Trustwave® SpiderLabs®

IoT and JTAG Primer

Michel Chamberland
Practice Lead - Americas

September 13, 2018

Agenda

- About the Presenter/Trustwave SpiderLabs
- What is IoT?
- Trustwave Study/Statistics
- State of IoT Security
- Attacking IoT Devices
- JTAG
- Handling IoT Growth

Introduction

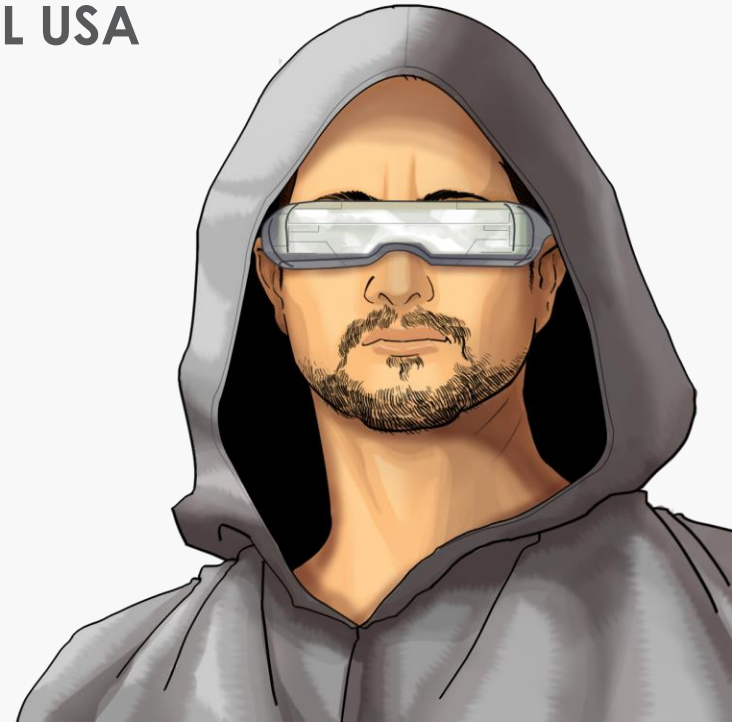
Session Goals

- **This is an entry level session (101)**
- **Will help clarify what IoT is and isn't**
- **You should better understand the rate of adoption of IoT**
- **You will learn about the state of IoT Security**
- **You should leave with a overview understanding of IoT security testing**
- **We'll get deeper into what JTAG is and why should you care**
- **You will learn about some ways organizations can be better prepared to handle IoT in their environment**
- **We'll start with the very basics and work our way up to more technical material**

Introduction

About the Presenter

- **Michel “Mike” Chamberland**
- **Practice Lead (Americas Region) with Trustwave SpiderLabs**
- **CISSP, OSCE, OSCP, OSWP, CEH, CHFI, CCSK, MCP, GIAC, MCTS, etc..**
- **Grew up in Sherbrooke, QC Canada and now lives in Sarasota, FL USA**
- **Work closely with all SpiderLabs resources globally**



Introduction

About Trustwave SpiderLabs

- **A division within Trustwave**
- **Consists of 150+ specialized security experts**
- **Focuses on penetration testing, red teaming, research and incident response**
- **Performed millions of scans and thousands of penetration tests**
- **Routinely perform embedded and IoT testing**
- **We are HIRING penetration testers for our team located in Makati!!!**
  - Email me at mchamberland@trustwave.com

What is IoT?

What is IoT?

What is embedded?

- An embedded system is a programmed controlling and operating system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts. Embedded systems control many devices in common use today. Ninety-eight percent of all microprocessors are manufactured as components of embedded systems. (Source: Wikipedia)
- Dedicated function
- Not a general computing device
- May or may not be interconnected

What is IoT?

Definition

- The Internet of Things (IoT) is the **network of physical devices**, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to **connect and exchange data**, creating opportunities for more direct **integration of the physical world** into computer-based systems, **resulting in efficiency improvements, economic benefits, and reduced human exertions** (Source: Wikipedia)
- Networked embedded systems
- Usually assigned an IP address and connected to the Internet
- Often labeled as “Smart Devices”

What is IoT?

Description

- **An IoT device is always an embedded device**
- **An embedded device is not always an IoT device**
- **An IoT device is interconnected**
- **An IoT device is built for a specific purpose**

What is IoT?

Examples

What is IoT?

Examples

What is IoT?

Examples

What is IoT?

Examples

What is IoT?

Examples

What is IoT?

