The Current State of Hardware Hacking

(even a 2-year-old can do it...)

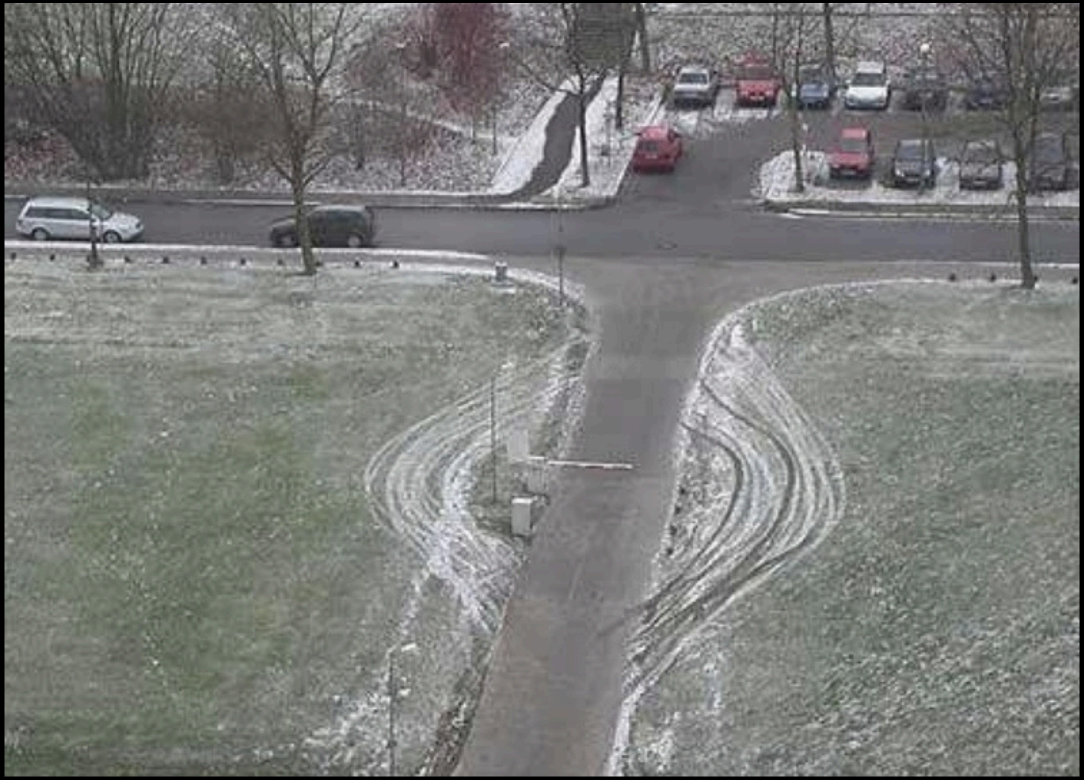
Joe Grand, Grand Idea Studio

joe@grandideastudio.com

Governmental Affairs
Committee
SD-342

We Need to Open Our Eyes...

- Hardware hacks becoming more common
- Not many use new or novel techniques
- Most "security" has been a mere roadblock



We Are Part of the Problem

- Many attacks are so easy that we (engineers & vendors) should be blamed
- We are trained to think like engineers
- We are not trained to think like hackers
- We are constrained by budget and time-to-market
- Security is an afterthought (if at all)
- Our response to hardware attacks is antiquated
  - Knee-jerk reactions
  - Denial of any issue (and refusal to fix it)

Hardware Hacking Areas

- Information Gathering
  - Obtaining data about the target by any means necessary
- Hardware Teardown
  - Product disassembly, component/subsystem identification, modification
- Firmware Reverse Engineering
  - Extract/modify/reprogram code or data
  - OS exploitation/device jailbreaking
- External Interface Analysis
  - Communications monitoring, protocol decoding/emulation
- Silicon Die Analysis
  - Chip-level modification/data extraction

Common Attack Surfaces

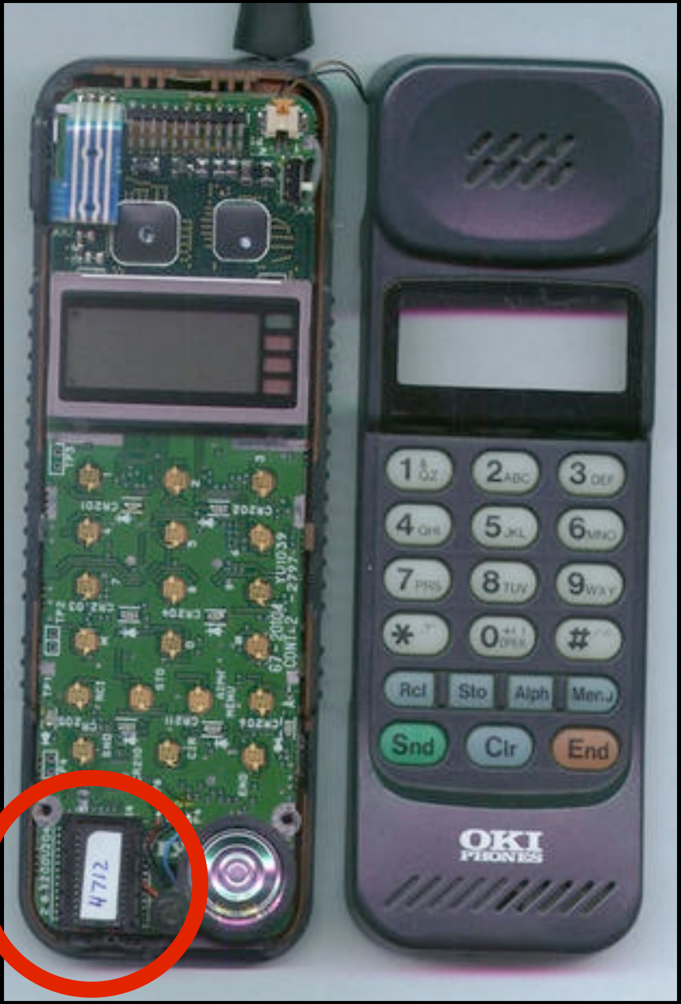
- Memory & Firmware
- Exposed Buses & Interfaces
- Passwords & Cryptography

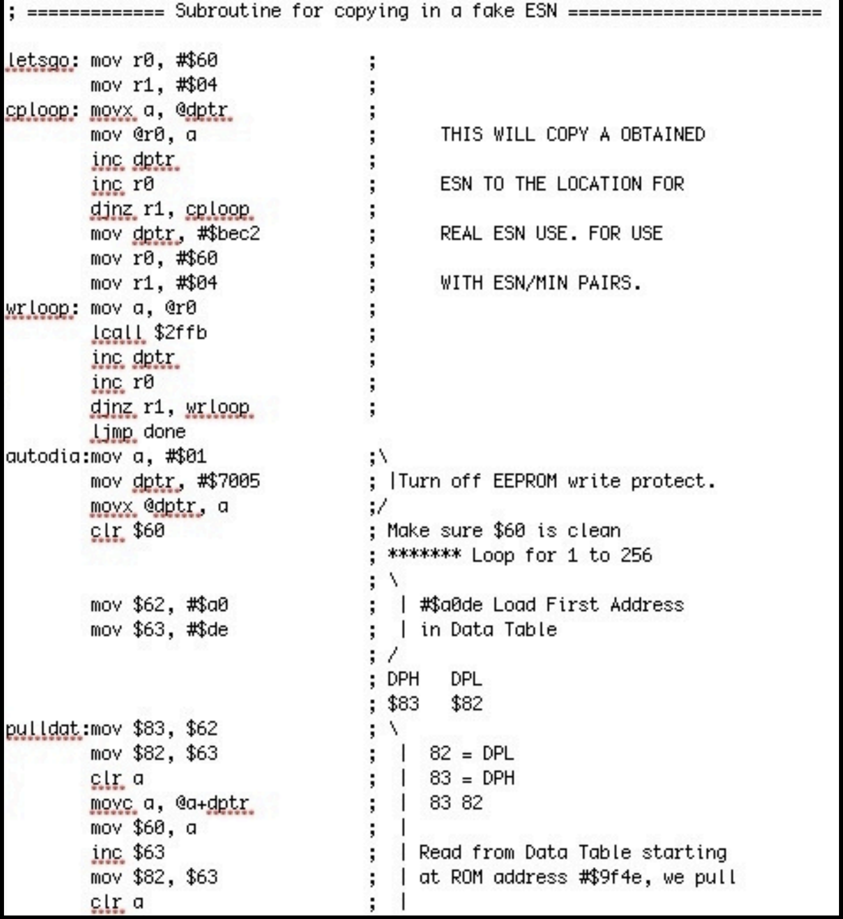
Memory & Firmware

Memory & Firmware

1993: Oki 900 Cellphone Cloning (8051)

