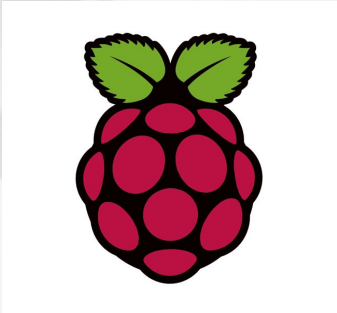
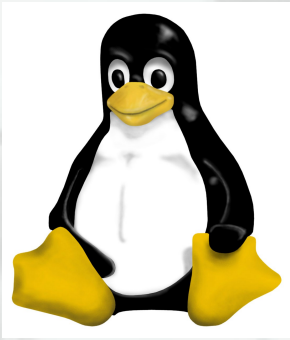
Raspberry Pi & Security
Software Freedom Day 2013

Peter Oakes





IT/Cyber Security

- What is it?
  - Covers everything from 'physical' to user interactions
- Why care?
  - IT provides assets/resources
  - We depend on these resources
  - Store our information (confidential)
  - Control our information (integrity)
  - Provide information (availability)

Security = Easy

- Kind of...
  - Lots of terms and technologies, Firewall, port, encryption, RSA etc
- Back to basics
  - Think about we want to secure
  - Understand how security is configured
  - Similar to securing a house..

Raspberry Pi

- Aim to monitor and report security threats
  - Protecting and securing the device
- Out of the box install is insecure
  - Requires user to configure (harden)
- Electronics provide enhancements
  - Alerting/notification

Hack Yourself

- Need to understand what needs securing
- 'Discovery' exercise
  - Who, what is on your network
  - Types of traffic
  - What ports are available
  - Incorrect configurations, out of date software
- Several utilities
  - Kali (Linux distribution 300+ tools)
  - Command line utilities
  - Web based (www.grc.com)

Example Usage

- Kali
  - Netdiscover
  - Zenmap
  - Nmap
  - Intrace
  - Tcpflow

Securing The House

- Secure the house
  - Fit doors
  - Add locks
  - Secure Windows....Not the Microsoft type
  - Establish secure entry i.e. letterbox
  - Hide away valuables
  - Fit alarms and video camera
  - ... Have a guard dog or hire a bouncer

- Result
  - Allows communication (letters)
  - Protects assets
  - Monitors and alerts owner

Securing The Pi

- Lock our doors
  - IP Tables installed

- Monitor for suspicious behaviour
  - Log events
  - This is our video camera...

- Alert
  - Analyse events
  - Report events
  - This is our alarm/guard dog

IP Tables

- Its a rule-based firewall
- By default no rules defined
- To block an IP
  - /sbin/iptables -I INPUT -s 192.168.0.5 -j DROP
  - DANGER: You can lock yourself out
- To accept an IP
  - /sbin/iptables -I INPUT -s 192.168.0.5 -j ACCEPT
- To view the rules
  - /sbin/iptables -L

Logging

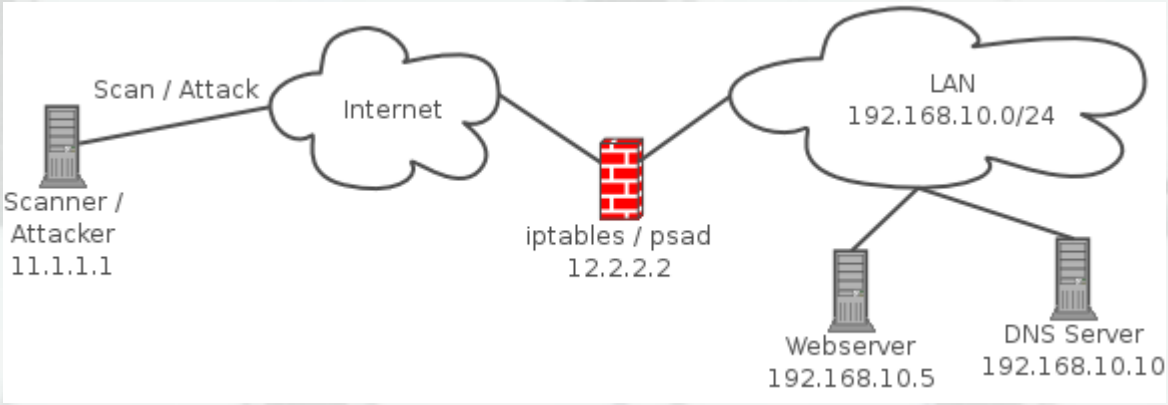
- By default most messages are recorded in:
  - /var/log/messages
- View it in real-time
  - Tail -f /var/log/messages
- Try it
  - Logger “hello SFD 2013”
- Very important resource
- Used for audit/diagnosing problems
- Other applications depend on these logs

