Can You Really Trust Hardware? Exploring Security Problems in Hardware Devices

The Black Hat Briefings 2005

Joe Grand

Grand Idea Studio, Inc.

joe@grandideastudio.com

Goals

- Become familiar with classes of hardware attacks
- Learn from history
  - Explore prior attacks against hardware products
- Gain knowledge to attack/analyze new devices
- Understand and accept that hardware-based security is extremely difficult
  - Just because it's a hardware product does not mean it's secure

Threat Vectors

- Interception (or Eavesdropping)
  - Gain access to protected information without opening the product
- Interruption (or Fault Generation)
  - Preventing the product from functioning normally
- Modification
  - Tampering with the product, typically invasive
- Fabrication/Man-in-the-Middle
  - Creating counterfeit assets of a product

Attack Goals

- Competition (or Cloning)
  - Specific IP theft to gain marketplace advantage
- Theft-of-Service
  - Obtaining service for free that normally requires $$$
- User Authentication (or Spoofing)
  - Forging a user's identity to gain access to a system
- Privilege Escalation (or Feature Unlocking)
  - Gaining increased command of a system or unlocking hidden/undocumented features

Thinking Like An Attacker...

Attacks Against...

- Access control
  - Biometrics
  - Authentication tokens
  - RFID
- Network appliances
  - Cryptographic accelerators
  - Wireless access points
  - Network adapters/NICs
  - PDAs/Mobile devices

Biometrics

- Measure and analyze human body characteristics in order to authenticate identity
  - Ex.: Fingerprint, hand geometry, eye pattern (iris or retina), facial features, or voice or written signature
- Considered more secure than systems that use passwords, but physical characteristics are hard to keep secret
  - Ex.: Fingerprint lifted from keyboard, picture can be taken of a face, voice can be recorded

Biometrics 2

- Usually composed of two or three components:
  - Biometric device, application software, back-end server
- Potential problems with storage of characteristics if not implemented properly
  - Biometric data could be stolen and/or cloned
  - Most glossy marketing sheets state they store "a set of unique data points" that cannot be reverse engineered
- Some characteristics can change over time
  - Ex.: Glaucoma medicine changes retina color and vein pattern, scars on a finger, etc.

Biometrics 3

- If fingerprint is stolen, you only have nine more to use...
  - Gives a whole new meaning to "hacking" and "digital theft"!

Biometrics: Fingerprint Cloning

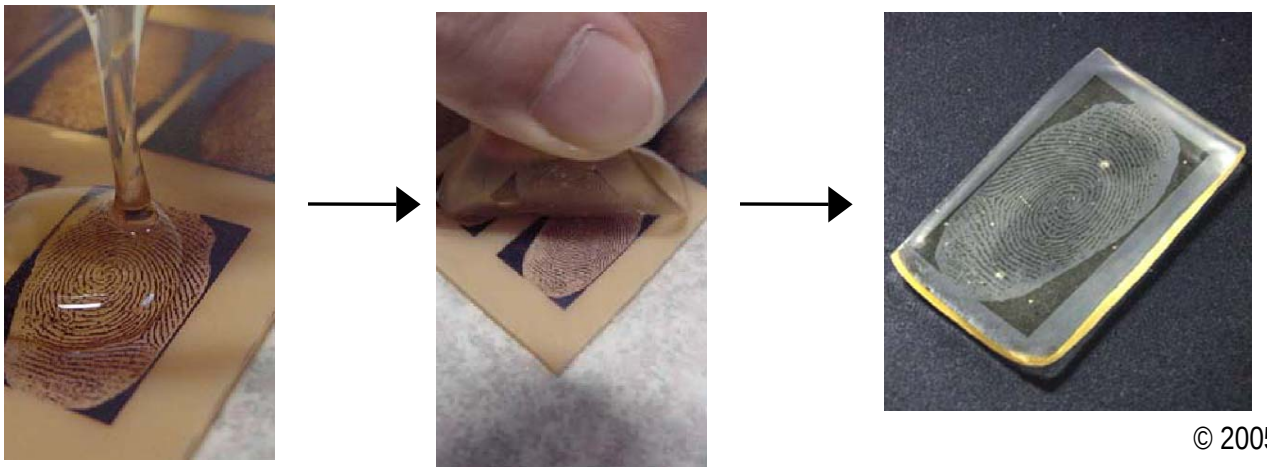
- Current biometric fingerprint systems (optical & capacitive) are notoriously simple to bypass
- In May 2002, Tsutomu Matsumoto presented methods to defeat scanners by using a fake finger molded out of gelatin
  - **`http://cryptome.org/gummy.htm`**
- Defeated 11 different fingerprint systems 80% of the time