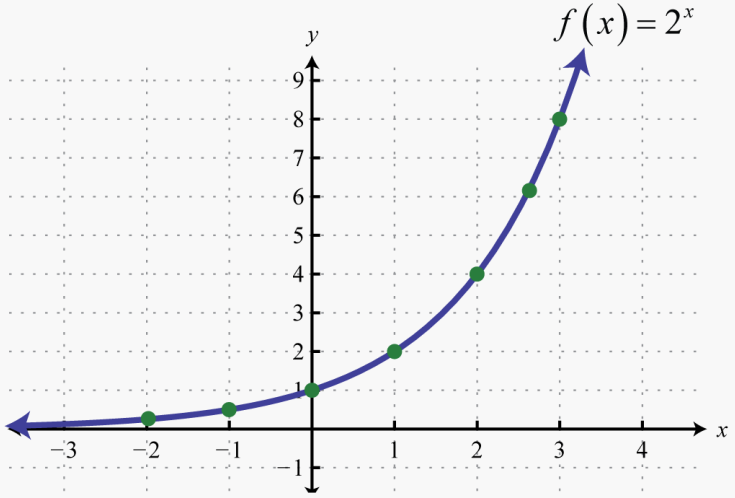
Examples

- **Belkin Wemo**
- **Nespresso Prodigio**
- **Nest**
- **Phillips Hue**
- **Garmin Forerunner**
- **Fitbit**
- **Whiting Blood Pressure Monitor**
- **Meat Thermometers**
- **Weather Stations**
- **Ring doorbell**
- **IP Cameras**
- **Amazon Dash Buttons**
- **Amazon Echo (Alexa)**
- **IP Phones**
- **Pool Pumps**
- **Door Locks**
- **Video Game Consoles**
- **Alarm Systems**

What is IoT?

Why it is important

- **Explosive growth of IoT both in homes and in the enterprise**
- **IoT Security still at its infancy**
- **Lack of security standards**
- **Lack of mature testing methodologies**
- **Not enough research is being done in this domain**



What is IoT?

Example Attacks/Breaches

- **Casino customer database breached**
  - Breached via smart thermostat in fish tank
- **Stuxnet**
  - Targeted Iranian nuclear program
  - Successfully destroyed centrifuges
  - Very sophisticated attack
- **Mirai Botnet**
  - Large botnet composed of IoT Devices such as IP cameras and routers
  - Mostly used for DDoS attacks (1.1 Tbps)
  - Took advantage of outdated software and default credentials

What is IoT?

Example Attacks/Breaches

- **Cardiac Devices and Insulin Pumps**
  - Implantable pacemakers and defibrillators found to be hackable
  - Can cause incorrect pacing or shock by draining the battery
  - Cause overdose of insuline
- **Connected Car**
  - Control car remotely
- **Sniper Rifles**
  - As demonstrated at Black Hat
  - Gun WIFI network with default password

Trustwave Study/Statistics

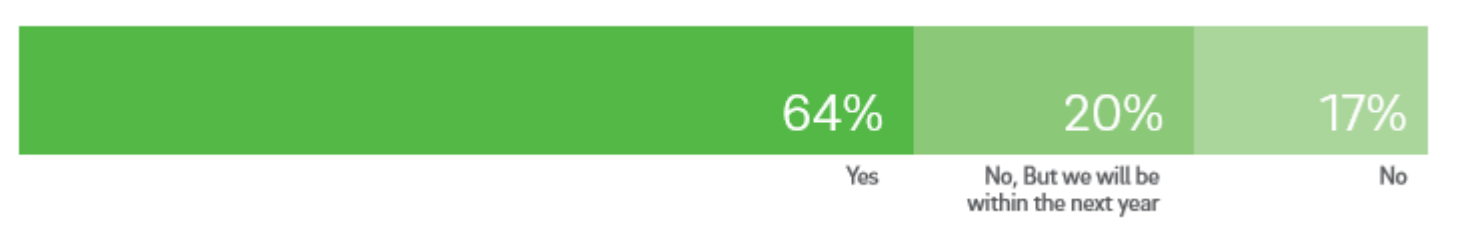
Trustwave Study/Statistics

About the Study/Methodology

- **Study commissioned to assess**
  - The current and future use of IoT
  - Corresponding security practices and implementation challenges
- **Sponsored by Trustwave**
- **Conducted by Osterman Research in November 2017**
- **Targeted midsize to large organizations in North America**
- **137 respondents**
- **Mean number of employees at organizations surveyed was 1000**
- **Margin of error +/- 8.4%**

