these
slides have been included in a CD distributed to DEFCON attendees.

We will try to give you a call as early as possible tomorrow in light of the time difference. We will aim for 9:00 ET/6:00 PT.

Best regards,

Marcia

Marcia Hofmann, Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
tel: (415) 436-9333 x. 116 | fax: (415) 436-9993 marcia@eff.org | http://www.eff.org

Join EFF today: http://www.eff.org/support

ieuan.mahony@hklaw.com wrote:
> Kurt, Marcia, and Jennifer:
> Per our 11:30 call, I will be available for another hour or so
> tonight. I have not circulated your inquiry about possible
> willingness to postpone the hearing. Please let me know if you wish
> us formally to consider this as a request.
> I note that we still do not have your clients' presentation materials.
> I am inclined to object to any discussion of a postponement, as the
> decision to continue to withhold these materials makes me concerned.
> As I stated during our 9:00, and 11:30 calls this evening, I see no
> basis for continuing to withhold this information.
> With that said, we remain interested in discussing an amicable
> resolution. Once I have finished the Supplemental Declaration I
> discussed, I will begin work on a proposed Consent Judgment and format
> for your review.
> Ieuan
> *Holland + Knight*
> "Ieuan G. Mahony"
> Partner
> Holland & Knight LLP
> 10 St. James Avenue
> Boston, MA 02118
> Main 617 523 2700
> Direct 617 573 5835
> Cell 781-789-4230
> Fax 617 523 6850
> Email ieuan.mahony@hklaw.com
> www.hklaw.com
> "NOTICE: This e-mail is from a law firm, Holland & Knight LLP
> ("H&K"), and is intended solely for the use of the individual(s) to
> whom it is addressed. If you believe you received this e-mail in
> error, please notify the sender immediately, delete the e-mail from
> your computer and do not copy or disclose it to anyone else. If you
> are not an existing client of H&K, do not construe anything in this
> e-mail to make you a client unless it contains a specific statement to
> that effect and do not disclose anything to H&K in reply that you
> expect it to hold in confidence. If you properly received this e-mail
> as a client, co-counsel or retained expert of H&K, you should maintain
its contents in confidence in order to preserve the attorney-client or
work product privilege that may be available to protect confidentiality.