Exhibit 7

Anatomy of a Subway Hack

Russell Ryan

Zack Anderson

Alessandro Chiesa

For updated slides and code, see: http://web.mit.edu/zacka/www/subway/

what this talk is:

Pen-testing a subway system

what this talk is not:

evidence in court
(hopefully)

3

You'll learn how to

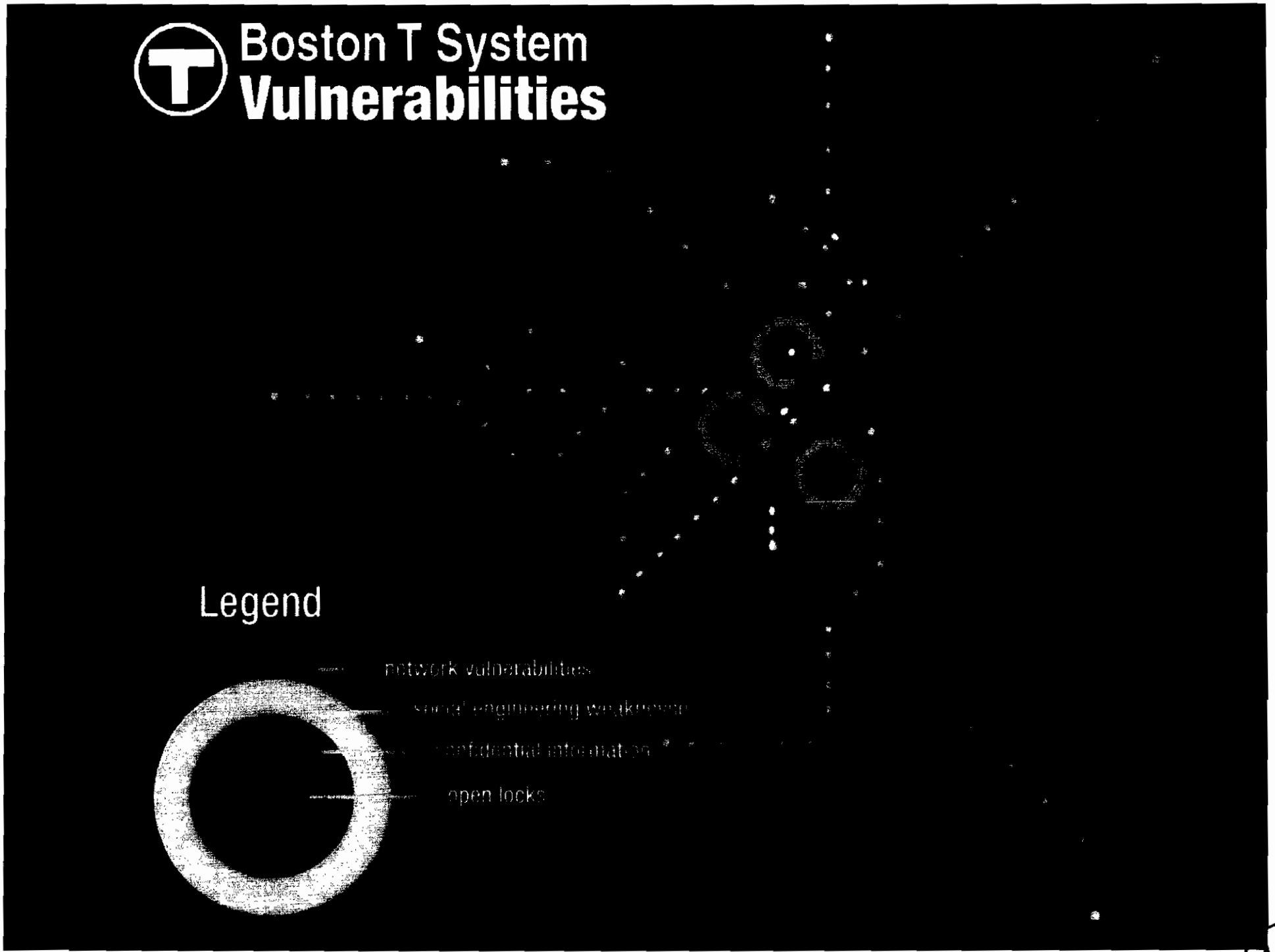
- Generate stored-value fare cards
- Reverse engineer magstripes
- Hack RFID cards
- Use software radio to sniff
- Use FPGAs to brute force
- Tap into the fare vending network
- Social engineer
- WARCART!

AND THIS IS VERY ILLEGAL!

So the following material is for educational use only.

(5)

Boston T System Vulnerabilities

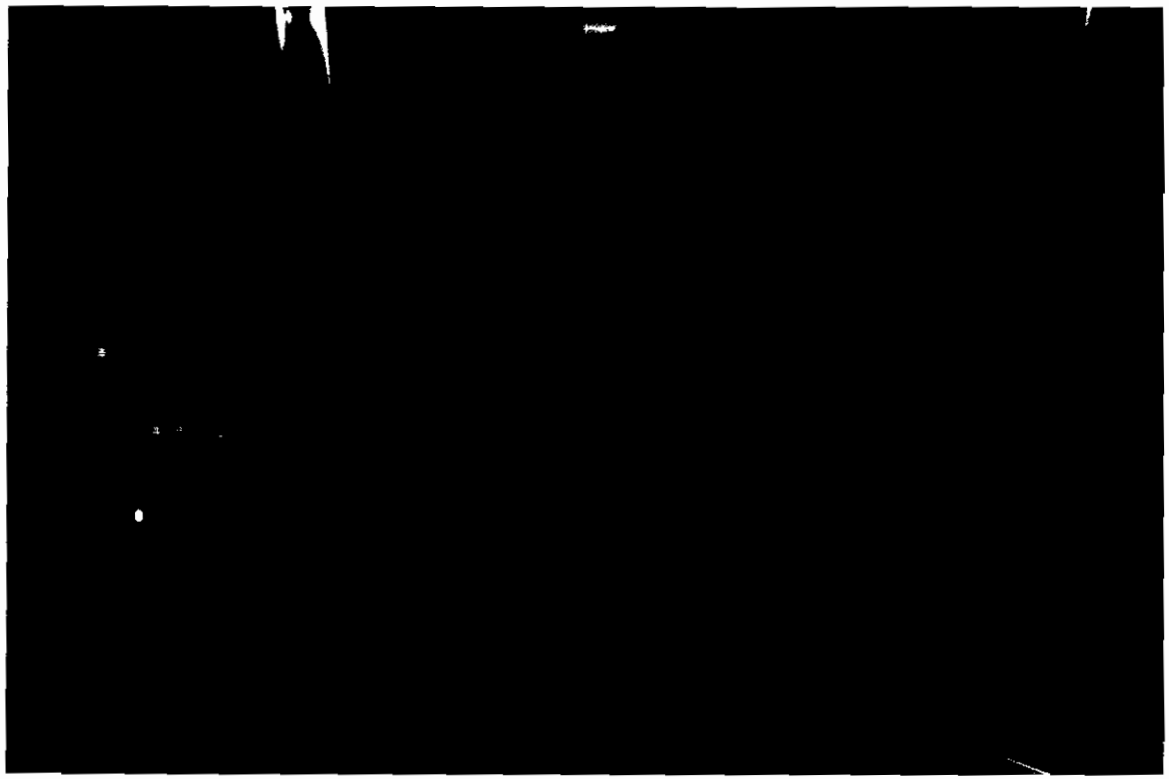


ATTACK
PHYSICAL
SECURITY

there is almost always a free way to get in

8

turnstile control boxes open... almost everywhere



(9)