Port Scan Attack Detector

- Software to report on attacks
- Monitors log events
- Has own rules
- View status:
  - Psad -S
- Can set blacklist and whitelists
- Custom Python script
  - Electronics via GPIO

PSAD

- Typical deployment of PSAD
- Detect probes for various backdoor programs



Launch an Attack

- Virtual Machine with Kali
- Probing the network
  - Nmap -sV 192.168.0.2 #what services
  - Nmap -O 192.168.0.2 #what OS
  - Nmap --open 192.168.0.2 #open ports
  - Nmap -sA 192.168.0.2 #is there a FW?
  - Nmap –iflist
  - Nmap -sF 192.168.0.2
- Attack example:
  - sudo hping3 -i u1 -S -p 80 192.168.0.2

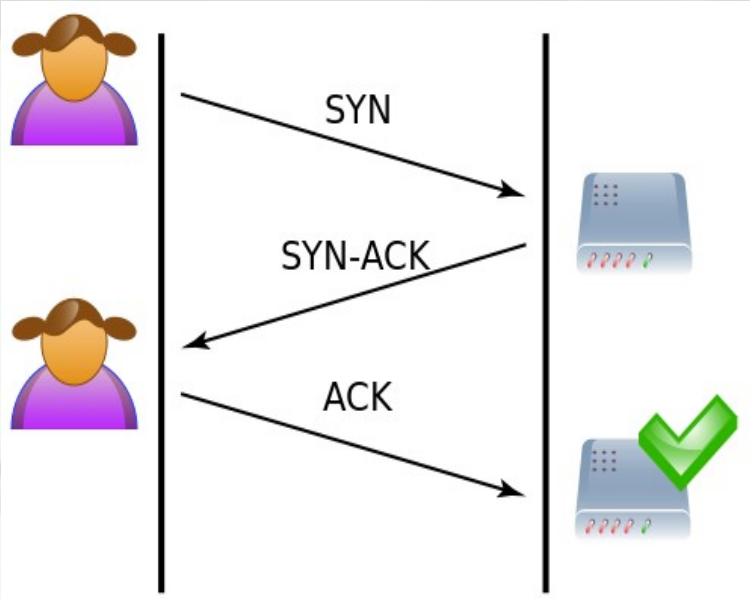
The Pi

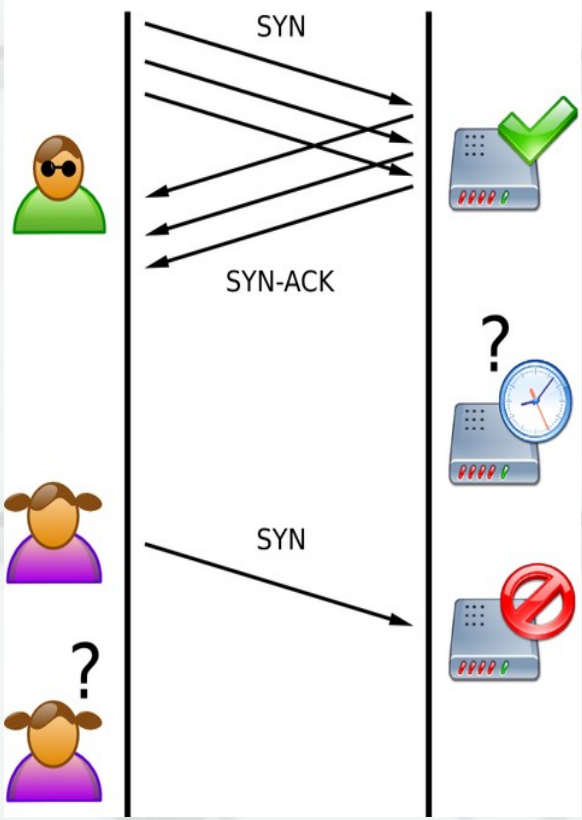
- 'Attack' VM is Kali
- Attacker using Kali probes network
- Pi logs activity from probe
- Pi flags activity as suspect
- Pi alerts user via LEDs and LCD

Tools

- Wireshark
- Capture and filter packets (network traffic)
- Previous attack, all SYN flags set, syn flood attack = Denial of Service
- Can filter tcp.flags.syn==1
- IP tables stop/limit this:
  - iptables -A INPUT -p tcp --syn -m limit --limit 1/s --limit-burst 3 -j RETURN

Denial of Service





Pi Development

- Hardware
  - LCD
  - LEDs
  - I2C (provides more Pins/IOs)
  - Button
- Software
  - Python
  - Various libraries SMBus for I2C, GPIO
  - Notepad++

Raspberry Pi
GPIO Cheat Sheet

CYNTECH COMPONENTS
ELECTRO-MECHANICAL SPECIALISTS

PIMORONI

I²C

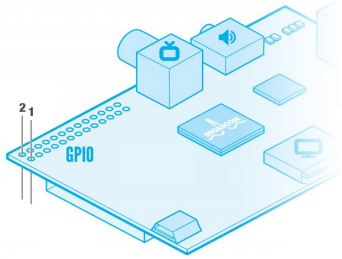
A low-speed interface used to communicate with multiple simple devices and sensors via a two-wire interface.

