



# Wireless Networking

Part three

Linux and Wireless Security

# Secure your network

- Would you put a sign like this outside your house?
  - Free internet access
  - Use my download allowance
  - Send emails at my expense and risk
  - Come and access my files and documents
- No? Then secure your wireless network

# Insecure Measures

- Not broadcasting the SSID
  - Casual hackers cannot identify your network
- MAC address filtering
  - Only allows known devices onto network
  - Easy to 'spoof' MAC address
  - 'Spoofer' is inside your firewall

## More b\*\*\*\*y acronyms

- Some familiar ones (or not):
  - 802.11 , WEP, WPA
- Some even less familiar:
  - PSK, TKIP, 802.11i, 802.1x
  - EAP, LEAP, RC4, AES
  - Michael, MIC
  - And so on

# Basic Security

- Available on every Router/Access Point and Wireless adapter
- Wired Equivalent Privacy (WEP)
- Up to four security keys defined
- Only one in use at a time
- Manual, co-ordinated change
- Key length
  - 64 bits (really 40), or
  - 128 bits (really 104)

# WEP Risks

- Keys are short
  - 128 bits are better
  - Encryption algorithm not very secure
  - Brute force guessing possible
- Users rarely change keys
- Packet sniffing
  - Hacker can work out key
- **Still much better than nothing**
  - Risk not high for home network

# WEP Example

- WEP definition on router

## Authentication & Encryption

This page allows you to configure the setting of network authentication and data encryption.

<b>Network Authentication</b>	Shared Key ▾	
<b>Encryption Type</b>	WEP ▾	
<b>WEP Key 1</b>	*****	128-bit ▾
<b>WEP Key 2</b>		64-bit ▾
<b>WEP Key 3</b>		64-bit ▾
<b>WEP Key 4</b>		64-bit ▾

✓ Apply

X Cancel

? Help

# WEP Example

- WEP definition in Linux (Ubuntu)



The screenshot shows the 'Interface properties' dialog box for the interface 'ra0'. The 'Connection' section is checked and enabled. The 'Wireless settings' section shows the network name as 'NSLIG', the key type as 'Plain (ASCII)', and the WEP key as a series of asterisks. The 'Connection settings' section shows the configuration as 'DHCP'.

**Interface properties**

**Connection**  
Interface name: ra0  
 Enable this connection

**Wireless settings**  
Network name (ESSID): NSLIG  
Key type: Plain (ASCII)  
WEP key: \*\*\*\*\*

**Connection settings**  
Configuration: DHCP  
IP address:  
Subnet mask:  
Gateway address:

Help Cancel OK

## Next Level - WPA

- Wifi Protected Access
  - Really an interim measure
- Two levels
  - Personal – simpler to implement
  - Enterprise – more complex and more secure
- Eliminates most WEP risks
- Not supported by older devices and/or some Linux drivers

# WPA Personal

- Intended for Home/SOHO users
- Uses a pre-shared key (PSK)
- Implements the Temporal Key Integrity Protocol (TKIP)
- Fairly simple to implement
- Only some Linux drivers have native support

# Implementing WPA - Personal

- Check your adapter/router/access point to make sure WPA is supported
- Find out if your Linux driver has native support for WPA PSK/TKIP
  - e.g. the rt2500 driver has support
- If supported, use distro. network definition or **iwpriv** command set
  - Examples follow
- If no native support, all is not lost

# Implementing WPA – Personal - 2

- WPA definition on a router



The screenshot shows a web-based configuration interface for a router's wireless settings. The window title is "Wireless". The main heading is "Authentication & Encryption". Below the heading is a descriptive paragraph: "This page allows you to configure the setting of network authentication and data encryption." The configuration is presented in a table-like form with five rows. The first row is "Network Authentication" with a dropdown menu set to "WPA-PSK". The second row is "WPA Pre-Shared Key" with a text input field containing "\*\*\*\*\*" and a dropdown menu set to "Passphrase". The third row is "Confirm WPA Pre-Shared Key" with a text input field containing "\*\*\*\*\*". The fourth row is "WPA Group Rekey Interval" with a text input field containing "3600" and the unit "seconds". The fifth row is "Encryption Type" with a dropdown menu set to "TKIP". At the bottom right of the window are three buttons: "Apply", "Cancel", and "Help".

Authentication & Encryption	
Network Authentication	WPA-PSK
WPA Pre-Shared Key	***** Passphrase
Confirm WPA Pre-Shared Key	*****
WPA Group Rekey Interval	3600 seconds
Encryption Type	TKIP

✓ Apply    ✕ Cancel    ? Help

# Implementing WPA – Personal - 3

- Using the iwpriv commands
  - modprobe rt2500 # may not be needed
  - iwconfig ra0 essid NSLIG channel 6 mode managed
  - iwpriv ra0 set AuthMode=WPAPSK
  - iwpriv ra0 set EncrypType=TKIP
  - iwpriv ra0 set WPAPSK="Hello Sailor"
  - dhcpcd -t 10 -d ra0

# Driver does not have full support?

- There is a further support program called
  - `wpa_supplicant`
- Takes over the functions of `iwconfig` and handles security
- Needs a configuration file to tell it what to do about security
- Example follows

# wpa\_supplicant example

- Configuration file:

```
ctrl_interface=/var/run/wpa_supplicant
network= {
    ssid="NSLIG"
    proto=WPA
    key_mgmt=WPA-PSK
    pairwise=TKIP
    group=TKIP
    psk="Hello Sailor"
}
```

- Commands

- modprobe rt2500 # may not be needed
- wpa\_supplicant -i ra0 -D wext -c /etc/wpa.conf -B
- dhcpcd -t 10 -d ra0

# What's so smart about WPA

- Uses your key as the basis for an encrypted version that changes for each packet
- Creates a new internal key each time a wireless station associates (joins) and after set interval
- The keys are longer – more difficult to break
  - Up to 64 hex digits
  - Years before repeat
  - If using a passphrase, more than twenty characters recommended
    - “Hello Sailor” wouldn't cut it

# Why is WPA only “interim”

- The full implementation uses a changed encryption program
- WPA uses the RC4 encryption algorithm
  - Known weaknesses
- WPA2 (the full implementation)
  - Uses the Advanced Encryption Standard (AES) algorithm
  - Computationally intensive
    - Not all current equipment has enough compute power
    - Only some routers/access points/adapters support WPA2

# What about WPA – Enterprise

- Expects a separate server for encryption
  - Called a Remote Authentication Dial-in User Service (Radius)
- Covers authentication, authorisation and accounting
- Meets the 802.1x standard
  - Uses AES, and Extensible Authentication Protocols (EAP, PEAP, LEAP)
- Heavyweight tool for home networking

# Summary

- Sensible to test a wireless network unsecured initially
- Do not leave your wireless network unsecured unless you understand and accept the risks
- WEP not highly secure, but widely available and **much** better than nothing
- WPA more secure, but check if your adapter/router/access point/distro./driver all support it