A Day In The Life of a Hacker

Things we get up to when nobody is looking, and that keep me awake at night...

Adam Laurie

adam@thebunker.net

http://www.thebunker.net

FIRST Geek Zone
Seville, 2007
Contents

• InfraRed

• RFID

• ATMs / (Magstripes?)
Who am I?

- Co-Maintainer of apache-ssl
- DEFCON goon
- Bunker non-exec
- Freelance Hacker
  - White Hat!
What do I do?
InfraRed

- IR is the ultimate in 'security by obscurity'
  - Invisible rays hide a multitude of sins
    - Simple codes
    - Total control
    - Inverted security model
      - End user device filters content
        - e.g. Hotel PPV TV
InfraRed

- Car keys
- Garage doors
- TVs
Garage Door Openers

- Simple code, manually configurable

- Dipswitch with 8 on / off bits = 256 possible codes
Analyse Data Bits With XMODE2

All on
S 11111111 s s s s

All off
S 00000000 s s s s

1-7 off, 8 on
S 00000001 s s s s

1 on, 2-8 off
S 10000000 s s s s

1-3 off, 4-6 on, 7-8 off
S 00011100 s s s s

Conclusion: 1 start bit, 8 data bits, 4 stop bits
TV Remotes

More complex codes (more bits)
OWNED BY
MAJOR MALFUNCTION
<table>
<thead>
<tr>
<th>SYSTEM STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MODE</td>
</tr>
<tr>
<td>COMMERCIAL</td>
</tr>
<tr>
<td>CHANNEL</td>
</tr>
<tr>
<td>TV 60 (ANTENNA)</td>
</tr>
<tr>
<td>DCM</td>
</tr>
<tr>
<td>ON</td>
</tr>
<tr>
<td>CODES</td>
</tr>
<tr>
<td>192 48 13 202 43</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>4 192 0 0 0</td>
</tr>
<tr>
<td>SIGNAL</td>
</tr>
<tr>
<td>TUNED</td>
</tr>
<tr>
<td>OP HRS</td>
</tr>
<tr>
<td>12DEh</td>
</tr>
<tr>
<td>ERRORS</td>
</tr>
<tr>
<td>0 0 0 0 0</td>
</tr>
<tr>
<td>L9USITY</td>
</tr>
<tr>
<td>2.51</td>
</tr>
<tr>
<td>TEAM AMERICA</td>
</tr>
<tr>
<td>WORLD POLICE</td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>---------------------------</td>
</tr>
<tr>
<td>mtiltree-30 version</td>
</tr>
<tr>
<td>File</td>
</tr>
<tr>
<td>Created</td>
</tr>
<tr>
<td>Started</td>
</tr>
<tr>
<td>Modulator</td>
</tr>
<tr>
<td>TV Channel</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Audio Channel</td>
</tr>
<tr>
<td>Screen pos</td>
</tr>
<tr>
<td>Slide file</td>
</tr>
<tr>
<td>Start time</td>
</tr>
<tr>
<td>Last session</td>
</tr>
<tr>
<td>Total sessions</td>
</tr>
<tr>
<td>Alives sent</td>
</tr>
<tr>
<td>Running on</td>
</tr>
<tr>
<td>Free RAM</td>
</tr>
</tbody>
</table>
HTTP/1.0 404 Object Not Found
You are not authorized to view this page

You might not have permission to view this directory or page using the credentials you supplied.

If you believe you should be able to view this directory or page, please try to contact the Web site by using any e-mail address or phone number that may be listed on the 192.0.1.192 home page.

You can click Search to look for information.

HTTP Error 403 - Forbidden
Internet Explorer
The page cannot be found

The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Please try the following:

- If you typed the page address in the Address bar, make sure that it is spelled correctly.
- Open the 192.0.1.192 home page, and then look for links to the information you want.
- Click the Book button to try another link.
- Click Search to look for information on the Internet.