Inter-Integrated Circuit (I²C) is a serial bus interface which supports multiple devices and only requires two wires for communication (no separate clock or device select needed). It is, however, limited to relatively low speeds (usually 10-100kbit/s).

CLK

Clock signals are used to provide a pulse that can synchronise different parts of a system that perform actions which are time sensitive to each other.

GPCLK0 is a general purpose clock that generates a square-wave clock signal up to a maximum frequency of around 75MHz.



UART

The UART pins on the Raspberry Pi are primarily provided for access to the serial console which is a relatively advanced feature that most people won't need to use.

Universal Asynchronous Receiver/Transmitter (UART) is a method of transmitting data over a serial connection. Both of the communicating devices contains a shift register that converts the bytes of data being transmitted into a stream of bits.

PWM

Provides an 'analogue style' supply that can be used for controlling motors and LEDs.

With PWM (pulse-width modulation) the amount of power delivered to the device is controlled by switching the supply on and off very quickly, typically thousands of times a second.

			3V3	1	2	5V0	
I²C		GPIO 2	SDA0	3	4	5V0	
I²C		GPIO 3	SCL0	5	6	GND	
CLK		GPIO 4	GPCLK0	7	8	TXD	GPIO 14
			GND	9	10	RXD	GPIO 15
		GPIO 17	P17	11	12	PWM	GPIO 18
		GPIO 27	P27	13	14	GND	
		GPIO 22	P22	15	16	P23	GPIO 23
			3V3	17	18	P24	GPIO 24
SPI		GPIO 10	MOSI	19	20	GND	
SPI		GPIO 9	MISO	21	22	P25	GPIO 25
SPI		GPIO 11	SCLK	23	24	CE0	GPIO 8
		GND	GND	25	26	CE1	GPIO 7

UART

PWM

Original (Rev 1) Raspberry Pi users:
The original Raspberry Pi had slightly different GPIO pin numbering. GPIO 2 was GPIO 0, GPIO 3 was GPIO 1, and GPIO 27 was GPIO 21.

