

Hacking Exposed 7

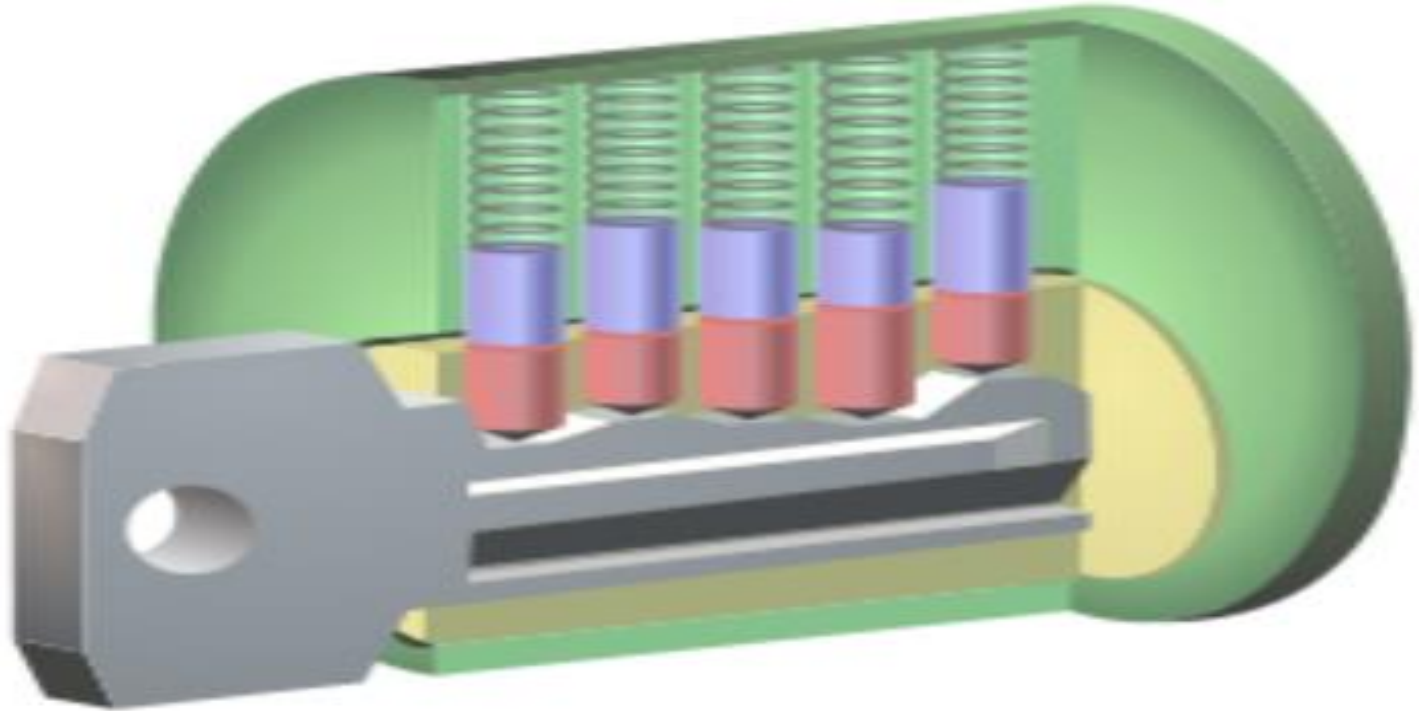
Network Security Secrets & Solutions

Chapter 9 Hacking Hardware

Hacking Hardware outline

- Physical Access: Getting In The Door
- Hacking Devices
- Reverse Engineering Hardware

Normal Key



When the correct key is inserted, the gaps between the key pins (red) and driver pins (blue) align with the edge of the plug, called the shear line(yellow).



Bump Key



- Every key pin falls to its lowest point
- The key is hit with a screwdriver to create mechanical shocks
- The key pins move up and briefly pass through the shear line
- The lock can be opened at the instant the key pins align on the shear line

Results of Bump Key Use

- A experienced bumper can open the lock as quickly as a person with the correct key
- Bumping does not damage the lock
 - Unless it is done many times, or clumsily
- Bumping leaves no evidence behind
- Open Doors, Racks, PC cases, Laptop cable locks, ...

White House High-Security Locks Broken: Bumped and Picked at DefCon

By Kim Zetter 

August 05, 2007 | 4:19:00 PM

Categories: [DefCon](#), [Hacks And Cracks](#)

A group of researchers has cracked the security features in what are supposed to be some of the world's most secure locks -- locks that are used at the White House, the Pentagon, embassies and other critical locations.

The researchers presented their findings for the first time at the DefCon hacker conference this weekend and showed how they could easily bump and pick the newest high-security M3 locks made by Medeco, a company that owns an estimated 70 percent of the lock market.



- Even Medeco locks used in the White House can be bumped

Bump Key Countermeasures

- Some locks (like Medeco) are designed to make bumping difficult
- They use a sidebar and angled pins to make normal picking and bumping ineffective
 - Don't trust their claims too far
- Don't rely solely on locks: use two-factor authentication
 - PIN keypad
 - Fingerprint
 - Security guard
 - etc.