Biometrics: Fingerprint Cloning 2

1. Obtained latent fingerprint from a glass
2. Enhanced with cyanoacrylate adhesive (super glue) and photographed with digital camera
3. Edited contrast in Photoshop and printed onto transparency sheet
4. Use transparency to etch fingerprint onto photo-sensitive printed circuit board
5. Created gelatin finger from circuit board "mold"

Biometrics: Fingerprint Cloning 3

- Gelatin finger also fools capacitive sensors due to moisture and resistance characteristics similar to a real human finger
- Unlikely that gelatin finger will work on RF fingerprint scanning technologies
  - Used to capture fingerprint image below the surface layer of the skin



Authentication Tokens

- Used to provide identity in order to gain access to an asset
  - How do you prove you are who you say you are?
- Typically used in combination with a password
  - Two-factor
  - Something you know and something you have
- Common security-related uses
  - Private data storage (credentials, crypto keys, certs, passwords)
  - One-time-password generation

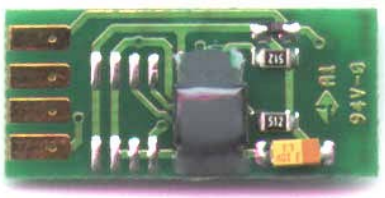
USB Authentication Token: Rainbow iKey 1000 (old revision)

- All data stored in easily accessible, unprotected Serial EEPROM
- Can gain full administrator access to device by generating a new key based on weak algorithm
  - "Attacks on and Countermeasures for USB Hardware Token Devices," **`www.grandideastudio.com/files/security/tokens/usb_hardware_token.pdf`**
- Devices created after November 1999 have been updated to prevent these attacks

USB Authentication Token 2: Rainbow iKey 1000 (old revision)

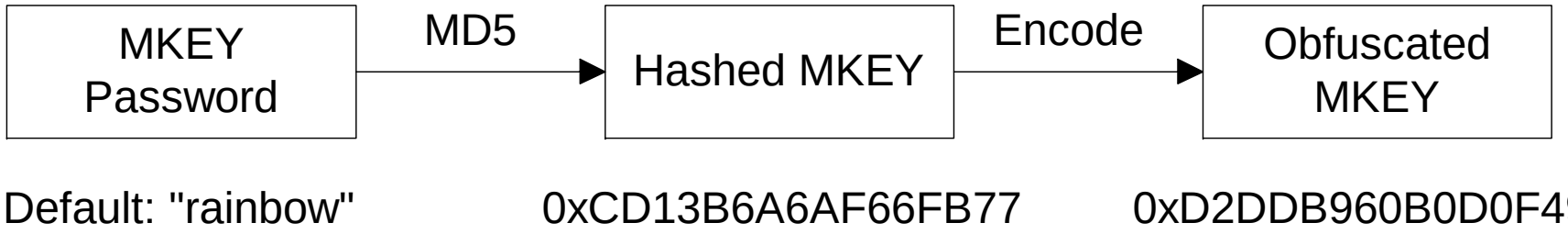
- Extremely easy to open with X-ACTO knife
  - Under 30 seconds with no visible damage

- Can attach probes to the unpopulated footprint and read the "encapsulated" EEPROM
  - 24LC64 uses I^2C bus (serial clock and data)



USB Authentication Token 3: Rainbow iKey 1000 (old revision)

- MKEY (Master Key) serves as administrative password (gives full access to device)
  - 256 character ASCII, default = "rainbow"
  - Hashed MKEY stored at address 0x8