SPI

Often used to read more complicated sensors, drive simple displays, or communicate between devices.

Serial Peripheral Interface Bus (SPI) is a synchronous full-duplex (two way) serial connection. Communication happens between a master device and slave device with the master device providing synchronisation.

The data is transmitted on the MOSI (master-out, slave-in) and MISO pins (master-in, slave-out) pins. Each transmission is synchronised by a clock pulse on SCLK.

Pi Development

- Code maintained on Pi
- Developed on laptop
- Uses SFTP (SSH)
  - Accesses Pi remotely (download/upload)
  - Can't test on laptop i.e. libraries and devices on Pi
- Code managed by Git (VCS to bitbucket)
- Adafruit provides an excellent IDE called WebIDE
  - Web based, allows debugging from any device

Raspberry Pi
GPIO Cheat Sheet

CYNTECH COMPONENTS
ELECTRO-MECHANICAL SPECIALISTS

PIMORONI

I²C

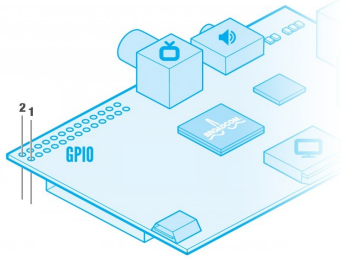
A low-speed interface used to communicate with multiple simple devices and sensors via a two-wire interface.

Inter-Integrated Circuit (I²C) is a serial bus interface which supports multiple devices and only requires two wires for communication (no separate clock or device select needed). It is, however, limited to relatively low speeds (usually 10-100kbit/s).

CLK

Clock signals are used to provide a pulse that can synchronise different parts of a system that perform actions which are time sensitive to each other.

GPCLK0 is a general purpose clock that generates a square-wave clock signal up to a maximum frequency of around 75MHz.



UART

The UART pins on the Raspberry Pi are primarily provided for access to the serial console which is a relatively advanced feature that most people won't need to use.

Universal Asynchronous Receiver/Transmitter (UART) is a method of transmitting data over a serial connection. Both of the communicating devices contains a shift register that converts the bytes of data being transmitted into a stream of bits.

PWM

Provides an 'analogue style' supply that can be used for controlling motors and LEDs.

With PWM (pulse-width modulation) the amount of power delivered to the device is controlled by switching the supply on and off very quickly, typically thousands of times a second.

			3V3	1	2	5V0	
I²C		GPIO 2	SDA0	3	4	5V0	
I²C		GPIO 3	SCL0	5	6	GND	
CLK		GPIO 4	GPCLK0	7	8	TXD	GPIO 14
			GND	9	10	RXD	GPIO 15
		GPIO 17	P17	11	12	PWM	GPIO 18
		GPIO 27	P27	13	14	GND	
		GPIO 22	P22	15	16	P23	GPIO 23
			3V3	17	18	P24	GPIO 24
SPI		GPIO 10	MOSI	19	20	GND	
SPI		GPIO 9	MISO	21	22	P25	GPIO 25
SPI		GPIO 11	SCLK	23	24	CE0	GPIO 8
		GND	GND	25	26	CE1	GPIO 7