Cloning Access Cards

- Two Varieties
 - Magnetic stripe cards
 - RFID (Radio Frequency Identification) cards
 - Often called *proximity cards*

Magstripe Cards

- ISO Standards specify three tracks of data
- There are various standards, but usually no encryption is used
 - Link Ch 922

Track one, Format B:

- **Start sentinel** — one character (generally '%')
- **Format code="B"** — one character (alpha only)
- **Primary account number (PAN)** — up to 19 characters. Usually, but not always, matches the **credit card number** printed on the front of the card.
- **Field Separator** — one character (generally '^')
- **Name** — two to 26 characters
- **Field Separator** — one character (generally '^')
- **Expiration date** — four characters in the form YYMM.

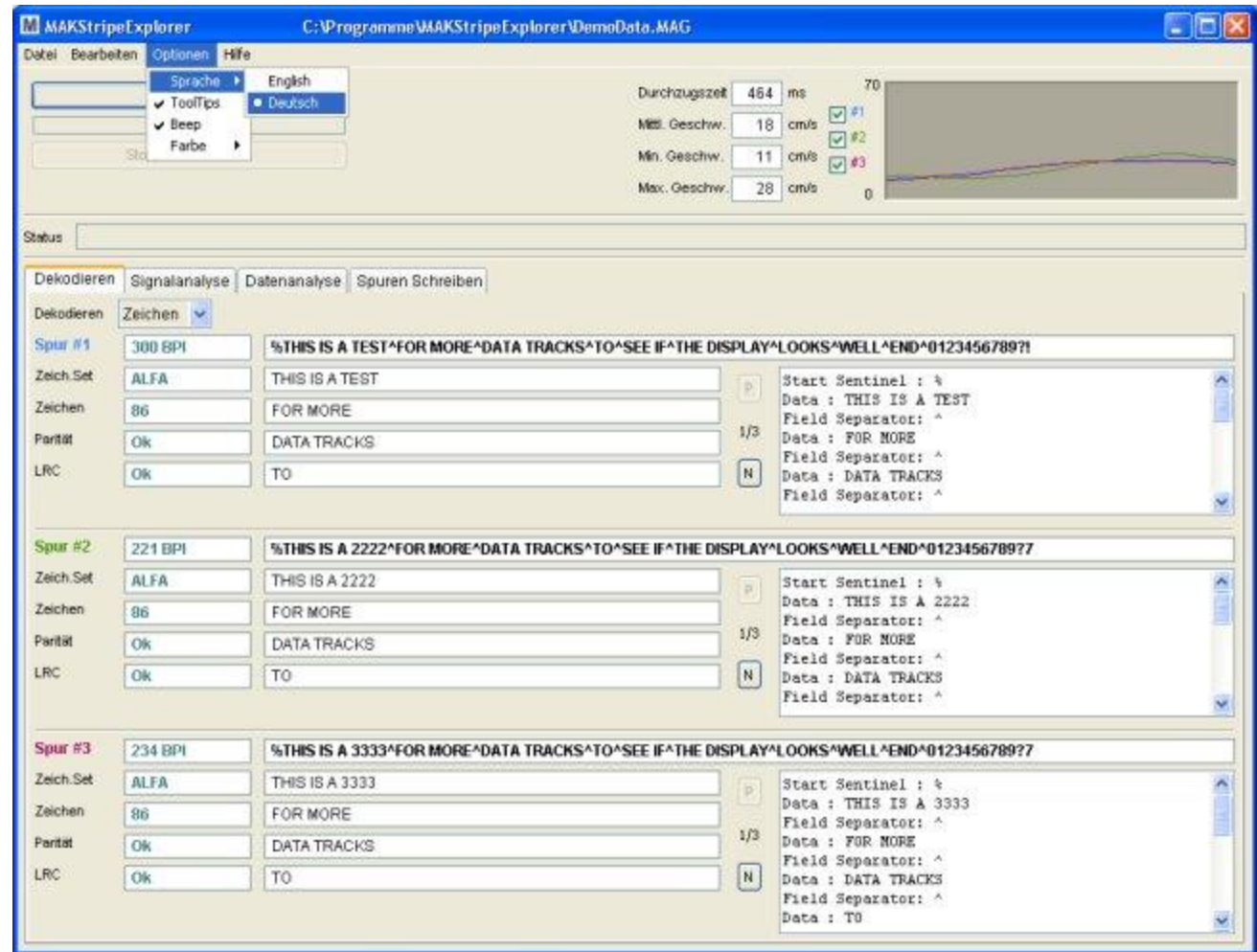
Magstripe Card Reader/Writer

- USB connector
- About \$35.00



Magnetic-Stripe Card Explorer

- Software



Physical Access: Getting In The Door

Cloning Access Cards

1. Magnetic stripe

- Contain three tracks of data, e.g., ID number, serial number, name, address, etc.
- No security measures to protect data
- Not clear encoding

– Tools

- A magstripe card reader/writer
 - Magnetic-Stripe Card Explorer (software)
 - Read
 - » read multiple cards of the same type to detect the different bits
 - Write
 - » determine what checksum is used → recalculate a new one

Hacking RFID Cards

- RFID cards use radio signals instead of magnetism
- Now required in passports
- Data can be read at a distance, and is usually unencrypted

MiFare Classic

- Mifare is most widely deployed brand of secure RFID chips
- **Radboud University Nijmegen** researchers found weaknesses in MiFare proprietary encryption in 2008
 - *Don't roll your own crypto!*