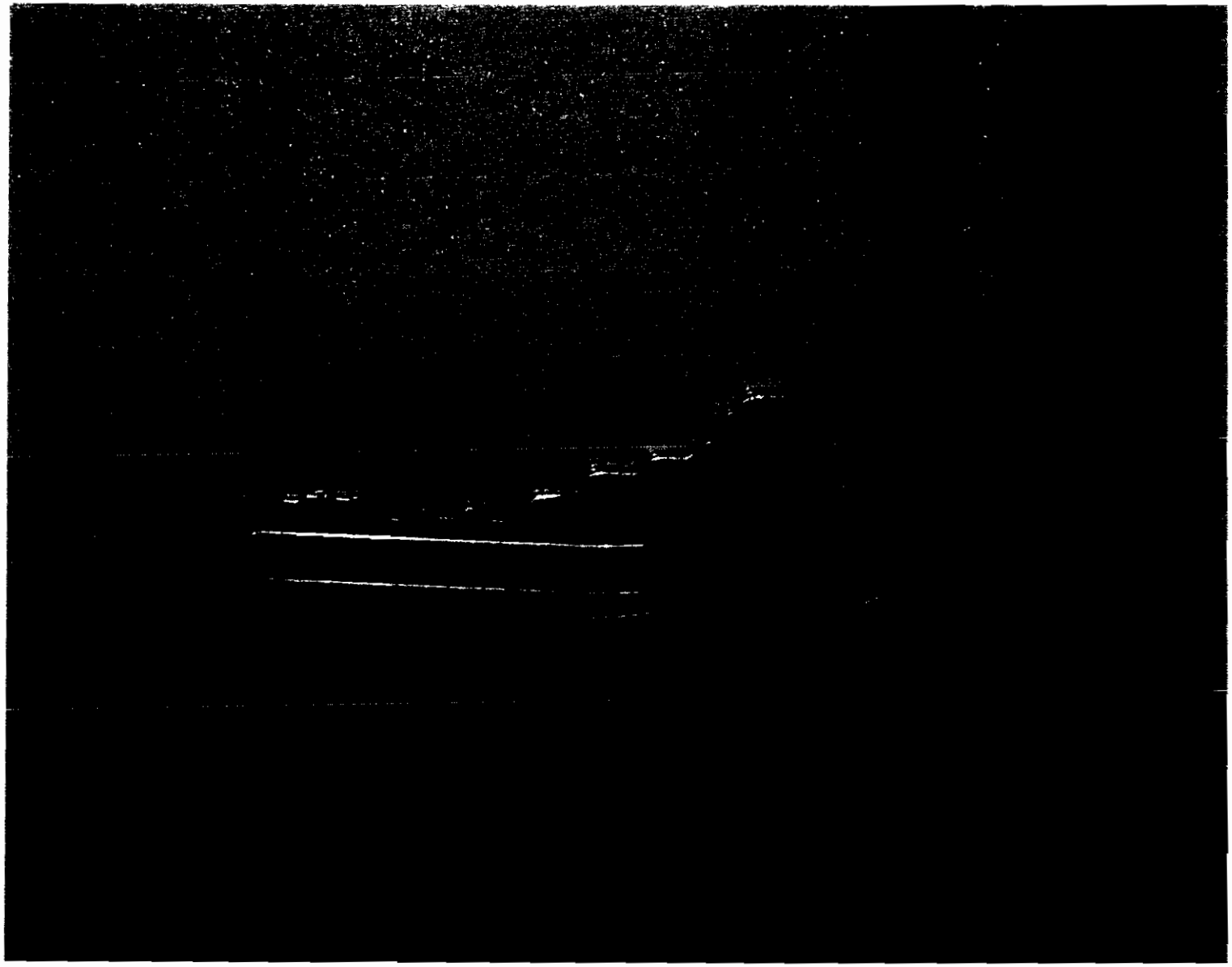
10

computer screens visible through windows

11

door keys left in open boxes

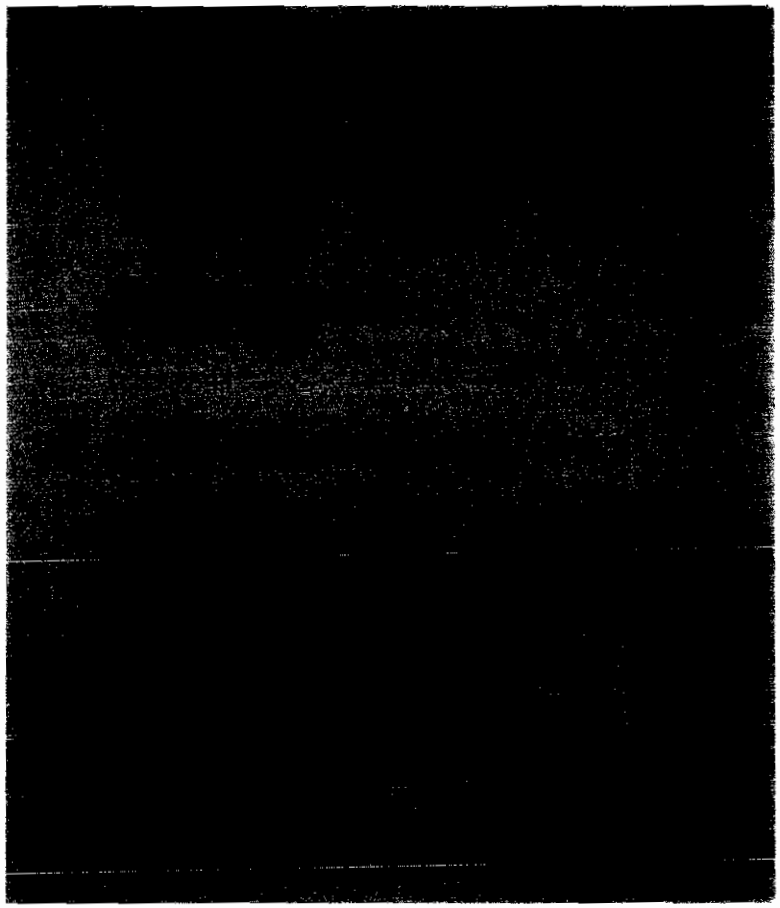
door keys left in open boxes

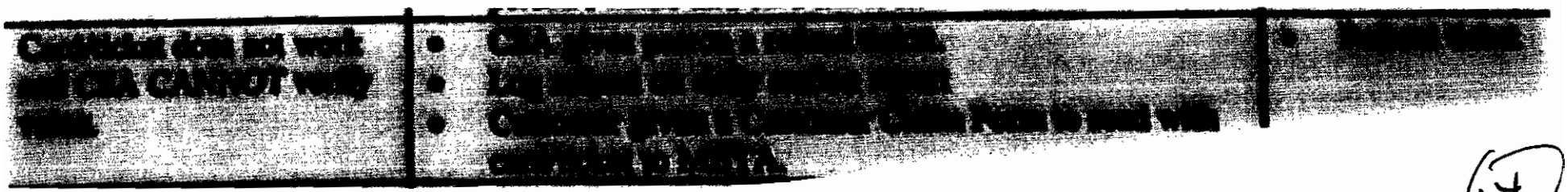


(12)

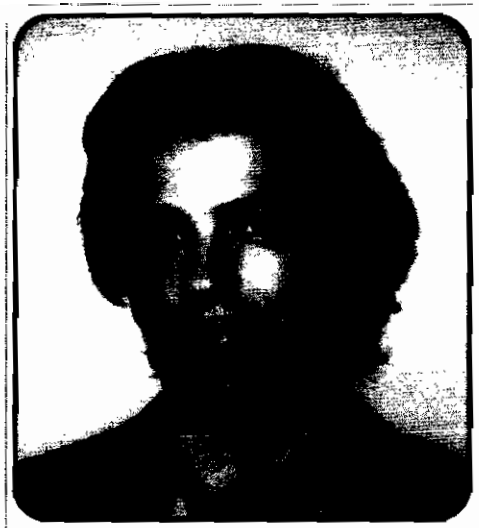
state-of-the-art surveillance... often unattended

documents left in the open





(17)



Employee

Zackary Anderson
Director of Operations,
Red Line
10 Park Plaza

Expires 04/27/2010
5 - 1979832024

Emp. #
9358211

15

ebY Sign in

Categories ▾ Motors Express Stores

Back to list of items Listed in category: Computers & Networking > Printers

Fargo DTC515 Thermal Card Printer

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

1 of 2

View larger picture

Current bid:	**US $79.99**
Your maximum bid:	**US $** [ ] Place Bid > (Enter US $80.99 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

16

what we found on Ebay

17

ATTACK THE MAGCARD

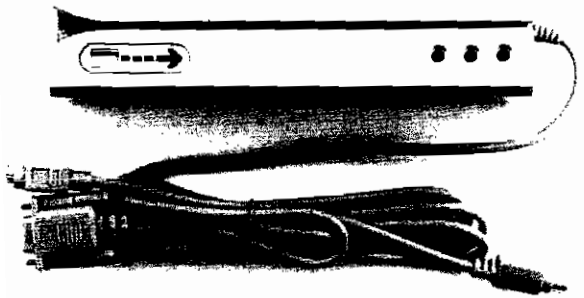
pick the hardware

$5<

Homebrew reader

With inserts, can read 3-tracks

stripesnoop.sourceforge.net

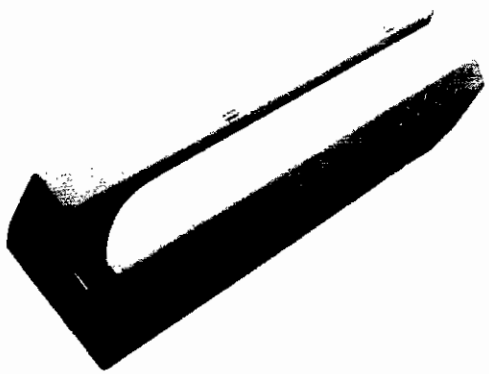


$139.95

Spark Fun Electronics

3-Track Lo-Co

Includes source code



$300

MSR206 or MAKStripe

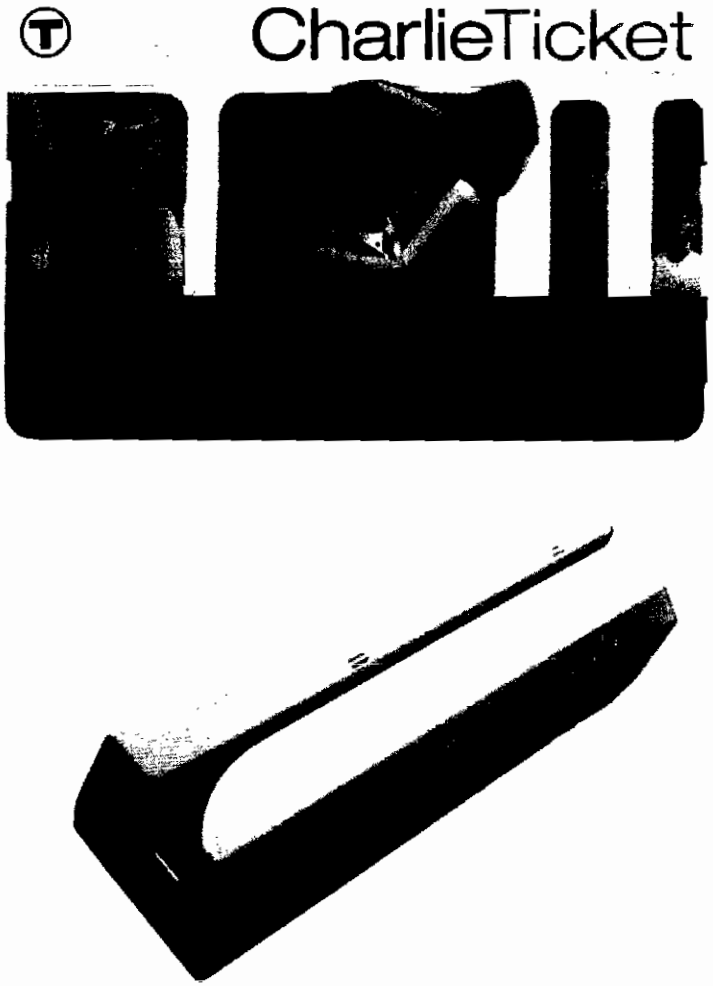
3-Track Hi/Lo-Co

Works with our GPL'd software

20

12

27



EC9010402AC9D000000005B800C80150342248A
84EBD132BE10280002000000002025D0000FD60

23

Is value stored on the card?