www.hackcanada.com/blackcrawl/cell/oki/oki900.html



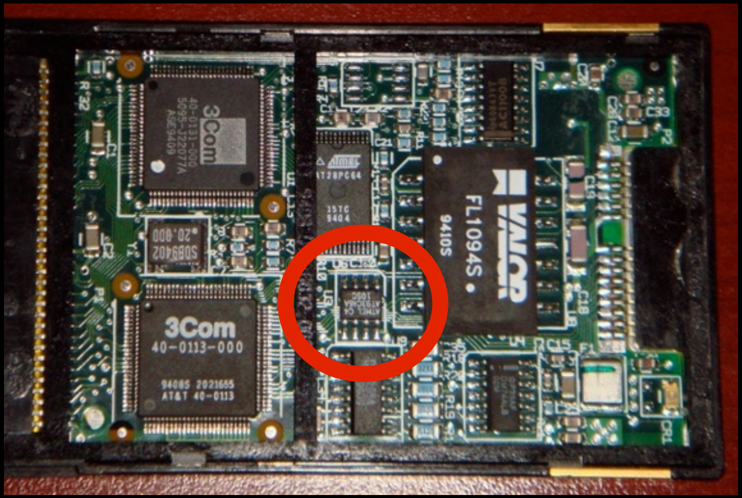


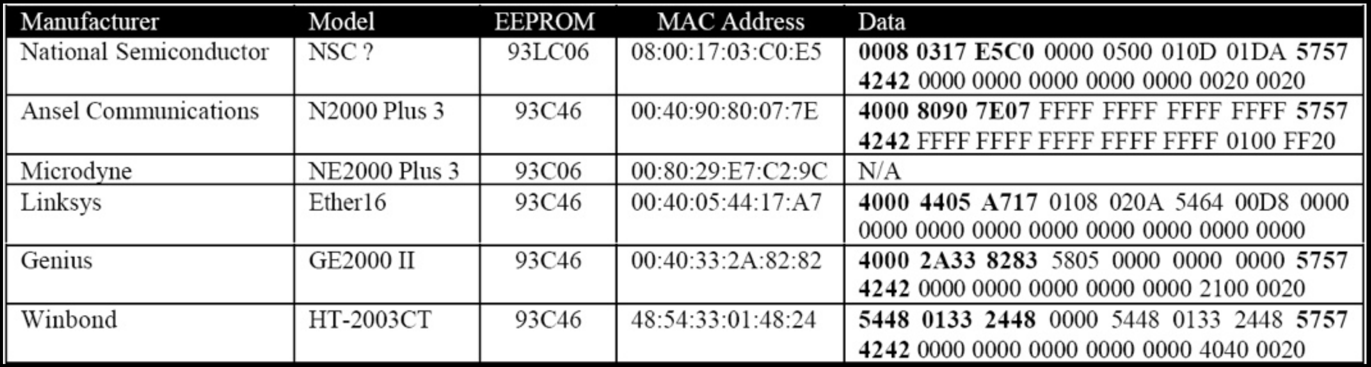
```
; ============= Subroutine for copying in a fake ESN =========================

letsgo: mov r0, #$60                ;
        mov r1, #$04                ;
cploop: movx a, @dptr               ;
        mov @r0, a                  ;       THIS WILL COPY A OBTAINED
        inc dptr                    ;
        inc r0                      ;       ESN TO THE LOCATION FOR
        djnz r1, cploop             ;
        mov dptr, #$bec2            ;       REAL ESN USE. FOR USE
        mov r0, #$60                ;
        mov r1, #$04                ;       WITH ESN/MIN PAIRS.
wrloop: mov a, @r0                  ;
        lcall $2ffb                 ;
        inc dptr                    ;
        inc r0                      ;
        djnz r1, wrloop             ;
        ljmp done
autodia:mov a, #$01                 ;\
        mov dptr, #$7005            ; |Turn off EEPROM write protect.
        movx @dptr, a               ;/
        clr $60                     ; Make sure $60 is clean
                                    ; ******* Loop for 1 to 256
                                    ; \
        mov $62, #$a0               ;  | #$a0de Load First Address
        mov $63, #$de               ;  | in Data Table
                                    ; /
                                    ; DPH   DPL
                                    ; $83   $82
pulldat:mov $83, $62                ; \
        mov $82, $63                ;  |  82 = DPL
        clr a                       ;  |  83 = DPH
        movc a, @a+dptr             ;  |  83 82
        mov $60, a                  ;  |
        inc $63                     ;  | Read from Data Table starting
        mov $82, $63                ;  | at ROM address #$9f4e, we pull
        clr a                       ;  |
```

Memory & Firmware

1998: NIC MAC Address Cloning (Serial EEPROM)

`www.grandideastudio.com/portfolio/mac-address-cloning/`



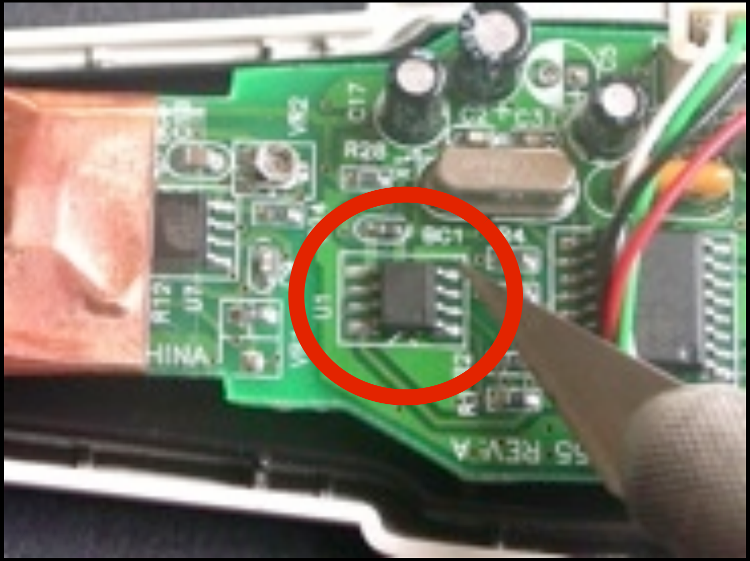


Manufacturer	Model	EEPROM	MAC Address	Data
National Semiconductor	NSC ?	93LC06	08:00:17:03:C0:E5	**0008 0317 E5C0** 0000 0500 010D 01DA **5757 4242** 0000 0000 0000 0000 0000 0020 0020
Ansel Communications	N2000 Plus 3	93C46	00:40:90:80:07:7E	**4000 8090 7E07** FFFF FFFF FFFF FFFF **5757 4242** FFFF FFFF FFFF FFFF FFFF 0100 FF20
Microdyne	NE2000 Plus 3	93C06	00:80:29:E7:C2:9C	N/A
Linksys	Ether16	93C46	00:40:05:44:17:A7	**4000 4405 A717** 0108 020A 5464 00D8 0000 0000 0000 0000 0000 0000 0000 0000 0000
Genius	GE2000 II	93C46	00:40:33:2A:82:82	**4000 2A33 8283** 5805 0000 0000 0000 **5757 4242** 0000 0000 0000 0000 0000 2100 0020
Winbond	HT-2003CT	93C46	48:54:33:01:48:24	**5448 0133 2448** 0000 5448 0133 2448 **5757 4242** 0000 0000 0000 0000 0000 4040 0020

Memory & Firmware

2000: Declawing the CueCat (Serial EEPROM)

