MWR Labs

++

WiFi Security: Wireless Weaknesses and Router Rooting

Nick Jones and Dan Clifford

17th May 2016

MWR LABS

++
Who Are We?

+ MWR InfoSecurity – A global, independent, research-led cyber security consultancy

+ Global – Offices in UK, South Africa, Dubai, Singapore, New York

+ Research-led – industry leaders producing novel research on interesting topics

+ Cyber security consultancy – working with our clients to secure their systems and applications

++

Why Are We Awesome?

+ Consultants present at Black Hat, DEF CON, Troopers, SyScan, 44Con and many others

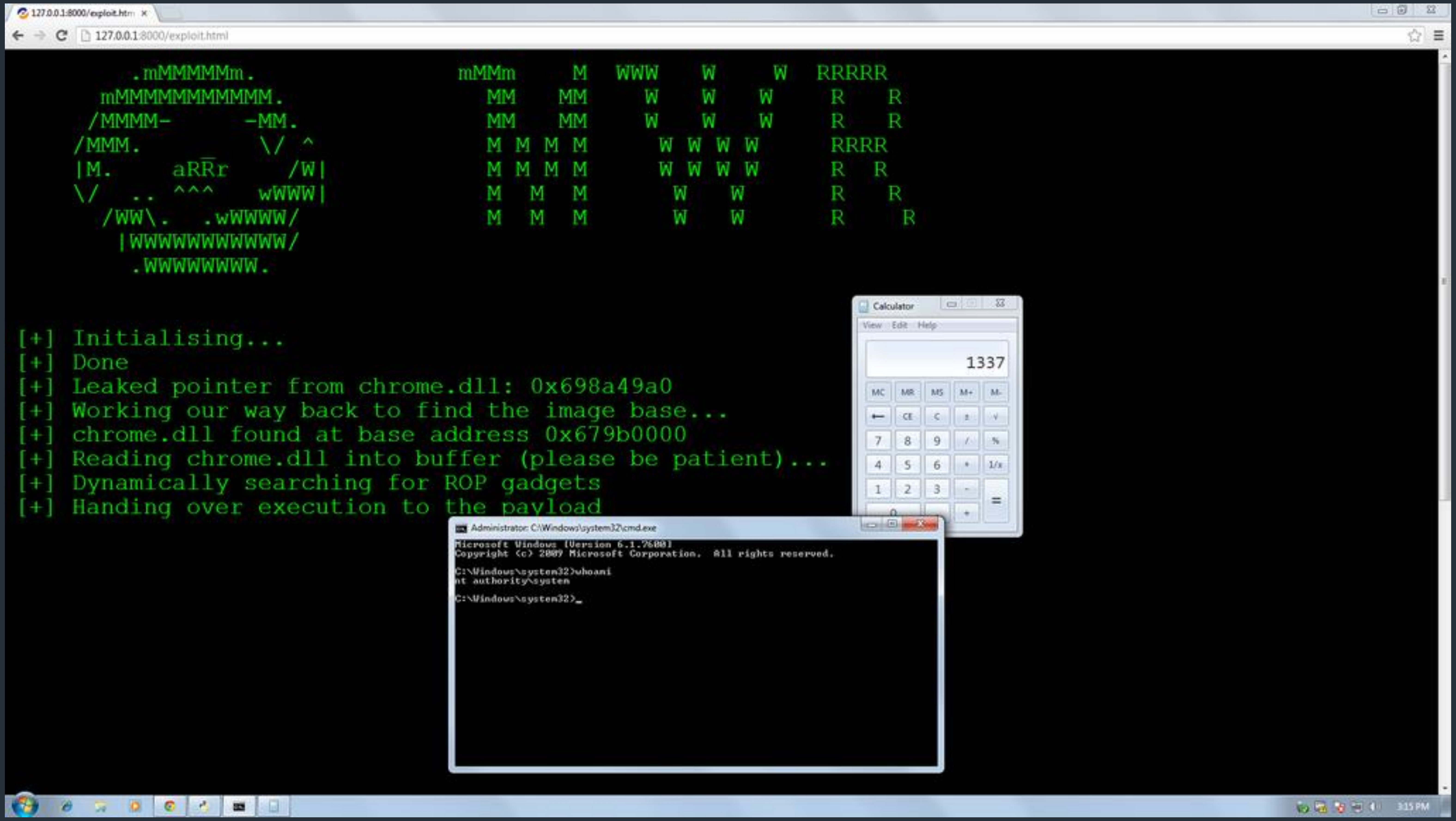
+ Multiple Pwn2Own and Mobile Pwn2Own wins