Security of MIFARE Classic, MIFARE DESFire and MIFARE Ultralight [edit]

The encryption used by the MIFARE Classic IC uses a 48-bit key.^[23]

A presentation by Henryk Plötz and **Karsten Nohl**^[24] at the [Chaos Communication Congress](#) in December 2007 described a partial reverse-engineering of the algorithm used in the MIFARE Classic chip. Abstract and slides^[25] are available online. A paper that describes the process of reverse engineering this chip was published at the August 2008 [USENIX](#) security conference.^[26]

In March 2008 the Digital Security^[27] research group of the [Radboud University Nijmegen](#) made public that they performed a complete reverse-engineering and were able to clone and manipulate the contents of an [OV-Chipkaart](#) which is using MIFARE Classic chip.^[28] For demonstration they used the Proxmark device, a 125 kHz / 13.56 MHz research instrument.^[29] The schematics and software are released under the free [GNU General Public License](#) by [Jonathan Westhues](#) in 2007. They demonstrate it is even possible to perform card-only attacks using just an ordinary stock-commercial NFC reader in combination with the libnfc library.

The Radboud University published four scientific papers concerning the security of the MIFARE Classic:


- A Practical Attack on the MIFARE Classic^[30]
- Dismantling MIFARE Classic^[31]
- Wirelessly Pickpocketing a MIFARE Classic Card^[32]
- Ciphertext-only Cryptanalysis on Hardened MIFARE Classic Cards^[33]

In response to these attacks, the Dutch [Minister of the Interior and Kingdom Relations](#) stated that they would investigate whether the introduction of the Dutch Rijkspas could be brought forward from Q4 of 2008.^[34]

NXP tried to stop the publication of the second article by requesting a preliminary injunction. However, the injunction was denied, with the court noting that, "It should be considered that the publication of scientific studies carries a lot of weight in a democratic society, as does informing society about serious issues in the chip, because it allows for mitigating of the risks."^{[35][36]}

Both independent research results are confirmed by the manufacturer NXP.^[37] These attacks on the cards didn't stop the further introduction of the card as the only accepted card for all Dutch public transport the [OV-chipkaart](#) continued as nothing happened^[38] but in October 2011 the company [TLS](#), responsible for the OV-Chipkaart announced that the new version of the card will be better protected against fraud.^[39]

Ciphertext-only Cryptanalysis on Hardened Mifare Classic Cards


Full Text:  [PDF](#)Authors: [Carlo Meijer](#) [Radboud University, Nijmegen, Netherlands](#)
[Roel Verdult](#) [Radboud University, Nijmegen, Netherlands](#)

Published in:








• Proceeding
[CCS '15](#) Proceedings of the 22nd ACM SIGSAC Conference on
 Computer and Communications Security
 Pages 18-30

Denver, Colorado, USA — October 12 - 16, 2015

[ACM](#) New York, NY, USA ©2015[table of contents](#) ISBN: 978-1-4503-3832-5doi> [10.1145/2810103.2813641](https://doi.org/10.1145/2810103.2813641) 2015 Article[Bibliometrics](#)

- Citation Count: 0
- Downloads (cumulative): 533
- Downloads (12 Months): 75
- Downloads (6 Weeks): 9

Tools and Resource

 [Request Permissions](#)TOC Service:
 [Email](#)  [RSS](#)  [RSS](#) [Save to Binder](#)Export Formats:
[BibTeX](#) [EndNote](#) [ACM](#) Upcoming Conference
[CCS '18](#)

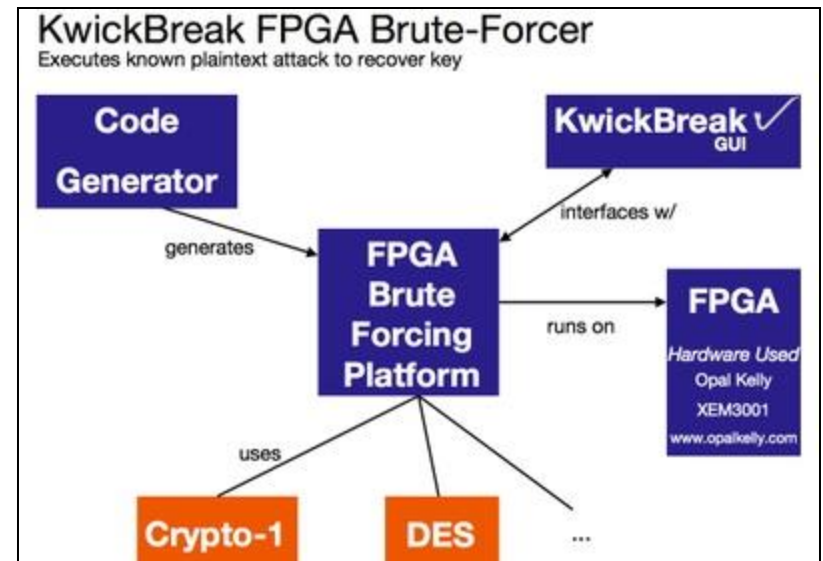
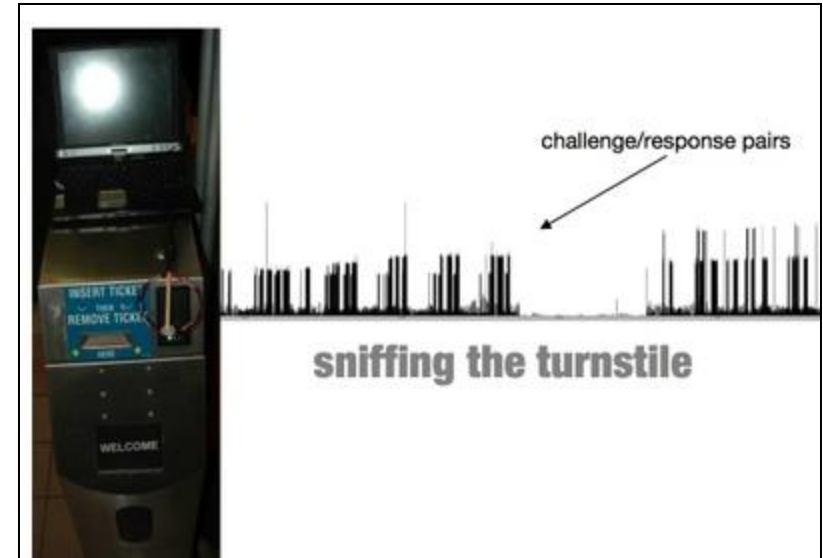
Share:

     [Author Tags](#) ▼[Similar Patents and Articles](#) ▼[Contact Us](#) | Switch to [single page view](#) (no tabs)[Abstract](#)[Authors](#)[References](#)[Cited By](#)[Index Terms](#)[Publication](#)[Reviews](#)[Comments](#)[Table of Contents](#)

Despite a series of attacks, MIFARE Classic is still the world's most widely deployed contactless smartcard on the market. The Classic uses a proprietary stream cipher CRYPTO1 to provide confidentiality and mutual authentication between card and reader. However, once the cipher was

Boston Subway Hack

- The Massachusetts Bay Transportation Authority claims that they added proprietary encryption to make their MiFare Classic cards secure
- But Ron Rivest's students from MIT hacked into it anyway



Physical Access: Cloning Access Cards

RFID

- Most cards access RFID on two different spectrums
 - 135 kHz or 13.56 MHz.
 - Many RFID cards are unprotected
 - » Recently, more RFID cards employ cryptography
 - Hardware tools are available at Openpcd.org for the reader and for common RFID cards
 - More advanced tools:
 - » **Proxmark3 + on-board FPGA** for the decoding of different RFID protocols
 - » **Universal Software waves Radio Peripheral (USRP)** to intercept the RFID traffic
 - Send and receive raw signals (capture and replay)

Countermeasures for Cloning RFID Access Cards

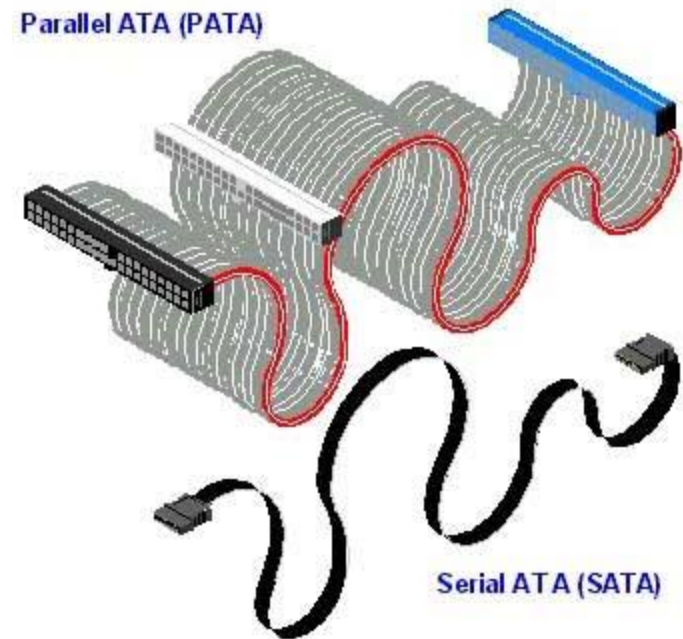
- Before: Card vendor want to lower their costs
RFID technology as inexpensive as possible
- Now: Fully cryptographic to prevent cloning, replay, etc.
 - Private key stored on the card
 - Challenge-response algorithm
 - » RFID Card receive challenge when energized.
 - » RFID send reply based on local private key to reader
 - » Reader validates the response before access
 - Some use open algorithms, others are proprietary

Hacking Devices

ATA Interfaces for Hard Drives

- Two kinds of ATA (Advanced Technology Attachment) interfaces are used
- PATA (Parallel ATA)
 - IDE is now called PATA
- SATA (Serial ATA)
 - Newer and faster than PATA

From Computer Desktop Encyclopedia
© 2004 The Computer Language Co. Inc.



ATA Security

- Requires a password to access the hard disk
- Virtually every hard drive made since 2000 has this feature
- It is part of the ATA specification, and thus not specific to any brand or device.
- Does not encrypt the disk, but prevents access

New ATA Password Virus?