HTTP 404 - File not found
Internet Explorer
Internet Service Manager
for Internet Information Server 3.0

Introduction

Welcome to the Microsoft Internet Information Server (IIS) Web-based administration tool. You can use this tool to administer or view your Microsoft Internet Information Server from remote locations. In order to log on successfully, please ensure that your Windows NT user account is a member of the Windows NT Administrators group. Note that it is not possible to start or stop IIS services with this Web administration tool.

Best experienced with

Microsoft

[Powered by BackOffice]

Click here to start.
Microsoft ScanDisk

ScanDisk is now checking the following areas of drive C:

CHANNEL INSTALLATION

CHANNEL  TV 67
CHANNEL RING  DELETED
LABEL  NONE
VIDEO BLANK
AUDIO BLANK
AUTO PROGRAM
EXIT

Pass  More Info  Exit

16x complete
EEPROM/SRAM Erase Program 1.2

Erasing 4K EEPROM
4K Erase OK

Erasing 16K EEPROM
16K Erase OK

Erasing 256K SRAM
256K Erase OK

EEPROM/SRAM Erase Successful
Please wait - we are looking for a free channel!
VALLEY GIRLS Vol. 1

All records required to be created and maintained pursuant to 18 U.S.C. §2257 and 28 C.F.R. 75, with respect to this videotape, including all original

CHANNEL INSTALLATION

CHANNEL TV100

CHANNEL RING DELETED

LABEL (NONE)

VIDEO BLANK OFF

AUDIO BLANK OFF

AUTO PROGRAM

EXIT

Madness Pictures 
All rights reserved © 2004.
I believe this makes sense in order to meet the EDT's requirements, as stated. However, it will be critical to determine very early on whether or not consultation is part of the assessment with the communication effectiveness. This is happens a lot in the field. Can engage to be a channel installation, label, video blank, audio blank, auto program, exit, priority, normal, request receipt, none, close window.
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/25</td>
<td>Room Charge</td>
<td>£87.00</td>
</tr>
<tr>
<td>04/25</td>
<td>Room Charge</td>
<td>£15.23</td>
</tr>
<tr>
<td>04/26</td>
<td>Room Charge</td>
<td>£87.00</td>
</tr>
<tr>
<td>04/26</td>
<td>Room Charge</td>
<td>£15.23</td>
</tr>
<tr>
<td>04/26</td>
<td>Room Service</td>
<td>£13.95</td>
</tr>
<tr>
<td>04/26</td>
<td>Room Service</td>
<td>£3.50</td>
</tr>
<tr>
<td>04/27</td>
<td>Room Charge</td>
<td>£87.00</td>
</tr>
<tr>
<td>04/27</td>
<td>Room Charge</td>
<td>£15.23</td>
</tr>
</tbody>
</table>

**Balance:** £983.00

**MORE**

**Return to Previous Menu**
Enter 4 digit wake up time (Example: 0630)
First two digits = hour (00-23)
Second two digits = minute (00-59)

Wake Up Time

0530

Is this time correct?
10 Yes

menu No
Guest Checkout Successful.
Thank You and Come Again

Hilton

Press the menu Button On Your
Hotel TV – New Capabilities

- Room enumeration
  - %age occupancy
  - Who's where
  - With who
  - Who's eating, drinking & viewing what
  - Where they've called
  - For how long
<table>
<thead>
<tr>
<th>AUTO-PROGRAMMING ACTIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 2 3 4 5 6 7</td>
</tr>
<tr>
<td>8 9 10 11 12 13 14</td>
</tr>
<tr>
<td>15 16 17 18 19 20 21</td>
</tr>
<tr>
<td>22 23 24 25 26 27 28</td>
</tr>
<tr>
<td>29 30 31 32 33 34 35</td>
</tr>
<tr>
<td>36 37 38 39 40 41 42</td>
</tr>
<tr>
<td>43 44 45 46 47 48 49</td>
</tr>
<tr>
<td>50 51 52 53 54 55 56</td>
</tr>
<tr>
<td>57 58 59 60 61 62 63</td>
</tr>
<tr>
<td>64 65 66 67 68 69 70</td>
</tr>
<tr>
<td>71 72 73 74 75 76 77</td>
</tr>
<tr>
<td>78 79 80 81 82 83 84</td>
</tr>
</tbody>
</table>