+ HackFu – Internal two-day team information security challenge

+ MWRICON – Internal conference

++

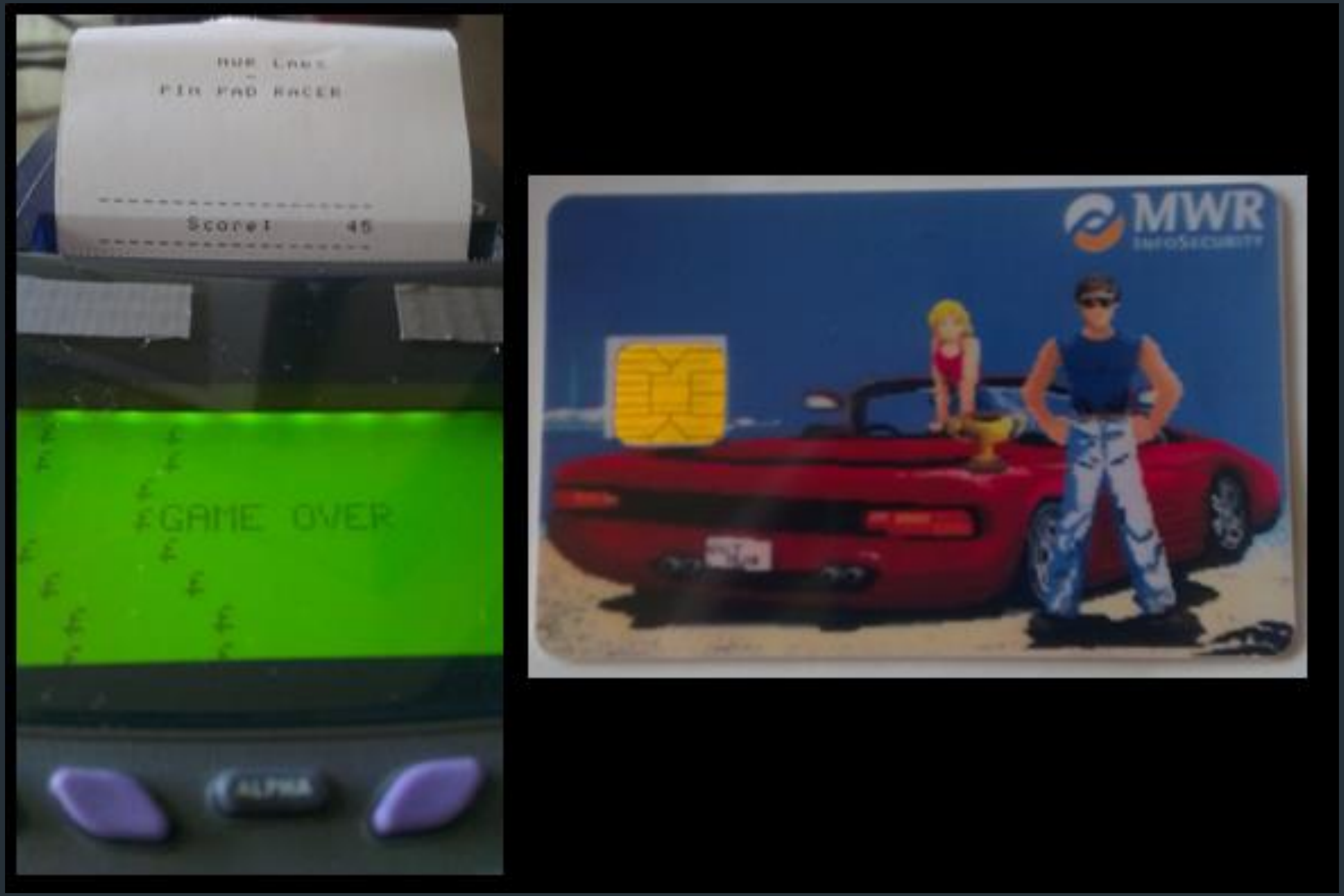
Why Are We Awesome?