Trustwave Study/Statistics

A disparity between IoT use and security
IoT use is growing rapidly



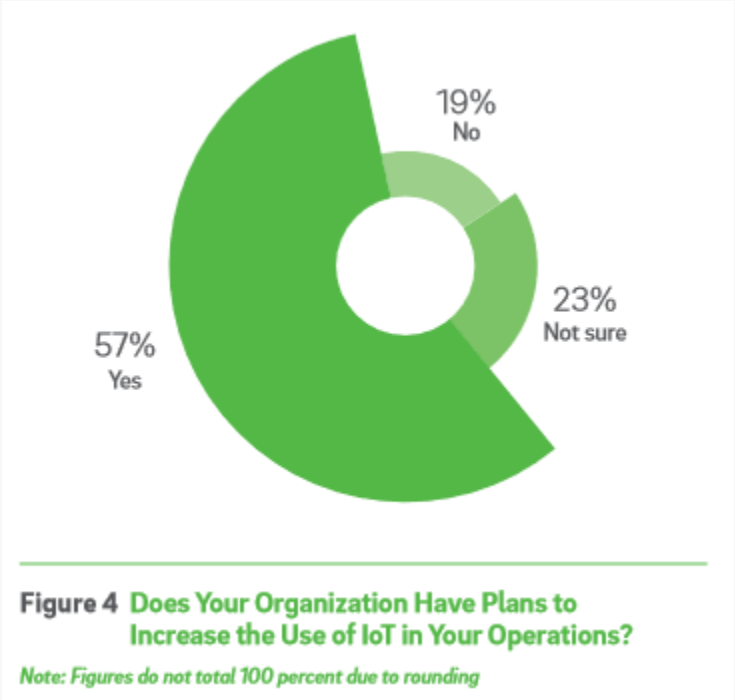


Figure 4 Does Your Organization Have Plans to Increase the Use of IoT in Your Operations?

Note: Figures do not total 100 percent due to rounding

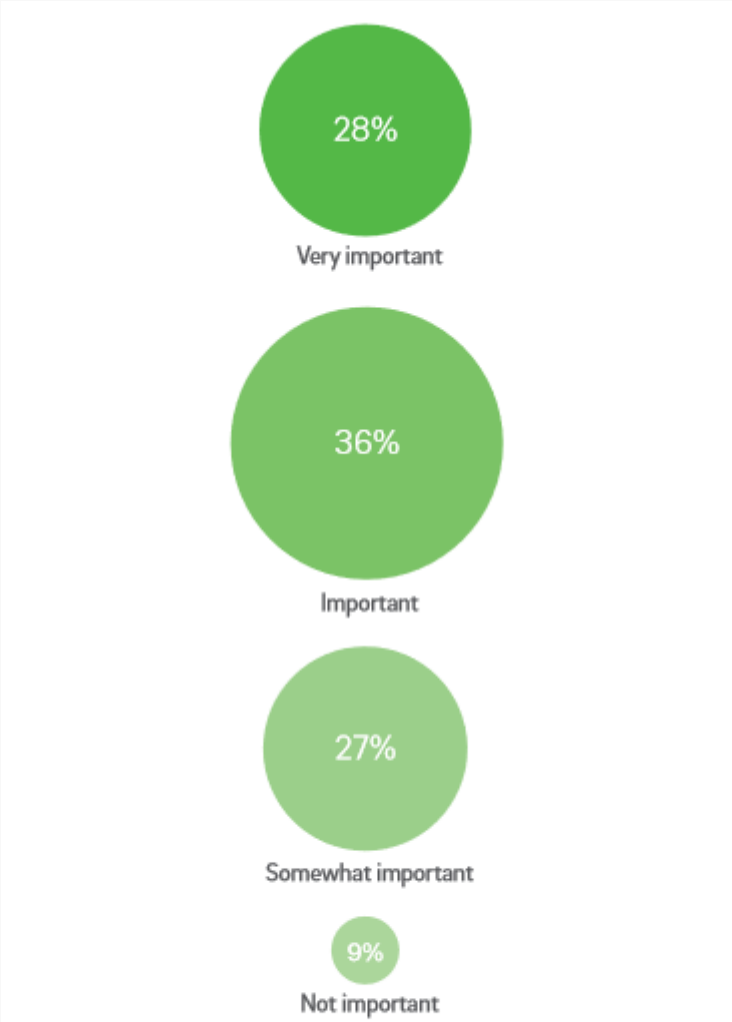
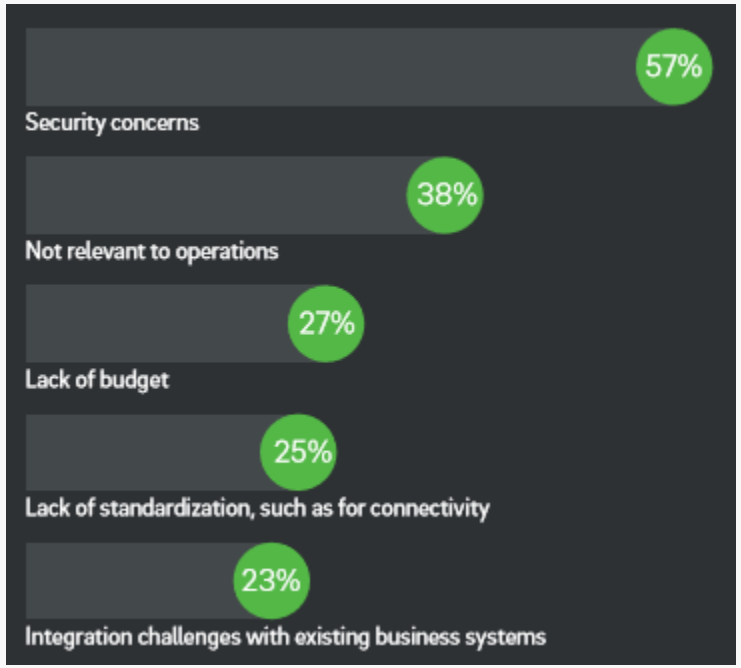
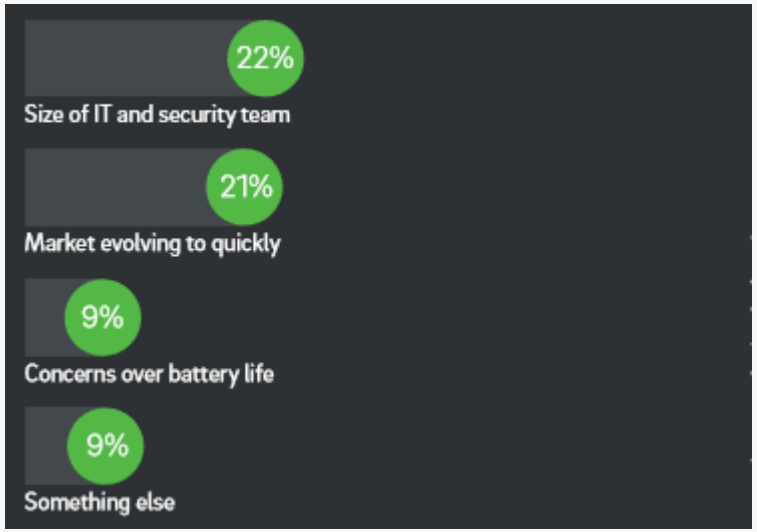