try a cloning attack

If yes, then

you now have free subway rides for life

24

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

27

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

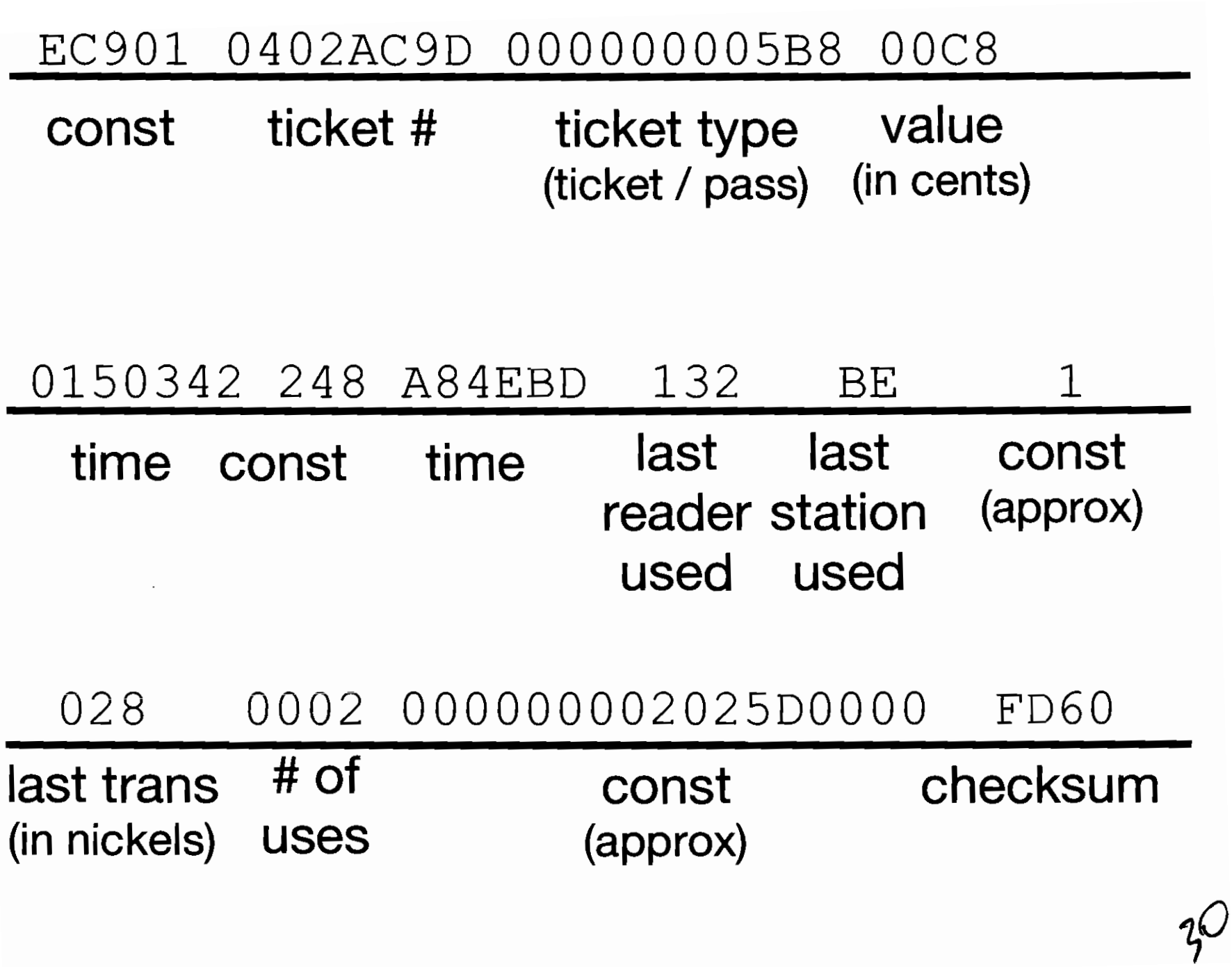
28

EC901 0402AC9D 000000005B8 00C8

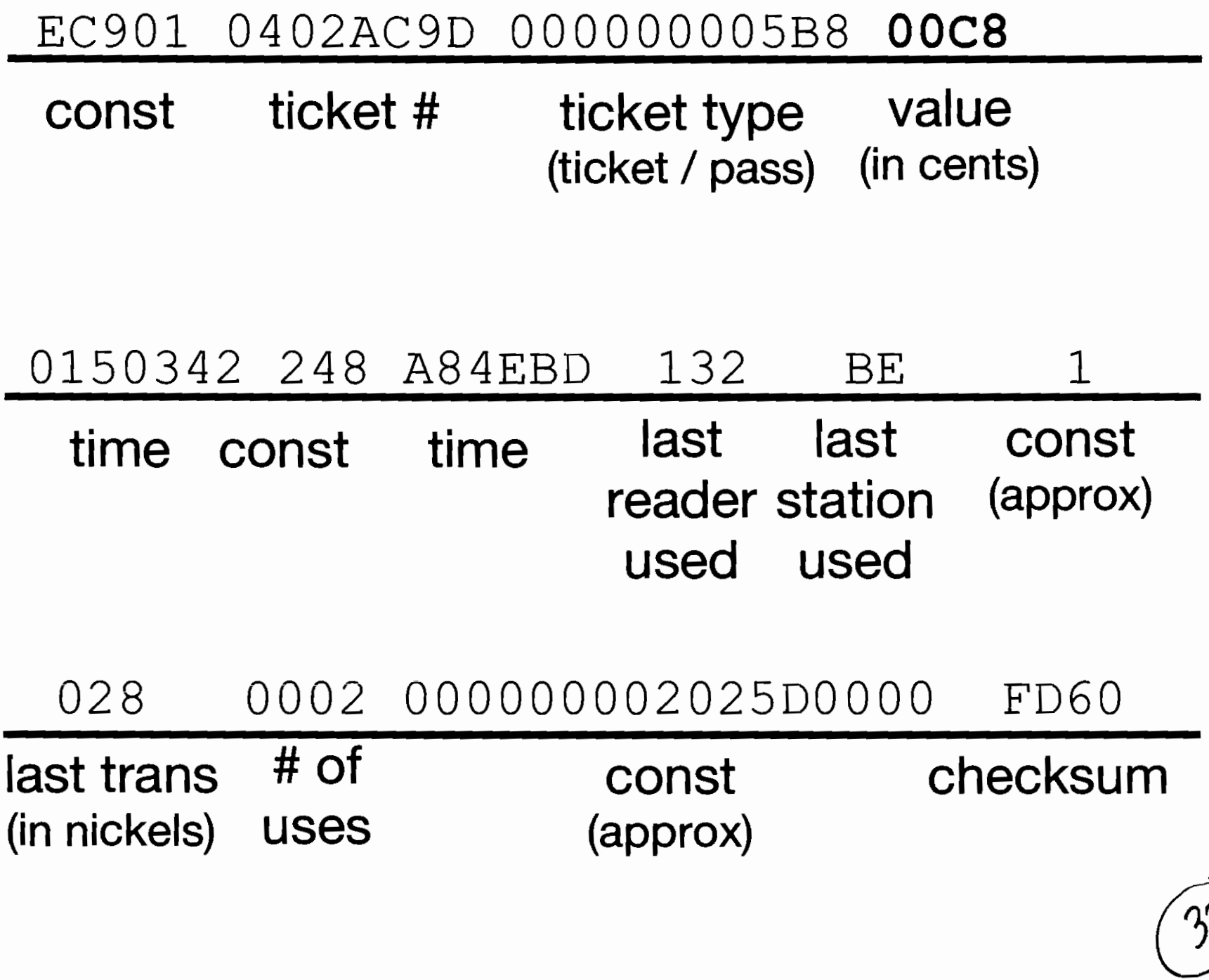
0150342 248 A84EBD 132 BE 1

028 0002 000000002025D0000 FD60

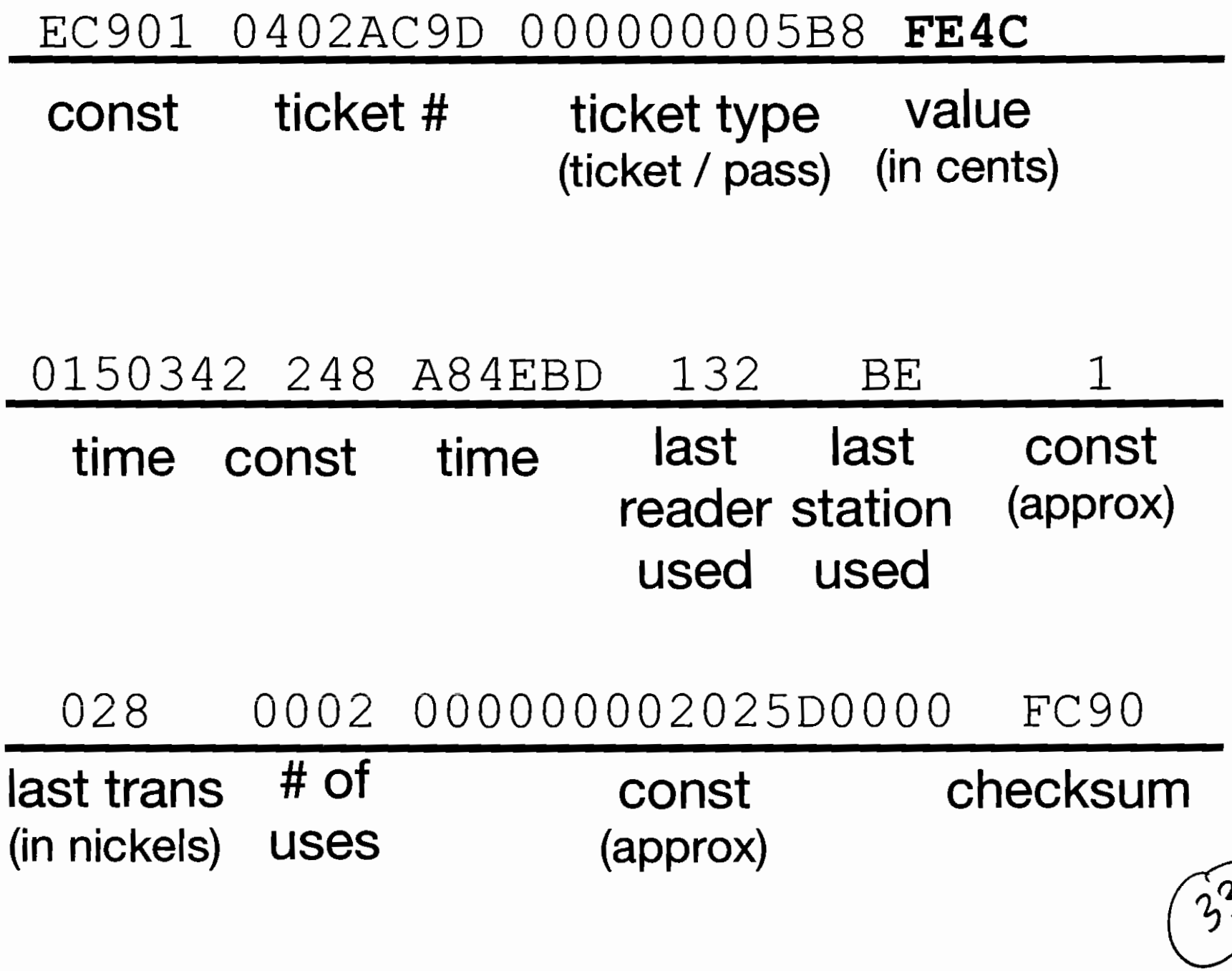
29

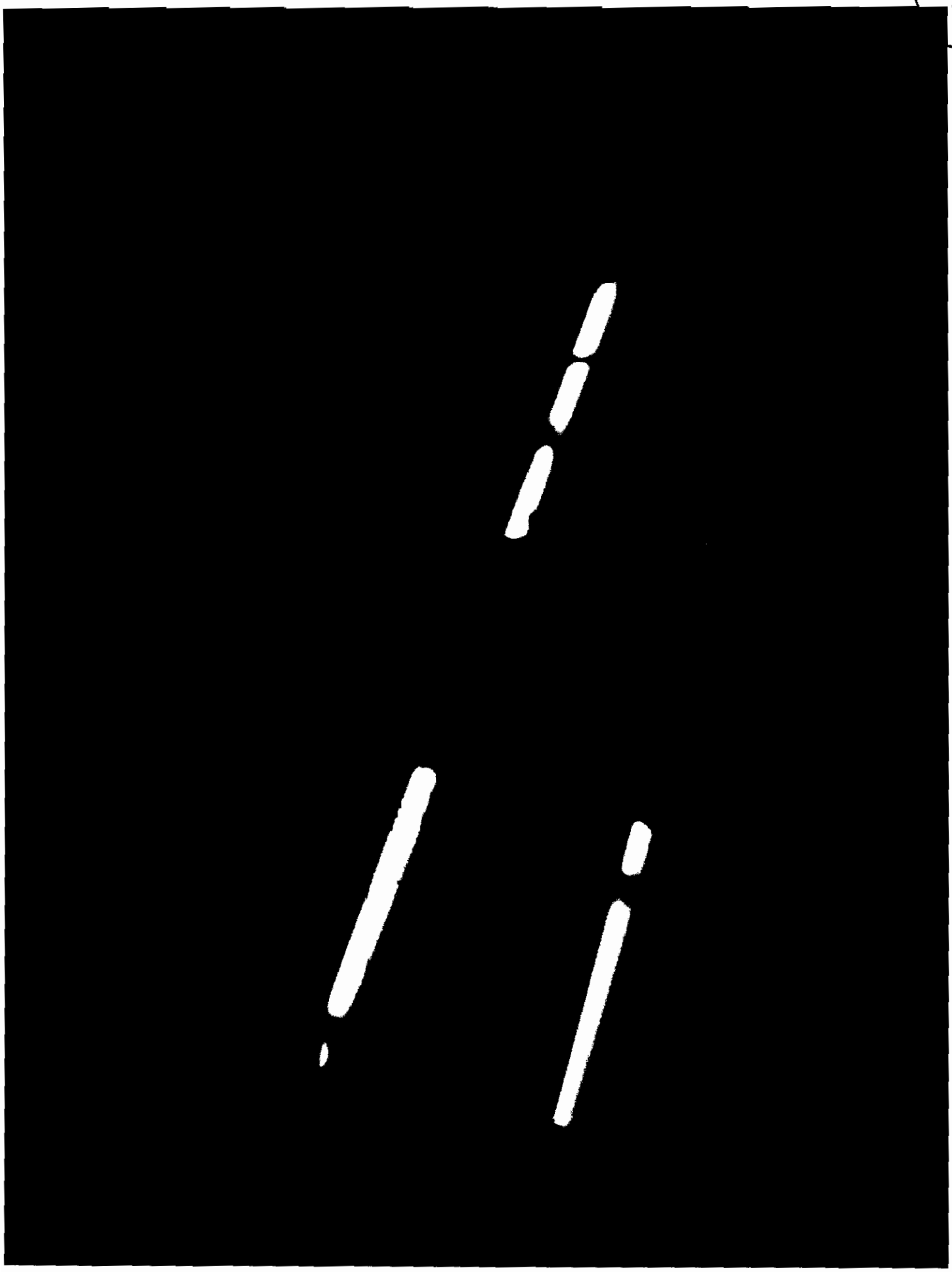


forging
The Charlie Ticket



32





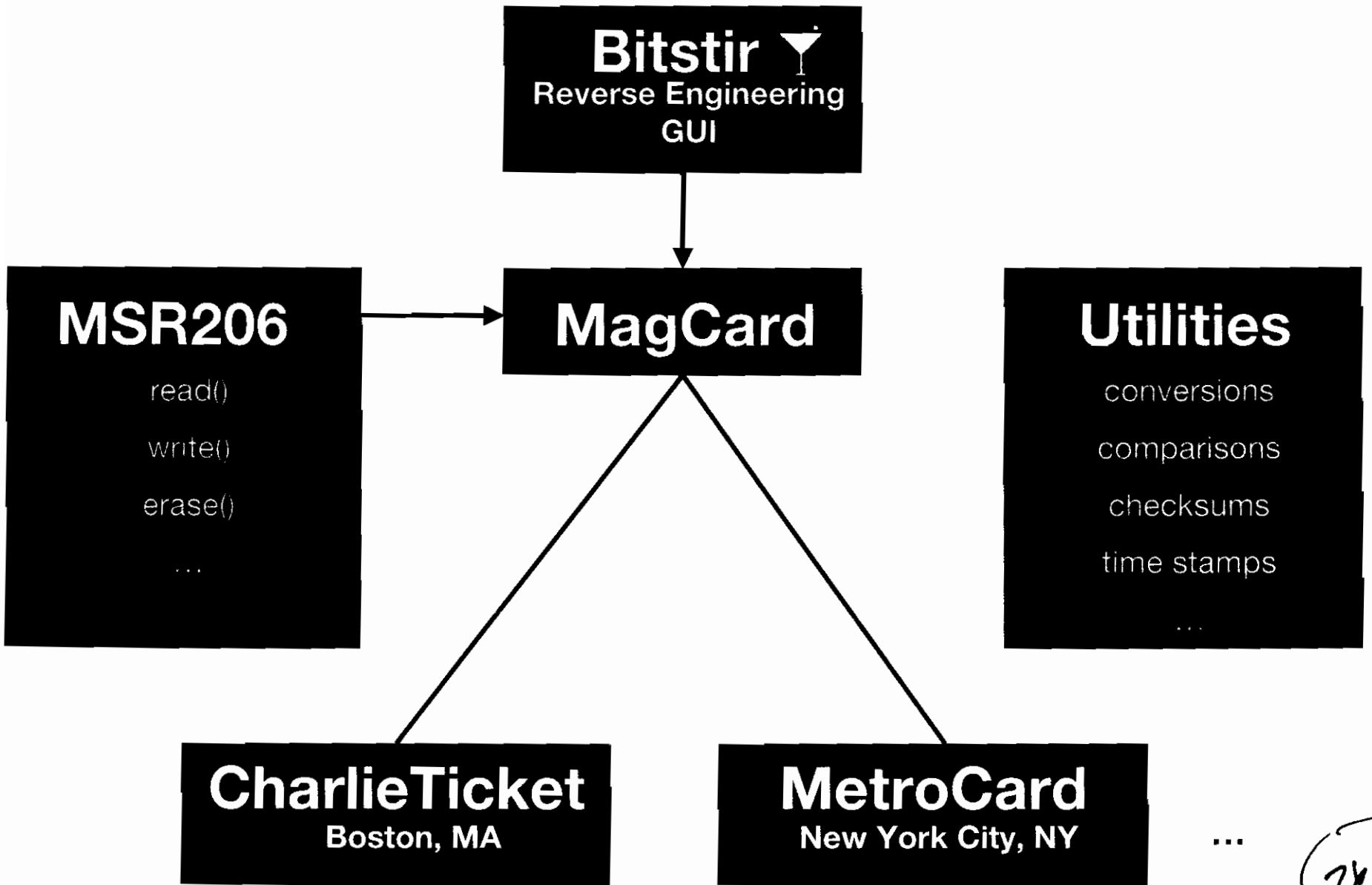
Stored Value
CharlieTicket
Initial Value = 100.00
Ticket-No: 1 - 07
Cash
06/29/2008 06:45 PM
Subject to applicable tariff regulations and conditions of use. Ticket may be confiscated for misuse. Not replaceable if lost or stolen. Non-refundable.
100.00
Kendall/ MIT
Dec/ice: 20114
Schedule & Fare Information: 617-222-3200 Website: www.mbta.com © MBTA
Massachusetts Bay Transportation Authority

=

+

ADULT
Stored Value
NOT VALID FOR TRANSFER
Initial Value = 1.25
Cash
08/25/2006 01:17 PM
Subject to applicable tariff regulations and conditions of use. Ticket may be confiscated for misuse.
1.25
Kendall/ MIT
Dec/ice: 20114
Schedule & Fare Information: 617-222-3200 Website: www.mbta.com © MBTA
Massachusetts Bay Transportation Authority

MagCard Reverse-Engineering Framework



Demo: MagCard and Reverse Engineering Toolkit

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

37

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!