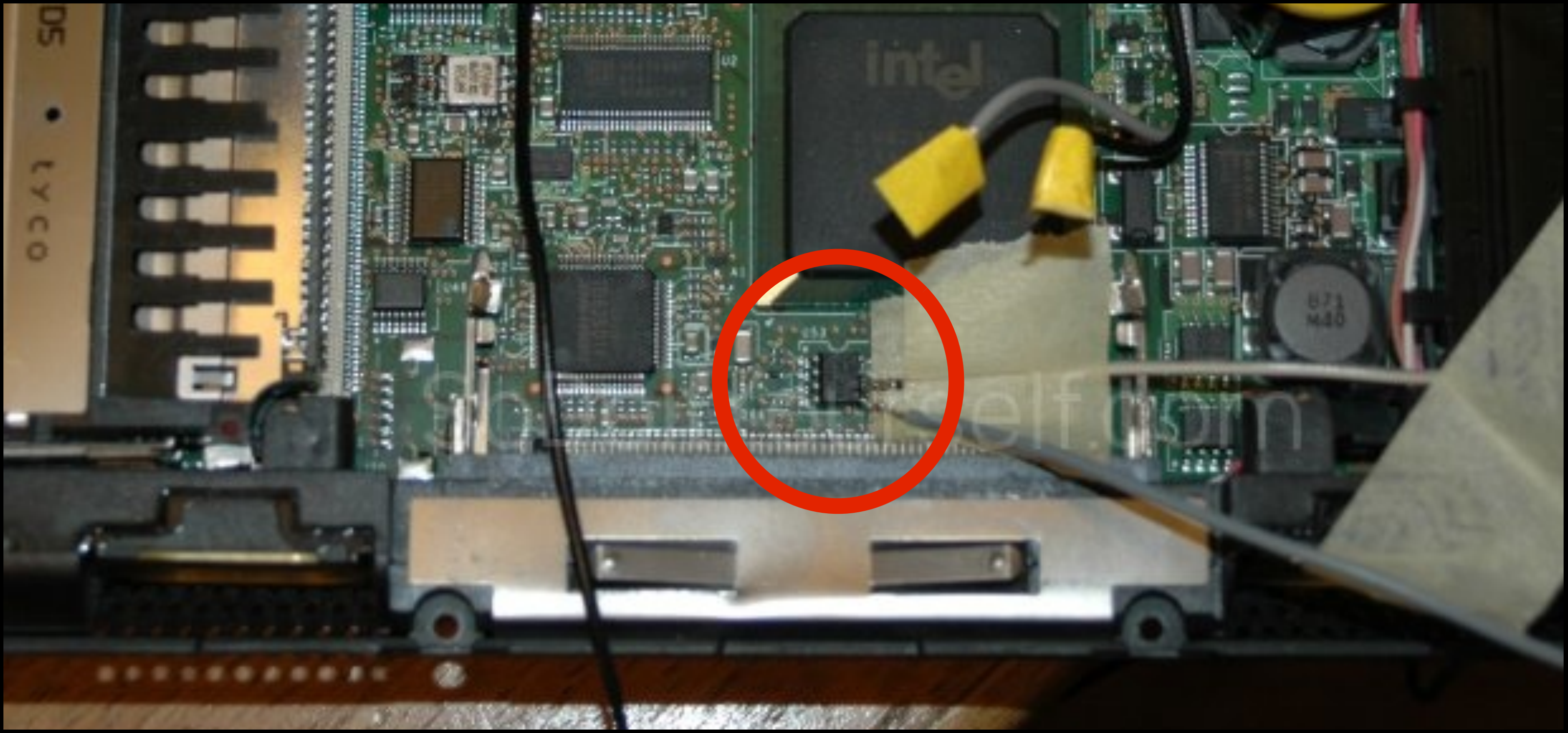
`www.sujal.net/tech/declaw/`

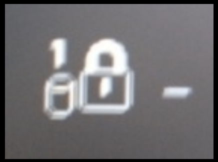


Memory & Firmware

2006: IBM ThinkPad BIOS Password (Serial EEPROM)

http://sodoityourself.com/hacking-ibm-thinkpad-bios-password/

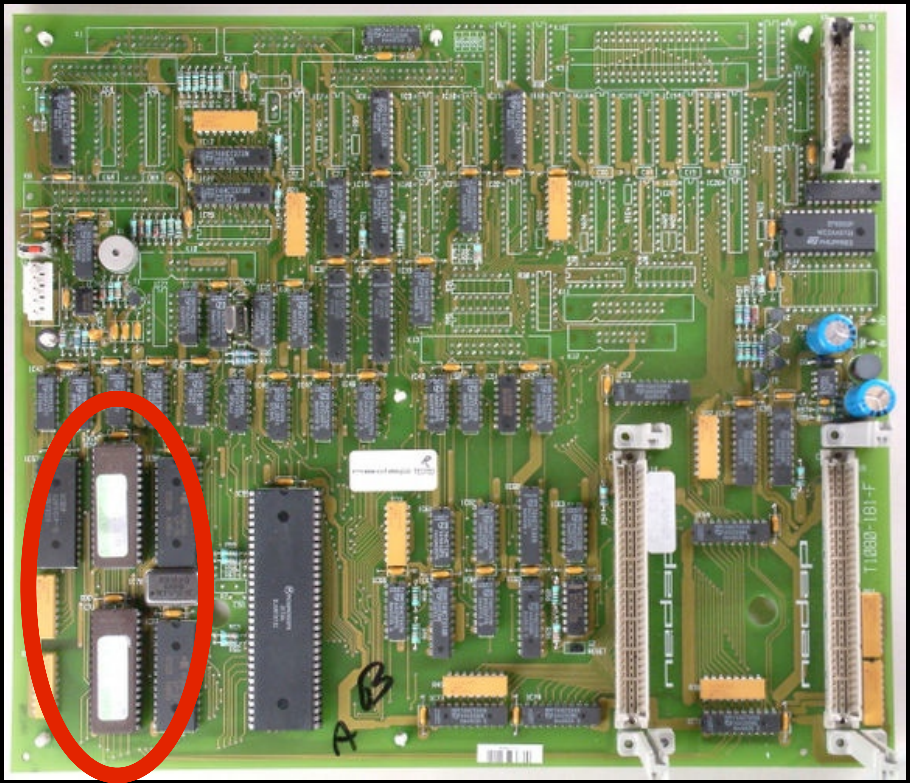




Memory & Firmware

2006: The Netherlands Electronic Voting Machines (68K)

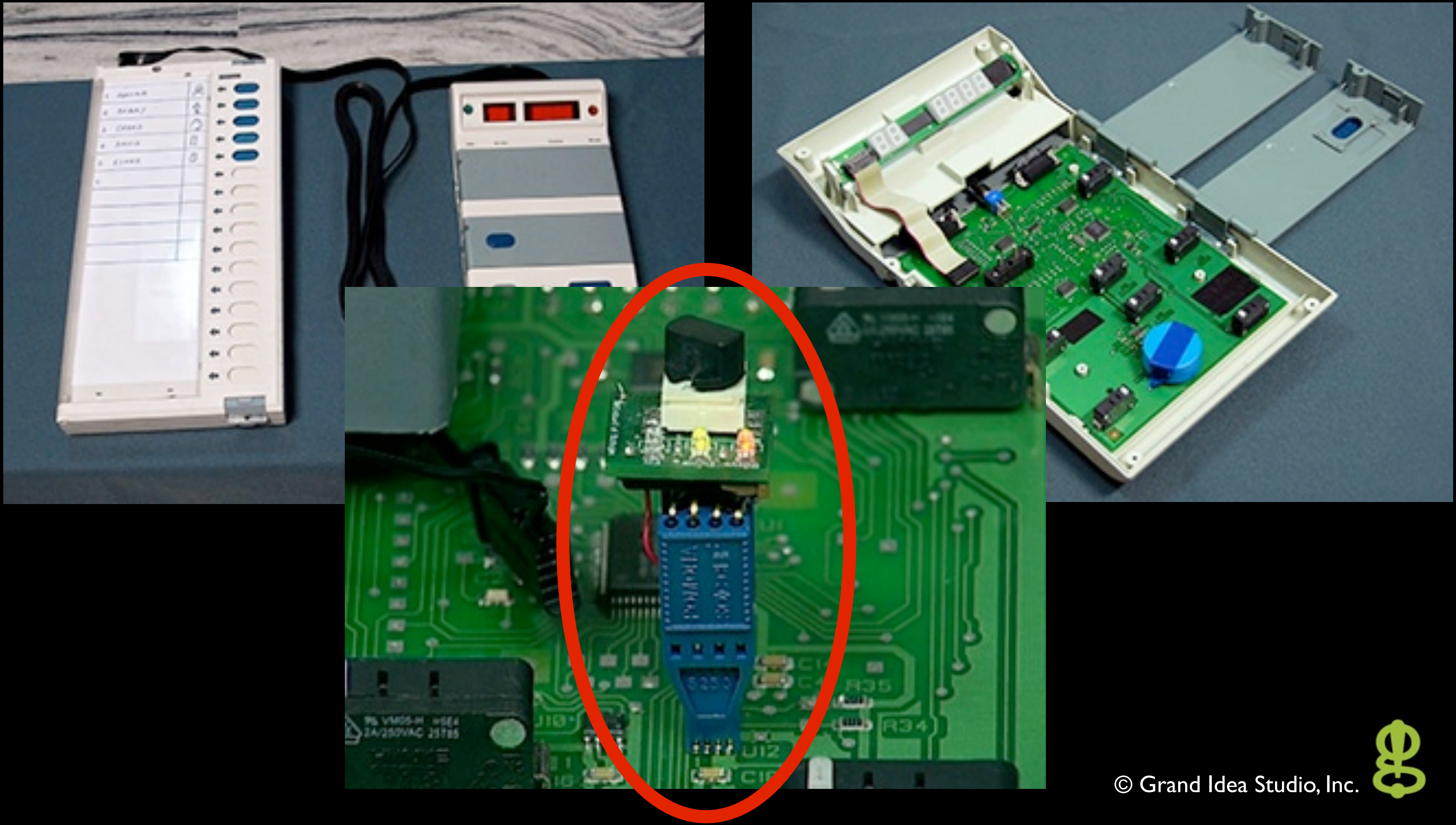
www.wijvertrouwenstemcomputersniet.nl



Memory & Firmware

2010: India Electronic Voting Machines (Serial EEPROM)