Figure 3 Compared to the Other Cyber Security Priorities in Your Organization, How Critical is Your IoT Security Strategy?

Trustwave Study/Statistics

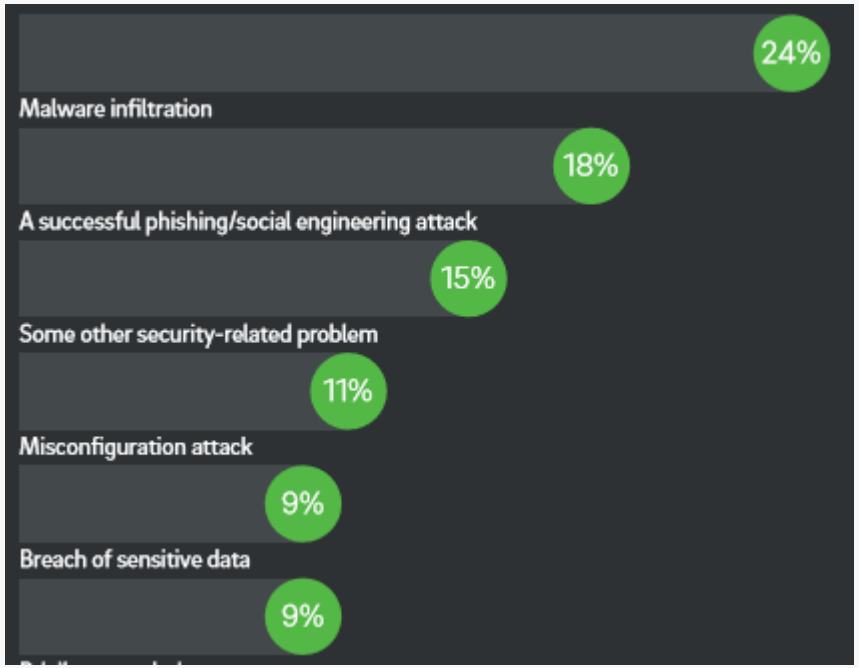
Security concerns cited as top barrier to increased IoT adoption