127.0.0.1:8000/exploit.html
Calculator
View Edit Help
1337
Administrator: C:\Windows\system32\cmd.exe
3:15 PM

```
       .mMMMMMm.                  mMMm     M   WWW    W     W   RRRRR
     mMMMMMMMMMMMM.                 MM    MM     W    W    W     R    R
    /MMMM-      -MM.                MM    MM     W    W    W     R    R
   /MMM.         \/  ^              M  M  M  M     W  W  W  W      RRRR
   |M.     aR̄R̄r      /W|            M  M  M  M     W  W  W  W      R   R
   \/   ..  ^^^    wWWW|            M    M    M       W    W       R    R
     /WW\.   .wWWWW/                M    M    M       W    W       R     R
      |WWWWWWWWWWWW/
       .WWWWWWWW.

[+] Initialising...
[+] Done
[+] Leaked pointer from chrome.dll: 0x698a49a0
[+] Working our way back to find the image base...
[+] chrome.dll found at base address 0x679b0000
[+] Reading chrome.dll into buffer (please be patient)...
[+] Dynamically searching for ROP gadgets
[+] Handing over execution to the payload
```

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>_
```

Why Are We Awesome?



++

Why Are We Awesome?

++
Plan of Attack

- Intro
- MAC address filtering/SSID hiding
- Encryption Primer
- WEP
- WPA/WPA2
- WPS
- Once you’re inside, then what?

++

A Disclaimer and Word of Warning

- Don’t scan or attack anything you don’t own
- Computer Misuse Act 1990

Potentially 14 years in jail!

++

What is WiFi?

- IEEE 802.11 – Wireless LAN physical layer
- A radio standard for transmitting and receiving data
- Point to point – everything goes through AP
- Half-duplex – bi-directional but only one way at a time

++

Why Do We Care?

- Over 5 billion WiFi devices shipped by 2013[1]
- 73.3% of UK households had WiFi in 2011[2]
- Number of Wi-Fi hotspots is increasing

[1] https://www.abiresearch.com/press/growing-demand-for-mobility-will-boost-global-wi-f
[2] http://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5193

++

WiFi Security Protocols

- Wired Equivalent Protocol (WEP)
- Wireless Protected Access (WPA)
- Wireless Protected Access II (WPA2)
- Wi-Fi Protected Setup (WPS)

- Media Access Control (MAC) address filtering
- Hidden Service Set Identifiers (SSIDs)

++

Non-Technical Security