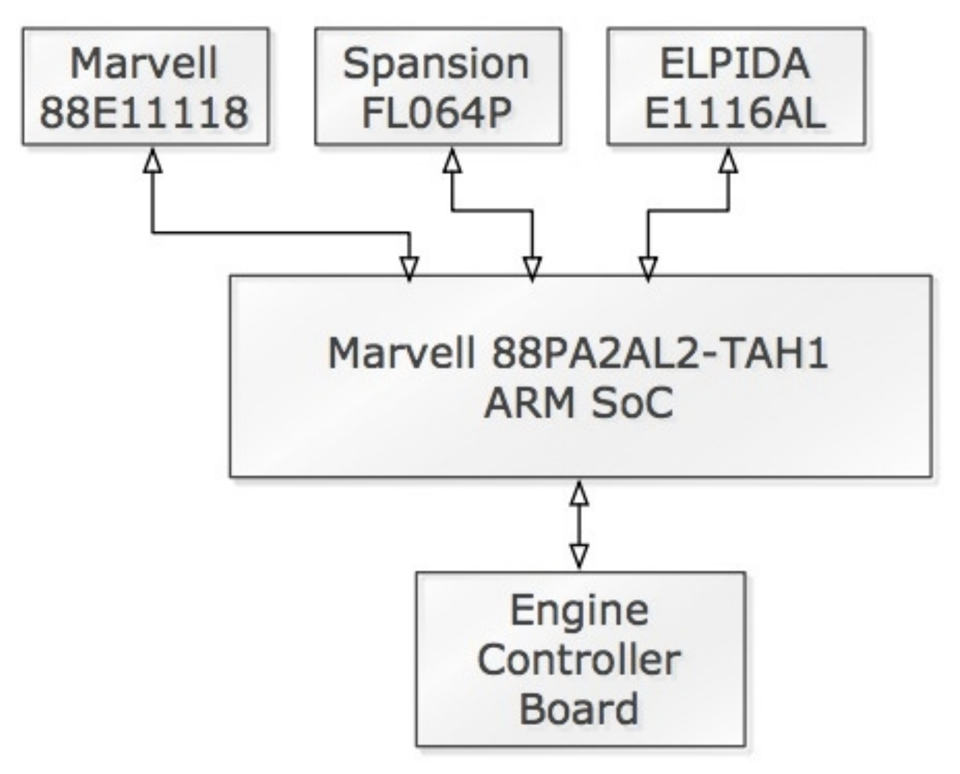
`www.indiaevm.org`



Memory & Firmware

2011: HP LaserJet Printer (VxWorks)

`http://ids.cs.columbia.edu/sites/default/files/CuiPrintMeIfYouDare.pdf`

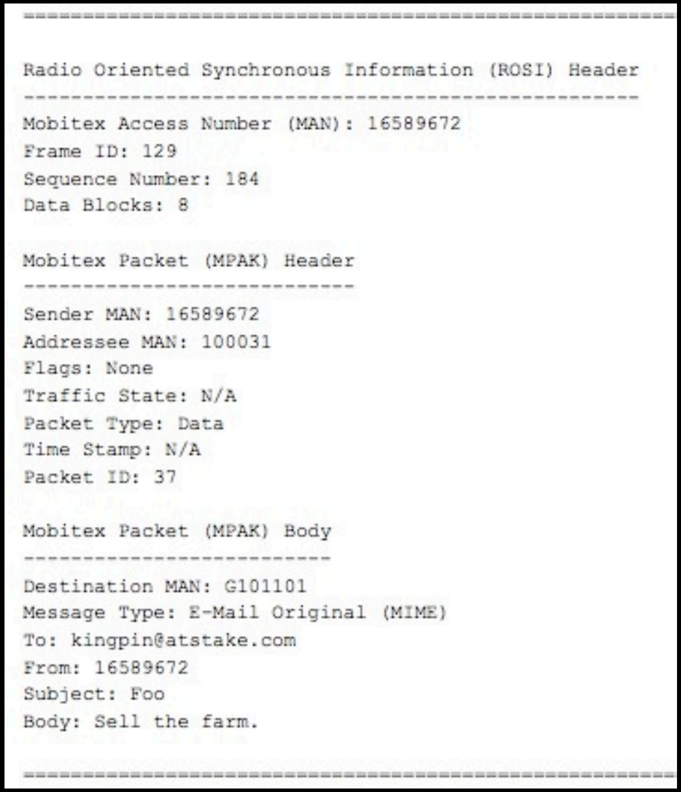


Exposed Buses & Interfaces

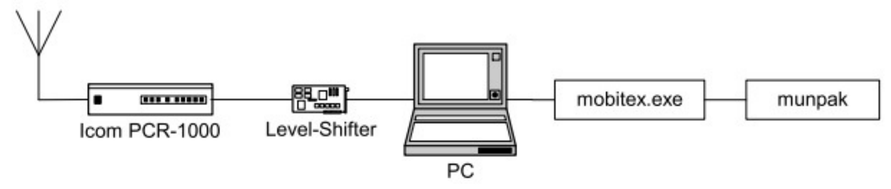
Exposed Buses & Interfaces

1997: BlackBerry RIM 950/957 (RF)

www.grandideastudio.com/portfolio/decoding-mobitex/



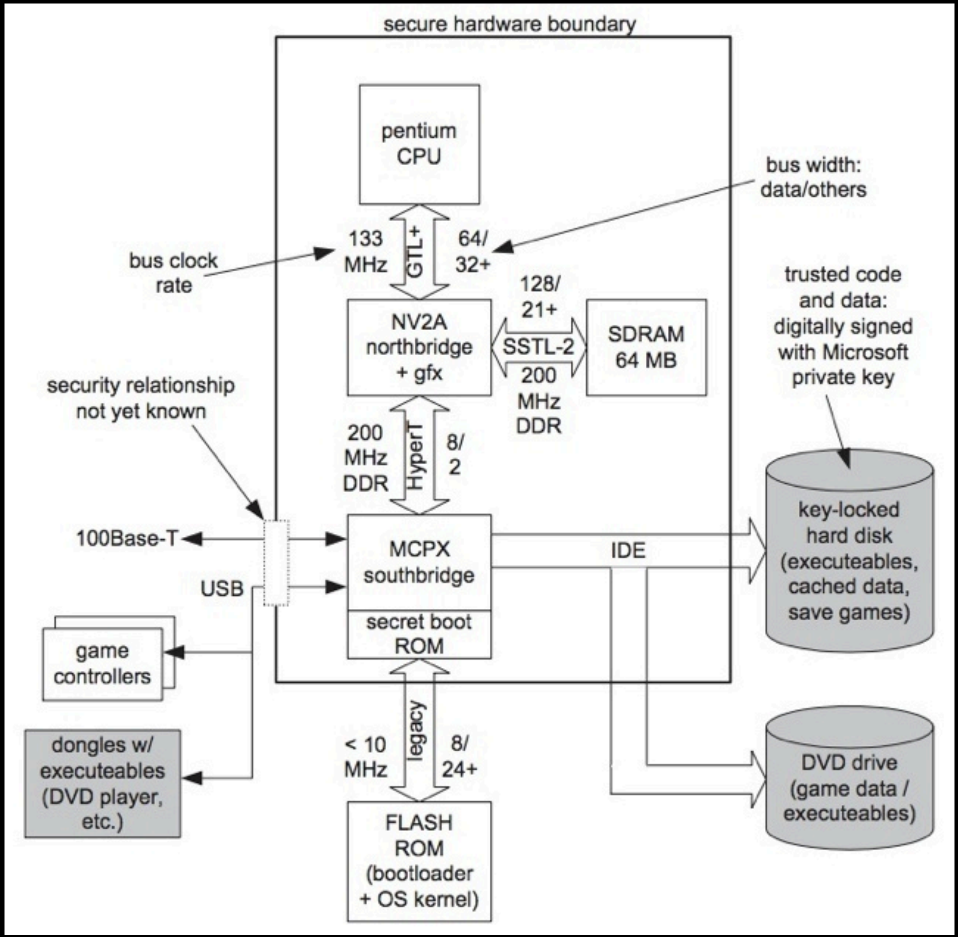
```
================================================================

Radio Oriented Synchronous Information (ROSI) Header
-----------------------------------------------------
Mobitex Access Number (MAN): 16589672
Frame ID: 129
Sequence Number: 184
Data Blocks: 8

Mobitex Packet (MPAK) Header
---------------------------
Sender MAN: 16589672
Addressee MAN: 100031
Flags: None
Traffic State: N/A
Packet Type: Data
Time Stamp: N/A
Packet ID: 37

Mobitex Packet (MPAK) Body
-------------------------
Destination MAN: G101101
Message Type: E-Mail Original (MIME)
To: kingpin@atstake.com
From: 16589672
Subject: Foo
Body: Sell the farm.

================================================================
```