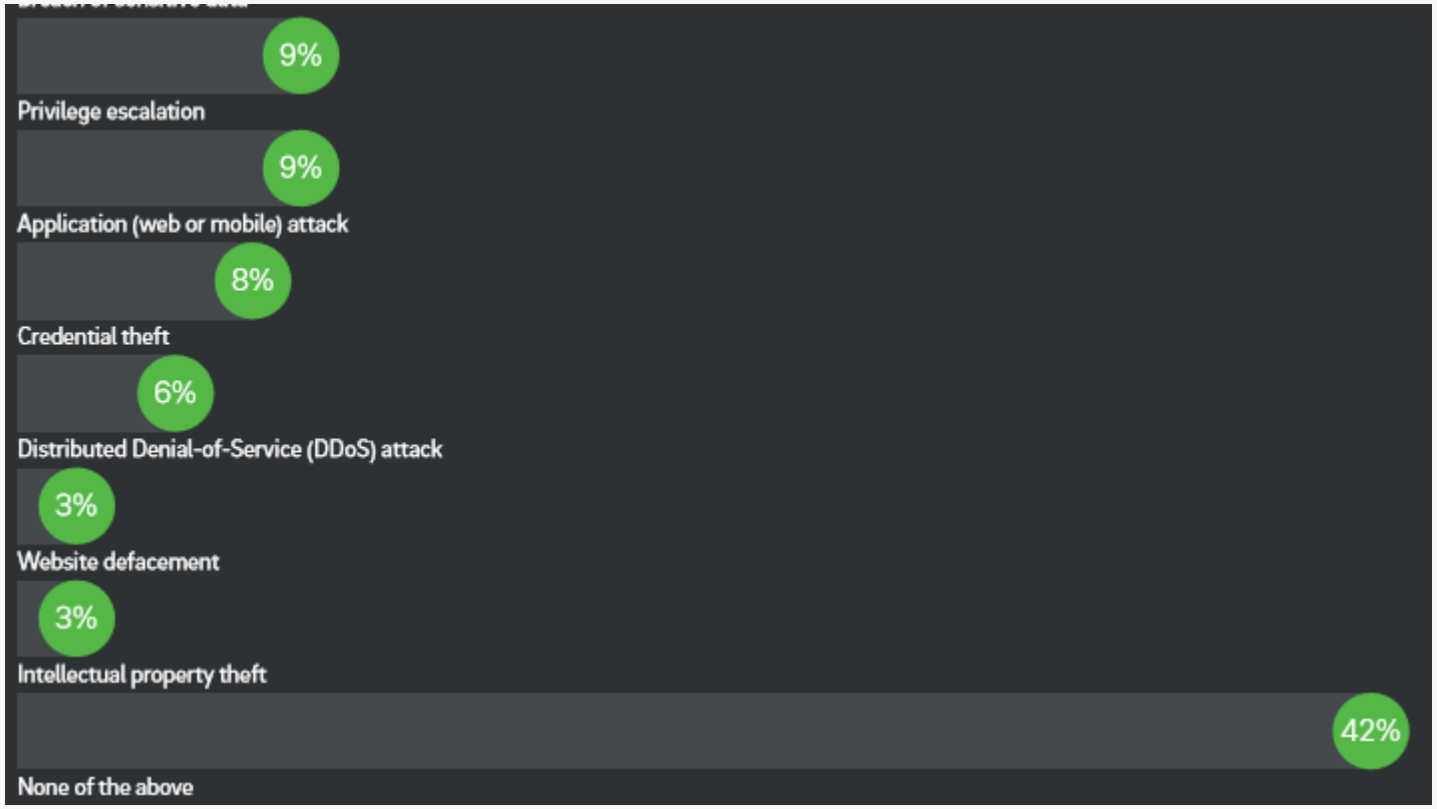




Trustwave Study/Statistics

Most have already experienced an IoT-related security incident





Trustwave Study/Statistics

A lack of patching policies and procedures

Figure 11 Does Your Organization Have IoT Patching Policies in Place?

Figure 12 Length of Time Required to Fully Implement an IoT Patch Once It Has Been Issued

Trustwave Study/Statistics

Insufficient risk assessment for third party-partners and testing of IoT vendors

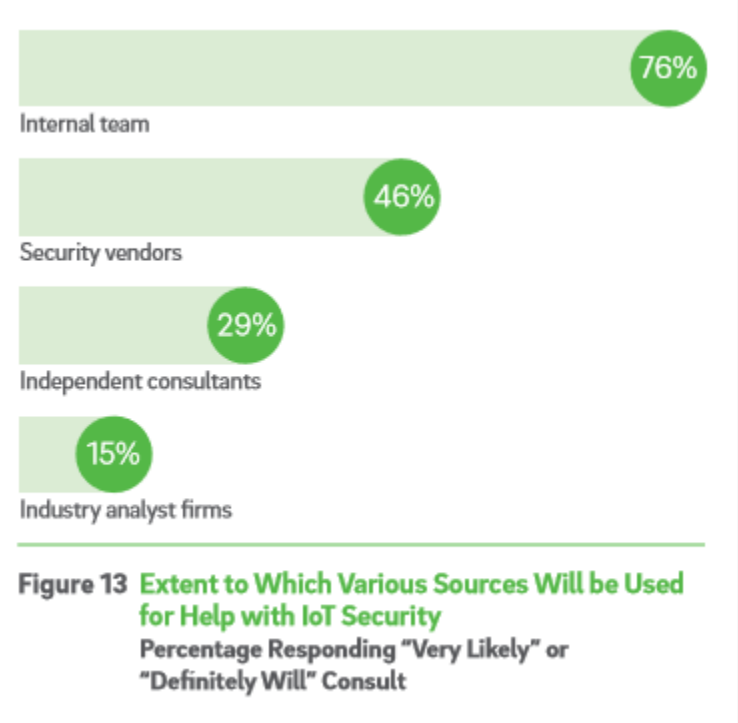


Figure 13 Extent to Which Various Sources Will be Used for Help with IoT Security
Percentage Responding "Very Likely" or "Definitely Will" Consult