USB Authentication Token 4: Rainbow iKey 1000 (old revision)

```
                                        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)

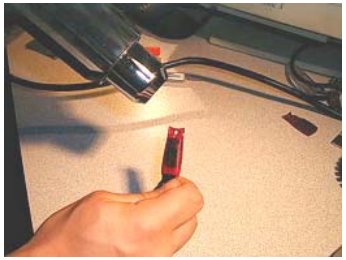
```
Example:  0xD2 = 0xCD XOR 0x1F
          0xDD = 0x13 XOR (0xCD + 0x01) ...
```


USB Authentication Token 5: Aladdin eToken 3.3.3.x

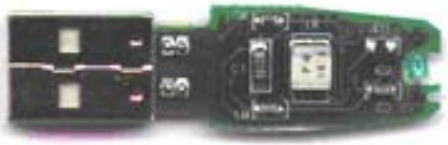
- All data stored in easily accessible, unprotected Serial EEPROM
- Can gain full user access to device by rewriting user PIN with default PIN
  - "Attacks on and Countermeasures for USB Hardware Token Devices," **`www.grandideastudio.com/files/security/tokens/usb_hardware_token.pdf`**
- Aladdin states that 3.3.3.x was not a released product

USB Authentication Token 6: Aladdin eToken 3.3.3.x

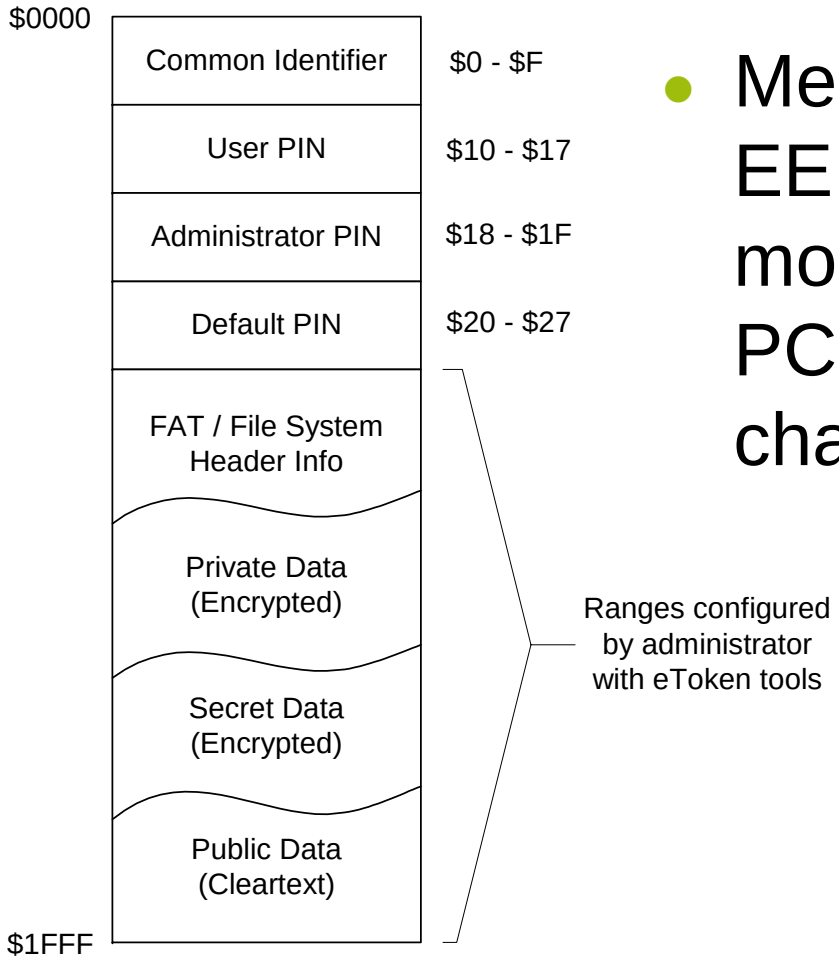
- Can use heat gun to soften glue around housing and split open with X-ACTO knife



- Can attach probes to the EEPROM and read with standard device programmer
  - Atmel 25640 uses SPI bus (serial clock, data in, data out)

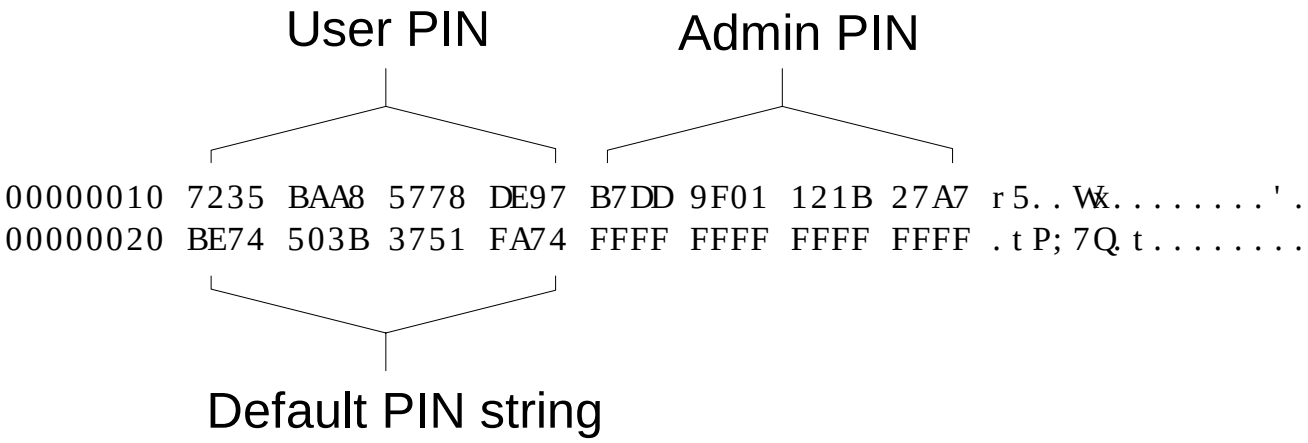



USB Authentication Token 7: Aladdin eToken 3.3.3.x



- Memory map of Serial EEPROM obtained by modifying eToken data on PC and viewing content changes in EEPROM

USB Authentication Token 8: Aladdin eToken 3.3.3.x



Initial memory dump, User and Admin PINs set to unknown values