38

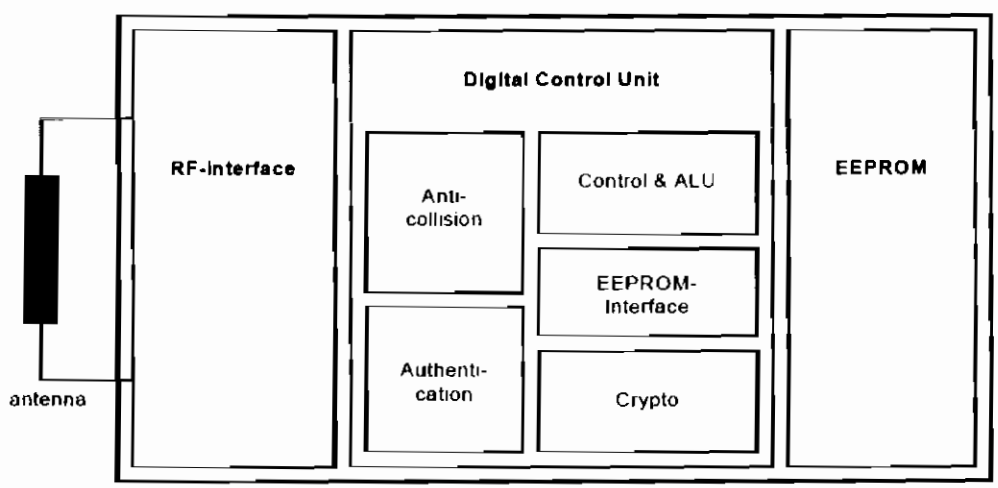
ATTACK THE RFID

9

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

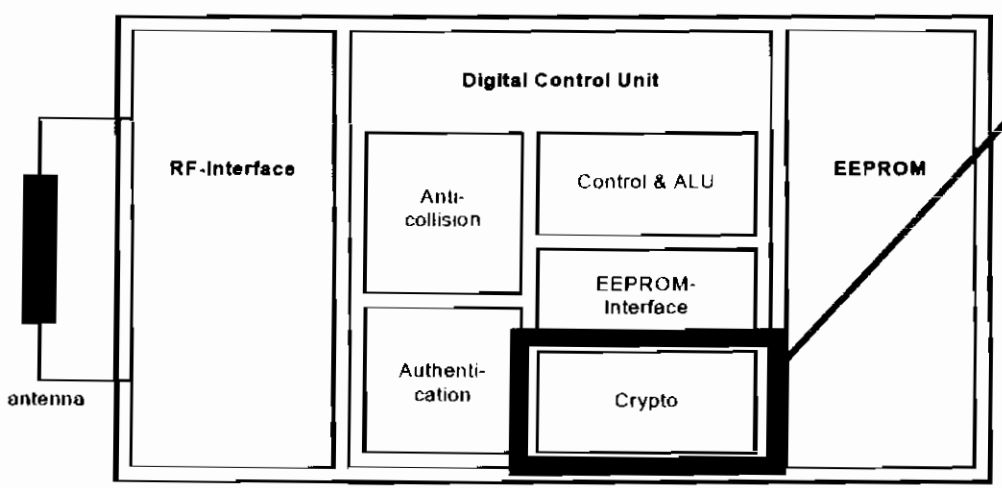


41

Crypto-1 Cryptanalysis

Crypto-1 reverse engineered by Karsten Nohl, University of Virginia, 2007:

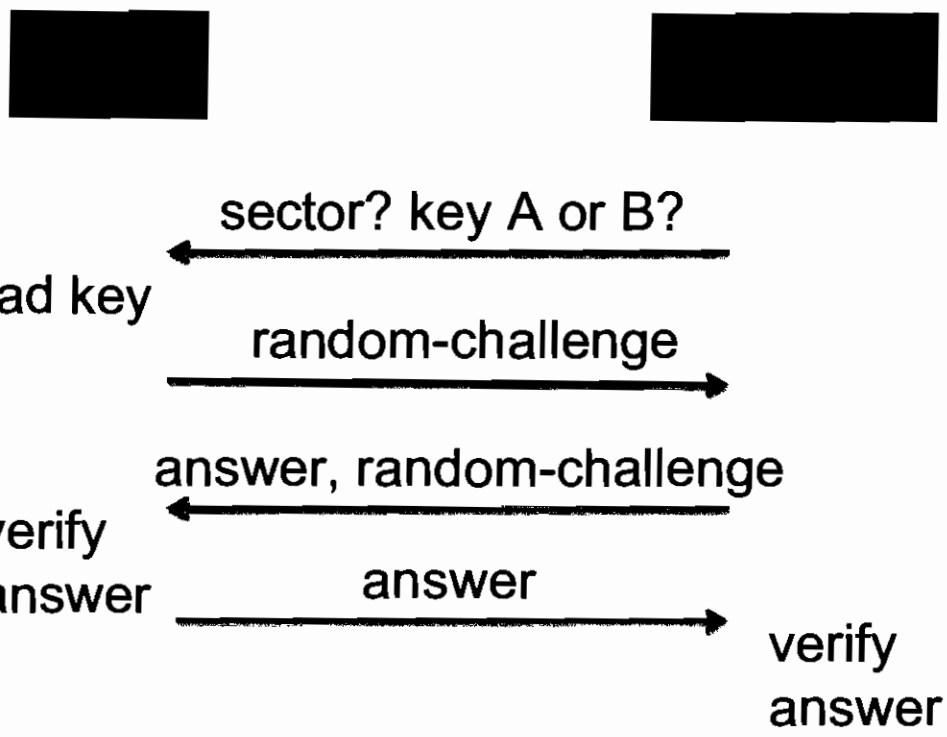
- Etched and inspected silicon wafer using high-powered imagery.
- Found and reconstructed crypto portions from over 10k gates.
- Found vulnerabilities in the cipher and implementation



42

security of the MIFARE card

Mutual 3-pass authentication



Each sector two keys

Non-linear filter functions

13

security of the MIFARE card

Mutual 3-pass authentication

[redacted] [redacted]

sector? key A or B?

read key

random-challenge

answer, random-challenge

verify answer

answer

verify answer

[redacted]

Non-linear filter functions

44

security of the MIFARE card

[redacted]

[redacted]

[redacted]

Non-linear filter functions

45

security of the MIFARE card

[redacted]

[redacted]

[redacted]

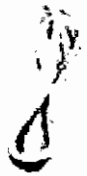
[redacted]

46

to execute these attacks we need to interact with the card

choose your hardware

47

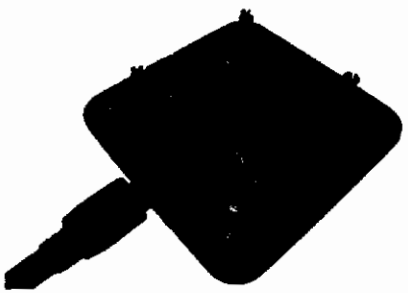


$50

MiFare RFID Reader/Writer

Comes with source code

Hard to hack, but doable

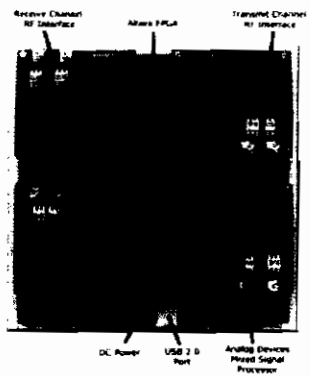


$220

OpenPCD + OpenPICC

Open design 13.56MHz RFID reader + emulator

Free schematics (www.openpcd.org)