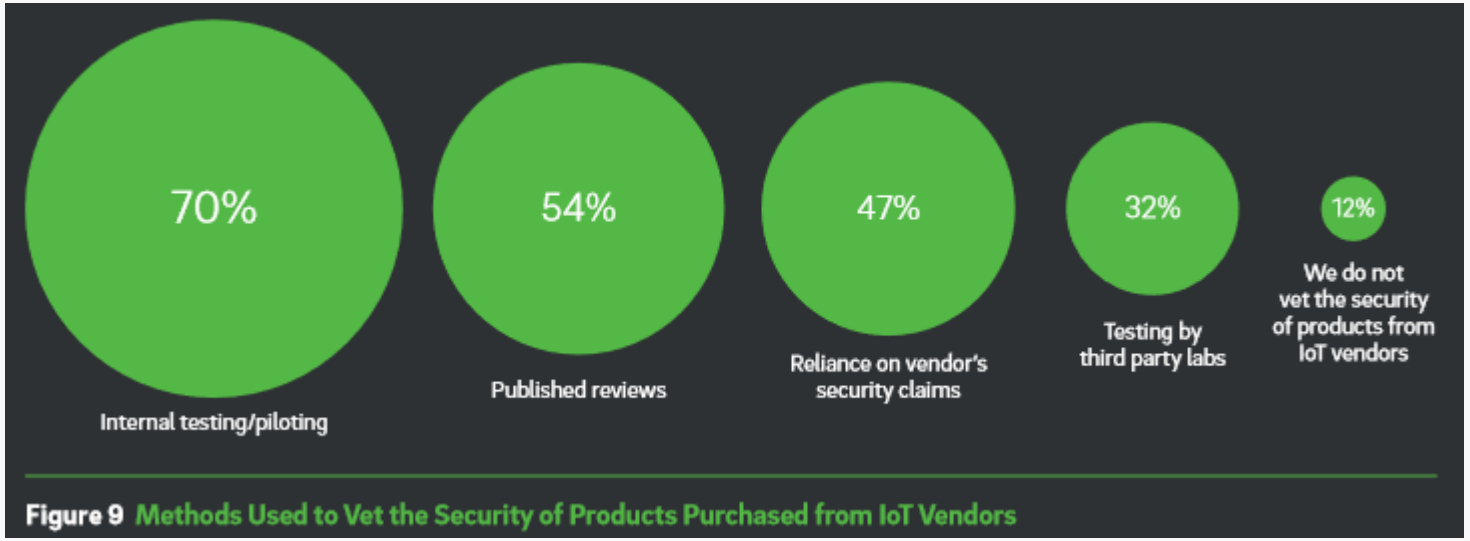


Figure 9 Methods Used to Vet the Security of Products Purchased from IoT Vendors

Trustwave Study/Statistics

Confidence in IoT security is not high

Figure 8 Confidence That Organizations Can Detect and Protect Against IoT-Related Security Incidents

Trustwave Study/Statistics

Key Findings Recap

- **A disparity between IoT use and security**
- **IoT use is growing rapidly**
- **Security concerns cited as top barrier to increased IoT adoption**
- **Most have already experienced an IoT-related security incident**
- **A lack of patching policies and procedures**
- **Insufficient risk assessment for third party-partners and testing of IoT vendors**
- **Confidence in IoT security is not high**

Trustwave Study/Statistics

Growth of IoT

- **Business Insider Intelligence**
  - Projects there will be 55 billion IoT devices by 2025, up from 9 billion in 2017
- **Juniper**
  - IoT devices, sensors and actuators will reach over 46 billion by 2021
- **Cisco**
  - From 16.3 billion in 2015 to 26.3 in 2020
  - 3.4 devices per capita in 2020 vs 2.2 in 2015
- **Ericsson**
  - Projecting annual growth rate of 23%

Trustwave Study/Statistics

Growth of IoT

- **Gartner**
  - 20.8 billion devices by 2020
- **IDC**
  - 25.6 billion in 2019 up to 30 billion in 2020
- **Goldman Sachs**
  - 10X as many (28 billion) by 2020

State of IoT Security

State of IoT Security

Top 10 IoT Vulnerabilities (2014)

- **I1 – Insecure Web Interface**
- **I2 – Insufficient Authentication/Authorization**
- **I3 – Insecure Network Services**
- **I4 – Lack of Transport Encryption**
- **L5 – Privacy Concerns**
- **L6 – Insecure Cloud Interface**
- **L7 – Insecure Mobile Interface**
- **L8 – Insufficient Security Configurability**
- **I9 – Insecure Software/Firmware**
- **I10 – Poor Physical Security**