Exposed Buses & Interfaces

2002: Hacking the Xbox (HyperTransport bus)

www.xenatera.com/bunnie/proj/anatak/xboxmod.html



secure hardware boundary

pentium CPU

bus clock rate

133 MHz

GTL+

64/ 32+

bus width: data/others

128/ 21+

NV2A northbridge + gfx

SSTL-2

200 MHz DDR

SDRAM 64 MB

trusted code and data: digitally signed with Microsoft private key

security relationship not yet known

200 MHz DDR

HyperT

8/ 2

100Base-T

USB

MCPX southbridge

secret boot ROM

IDE

key-locked hard disk (executeables, cached data, save games)

game controllers

dongles w/ executeables (DVD player, etc.)

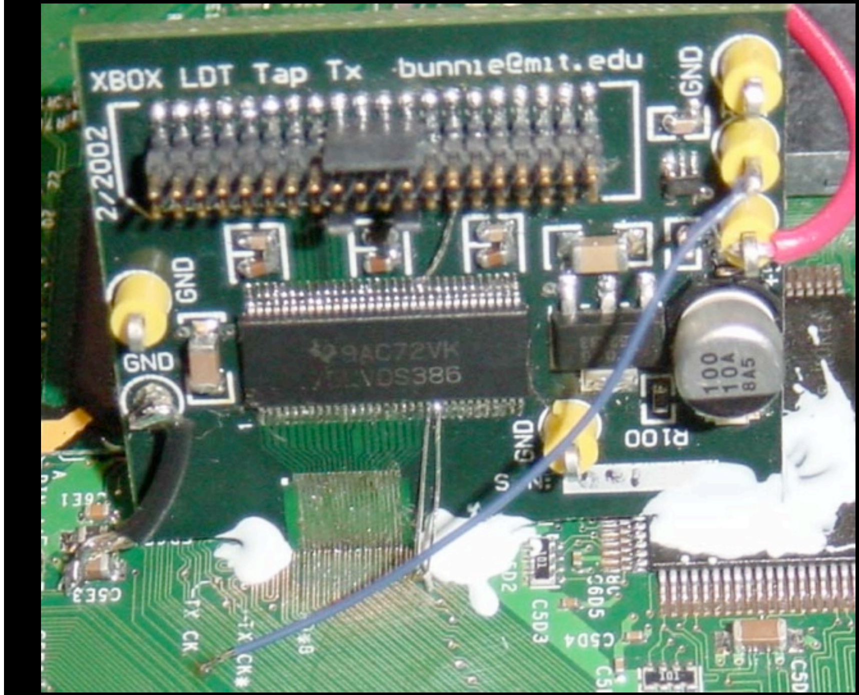
< 10 MHz

legacy

8/ 24+

FLASH ROM (bootloader + OS kernel)

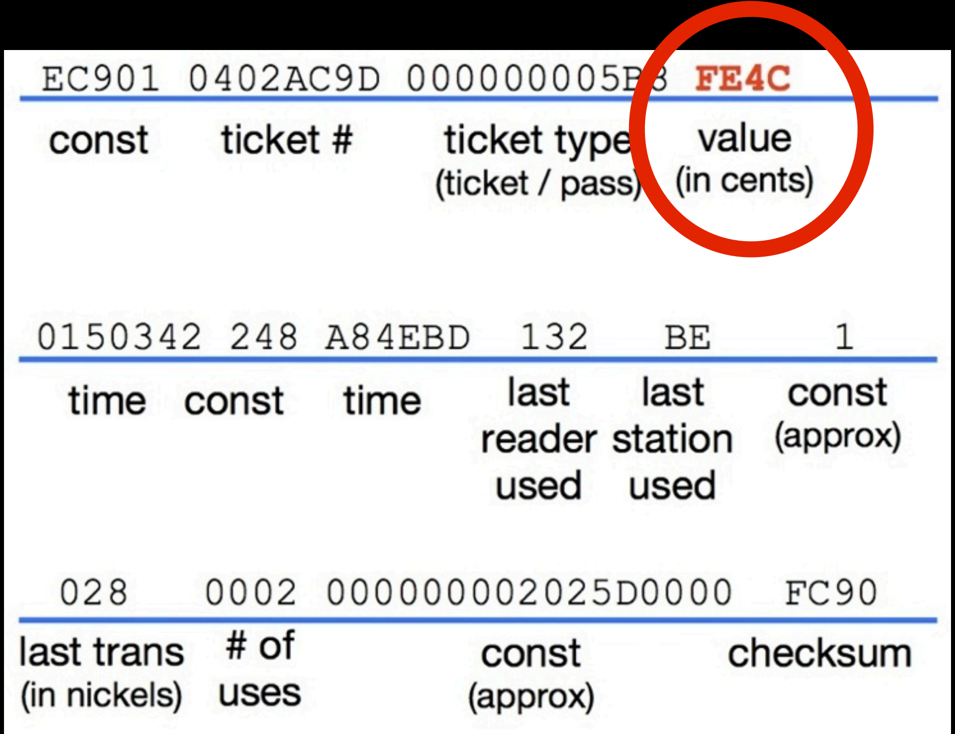
DVD drive (game data / executeables)



Exposed Buses & Interfaces

2008: MBTA CharlieTicket (Magnetic Stripe)

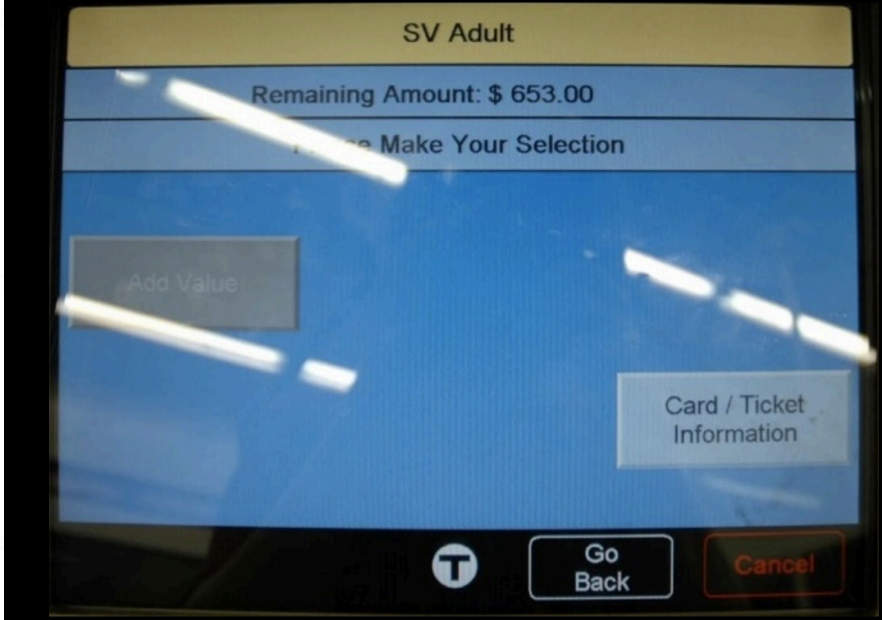
`http://web.mit.edu/zacka/www/mbta.html`