- Encryption and authentication only part of the story
- Weak passphrases ruin strong encryption
- Evil Twin attacks – Fake APs that look like what the user or device expects

++

Plan of Attack

- Intro
- MAC address filtering/SSID hiding
- Encryption Primer
- WEP
- WPA/WPA2
- WPS
- Once you’re inside, then what?

MAC Address Filtering

- Whitelist of MAC Addresses

MAC Address Spoofing

- Listen for connected devices
- Set your MAC address to match a connected device
- ????
- Profit!

++

Hidden SSIDs

- Stops your network showing up on an OS’s network list
- Not actually hidden, router will broadcast SSID in response to relevant probes
- Easy to disassociate a client and watch for reconnect
- Security by obscurity, it doesn’t work

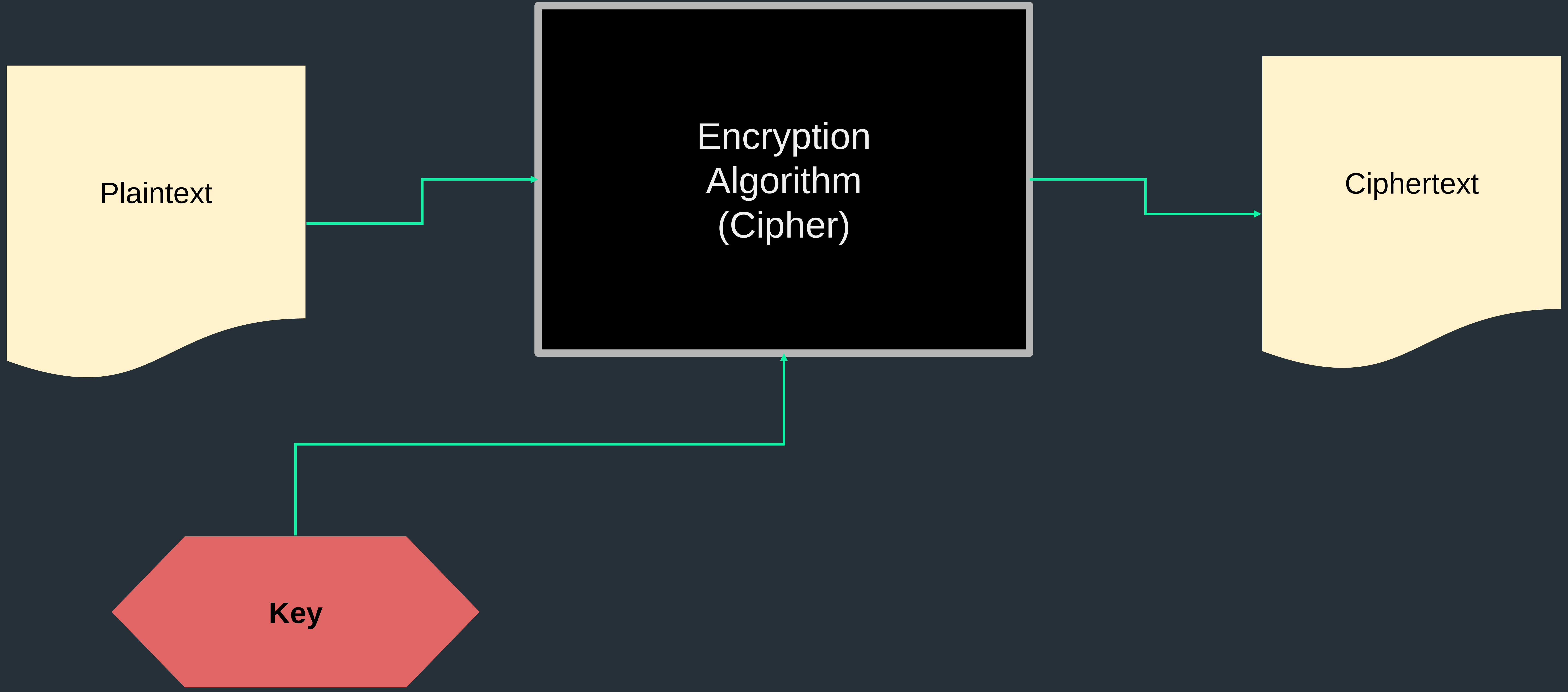
++

Plan of Attack

- Intro
- MAC address filtering/SSID hiding
- Encryption Primer
- WEP
- WPA/WPA2
- WPS
- Once you’re inside, then what?

++

Encryption



++

Stream Ciphers

- Acts on a single bit at a time
- Uses a pseudo random key stream
- Key stream generated by CSPRNG
- RC4, Salsa20

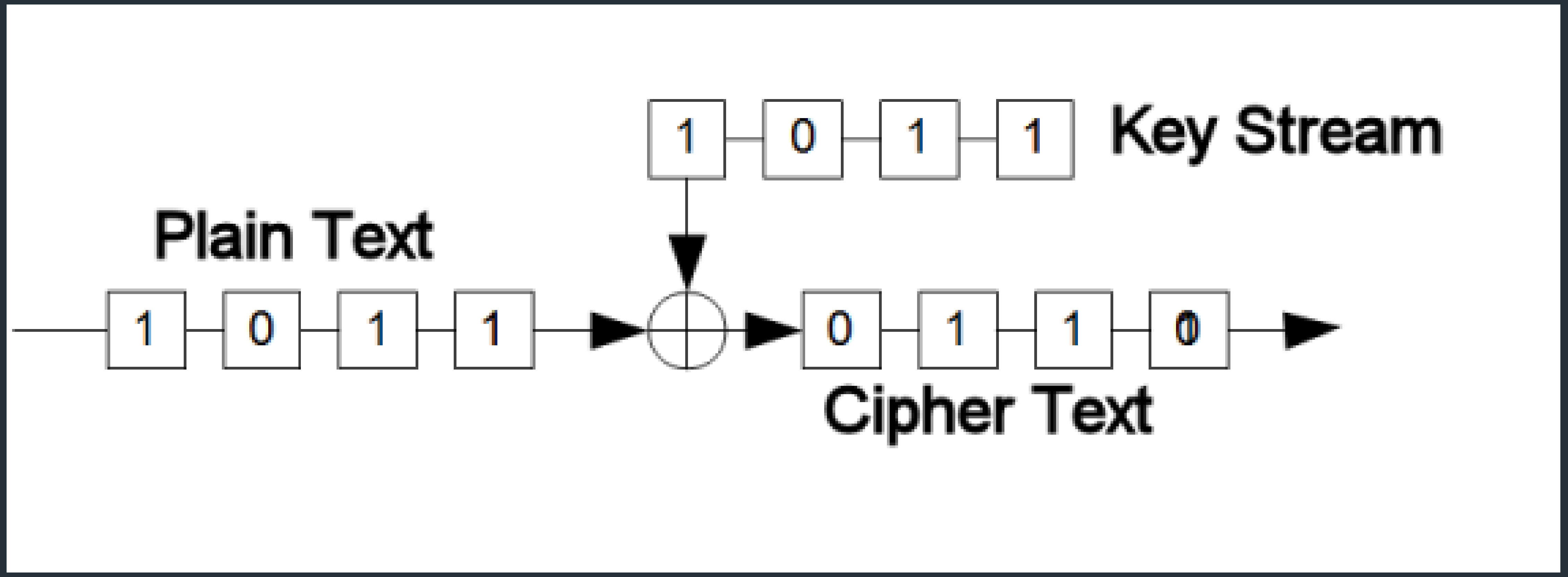