UART

PWM

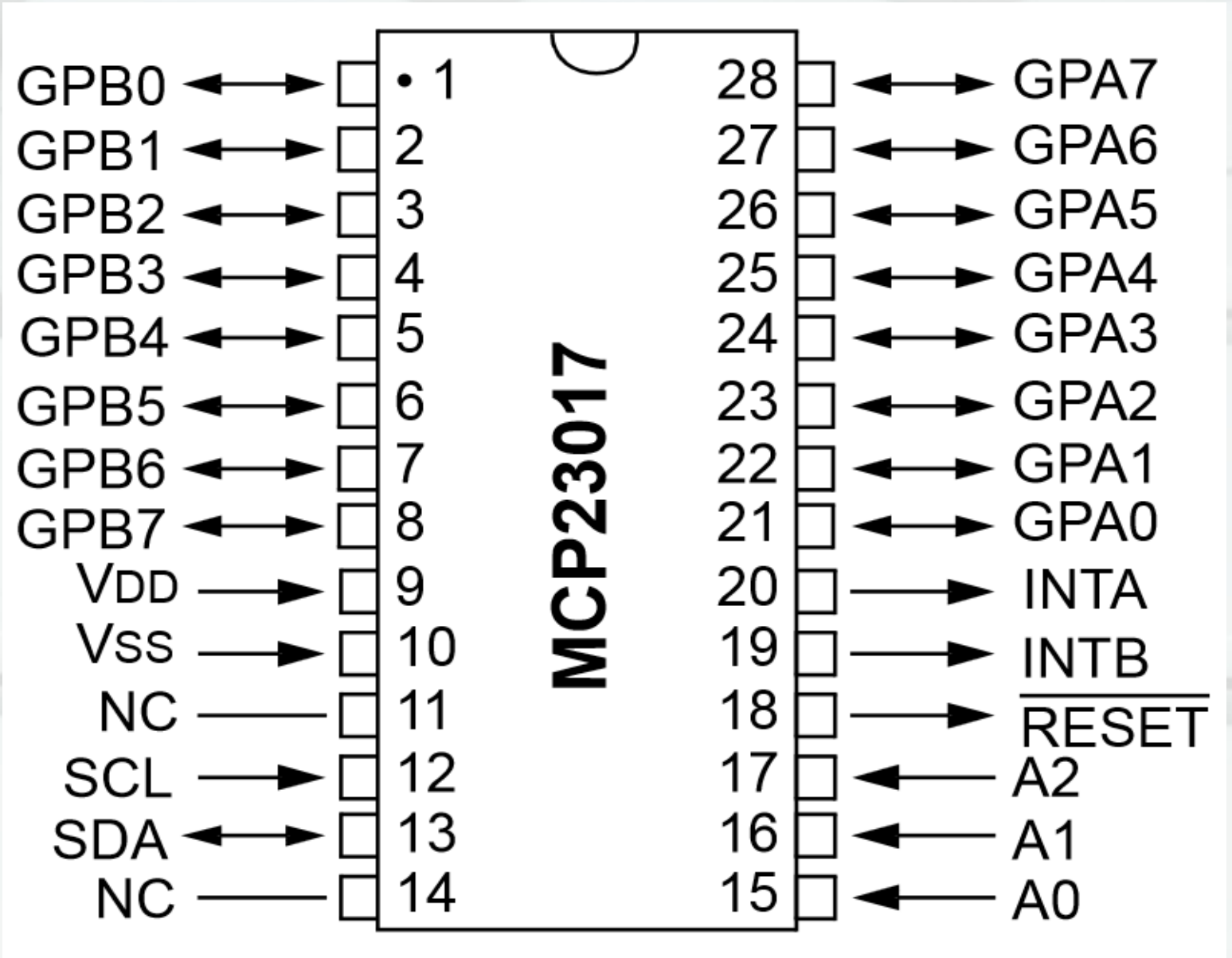
Original (Rev 1) Raspberry Pi users:
The original Raspberry Pi had slightly different GPIO pin numbering. GPIO 2 was GPIO 0, GPIO 3 was GPIO 1, and GPIO 27 was GPIO 21.

SPI

Often used to read more complicated sensors, drive simple displays, or communicate between devices.