State of IoT Security

What we see in IoT implementations

- **Security maturity about a decade behind**
  - Weak/default credentials
  - Replay attacks
  - Lack of or weak encryption
- **Often difficult or impossible to patch**
- **Very large ecosystem**
  - Many different connectors, standards, platforms, frameworks, etc.
- **Security thru obscurity**
- **Many embedded developer assume their code will operate in a trusted environment**

Attacking IoT Devices

Attacking IoT Devices

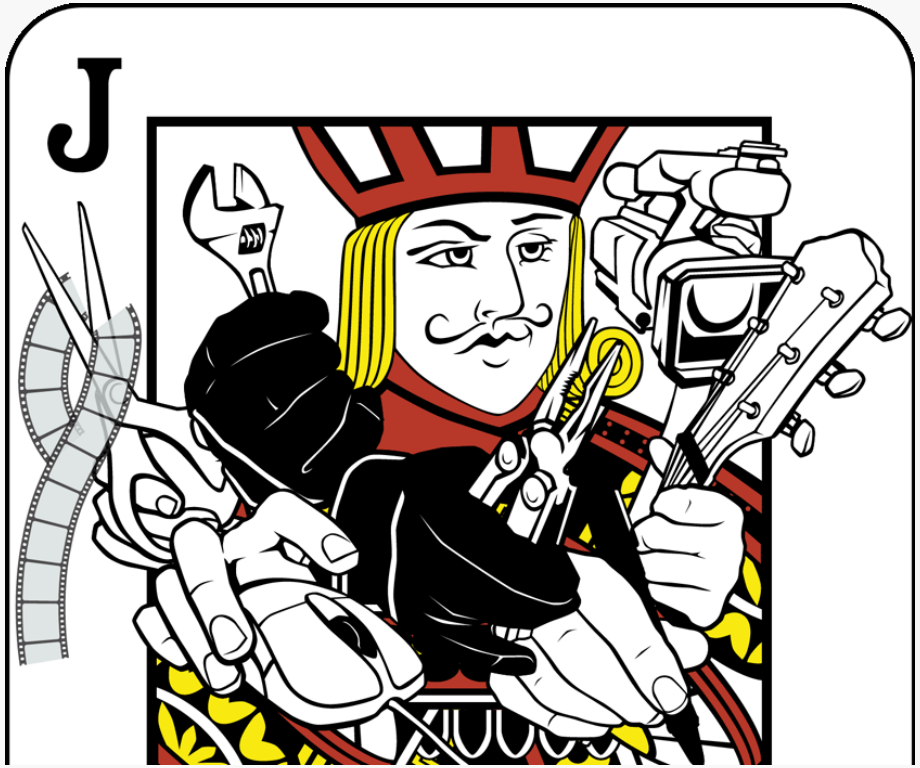
IoT Stack

- **Device**
- **User/Management Interfaces**
  - Mobile Apps
  - Web
  - Thick Client
- **Hardware Input and Output**
- **Hardware sensors**
- **Local/Global Network**
- **Wireless (BLE, ZigBee, Wifi, etc.)**
- **Cloud Services/API's**