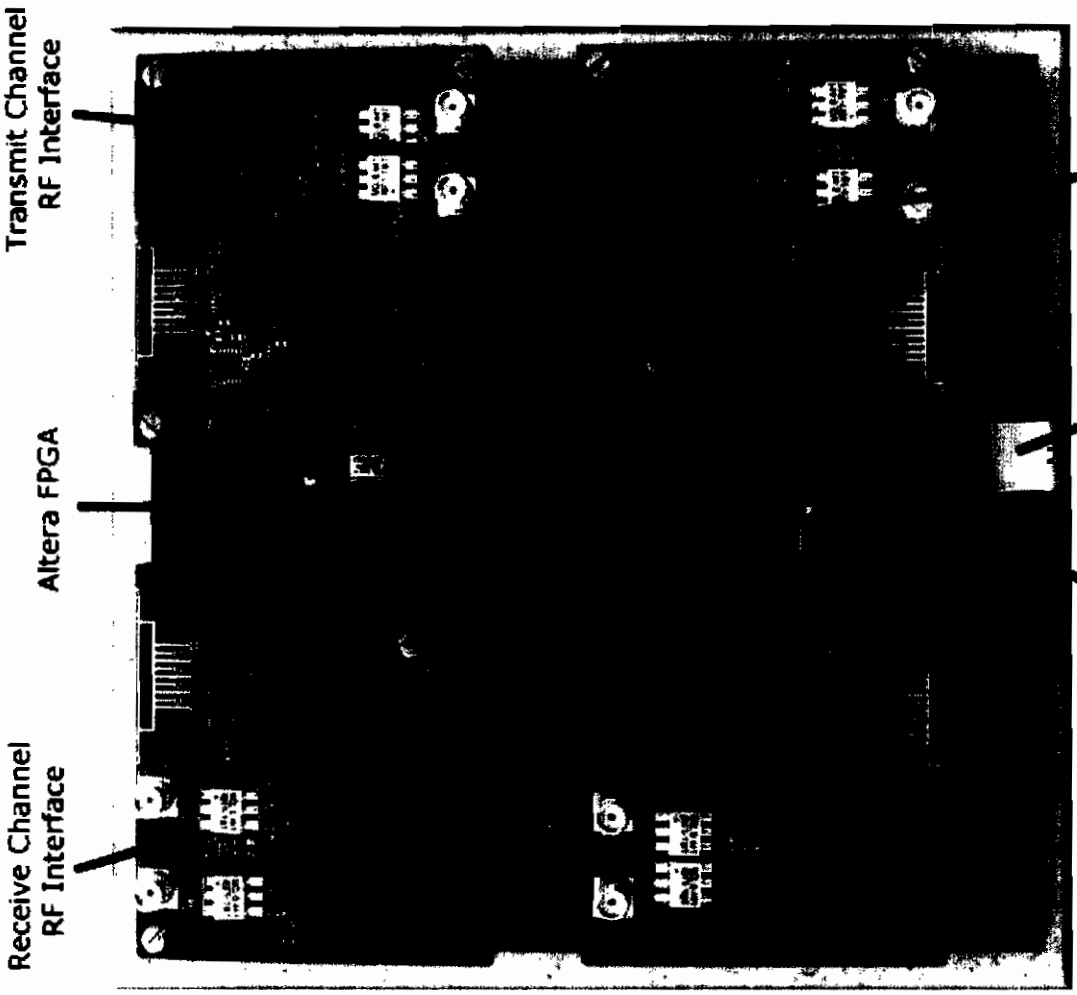
$700

USRP

Full control over signal input/output

Works with GNU Radio + our plugin

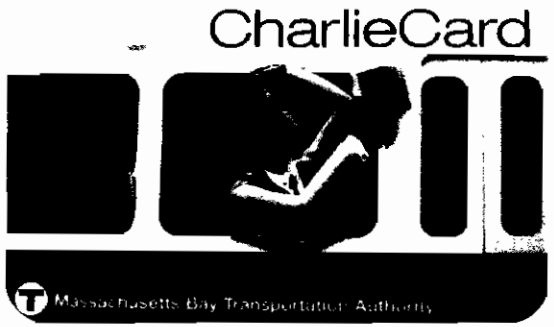
48


Transmit Channel
RF Interface
Altera FPGA
Receive Channel
RF Interface
Analog Devices
Mixed Signal
Processor
USB 2.0
Port
DC Power