- ATA Security is used on Microsoft Xbox hard drives and laptops
- BUT desktop machines' BIOS is often unaware of ATA security
- An attacker could turn on ATA security, and effectively destroy a hard drive, or hold it for ransom
 - The machine won't boot, and no BIOS command can help
 - This is only a theoretical attack at the moment

Hacking Locked Hard Disk

- Bypassing ATA (Advanced Technology Attachment) password security
- ATA security to deter the usage of a stolen laptop
 - ATA requires users type password before bios access hard disk
- Common and simple trick → Hot-swap attack (Fool BIOS)
 - **Hot-swap attack** steps
 - Find a computer (capable of setting ATA password and an unlocked drive)
 - Boot the computer with the unlocked drive
 - Enter BIOS interface → prepare to set a BIOS password
 - Replace the unlocked drive with the locked drive (Carefully)
 - Set the hddisk password using BIOS interface → The drive will accept the new password
 - Reboot → BIOS prompt you to unlock the drive bypassing the old one.
 - The password can be cleared from the system if a new password is not desired.

The logo for VOGON, with the letters 'VOGON' in a bold, white, sans-serif font. The letter 'O' is stylized with a red and yellow circular graphic behind it.

INVESTIGATION SERVICES

LABORATORY SERVICES

FORENSIC SYSTEMS

The Password Cracker: integration with the Imaging and Remote Preview Pod

The Password Cracker pod integrates into our [Imaging and Remote Preview Pod system](#). The Imaging and Remote Preview Pod can be used to access data files from a target or suspect hard drive with complete confidence that the data on the drive will not be changed. The computer system used to access the data files must be running a compatible operating system and application program. Alternatively, files may be viewed using our forensic software. When used with Vogon 32-bit Windows based imaging software, extremely high volumes of computer data can be captured quickly and efficiently with absolute assurance of data integrity. The imaging software has been developed by Vogon over the past decade to offer very high imaging performance together with comprehensive auditing and anti-repudiation techniques. This imaging process is independent of the file system(s) on the hard drive under investigation, and is recognised by courts around the world as the only valid means of capturing computer evidence.

Features of the Imaging and Remote Preview Pod

- Forensically sound imaging for IDE and SCSI disks
- Preview capability
- Automatic and full write protection
- Hard drive connectivity
- Password Cracker connectivity

Features of the 32-bit Imaging Software

- High performance
- Progress and status reporting
- Real-time reporting
- Anti-repudiation facility

- Home Page
- Emergency Help
- Evolution of Forensic Computing
- Hardware
- Software
- Password Cracker
 - The Solution
 - The Process
 - Integration
- Computer Electronic Disclosure
- Training



Bypassing ATA Passwords

- Vogon Password Cracker POD
 - Changes the password from a simple GUI
 - Allows law enforcement to image the drive, then restore the original password, so the owner never knows anything has happened
 - Works by accessing the **drive service area**
 - A special area on a disk used for firmware, geometry information, etc.
 - Inaccessible to the user

Hacking Devices

Locked Hard Disk

– Countermeasures

- The best defense
 - Do not rely on ATA security to protect drives
- Alternatively, use full disk encryption products
 - Bitlocker
 - TrueCrypt
 - SecurStar

U3 Drives

U3: Software on a Flash Drive

- Carry your data and your applications in your pocket!
- It's like a tiny laptop!



Meet the next generation of USB flash drives: the U3 smart drive. It's what's inside that makes them smart.

- Carry and access your files easily
- Keep your data safe and secure
- Comes with pre-loaded software
- Hundreds of software titles available

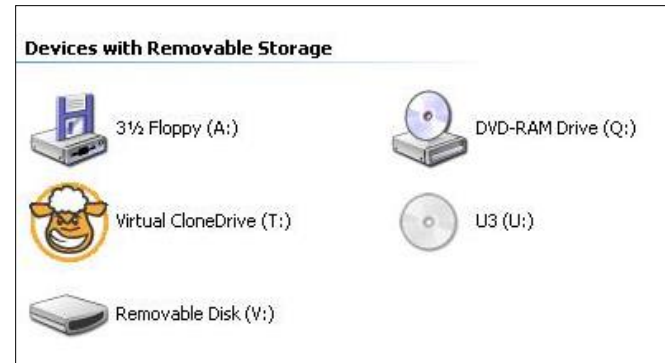
U3 Launchpad

- Just plug it in, and the Launchpad appears
- Run your applications on anyone's machine
- Take all data away with you



How U3 Works

- The U3 drive appears as two devices in My Computer
 - A “Removable Disk”
 - A hidden CD drive named “U3”
- The CD contains software that automatically runs on computers that have Autorun enabled
 - For more details, see <http://www.everythingusb.com/u3.html>



Hak9' s PocketKnife

Software On The Disk Partition

- PocketKnife is a suite of powerful hacking tools that lives on the disk partition of the U3 drive
- Just like other applications