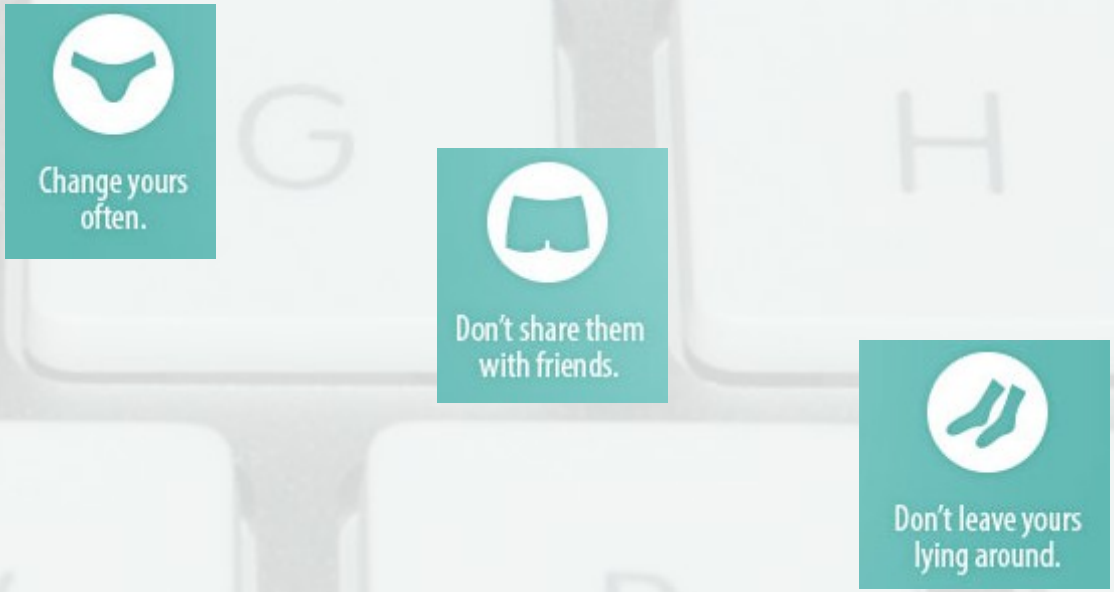
Serial Peripheral Interface Bus (SPI) is a synchronous full-duplex (two way) serial connection. Communication happens between a master device and slave device with the master device providing synchronisation.

The data is transmitted on the MOSI (master-out, slave-in) and MISO pins (master-in, slave-out) pins. Each transmission is synchronised by a clock pulse on SCLK.


MCP23017
GPB0
GPB1
GPB2
GPB3
GPB4
GPB5
GPB6
GPB7
VDD
Vss
NC
SCL
SDA
NC
1
2
3
4
5
6
7
8
9
10
11
12
13
14
28
27
26
25
24
23
22
21
20
19
18
17
16
15
GPA7
GPA6
GPA5
GPA4
GPA3
GPA2
GPA1
GPA0
INTA
INTB
RESET
A2
A1
A0

Closing Remarks

- Passwords are like underwear....



Useful Links

- How secure is your network: http://www.linuxuser.co.uk/tutorials/how-safe-is-your-network-kali-tutorial
- IP Tables: http://www.howtogeek.com/168132/using-iptables-on-linux/
- Essential Linux Commands: http://community.linuxmint.com/tutorial/view/244
- PSAD: http://www.cyberciti.biz/faq/linux-detect-port-scan-attacks/
- Nmap: http://www.cyberciti.biz/networking/nmap-command-examples-tutorials/
- HPING: http://www.binarytides.com/tcp-syn-flood-dos-attack-with-hping/
- IP Tables vs DOS: http://www.cyberciti.biz/tips/howto-limit-linux-syn-attacks.html
-

Mail Box Issue

- sudo touch /var/mail/pi
- sudo chown pi:mail /var/mail/pi
- sudo chmod o-r /var/mail/pi
- sudo chmod g+rw /var/mail/pi

Getting Started

- Kali (root/pa33word)
- Pi (pi/pwd123.card)
- Load IP tables =
- sudo /sbin/iptables-restore < ~/iptables.up.rules
- Restart PSAD
- sudo /etc/init.d/psad restart