PRESS ANY KEY TO STOP
Welcome To

Barker Chan
IS 4-

Hilton

PRESS MENU
FOR ALL VIDEO & GUEST SERVICES
CHANNEL '▼' FOR TELEVISION STATIONS
©ONCOMMAND™
Welcome To
Hilton

BARKER CHAN
IS 42

PRESS MENU
FOR ALL VIDEO & GUEST SERVICES
CHANNEL 42 FOR TELEVISION STATIONS
ON COMMAND™
InfraRED - MMIrDA

Full slides from IR presentation here:

http://www.alcrypto.co.uk/MMIrDA/
RFID – Moo am I?

- Animal ID
- Hotel Door Entry
- Passport
- Car immobiliser
- Ski Pass
- Goods
Human Implants

WE WANT TO IMPLANT THIS RFID TAG IN YOU.
THAT VIOLATES MY RIGHTS!

WE WANT TO IMPLANT THIS RFID TAG IN YOU AND IT'S ALSO A CELLPHONE, DIGITAL CAMERA, AND MP3 PLAYER.

↑ WRONG

↓ RIGHT

COOL!
Human Implants

- Military
  - Access Control
- Mental Patients
  - Tracking
- Beach Bars
  - Digital Wallets
Unique ID!!!

- Cannot be cloned
- Cannot be cloned
- Cannot be cloned
- Cannot be cloned
- Cannot be cloned
- Cannot be cloned
- Cannot be cloned
- Cannot be cloned
Unique ID?

Spot the original?

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

- Industry Defence:
  “Clones do not have the same form factor and are therefore not true clones”
Unique ID?

- Readers cannot 'see' so form factor irrelevant and...
Unique ID?

- Readers cannot 'see' so form factor irrelevant

identical blanks ARE available...
Demonstration

• Clone ISO 11784 'Animal' TAG
  – Cow implant
  – VeriChip paperweight

• Clone Trovan 'Unique' TAG
  – Door entry system
RFID implanted chip threats

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

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

• Pseudo random UID
  - Cannot determine presence of specific passport without logging in

• Strong Authentication
  - Basic Access Control
    • 3DES

• Content Encryption
  - Extended Access Control
Deriving the Keys

- MRZ
  - Machine Readable Zone

- Key
  - Document Number
  - Date of Birth
  - Expiry Date
ePassport Demonstration
ePassport Modification

- “Not Possible” due to cryptographic signatures
  - Certificate Authority (CA) not verifiable
    - Signatures provided by document
    - CA Key provided by same document
    - Public Key Directory (PKD) not available

- Self-Signed Forgery may not be detected!
ePassport Certificates

New Zealand genuine:

Certificate:
  Data:
Version: 3 (0x2)
  Serial Number: 1122333666 (0x42e573e2)
  Signature Algorithm: sha256WithRSASignature
  Issuer: C=NZ, O=Government of New Zealand, OU=Passports, OU=Identity Services Passport CA
Validity
  Not After : May 18 12:00:00 2012 GMT
  Subject: C=NZ, O=Government of New Zealand, OU=Passports, OU=MRTD, CN=Document Signer
200701241034
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
      Modulus (2048 bit):
        ...

New Zealand forgery:

Certificate:

Data:

Version: 3 (0x2)

  Serial Number: 1122333666 (0x42e573e2)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=NZ, O=Government of New Zealand, OU=Passports, OU=Identity Services Passport CA

Validity

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

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

Subject Public Key Info:

  Public Key Algorithm: rsaEncryption
  RSA Public Key: (2048 bit)

  Modulus (2048 bit):

    ...

...
Other ePassport threats

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

• Open Source Python library

• Hardware independent
  – ACG
  – Frosch
  – PC/SC
  – OpenPCD coming soon

http://rfidiot.org
ACG reaction to RFIDIOt

“Unfortunately your companies activities seem to be counter to ACG's interests so we will not be able to support you any further.”