U3 PocketKnife

- Steal passwords
- Product keys
- Steal files
- Kill antivirus software
- Turn off the Firewall
- And more...
- For details see <http://wapurl.co.uk/?719WZ2T>

```
USB Pocket Knife Utilities by Leapo

[ Select the number of an item to enable/disable ]

[ 1. Dump Cache Disabled ]
[ 2. Dump Firefox Passwords Disabled ]
[ 3. Dump Internet Explorer Passwords Disabled ]
[ 4. Dump LSA Secrets Disabled ]
[ 5. Dump Mail Passwords Disabled ]
[ 6. Dump MSN Messenger Passwords Disabled ]
[ 7. Dump Network Passwords Disabled ]
[ 8. Dump Product Keys Disabled ]
[ 9. Dump the Windows SAM using FGDUMP Disabled ]
[ A. Dump the Windows SAM using PWDUMP Enabled ]
[ B. Dump Windows Update list Disabled ]
[ C. Dump URL History Disabled ]
[ D. Dump WIFI Password Hex Disabled ]
[ E. Dump External IP Disabled ]
[ F. Dump Network Services Disabled ]
[ G. Run Port Scan Disabled ]
[ H. Dump System Information Disabled ]
[ I. Run AVKILL Disabled ]
[ J. Disable the Windows Firewall Disabled ]
[ K. Slurp Application Info Disabled ]
[ L. Slurp User Files [large Files] Disabled ]

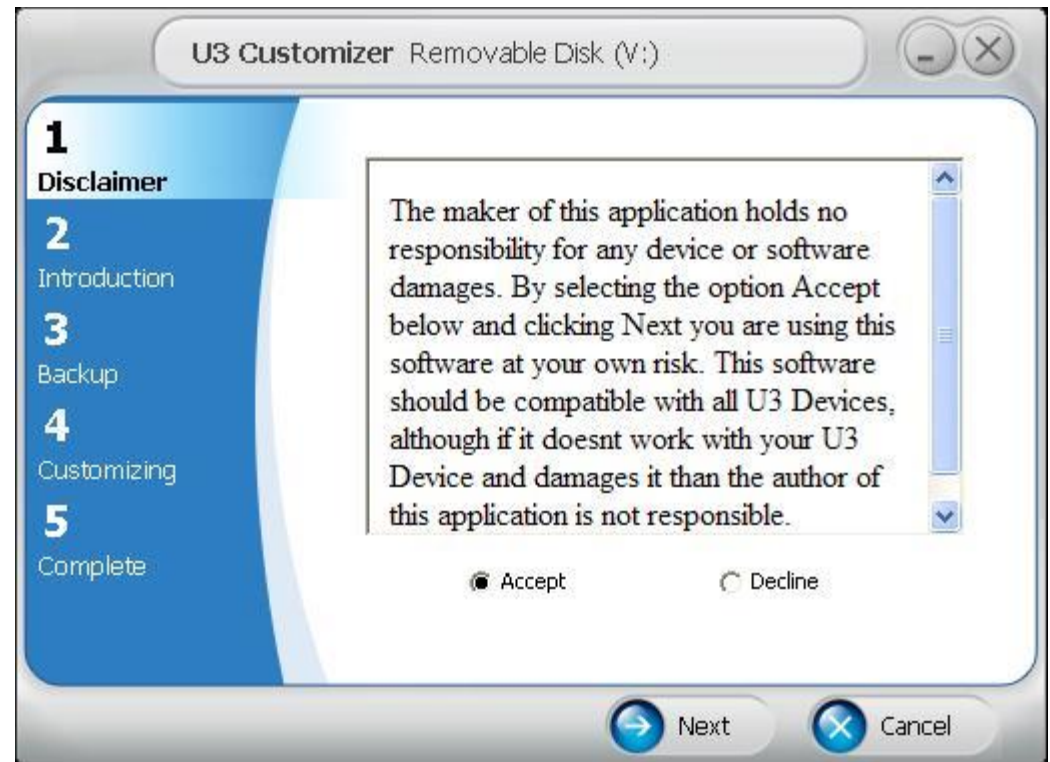
[ P. Back to Components Menu ]
[ M. Return to Main Menu ]
[ Q. Quit ]

Enter option: _
```

Custom Launchpad

Customizing U3

- You can create a custom file to be executed when a U3 drive is plugged in



Automatically Run PocketKnife

- **Universal_Customizer.exe** write ISO containing **Fgdump script** into flash disk
- The custom U3 launcher runs PocketKnife
- So all those things are stolen and put on the flash drive

Defense

Microsoft has Limited AutoRun

February 9, 2011, 2:21PM

Microsoft Pushes Fix to Disable AutoRun

by Dennis Fisher

 Like 3




 Follow

 +1 0



 Comment

As malware authors and attackers have continued to employ the Windows AutoRun functionality to help spread their malicious creations--culminating famously in the Stuxnet worm--Microsoft has been making gradual changes to help prevent these attacks. This week the company took the major step of putting an optional fix into Windows Update that will disable Autorun .

Military Bans USB Thumb Drives

Military USB Ban Meant to Stop 'Adversary Attacks'

By Noah Shachtman  November 20, 2008 | 3:03:20 PM Categories: [Info War](#)

The military isn't banning the use of "thumb" drives, CDs, and other data storage media just because of a simple, troublesome worm. It's banning the disks and drives because this worm demonstrates how vulnerable the armed force's networks are to enemy attack.

"It is apparent that over time, our posture to protect networks and associated information infrastructure has not kept pace with adversary efforts to penetrate, disrupt, interrupt, exploit or destroy critical elements of the GIG [Global Information Grid]," reads an e-mail from the head of U.S. Strategic Command, obtained by [Inside Defense](#).