Image from http://hyperploid.blogspot.co.uk/2010/08/digital-ciphers.html

++

Block Ciphers

- Acts on a fixed number of bits per cycle
- Several different modes of operation
- DES/3DES, AES, Blowfish, Twofish

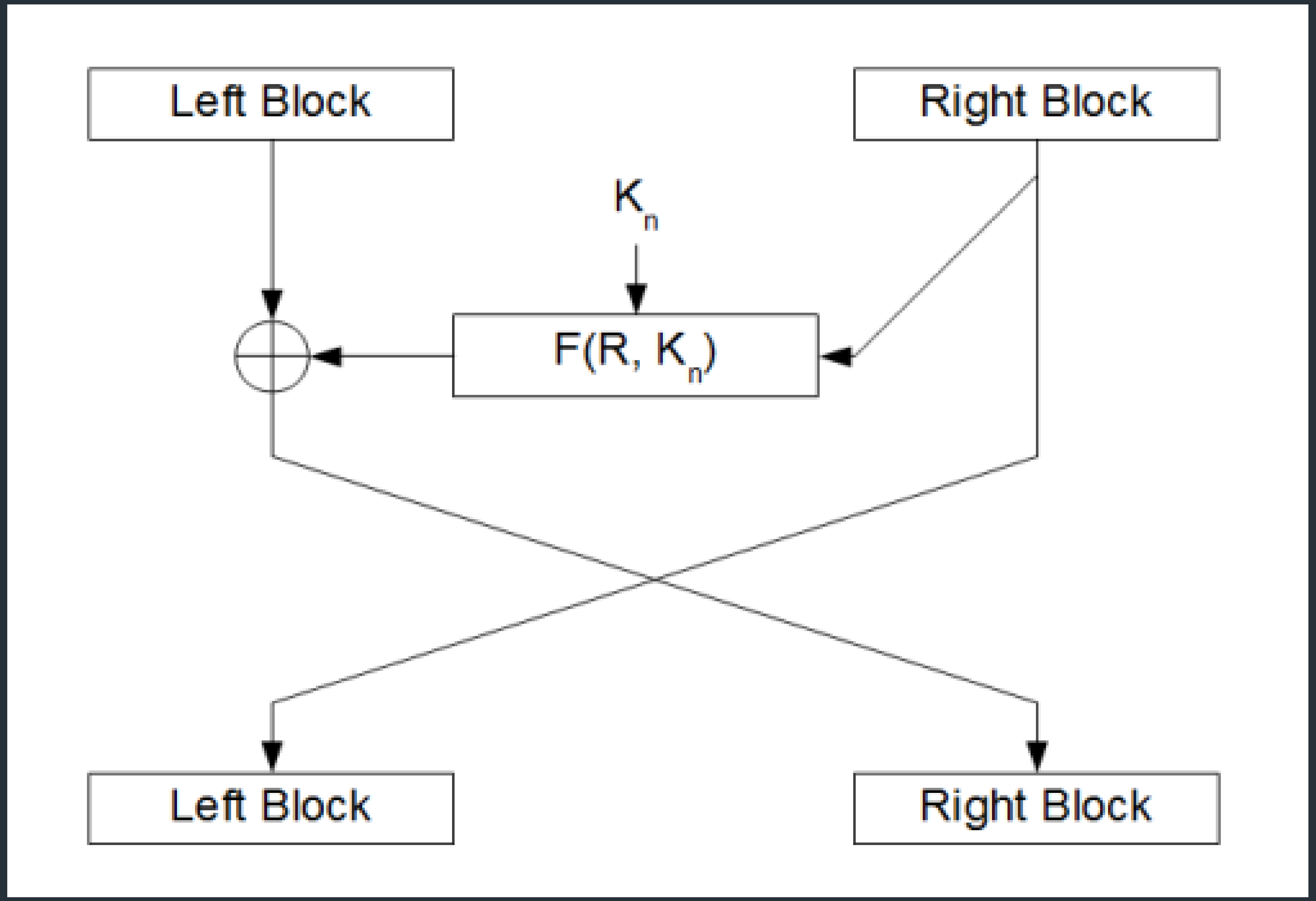


Image from http://hyperploid.blogspot.co.uk/2010/08/digital-ciphers.html

++

Plan of Attack

- Intro
- MAC address filtering/SSID hiding
- Encryption Primer
- WEP
- WPA/WPA2
- WPS
- Once you’re inside, then what?

++

WEP

- Wired Equivalent Protocol, defined in the first IEEE 802.11 draft
- WEP-40 used 10 hex digit keys, WEP-104 used 26
- 24-bit Initialisation Vector
- RC4 stream cipher
- CRC-32 checksum
- Shared Key

++

…Is Broken

- Officially deprecated by IEEE in 2004
- Game-breaking flaws in the cryptography
- Do not use WEP – Windows 8 won't allow it

++

Cracking WEP

- Fluhrer, Mantin and Shamir attack
- Stream ciphers require unique keys
- IVs are used to introduce this uniqueness

- 24-bit IVs aren't long enough
- 16,777,216 distinct values
- 50% probability IV repeats after 5000 packets

++

Hands-on WEP Cracking

Use airmon-ng to enter monitor mode