```
00000010 BE74 503B 3751 FA74 B7DD 9F01 121B 27A7 .tP;7Q.t.....'.
00000020 BE74 503B 3751 FA74 FFFF FFFF FFFF FFFF .tP;7Q.t.....
```

Memory dump, after modification, with User PIN now set to default

Dallas Semiconductor iButton

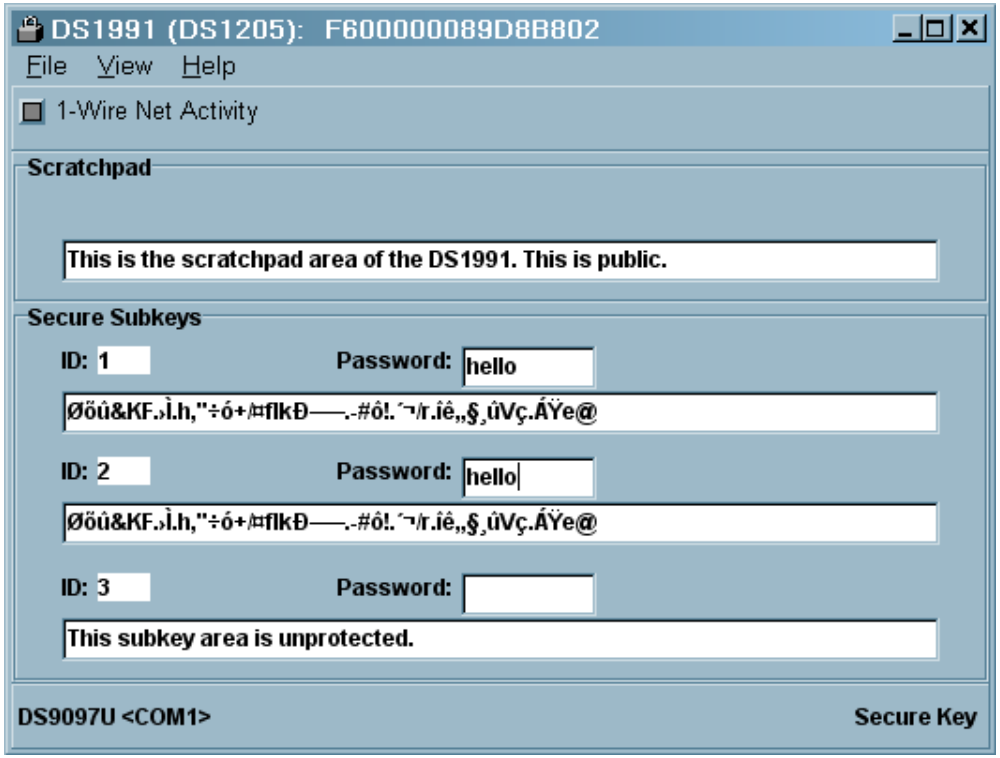
- Designed to replace barcodes, RFID tags, magnetic stripes, proximity and smart cards
- Physical features: Stainless steel, waterproof, rugged, wearable, tamper responsive
- 1-wire Interface
  - Actually, 2 wires (clock/data and ground)
  - Parasitically-powered
  - 16kbps (standard) and 142kbps (overdrive)
- Unique 64-bit ID (non-secret) for each device

iButton: DS1991 MultiKey

- 1,152 bits of non-volatile memory split into three 384-bit (48-byte) containers known as “subkeys”
- Each subkey is protected by an independent 8-byte password
- Only the correct password will grant access to the data stored within each subkey area and return the 48-bytes
  - Incorrect password supposed to return 48-bytes of "random" data
- Commonly used for cashless transactions (e.g., parking meters, public transportation) and access control

iButton: DS1991 MultiKey 2

- Initial experiments with iButton Viewer (part of free iButton-TMEX SDK) showed that "random" response is actually based on input password



iButton: DS1991 MultiKey 3

- Based on input password and 12kB constant block
  - Constant for all DS1991 devices
  - Can precompute the 48-byte return value expected for an incorrect password
  - If return value does not match, must be the correct password and subkey data
- Can perform dictionary attack to access protected subkey data
  - "DS1991 MultiKey iButton Dictionary Attack Vulnerability," **`www.grandideastudio.com/files/security/tokens/ds1991_ibutton_advisory.txt`**

iButton: DS1991 MultiKey 4

- How to precompute the expected incorrect password" string?
  - For any given character (256 possibilities), a unique 48-byte response is returned from iButton
  - Created application to set each single-byte password and monitor serial port for response
  - Trial and error to determine how response was generated for longer length passwords (XORs and shifts!)

Radio Frequency Identification (RFID)

- Generic term for non-contacting technologies that use radio waves to automatically identify people or objects
- Has been available for decades, but just now becoming popular for mainstream
  - Robotics navigation, inventory (human?) tracking, access control, automatic identification, payment systems, and car immobilization

Radio Frequency Identification (RFID) 2

- Most common use is to store unique serial number (read-only) on a microchip that is attached to an antenna
  - Combined antenna and microchip called a "transponder" or "tag"