Immediate Risk Reduction

- Block all USB devices in Group Policy
- Disable AutoRun
- Glue USB ports shut

Better Solution: IEEE 1667

- Standard Protocol for Authentication in Host Attachments of Transient Storage Devices
- USB devices can be signed and authenticates, so only authorized devices are allowed
- Implemented in Windows 7

Hacking Devices

USB U3 Hack to a System

- Easiest ways into a system
- U3 system is a secondary partition
 - USB flash drive made by SanDisk and Memorex
 - U3 menu is executed automatically when USB stick is inserted.
- Hack work by taking advantage of Win auto run feature
- Autorun.ini in U3 partition runs
 - U3 partition can be overwritten
 - Attack by reading the password hashes from the local Windows password file or install a Trojan for remote access
 - **Universal_Customizer.exe** write ISO containing **Fgdump script** into flash disk
- Countermeasures
 - Disable auto run (Check Windows support for how to)
 - Hold SHIFT key before inserting USB.
 - Prevent auto run from launching the default program.

Default Configurations

ASUS Eee PC Rooted Out of the Box

- The Eee PC 701 shipped with Xandros Linux
- The Samba file-sharing service was on by default
- It was a vulnerable version, easily rooted by Metasploit

Easy to learn, **Easy** to work, **Easy** to root

Default Passwords

Default Password List					
2008-03-14					
Vendor	Model	Version	Access Type	Username	PASSWORD
3COM	CellPlex		7000 Telnet	root	(none)
3COM	Switch	3300XM	Multi	admin	admin
3COM	LANplex		2500 Telnet	tech	tech
3COM	officeconnect		Multi	n/a	(none)
3COM	CellPlex		7000 Telnet	tech	tech

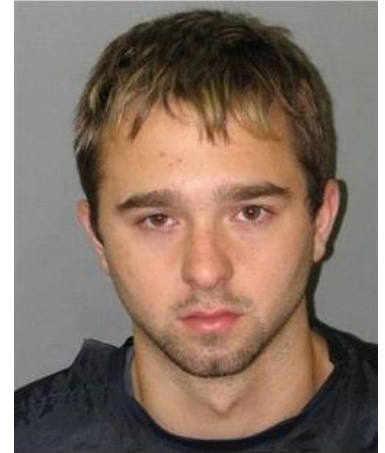
- Many devices ship with default passwords that are often left unchanged
 - Especially routers

ATM Passwords

Two Arrested in First Bust for ATM Reprogramming Scam

By Kevin Poulsen  September 23, 2008 | 4:44:48 PM Categories: [Crime](#)

- In 2008, these men used default passwords to reprogram ATM machines to hand out \$20 bills like they were \$1 bills



Nicholas Foster
Image: Lincoln Police Department



Jordan Eske
Image: Lincoln Police Department

ATM Machine at LayerOne Hacking Conference



Bluetooth Attacks

Eavesdropping on Bluetooth Headsets

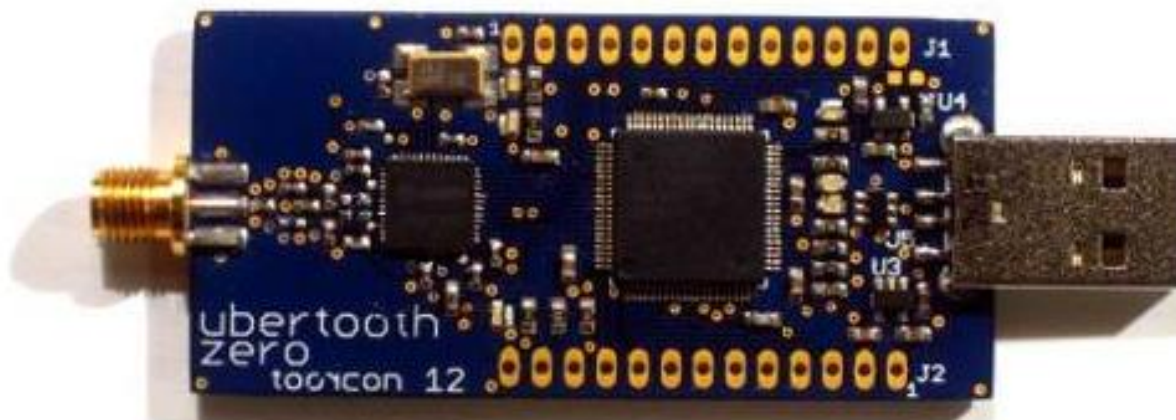


- Bluetooth supports encryption, but it's off by default, and the password is 0000 by default



Project Ubertooth

an open source 2.4 GHz wireless development platform suitable for Bluetooth experimentation



Hacking Devices

Hack Phone by Bluetooth

- Bluetooth can hack phone sync, make calls, transfer data, etc. (nearly Bluetooth protocol)
 - Steal contacts, social engineering
- **Ubertooth**, a hardware tool, for sniffing and playback of Bluetooth frames
 - 80 Bluetooth channels in 2.4 GHz ISM band
 - Spectrum analysis