```
sudo airmon-ng start [WIRELESS INTERFACE]
```

Use airodump-ng to capture packets

```
airodump-ng --ivs --channel [X] --essid [ESSID HERE] -w [OUTPUT FILE PREFIX]
```

Use aircrack-ng to crack the WEP key

```
aircrack-ng  -e [ESSID] [OUTPUT FILE FROM AIRODUMP]
```

Use aireplay-ng to spoof ARP packets and generate a tonne of IVs

```
aireplay-ng -3 -b  [AP MAC ADDRESS] -h [CLIENT MAC ADDRESS] [INTERFACE]
```

++

Plan of Attack

- Intro
- MAC address filtering/SSID hiding
- Encryption Primer
- WEP
- WPA/WPA2
- WPS
- Once you’re inside, then what?

++

WPA

+ A subset of Draft IEEE 802.11i
+ Stopgap measure between WEP and WPA2

+ Uses RC4 with TKIP
+ Requires only a firmware upgrade
+ Common for PCs, Rare for APs

++

TKIP

+ Temporal Key Integrity Protocol
+ Uses a per packet key
+ Generated by mixing rather than concatenation
+ Adds a counter to prevent replay attacks
+ Message Integrity Check (MIC)

++

…Is Still Fairly Broken

+ There are security concerns[1]
+ It is not strictly broken
+ Deprecated by the IEEE
+ RC4 has several serious attacks against it (NOMORE, Bar-Mitzvah, FMS)
+ NSA, GCHQ and other state actors are expected to have broken RC4 completely

[1] http://arstechnica.com/security/2008/11/wpa-cracked/

++

WPA2

- Wi-Fi Protected Access II
- Defined in IEEE 802.11i-2004
- Uses CCMP and AES

- This is what you should be using

++

CCMP

- Counter Mode CBC-MAC Protocol
- "Counter Mode Cipher Block Chaining Message Authentication Code Protocol"

- WPA2's equivalent of TKIP

++

WPA Personal Mode

- WPA-PSK (Pre-shared Key)
- 256-bit Key
- Can be entered as 64 Hexadecimal digits, more commonly as 8 to 63 ASCII characters
- PBKDF2 – SSID is used as a salt
- Password Based Key Derivation Function 2
- Susceptible to weak password attacks, rainbow tables exist

++

WPA Enterprise Mode

- 802.1x
- RADIUS
- MS-CHAP

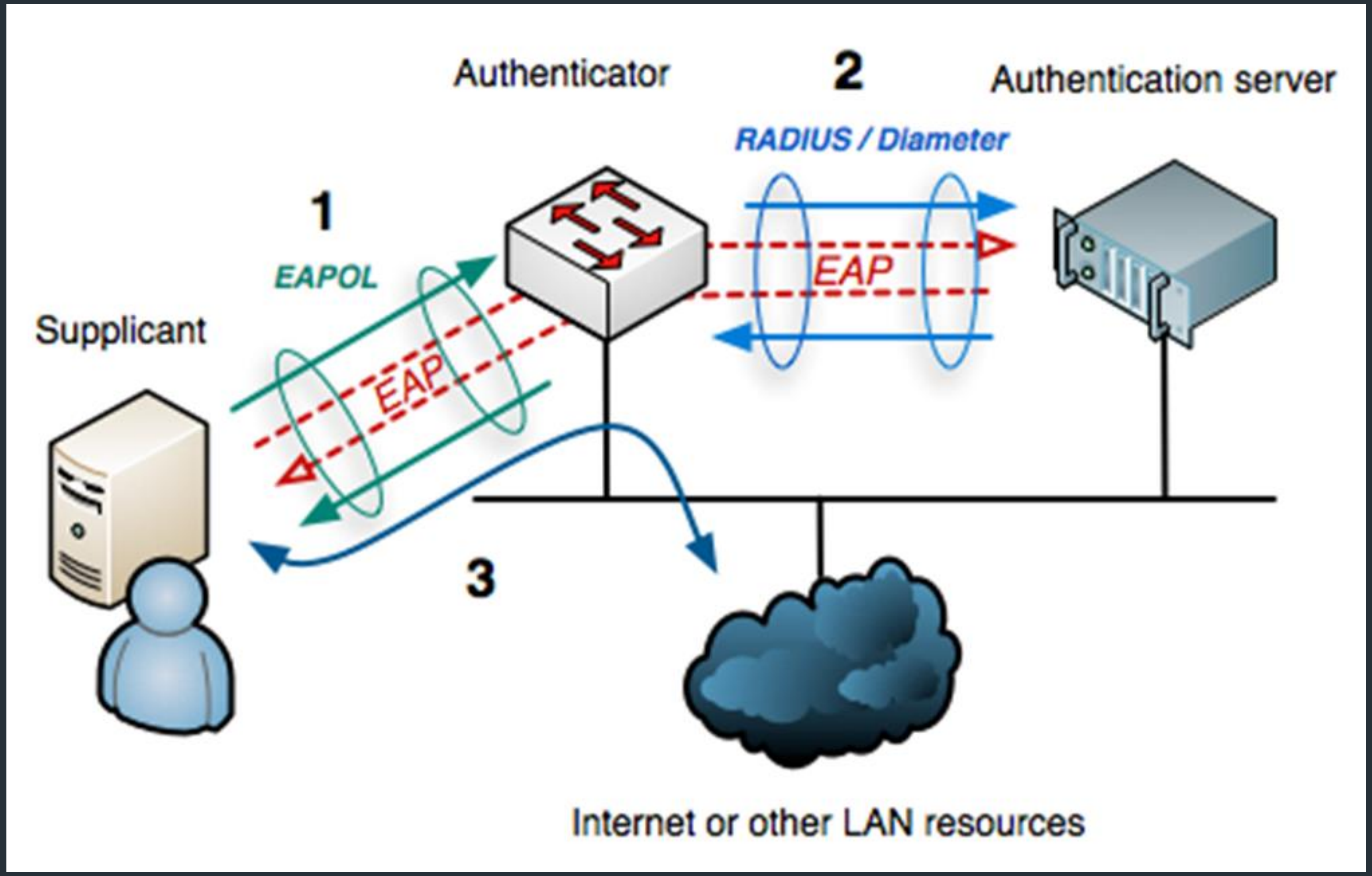


Image from http://en.wikipedia.org/wiki/File:802.1X_wired_protocols.png

Hands-On WPA Attacks

Use airmon-ng to enter monitor mode