- Typical RFID system contains a reader and one or more tags
  - Each tag's unique serial number identifies a specific person or object

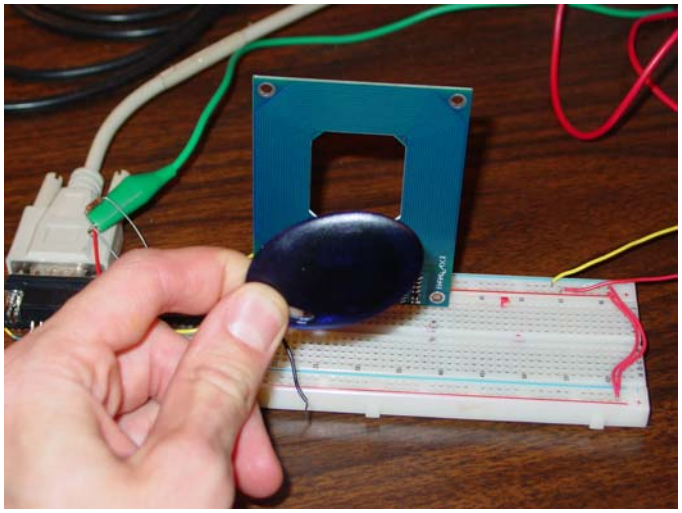
Radio Frequency Identification (RFID) 3

- Two major tag types:
  - Passive: No internal power source or transmitter, shorter range
  - Active: Power source (battery) and transmitter, longer range
- Four typical frequency ranges:
  - LF (Low Frequency), 125 to 134.2kHz
  - HF (High Frequency), 13.56MHz
  - UHF (Ultra-High Frequency), 868 to 928MHz
  - uW (Microwave), 2.45 and 5.8 GHz

Radio Frequency Identification (RFID) 4

1. Reader's antenna transmits RF energy
2. Energy "harvested" by tag's antenna and used to power up internal circuitry
3. Tag will modulate electromagnetic waves generated by the reader to transmit data
4. Receiver demodulates waves and converts to digital signal

Radio Frequency Identification (RFID) 5



Radio Frequency Identification (RFID) 6

- No security between most tag and reader transmissions
  - If you have a reader for the correct tag family and frequency, you can communicate with the tag
- Trivial to create system to read/write RFID tags
  - Parallax RFID Reader Module, **`www.parallax.com`**
  - Texas Instruments Web Page, **`www.tiris.com`**
  - MAKE Magazine, Issue 3 (coming soon...), **`www.makezine.com`**

Radio Frequency Identification (RFID) 7

- In January 2005, challenge/response scheme of Digital Signature Transponder (DST) tag was cracked
  - Used for Mobil SpeedPass, vehicle immobilizers, etc.
  - "Analysis of the Texas Instruments DST RFID," **`http://rfidanalysis.org`**
- Proprietary cipher (based on 40-bit key) reverse engineered from a single PowerPoint slide
- Over 150 **million** deployed devices are now at risk and could be cloned or spoofed!

Intel NetStructure 7110: Administrator Access

- SSL cryptographic accelerator
  - Offloads crypto functions from primary Web server to increase performance
- Standard PC motherboard, Pentium II 333MHz, Rainbow (now SafeNet) CryptoSwift Accelerator card

Intel NetStructure 7110: Administrator Access 2

- Serial port-based management console on front of unit
- Can be compromised to allow supervisor access
  - "Intel NetStructure Backdoors," **`www.atstake.com/research/advisories/2000/ipivot7110.html`**
  - "HPYN 2nd ed.: Hardware Hacking" chapter excerpt, **`www.grandideastudio.com/files/books/hpyn2e_chapter14.pdf`**

Intel NetStructure 7110: Administrator Access 3

1. Opened the unit
2. Retrieved filesystem
   - Stored on 32MB CompactFlash card
3. Examined filesystem
   - Used *strings* to determine BSD-flavor of Unix
4. Mounted filesystem on extra machine
5. Discovered password generator
   - Supervisor password based on MAC address of unit