EC901	0402AC9D	000000005B3	FE4C
const	ticket #	ticket type (ticket / pass)	value (in cents)

0150342	248	A84EBD	132	BE	1
time	const	time	last reader used	last station used	const (approx)

028	0002	000000002025D0000	FC90
last trans (in nickels)	# of uses	const (approx)	checksum



SV Adult

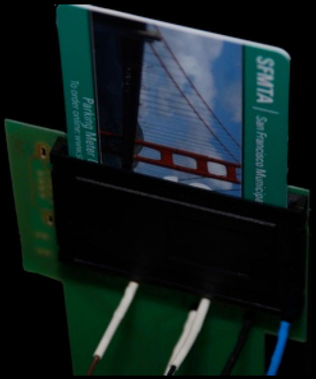
Remaining Amount: $ 653.00

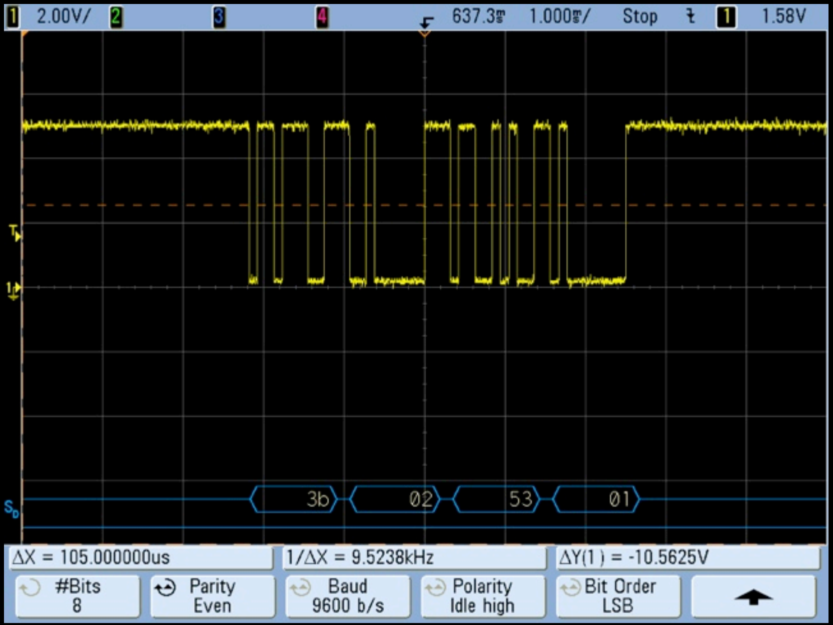
...e Make Your Selection

Exposed Buses & Interfaces

2009: San Francisco Smart Parking Meter (Smartcard)

www.grandideastudio.com/portfolio/smart-parking-meters/




1 2.00V/ 2 3 4 637.3µs 1.000ms/ Stop 1 1.58V

3b 02 53 01

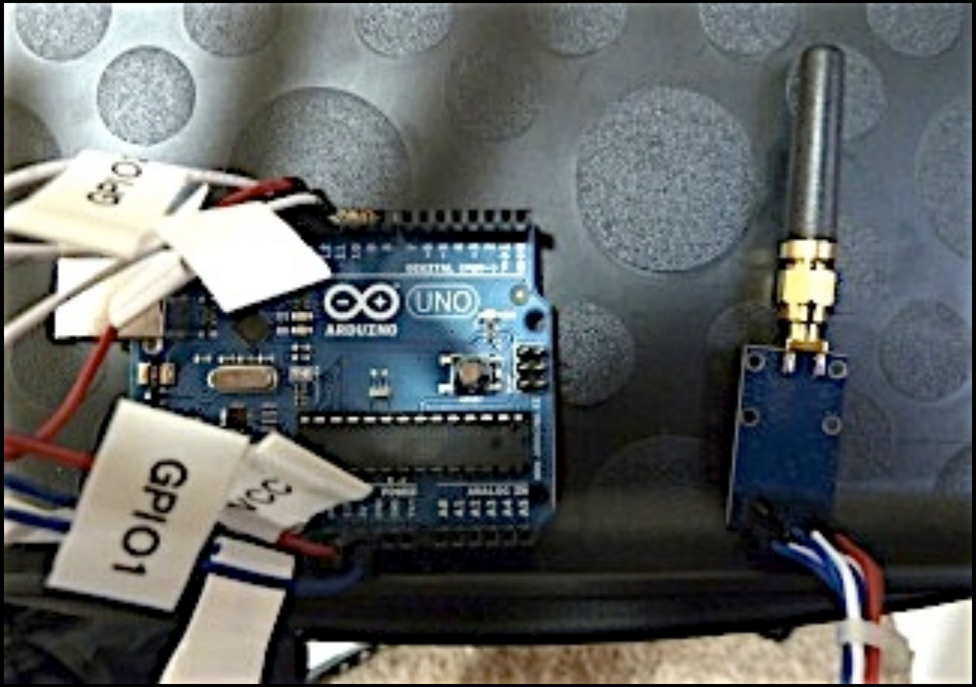
ΔX = 105.000000us
1/ΔX = 9.5238kHz
ΔY(1) = -10.5625V

#Bits 8
Parity Even
Baud 9600 b/s
Polarity Idle high
Bit Order LSB

Exposed Buses & Interfaces

2011: Medtronic Implantable Insulin Pump (RF)