USRP

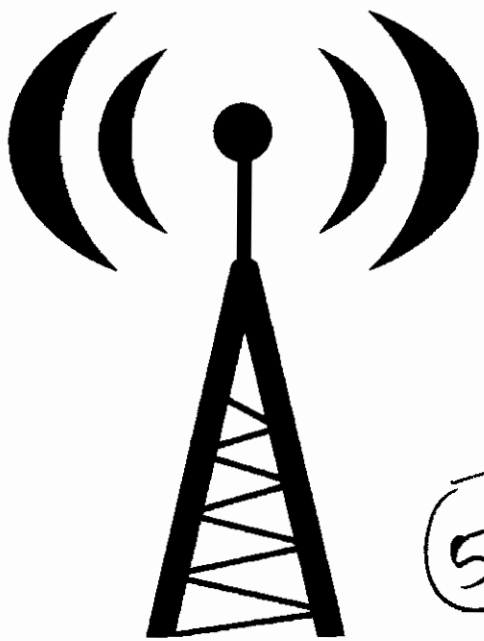
49

card/reader communication



13.56MHz
ASK modulation
Modified miller encoding

13.56MHz
+/- 847kHz
OOK modulation
Manchester encoding

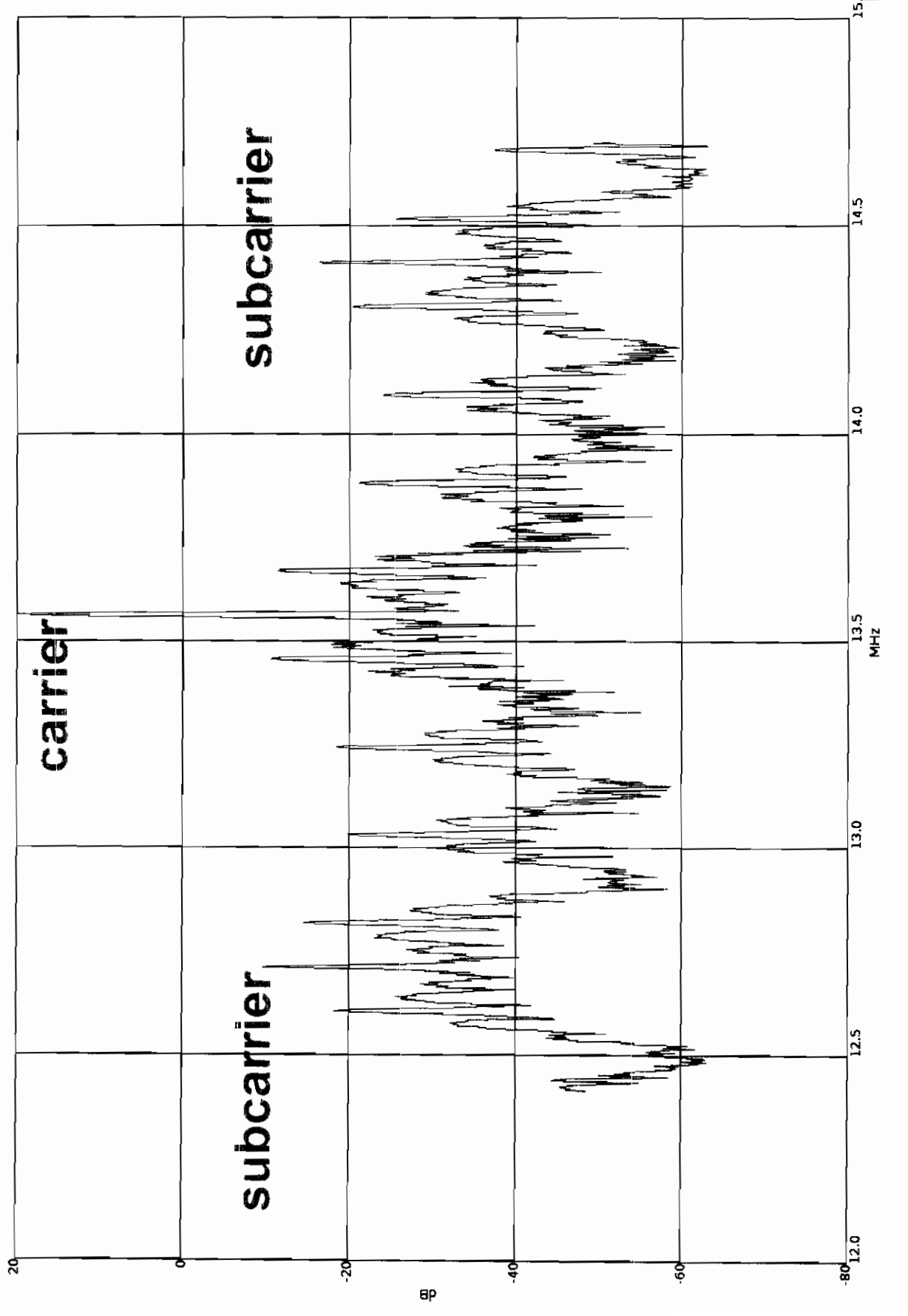


59

GNU radio RFID toolchain

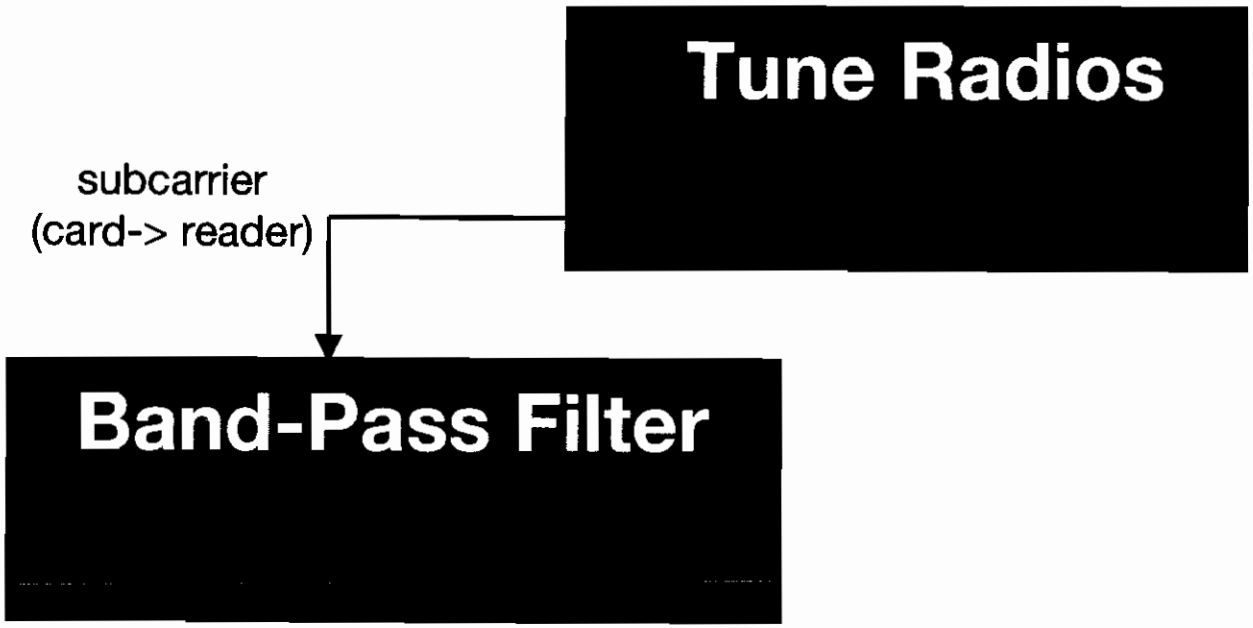
Tune Radios

charlie card + reader FFT

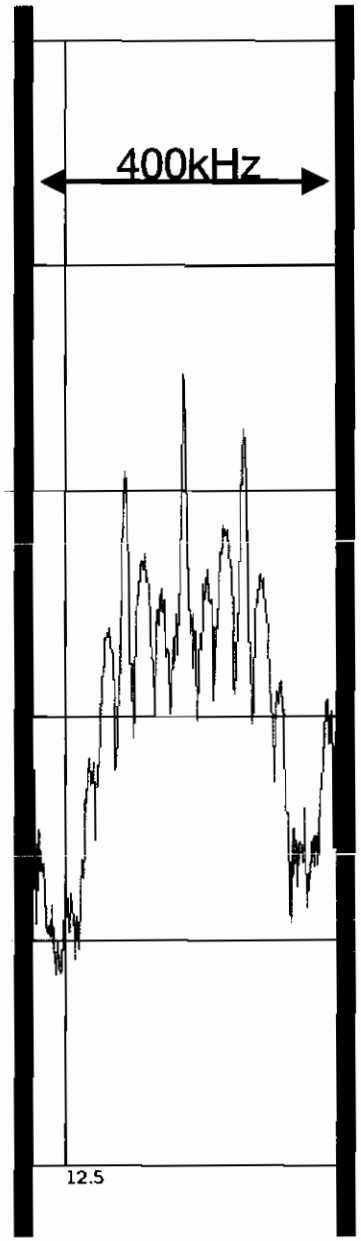


52

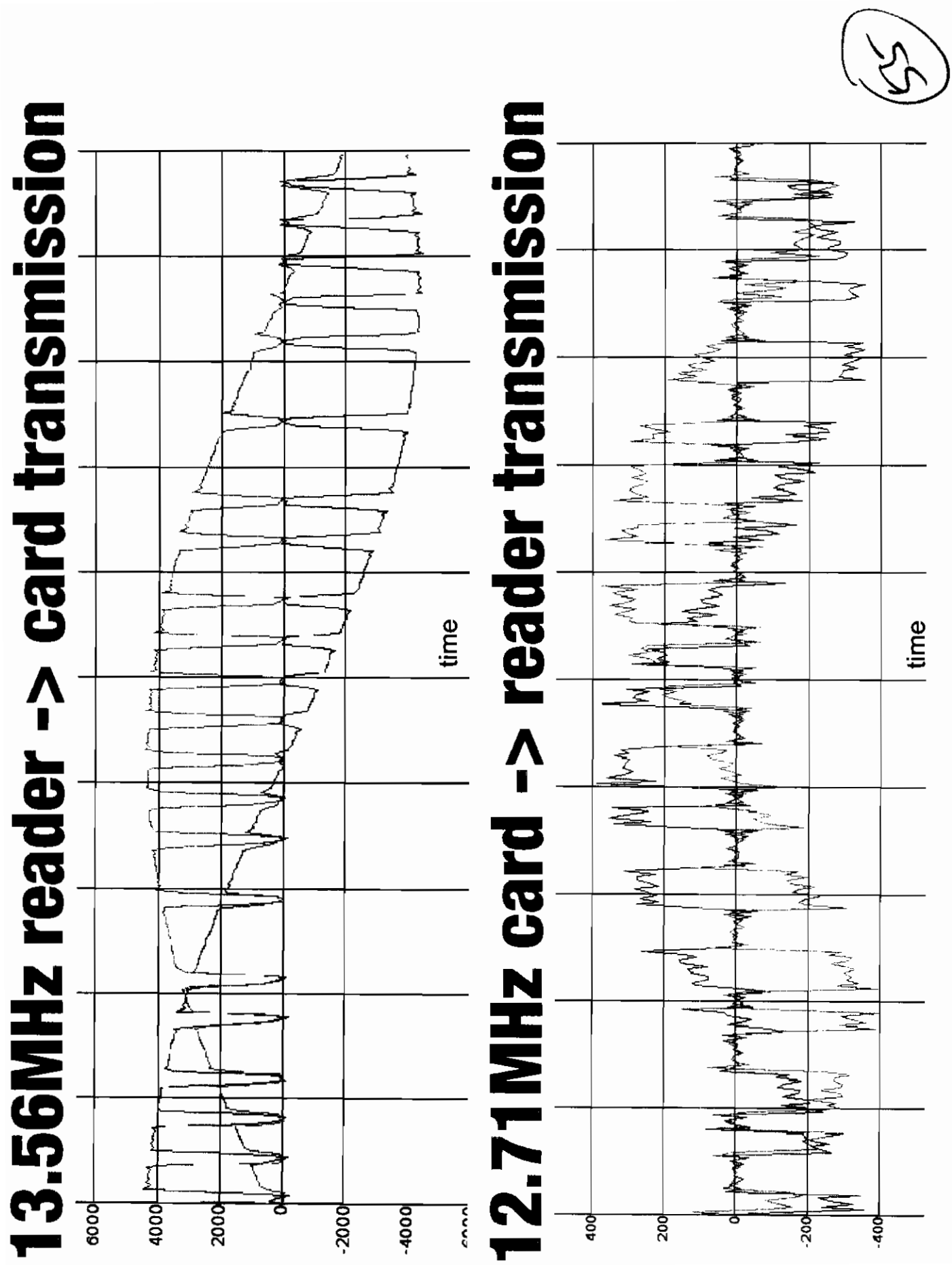
GNU radio RFID toolchain



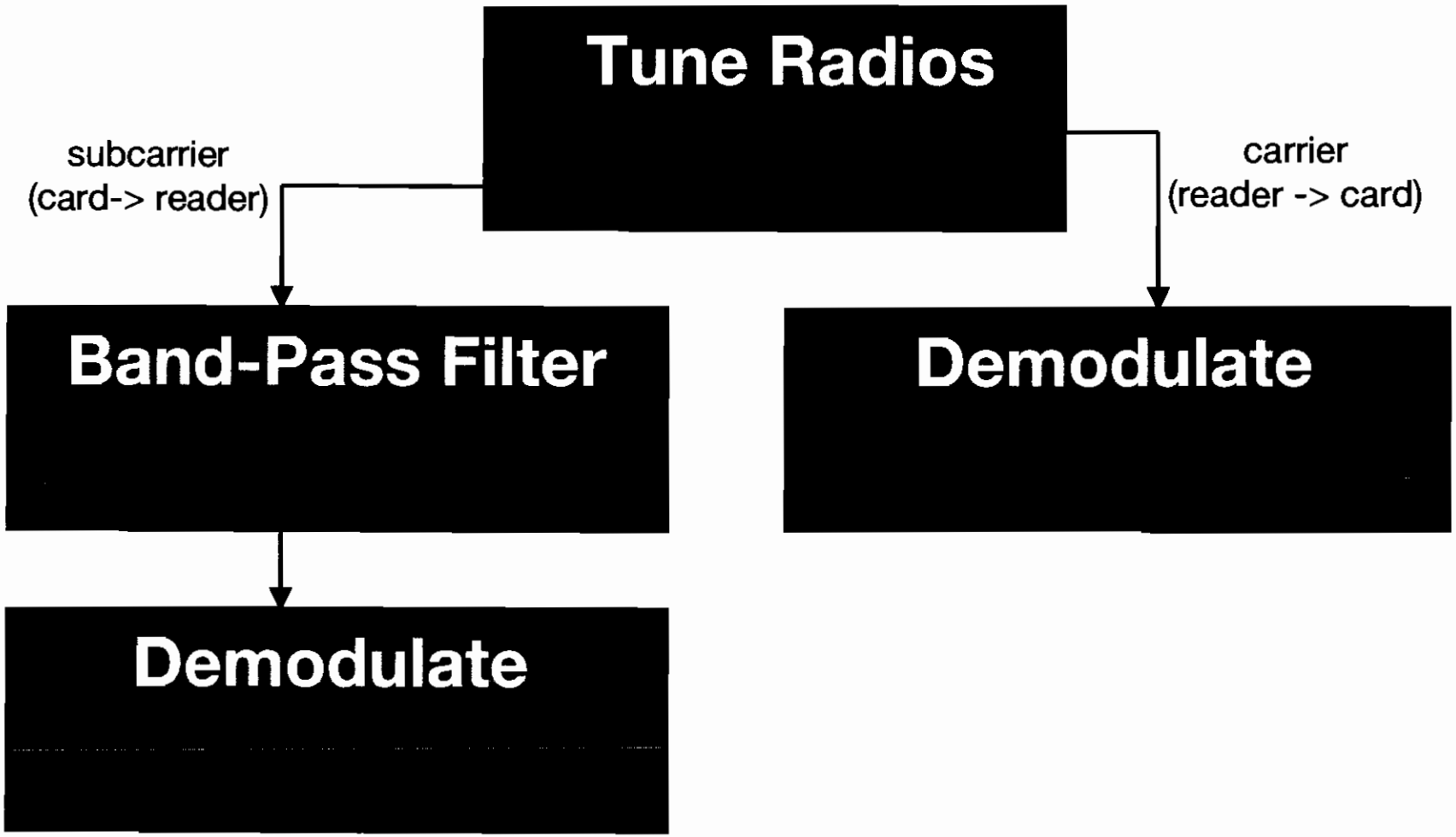
charlie card + reader FFT



Band Pass Filter

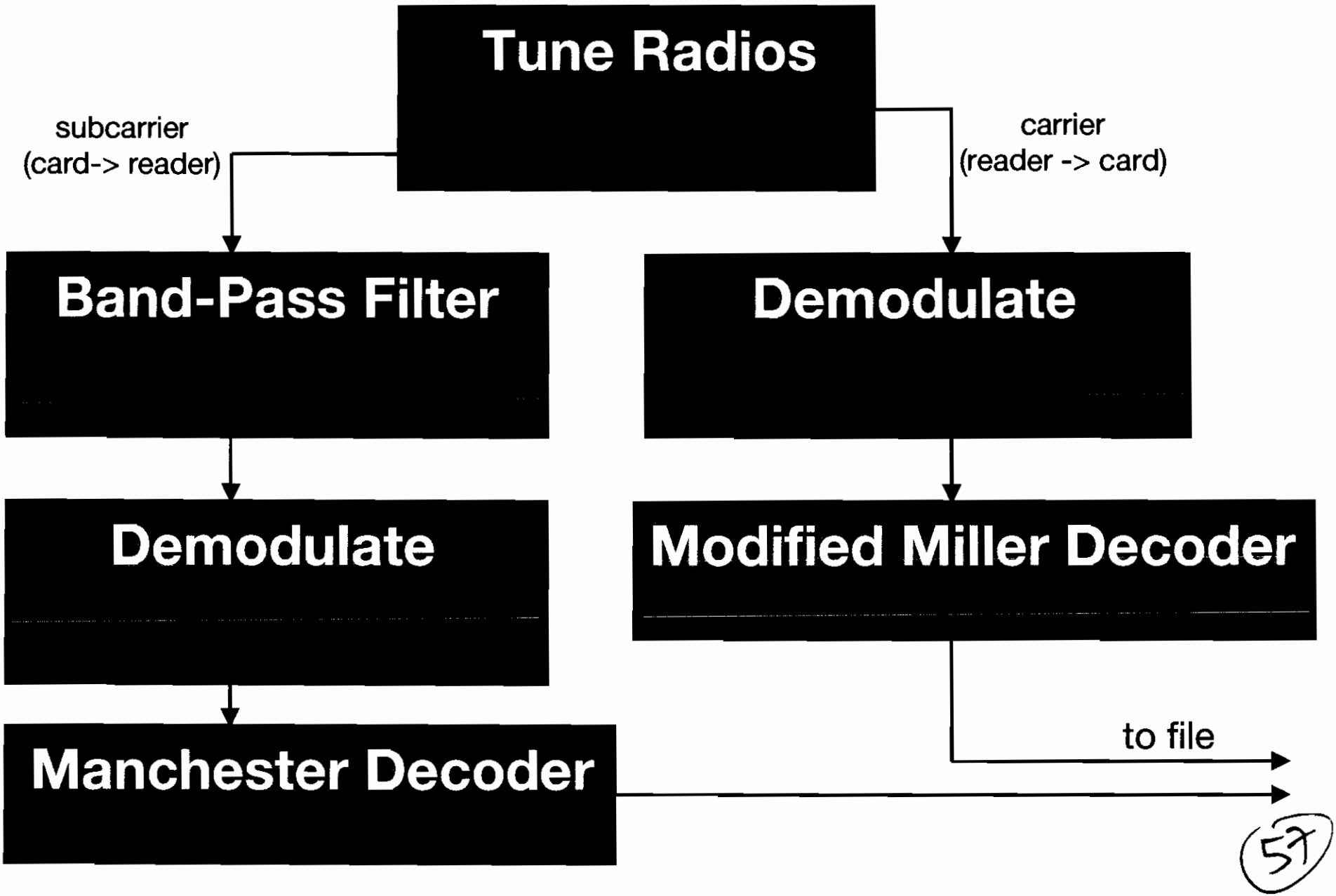

13.56MHz reader -> card transmission
time
6000
4000
2000
0
-2000
-4000
12.71MHz card -> reader transmission
time
400
200
0
-200
-400