Intel NetStructure 7110: Administrator Access 4

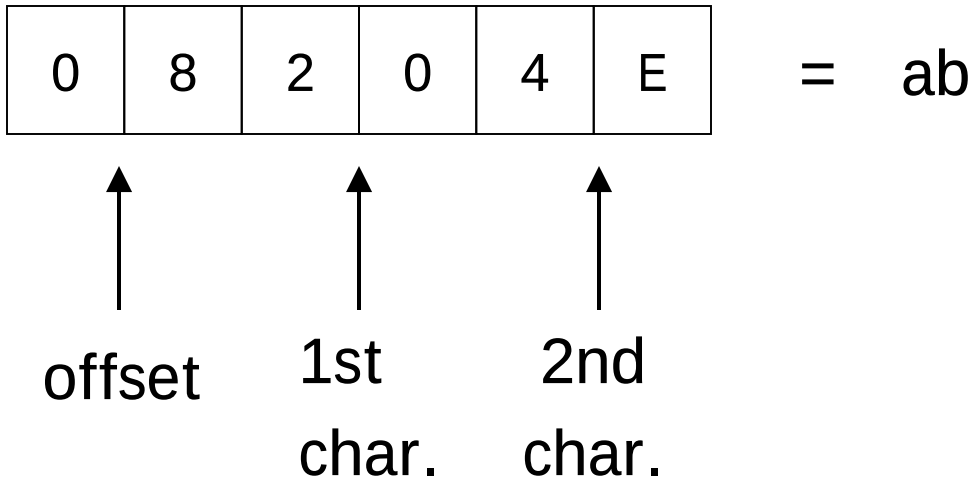
- Based on standard PC architecture
- Filesystem easily retrievable and mountable
- Executables compiled with debug symbols
- Homebrew crypto routines extremely weak

Cisco Router: Configuration Password

- User-selectable password types:
  - Type 0: Plaintext
  - Type 5: MD5 hash
  - Type 7: "Encrypted" (Encoded)
  - Others?
- “Encrypted” password stored on router
  - Stored in NVRAM and can be retrieved from configuration settings

Cisco Router: Configuration Password 2

- Passwords of type 7 encoded by XOR'ing plaintext against constant value
  - **`www.alcrypto.co.uk/cisco`** among others
- ASCII constant block
  - tfd;kfoA,.iyewrkldJKD
- Ex.:



IBM 4758 Secure Cryptographic Coprocessor

- Likely the most recognized, commercially available secure coprocessor system
  - A protected hardware subsystem designed to execute sensitive functions in a trusted manner
  - FIPS-140 Level 4 tamper responsive device with hardware cryptographic support and physical tamper protection
  - Also random number generation, authentication, general-purpose processor/coprocessor, etc.
- Commonly used in financial and banking transactions

IBM 4758 Secure Cryptographic Coprocessor 2

- In 2001, First known attack against IBM 4758 by taking advantage of a flaw in the Automated Teller Machine "Common Cryptographic Architecture" support software
  - "Extracting a 3DES key from an IBM 4758," **`www.cl.cam.ac.uk/~rnc1/descrack`**
- Can export all of the program's DES/3DES keys
  - Ex.: Communications Key, Pin Derivation Key, and Importer/Exporter Keys

IBM 4758 Secure Cryptographic Coprocessor 3

- Performed by an insider with physical access and a $995 Altera FPGA Development Board
  - As of February 2002, new version (2.41) of CCA fixes problems
- Even though hardware was strong, software was able to be compromised, thus breaking the whole system

Wireless Access Points: Dell TrueMobile 1184

- One of many broadband access point/routers
- Device based on vLinux distribution
  - **`www.onsoftwarei.com/product_vlinux.htm`**
  - "*Hardware Hacking: Have Fun While Voiding Your Warranty*" Wireless Hacks chapter
- Port scan reveals open ports 80, 333, 1863, 1864, 4443, 5190, 5566

Wireless Access Points 2: Dell TrueMobile 1184

- Can *telnet* into port 333 with default password to gain complete control of the device
  - username: root, password: admin
- No special hardware tools or reprogramming is necessary
- Many devices running Linux which can make hacking/experimentation easier
  - **`www.linuxdevices.com`**
  - **`www.ucdot.org`**

NIC MAC Address Cloning

- MAC (Media Access Control) Address often stored in easily reprogrammable Serial EEPROM