https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_Slides.pdf

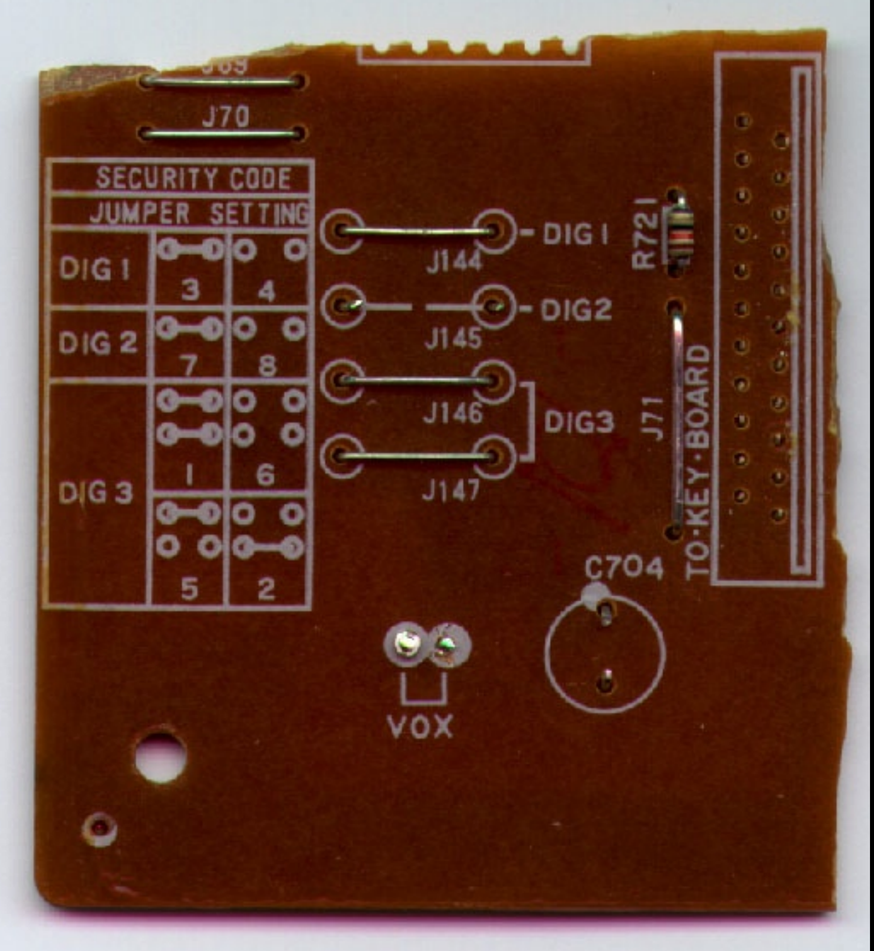


Passwords & Cryptography

Passwords & Crypto

1988: AT&T 1320 Answering Machine Security Code

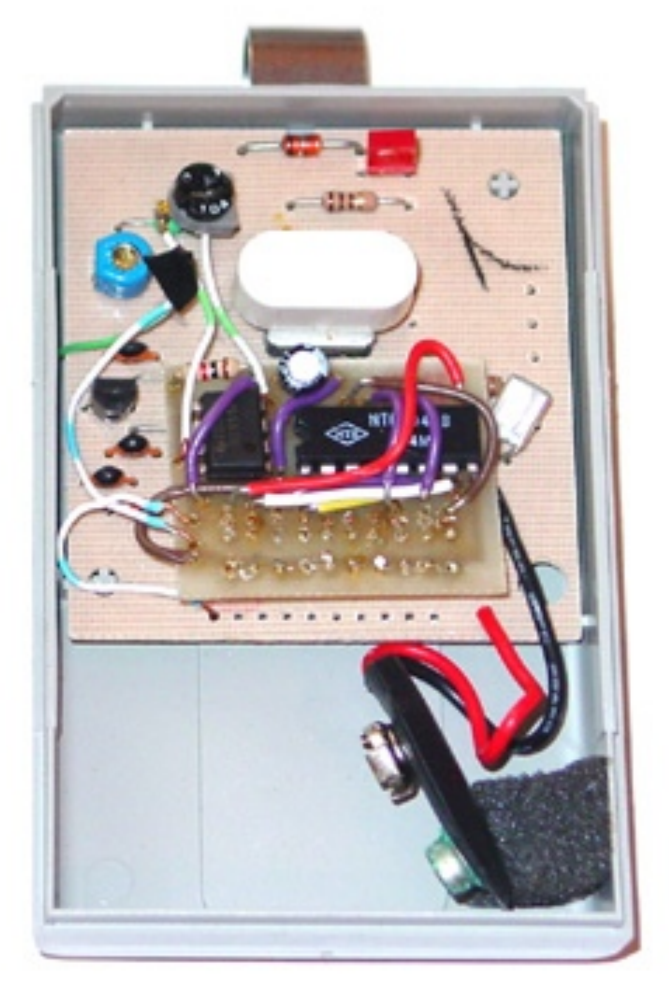
www.grandideastudio.com/portfolio/answering-machine-advisory/

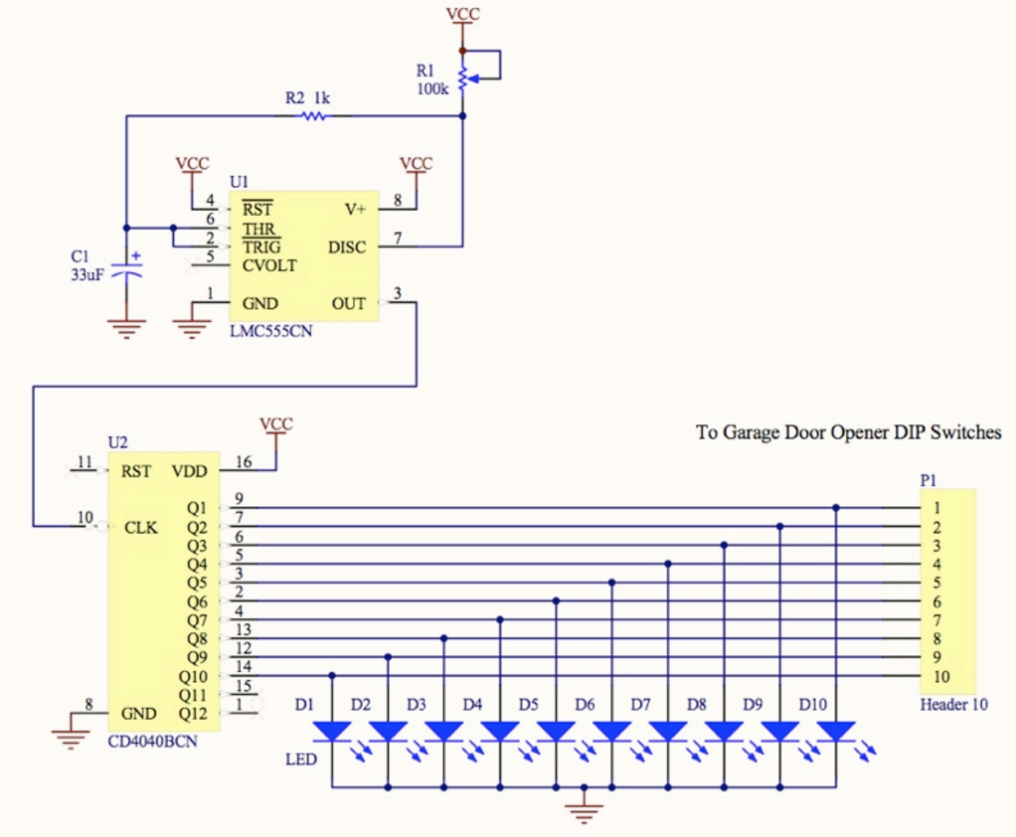


Passwords & Crypto

1994: Universal Garage Door Opener

`www.grandideastudio.com/portfolio/universal-garage-door-opener/`

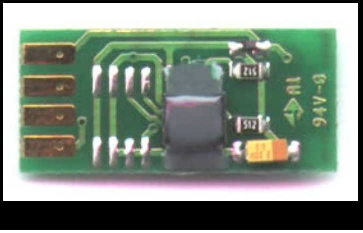


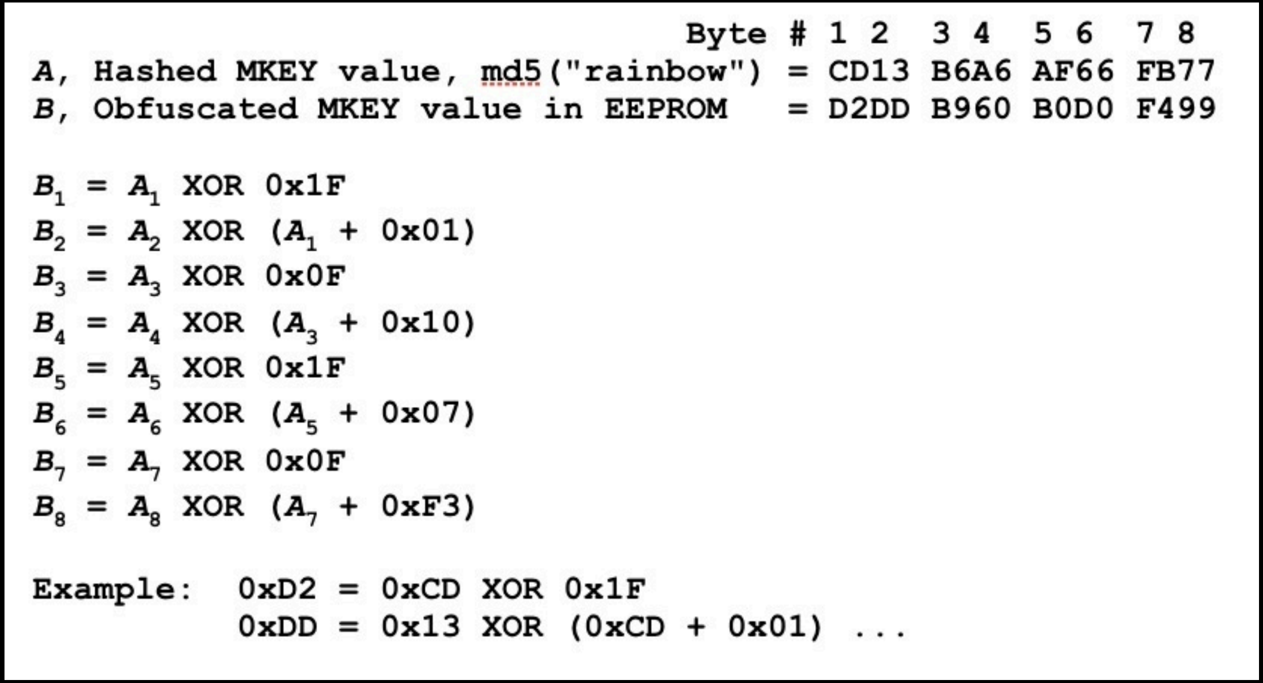


Passwords & Crypto

2000: Rainbow iKey 1000 Password Decoding

`www.grandideastudio.com/portfolio/attacks-on-usb-tokens/`





```
                                     Byte # 1 2  3 4  5 6  7 8
A, Hashed MKEY value, md5("rainbow") = CD13 B6A6 AF66 FB77
B, Obfuscated MKEY value in EEPROM   = D2DD B960 B0D0 F499
```

B_1 = A_1 XOR 0x1F

B_2 = A_2 XOR (A_1 + 0x01)