Reverse Engineering Hardware

Reverse Engineering Hardware

Integrated Circuit Chips

- To unlock the information inside customized devices
- Mapping the device
 - Identify Integrated Circuit (IC) chips
 - Google IC data sheet → packaging, pin diagram, etc.
 - Available external interfaces
 - HDMI, USB, JTAG, etc.
 - Identifying important pins
 - Modern boards are multilayer (Difficult)
 - Use **multimeter** (toning function) to create bus map
 - » Beep when a wire is connected

Reverse Engineering Hardware

IC Chips

—Sniffing bus data

- Generally unprotected → Man-in-the-middle attack
 - intercept, replay
- Encrypted information as chip to chip
 - DRM (Digital Right Management) systems
 - » E.g., HDMI-HDCP
 - (**H**igh-bandwidth **D**igital **C**ontent **P**rotection)
- Use **a logic analyzer** to see and record signal on the bus
 - Some provide built-in decoders for I2C, SPI, Serial

Reverse Engineering Hardware

Sniffing Wireless Interface

- Layer 2 software attack, i.e. [802.11](#) [Wi-Fi](#) operates at the data link layer.
- Hack steps
 - Identify FCC ID of the devices
 - Useful information
 - » Radio frequencies on which the device is to operate.
 - » Internal diagrams
 - Symbol decoding
 - Radio frequencies + type of modulation
 - Decode lowest level bits from wireless channel
 - Software-Defined Radio
 - » Tools: WinRadio or USRP

About the FCC

Proceedings & Actions

Licensing & Databases

Reports & Research

News & Events

Home / Engineering & Technology / Laboratory Division / Equipment Authorization Approval Guide /

FCC ID Search

Equipment Authorization Approval Guide

Approval Procedures

Measurement Procedures

Grantee Code

Importation

Knowledge Database

FCC ID Search

Equipment Authorization System

Testing Laboratory Search

FCC ID Search Form

Help

Advanced Search

Grantee Code: (First three or five characters of FCCID)

Product Code: (Remaining characters of FCCID)

search

Advanced Search

Reverse Engineering Hardware

Firmware Reversing

- A plethora of juicy information about the device
 - Default passwords, admin ports, unintentional backdoor, debug interfaces...
- Hex editor (Hex → ASCII)
 - Tools: 010 editor and IDA pro
 - Unix command strings
 - Guess: password, encryption used (i.e. AES)...
- EEPROM programmers
 - Read/write firmware file

Reverse Engineering Hardware

Firmware Reversing

- Microcontroller tools: MPLAB IDE
- ICE (In Circuit Emulator) tools
 - Hardware debugger
 - Contact manufacturer to check available ICE
- JTAG (Joint Test Action Group)
 - Testing interface among components on printed circuit boards (PCB)
 - One size does not fit all

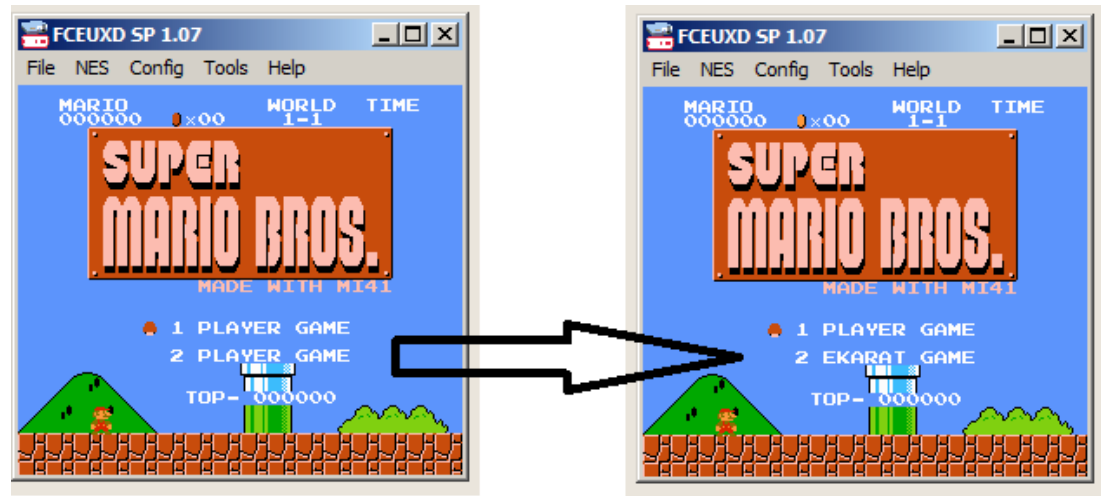
Homework Ch9 (1/2)

1) (60 points) Hacking (a game) ROM

1.1) Learn how to hack a game ROM from this link

<http://www.nintendoage.com/forum/messageview.cfm?catid=22&threadid=19733>

1.2) Change **2 PLAYER GAME** in menu to **2 Your Name GAME**, e.g., I change the **2 PLAYER GAME** to **2 EKARAT GAME**. Capture and paste your change.



* You can download the target game rom (Super Mario Adventure (SMB1 Hack).nes) at the course webpage.

Homework Ch9 (2/2)

2) (20 points) Use your Hex editor to modify any programs you want, and tell us

2.1 What is the target program?

2.2 What is your modification? Show the captured screen of the result.

3) (20 points) Do a research. What are the difference between PlayStation4 and PlayStation3 in terms of hardware security aspects?

\