  - **www.grandideastudio.com/files/security/general/mac_address_cloning.pdf**
- Cloning could be used to bypass copy protection, gain access to MAC-filtered networks, etc.
- MAC = 6-byte value
  - First 3 bytes = Manufacturer
  - Second 3 bytes = "Unique" serial number
- Depending on the NIC, other configuration data also accessible
  - Ex.: I/O base address, interrupt type, checksum

NIC MAC Address Cloning 2

- Tools available to change or spoof in software
  - No hardware tampering needed!
  - SunOS: ifconfig
  - SPARC: set in NVRAM with prom-monitor

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

Mobile Devices: Current Risks

- Business often mixed with personal
- Most devices have no security framework
  - No access control or data/memory protection
  - Existing security mechanisms are weak and/or flawed
- "Always on" technologies leave device open to the world...all the time
  - Ex.: WiFi, Bluetooth, IR, etc.
- External memory cards
  - Some devices load apps automatically upon insertion
  - Easy to steal

Mobile Devices: Palm OS < 4.0 Password Retrieval

- Max. 32 characters ASCII
- Reversible obfuscation method (XOR against constant)
  - "Palm OS Password Retrieval and Decoding," **`www.grandideastudio.com/files/security/mobile/palm_password_decoding_advisory.txt`**
- Can retrieve password/hash:
  - During HotSync operation (IR, Serial, Network)
  - On Palm: "Unsaved Preferences" database
  - On host PC: **`\Palm\users.dat`**
  - On host Mac: **`Palm:Users:Palm Users`**

Mobile Devices: Palm OS >= 4.0 Password Retrieval

- Max. 32 characters ASCII
- Encoded block is 128-bit MD5 hash (not reversible)
- Dictionary attack still possible using common words
  - Take advantage of short passwords

Mobile Devices: Palm OS Backdoor Debug Mode

- Exists for debugging during app development
- Can install/delete/run apps, view raw memory, hard reset, export databases
- Can use to bypass “System Lockout” functionality (OS < 4.0)
  - **`www.grandideastudio.com/files/security/mobile/palm_backdoor_debug_advisory.txt`**
- No notification of activity is evident on device
- Can use *pdd* or *PDA Seizure* to create exact forensic image of data

Mobile Devices: Pocket PC Password Retrieval

- ActiveSync used for all communication between PC and device
  - Available through serial, USB, IR, TCP/IP, Bluetooth
- Reversible obfuscation method (XOR against constant)
- Can retrieve password/hash:
  - In host PC registry: **`HKEY_CURRENT_USER\Software\Microsoft\Windows Ce Services\Partners`**

Mobile Devices: Pocket PC Password Retrieval 2

- On some devices, 4-digit PIN used for authentication can be manually brute-forced
- Pocket PC registry accessible by any user on the device
  - PHM Registry Editor, **`www.phm.lu/Products/PocketPC/RegEdit`**