GNU radio RFID toolchain

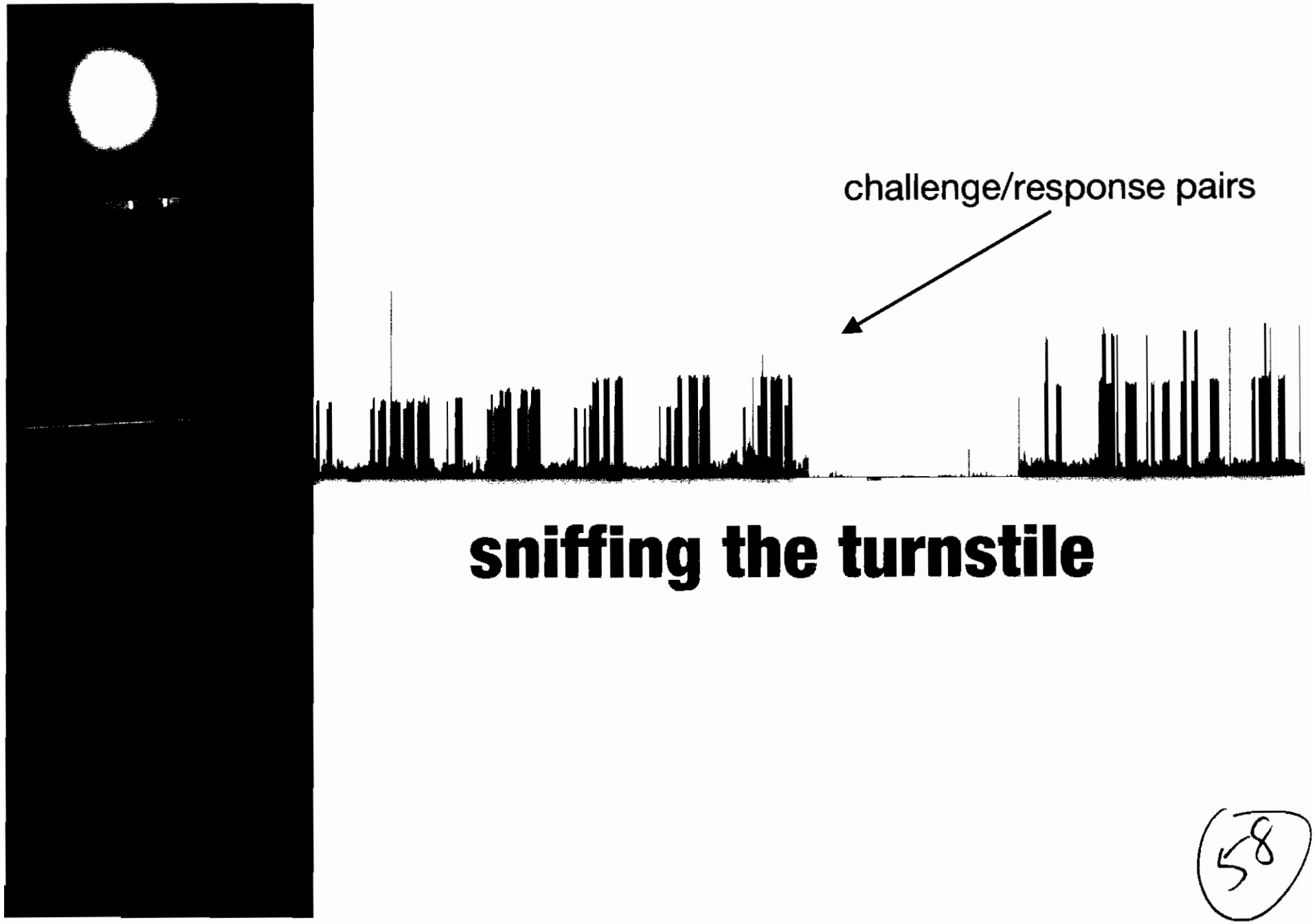


56

GNU radio RFID toolchain



57



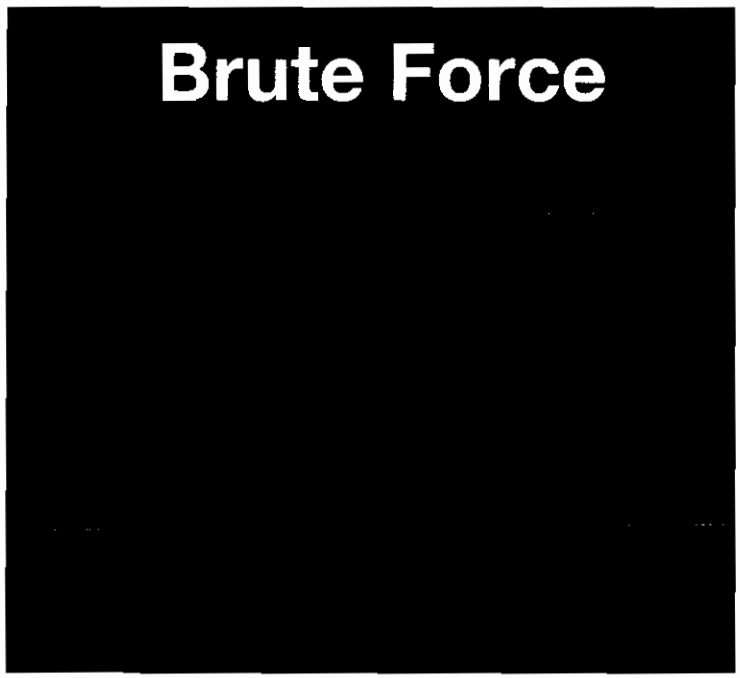
sniffing the turnstile

58

attacks on the MIFARE card

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

Brute Force



59

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

61

when all else fails

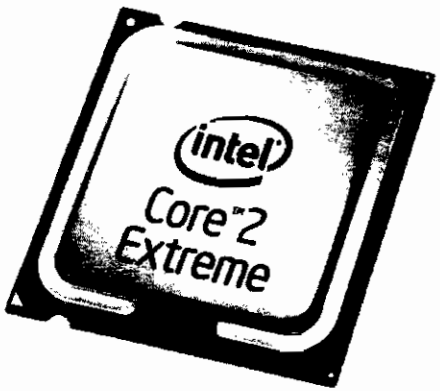
brute force it

62

Why Brute Force with an FPGA?

Because it's fast!

microprocessor



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

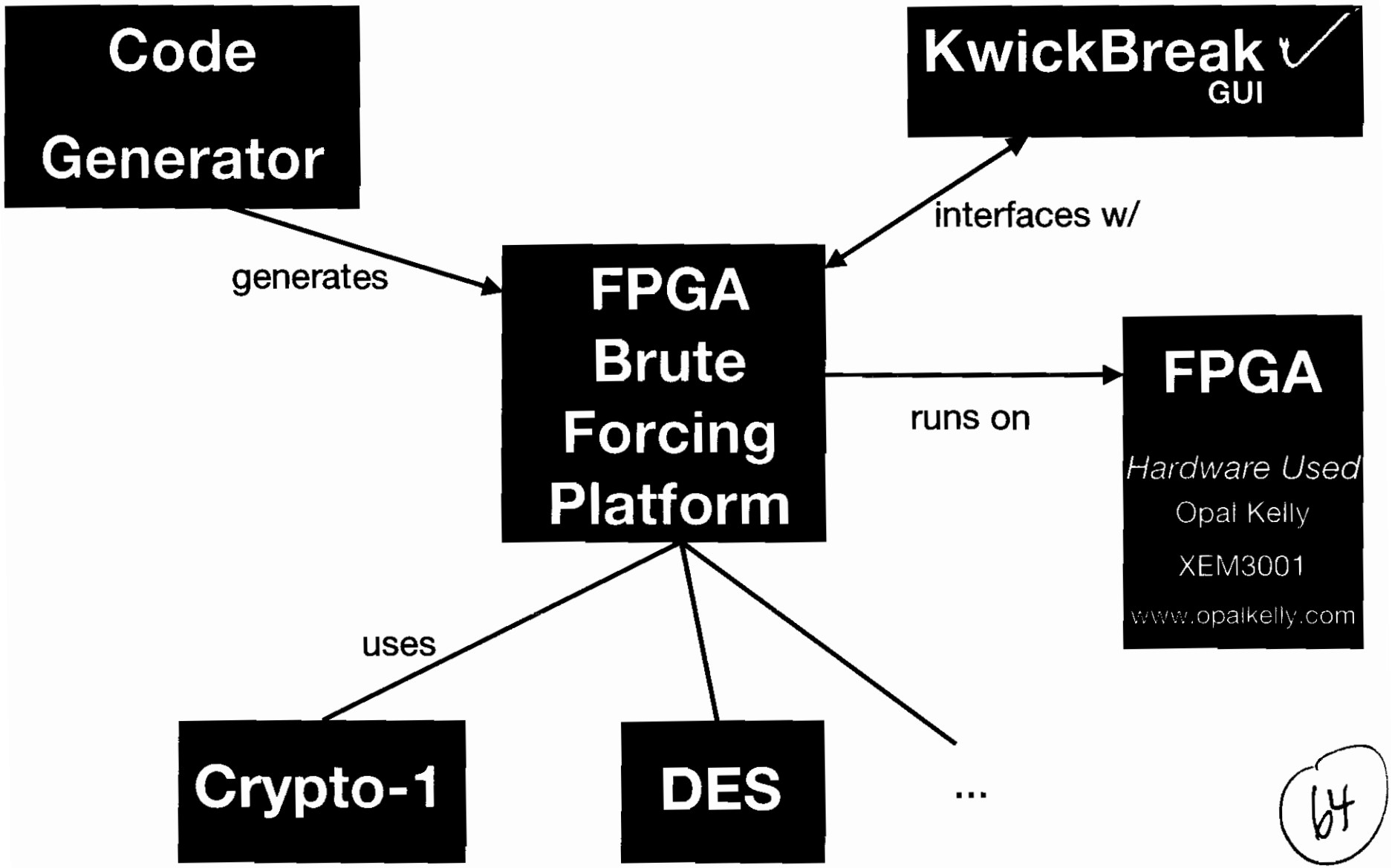
FPGA

- Dedicated logic
- Hardware description language defines hardware
- Hundreds of parallelizations