B_3 = A_3 XOR 0x0F

B_4 = A_4 XOR (A_3 + 0x10)

B_5 = A_5 XOR 0x1F

B_6 = A_6 XOR (A_5 + 0x07)

B_7 = A_7 XOR 0x0F

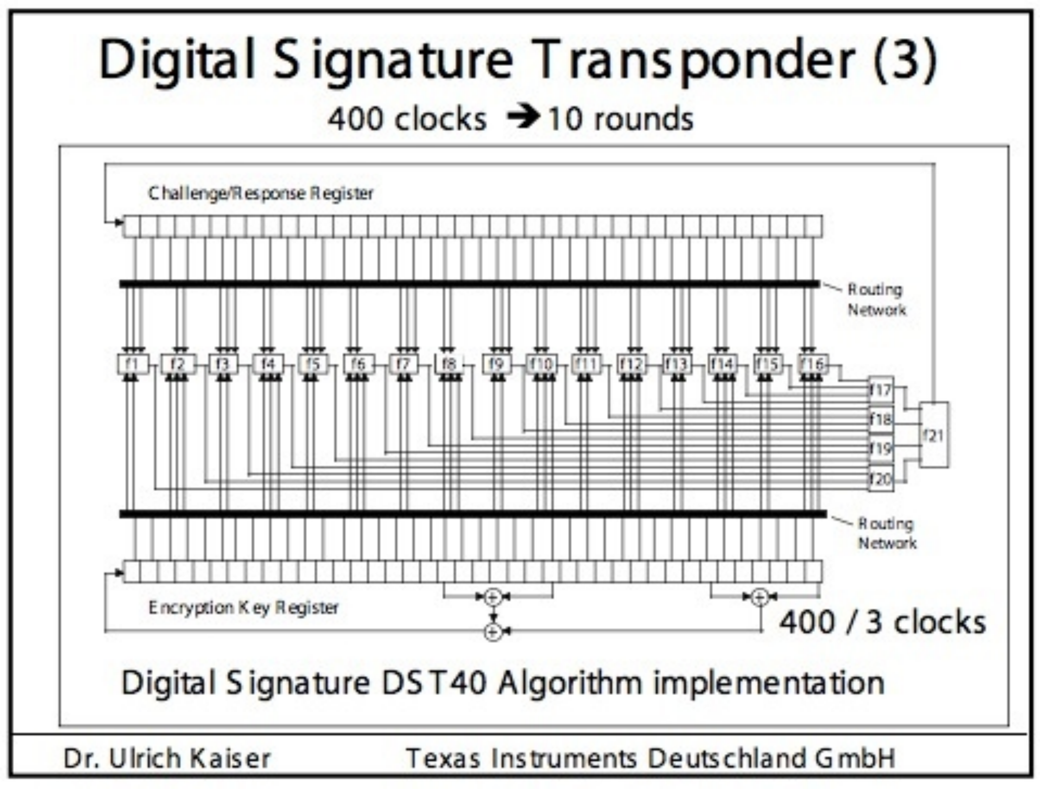
B_8 = A_8 XOR (A_7 + 0xF3)

```
Example:   0xD2 = 0xCD XOR 0x1F
           0xDD = 0x13 XOR (0xCD + 0x01)  ...
```

Passwords & Crypto

2005: Mobil SpeedPass (TI Digital Signature Transponder RFID)

`http://static.usenix.org/event/sec05/tech/bono/bono.pdf`



Digital Signature Transponder (3)

400 clocks → 10 rounds

400 / 3 clocks

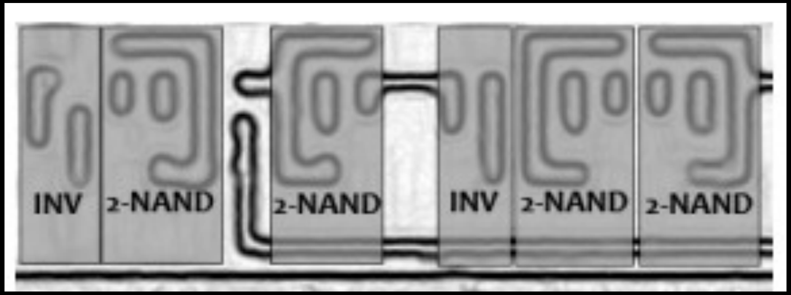
Digital Signature DST40 Algorithm implementation

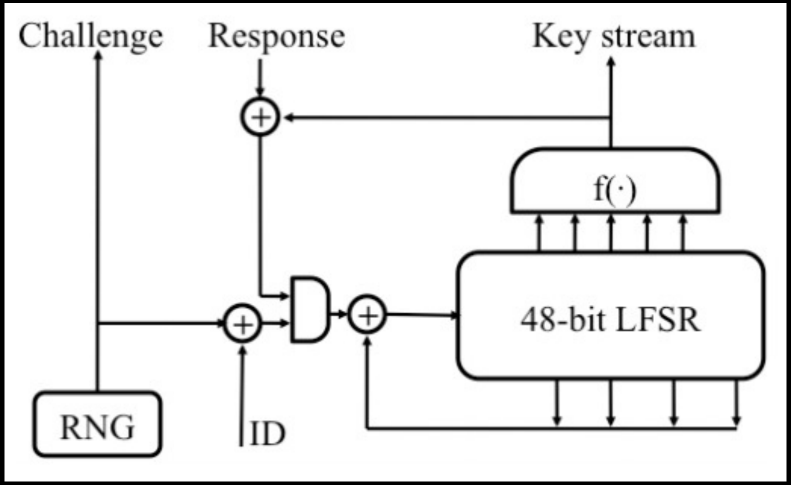
Dr. Ulrich Kaiser Texas Instruments Deutschland GmbH

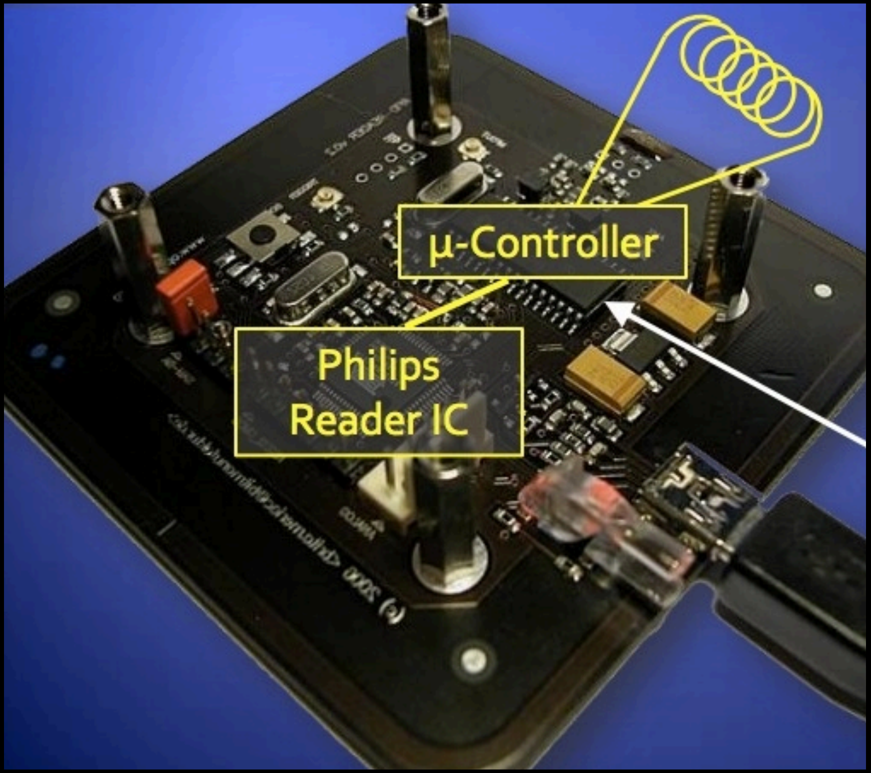
Passwords & Crypto

2008: Mifare Classic (RFID)

`www.cs.virginia.edu/~evans/pubs/usenix08/usenix08.pdf`







What Can Be Done?

- Acceptance
  - Admit that security needs to get better
  - Acknowledge that someone might be out to get you
- Education
  - Learn from history...don't repeat the same mistakes
- Awareness
  - Think like a hacker during the design phase
- Dedication
  - Security should be another tool in our toolbox
  - All facets of the organization need to put forth the effort to make products better

THANK-U+GOODNITE
FROM PACSAT:KU-1

WWW.GRANDIDEASTUDIO.COM