  - Ex.: PPP network passwords stored in plaintext
- Can change Control Panel Applet (cpl) entry in registry to redirect password screen
  - Microsoft "Let Me In" example, Q314989

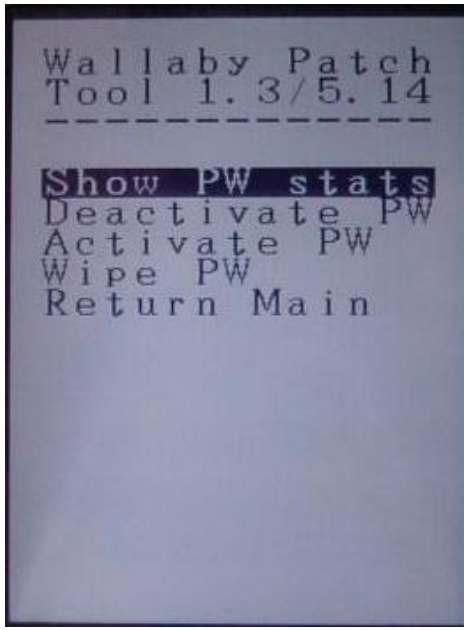
Mobile Devices: Visual Studio .Net Debugger

- Exists for debugging during app development
  - Provides remote debugging and device access to Windows CE / Pocket PC
  - Developer's documentation publicly available
  - Uses ActiveSync protocol
- Can access Pocket PC registry, install/delete/run apps, export databases

Mobile Devices: Pocket PC Phone Edition

- Allows access to a device without passing any access controls
  - **`http://forum.xda-developers.com`**
- Provides a detailed debugging and diagnostics interface through sync port
- Special mode to recognize diagnostic external memory cards and can execute code directly from them

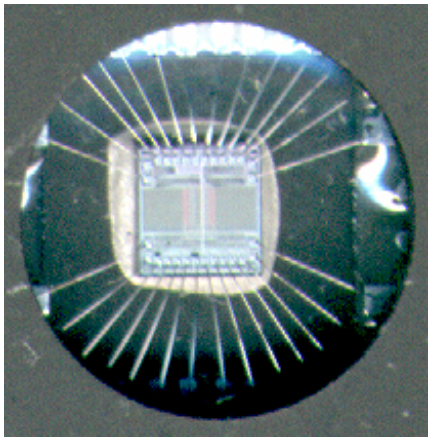
Mobile Devices: Pocket PC/XDA Bootloader

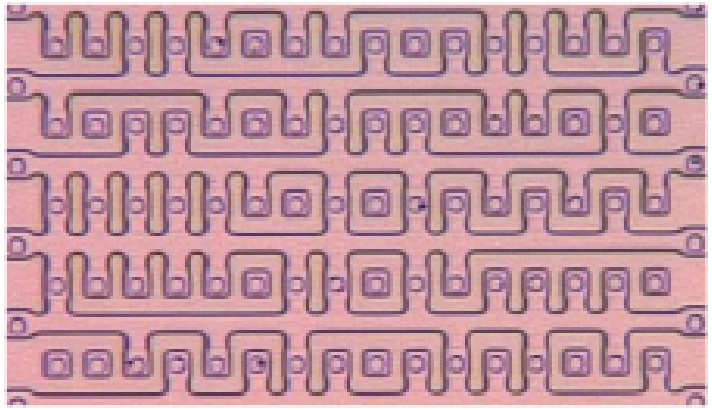


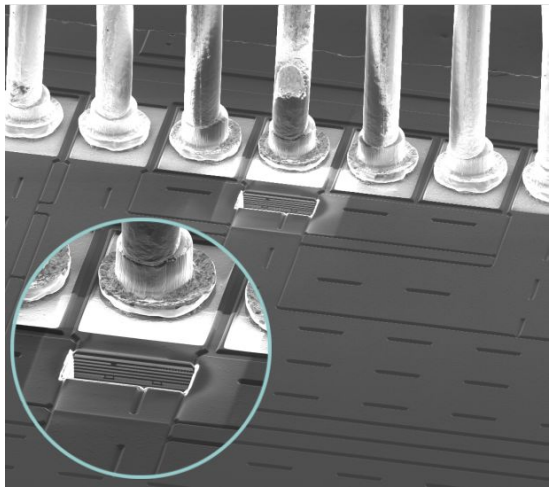
Source: "The Phone in the PDA," Job de Haas, Black Hat Amsterdam 2003

Advanced Attack Methods

- Chip Decapping and Die Analysis
  - Attacker can visually recreate contents or modify die (Ex.: to obtain crypto key or remove security bit)
  - Tools: Chip Decappers, Scanning Electron Microscope, Voltage Contrast Microscopy, Focused Ion Beam

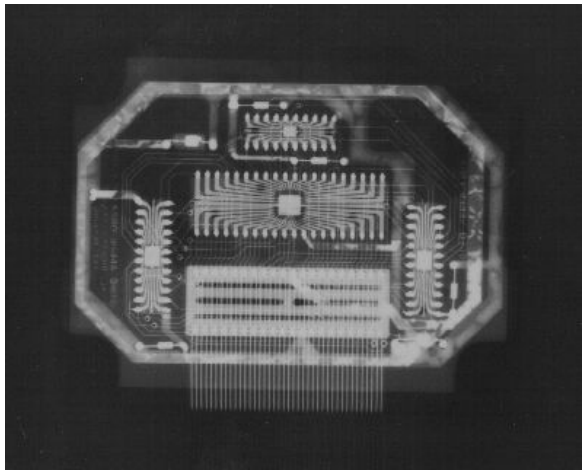






Advanced Attack Methods 2

- X-Ray
  - Attacker can bypass any encapsulation methods to determine inner bus structures and circuit configurations
  - "How to Crack a Pac Man Plus!," **`www.multigame.com/pacplus.html`**



Common Hardware Design Problems

- Most/many engineers not familiar with security
  - Ex.: Using XORs for "encryption" is recommended in some Verilog/VHDL books!
- Components easy to identify
  - Circuitry can easily be reverse engineered
- Many products based on publicly-available reference designs
- No anti-tamper mechanisms used
  - Easy to open up product and probe circuitry

Common Hardware Design Problems 2

- Improper protection of external memory
  - Most memory is notoriously insecure
  - Serial EEPROMs can be read in-circuit
  - SRAM-based FPGA configuration can be sniffed
- "Security through obscurity" still practiced
  - Hiding something does not make the problem go away

Conclusions

- Even though technology has advanced, same classes of problems still plague hardware
- Most, if not all, hardware solutions are open to attack
- Hardware is usually inherently trusted
  - Black box != security
- Blindly trusting hardware leads to a false sense of security
  - Hardware is not voodoo

Thanks!

Joe Grand
Grand Idea Studio, Inc.

www.grandideastudio.com