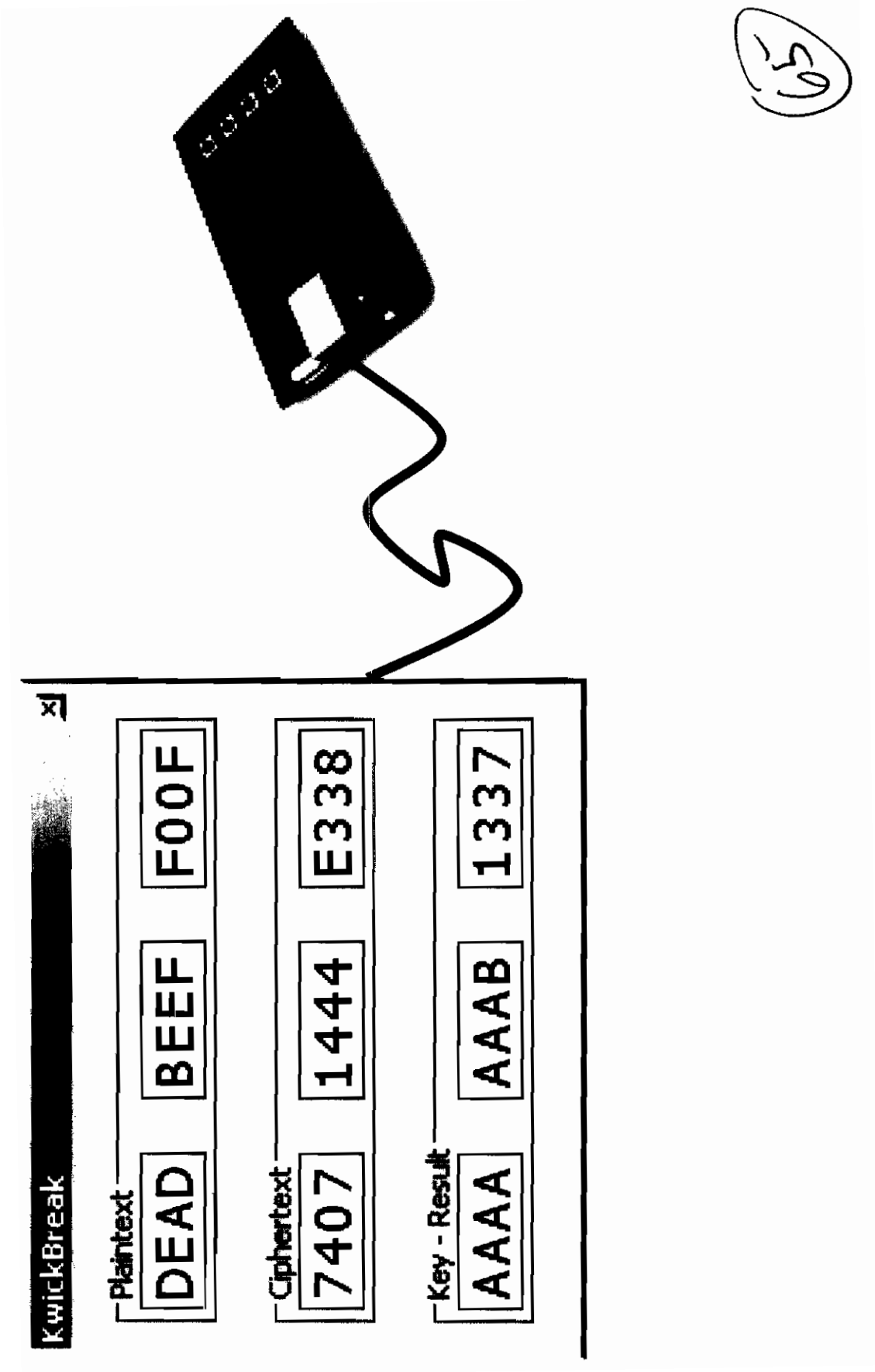
63

KwickBreak FPGA Brute-Forcer

Executes known plaintext attack to recover key



64


KwickBreak
Plaintext
DEAD
BEEF
F00F
Ciphertext
7407
1444
E338
Key - Result
AAAA
AAAB
1337

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
```

66

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!

67

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

68

69

ATTACK THE NETWORK

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

21

fiber switches in unlocked room

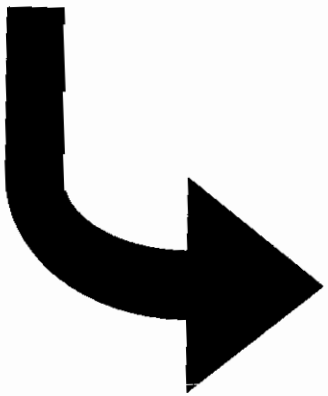
connect fare vending machines to the internal network

[redacted]

72

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.

73

first there was **wardialing**

c.**1983** - 2000 – 2001 – 2002 – 2006 – 2007 - 2008

74

then there was **wardriving**

c.1983 - **2000** – 2001 – 2002 – 2006 – 2007 - 2008

25

then there was **warwalking**

c.1983 - 2000 – **2001** – 2002 – 2006 – 2007 - 2008

26

then there was **warflying** and **warboating**

c.1983 - 2000 – 2001 – **2002** – 2006 – 2007 - 2008

77

then there was **war-rocketing**

c.1983 - 2000 – 2001 – 2002 – **2006** – 2007 - 2008

78

then there was **warballooning**

c.1983 - 2000 – 2001 – 2002 – 2006 – **2007** - 2008

79

80

and now... warcarting

c.1983 - 2000 – 2001 – 2002 – 2006 – 2007 - **2008**

WarCart

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

19dBi WiFi Antenna
directional

Two Laptops
for control and data logging

12dBi WiFi Antenna
omnidirectional

Scanner
to pick up various communications

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

Control Box
w/ key switch for activation

CCD Camera
trip documentation

Antenna Switch Box
To toggle between antennas and radios

Lights
2M candlepower for night operations

Flash Drive Dropper
for U3 hacksaws

PA Speaker
For announcements and intimidating music

900 MHz Antenna
directional, great for cordless phones

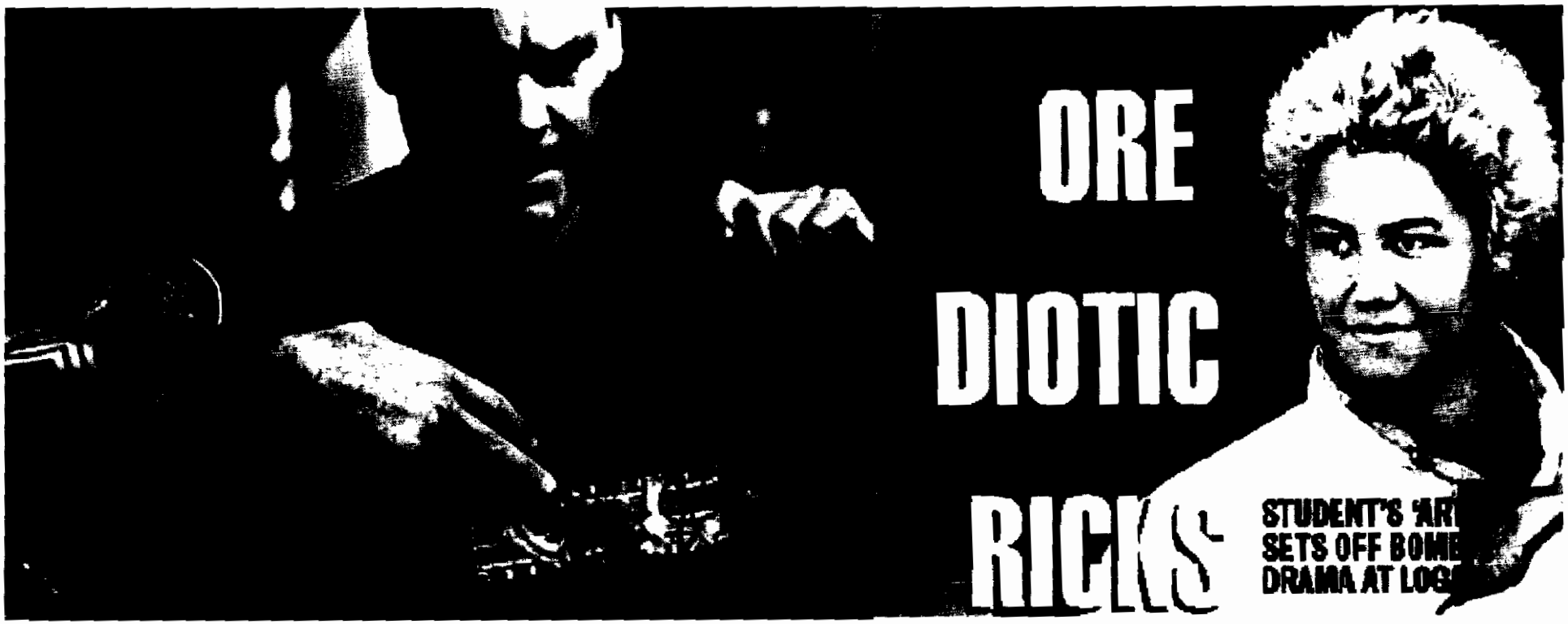
81

28

And then we ran into some problems with the police

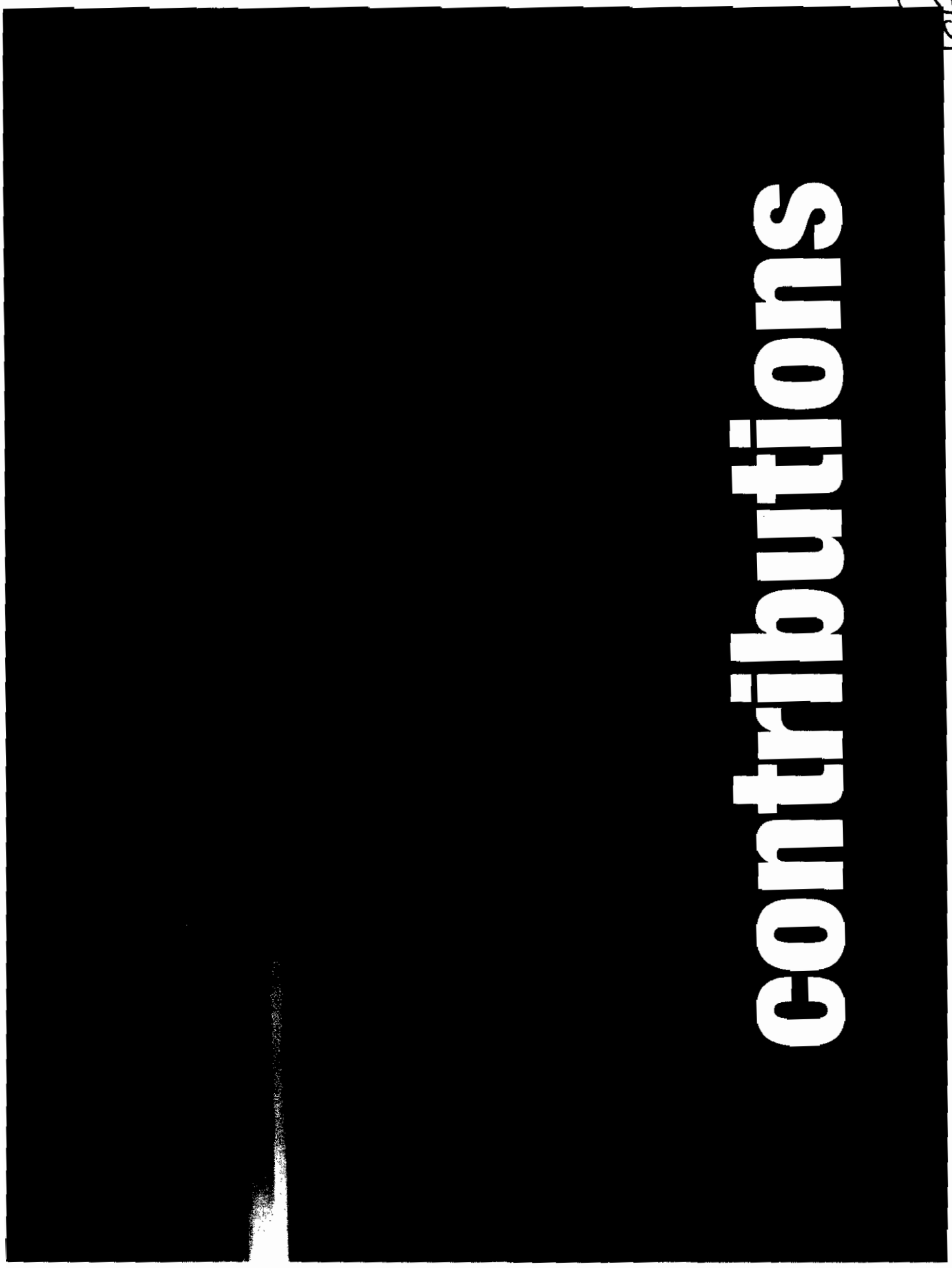
That's one of the WarCart's smoke grenades, by the way

So to avoid ending up like this



We turned back

64


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)

86

Exhibit 8

Mahony, Ieuan (BOS - X75835)

From: Marcia Hofmann [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

Attachments: defcon-16-anderson-ryan-cheisa.pdf

defcon-16-ander
son-ryan-cheisa..

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

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.
>
>

Exhibit 9

Mahony, Ieuan (BOS - X75835)

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

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.
>
>

Mahony, Ieuan (BOS - X75835)

From: Mahony, Ieuan (BOS - X75835)
Sent: Saturday, August 09, 2008 5:26 AM
To: 'Swope, Jeffrey'
Cc: 'Marcia Hofmann'; kurt@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 become 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.
>
>