Email - 3rd January, 2007
This top-up card enables you to add credit directly to your T-Mobile pay as you go or U-Fix account in a wide range of outlets. This card can only be used with the T-Mobile (UK) pay as you go and U-Fix service and is subject to these terms and conditions. Use of this card constitutes acceptance of those conditions. This is not a debit, credit or identity card, or a voucher of any kind. For more information, or if you experience difficulty whilst using this card, please dial 150, direct from your mobile phone.

This card belongs to:

T-Mobile
This top-up card enables you to add credit directly to your T-Mobile pay as you go or U-Fix account in a wide range of outlets. This card can only be used with the T-Mobile (UK) pay as you go and U-Fix service and is subject to these terms and conditions. Use of this card constitutes acceptance of those conditions. This is not a debit, credit or identity card, or a voucher of any kind. For more information, or if you experience difficulty whilst using this card, please dial 150, direct from your mobile phone.

This card belongs to:
ATM 'default password' attack

- Non-bank based cash machines
  - Grocers, Newsagents, Petrol Stations etc.
- 'In-Band' management
  - Management interface is front panel
  - AND NOTHING ELSE!
- Simple activation, simple passwords
  - Two-key combination to access menu
  - Master '123456'
  - Admin '987654'
The Top Menu allows you to choose one of two options, CUSTOMER TRANSACTIONS or MANAGEMENT FUNCTIONS. Selecting CUSTOMER TRANSACTIONS changes the display to the Customer Welcome screen so the terminal is ready to perform customer transactions. Selecting MANAGEMENT FUNCTIONS opens the password screen, which in turn provides access to menus that are used for changing or viewing terminal parameters.

Whenever the MANAGEMENT FUNCTIONS choice is selected, the terminal will ask for a password to be entered. For a first-time configuration, enter the default MASTER PASSWORD of ‘123456’ on the keypad and then press the <ENTER> key. This ‘default’ password will be valid until it is changed.

**NOTE**

The operator of the terminal must change the MASTER PASSWORD to a new password when the installation is complete.

The Top Menu serves an alternative purpose in the event of a machine malfunction or other error condition. Such conditions are normally reported by an “OUT OF SERVICE” message screen. The typical response to this message is to reset the terminal. After resetting the terminal the Top Menu screen will display any appli-
ATM Management

• No command to 'empty' cash trays
  - 'Purge' goes to internal tray

• No command to dispense cash
  - Test dispense goes to internal tray

• So what good is getting into the menu?
**FACTORY DEFAULT:** ‘$0.00’

**ACCESS INSTRUCTIONS:**

1. Select **TERMINAL CONFIGURATION** from the **MANAGEMENT FUNCTIONS** menu.
2. Select **SET TERMINAL PARAMETERS**.
3. Select **CASSETTE SETUP**.
4. Choose the **CASSETTE PARAMETERS** option.
5. Choose a cassette (A, B, C, or D).
6. Select the **VALUE** option.

**DESCRIPTION:**

The **VALUE** function allows the operator to set the value of a cash or non-cash item in a particular cassette. For cash, **VALUE** must be the denomination of the currency currently inside that particular cassette. For a non-cash item, **VALUE** sets the value of the item in a cassette.
The Attack

- Enter management mode
- Change value of high denomination notes
  - £20 becomes £5
- Withdraw '£100'
- Receive £400
- Change it back!
  - Or get caught... :)


The Response

• Manufacturers removed manuals from websites
  - Were still there 72 hours after international news items
  - Are still on 3\textsuperscript{rd} party sites today

• Too little, too late!
Defence

• Internal button or other secondary system
Defence

• Internal button or other secondary system
Lock Kit - spin dial for various model ATM machines (Complete) - B3330

Your Price: $59.00

Qty: 1

Add to Cart

Browse Parts for ATMs
Manufactured By: Triton

Email this to a friend
Lock-electronic combination for all Triton ATM machines as well as some Tidel and Tranax models. Includes keypad, locking mechanism, battery holder, 9 V battery and hardware, as well as 2 conversion screws for upgrading from spindal lock.

Your Price: $145.00

Qty: 1

Add to Cart
Keypads and PINs
Questions?

http://rfidiot.org

adam@algroup.co.uk