```
sudo airmon-ng start [WIRELESS INTERFACE]
```

Use airodump-ng to capture four way handshake

```
airodump-ng --channel [X] --essid [ESSID HERE] -w [OUTPUT FILE PREFIX] [INTERFACE]
```

Use aireplay-ng to force a handshake - -0 is deauth, 1 is number of deauths to send

```
aireplay-ng -0 1 -a [ACCESS POINT MAC] -c [MAC OF CLIENT TO DEAUTH] [INTERFACE]
```

Use aircrack-ng to perform a dictionary attack and recover the key

```
aircrack-ng -w [PASSWORD LIST] -b [ACCESS POINT MAC] [AIRODUMP OUTPUT FILE]
```

Kali has password lists in /usr/share/wordlists, wfuzz’s common.txt is a good place to start

++

Plan of Attack

- Intro
- MAC address filtering/SSID hiding
- Encryption Primer
- WEP
- WPA/WPA2
- WPS
- Once you’re inside, then what?

++
WPS

- Wi-Fi protected setup
- For home and small business Wi-Fi
- Designed to make it easier to connect new users to secure networks
- Several modes of operation: PIN, Push-Button, NFC, USB (Deprecated)

++

…Is Broken Too

- WPS uses an 8 digit PIN
- 8th digit is a checksum – 7 digits to guess
- PIN is verified in two rounds, first half then second half
- Only need to guess from 11000 PINs

- Can be cracked in ~4 hours by brute force guessing PINs
- Should be disabled, but not all home routers allow you to

++

Cracking WPS

Use airmon-ng to enter monitor mode

+ sudo airmon-ng start [WIRELESS INTERFACE]

Use wash to spot networks vulnerable to WPS brute forcing

+ wash -i [MONITOR INTERFACE]

Use reaver to brute force the WPS pin

+ reaver -i [MONITOR INTERFACE] -c [CHANNEL] -b [MAC OF AP] -vv

++

Plan of Attack

- Intro
- MAC address filtering/SSID hiding
- Encryption Primer
- WEP
- WPA/WPA2
- WPS
- Once you’re inside, then what?

++

We’re In, Now What?

- Default passwords for router admin panels
- Man-In-The-Middle attacks – ARP poisoning, SSLStrip
- Router vulnerabilities

++

Poor Password Choices

- Router manufacturers often do not randomise default admin passwords
- Usually something like admin/admin, admin/password
- Dictionary attacks using THC Hydra or similar usually effective

```
hydra -l [USERNAME] -P [PASSWORD LIST] -t 10 -m /
192.168.0.1 http-get
```

++

Man In The Middle

- Tell everyone you’re the router, watch traffic come pouring in
- No security at all on ARP traffic
- Forward on all traffic while capturing
- Filter for interesting stuff with Wireshark
- SSLStrip will redirect SSL connections

++

Router Vulnerabilities

+ Many run an embedded Linux variant
+ Security flaws in the firmware and web interfaces are very common
+ Remote code execution vulnerabilities also not uncommon
+ Admin interface web servers often run as root
+ Vendors often slow to patch, if at all

++

Thank You for Listening

Questions?