Attacking IoT Devices

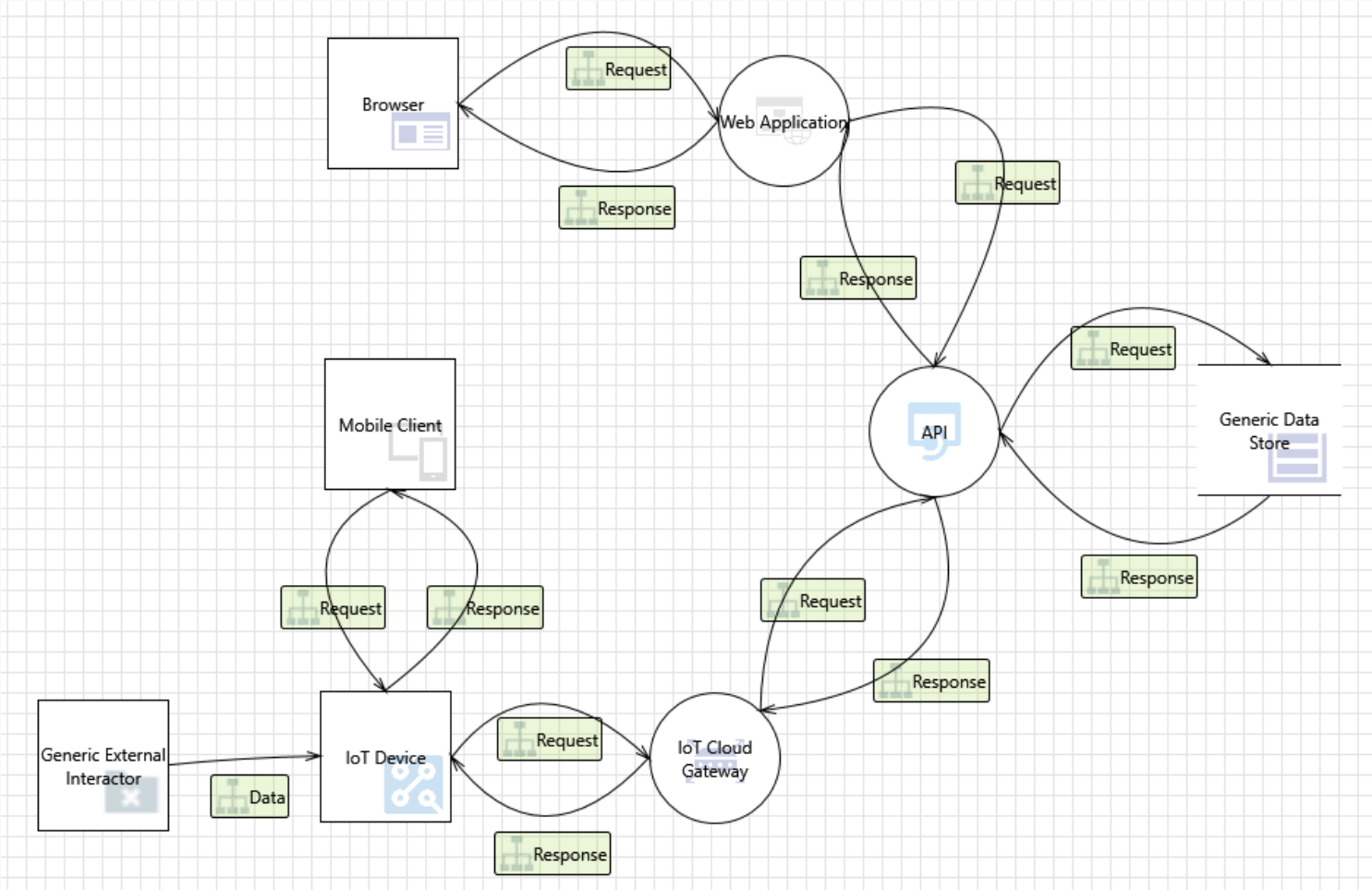
Required Skills

- **Web Application Security Testing**
- **Mobile Application Security Testing**
- **Wireless Testing**
- **Network Penetration Testing**
- **Reverse Engineering**
- **Electronics**
- **Strong appetite and aptitude for learning**
- **And more…**



Attacking IoT Devices

The IoT Attack Surface



Attacking IoT Devices

Research Target

- **Identify hardware components**
- **Download Firmware**
- **Download SDK's**
- **Public datasheets (alldatasheet.com)**
  - FCC ID
- **Identify Ports (UART, JTAG, etc)**
- **Shodan for target discovery**
- **Threat modeling**

Attacking IoT Devices

Common Attack Techniques

- **Reverse engineering firmware**
  - Hidden secrets (Passwords, Certs, API Keys, etc)
  - Backdoors, Debug or Administrative features
- **Radio Attacks (Sniff, Replay, MiTM)**
- **Monitor network traffic**
- **Port scan target/Network attacks**
- **Direct access to device memory**

Attacking IoT Devices

Ports

- **UART**
- **JTAG**
- **SPI**
- **I2C**
- **USB**
- **Ethernet**
- **Etc**

JTAG

JTAG

What is JTAG

How is JTAG Used

What can I get from JTAG as an Attacker

Identifying Pinouts

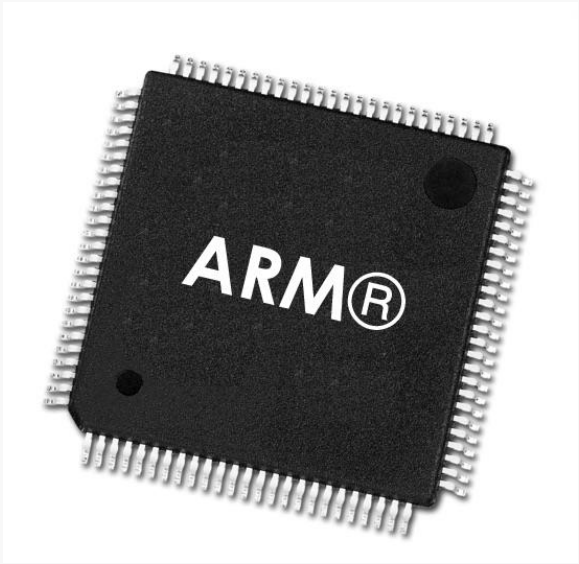
Interfacing with JTAG

Other Hardware Interfaces

JTAG

What is JTAG

- Named after the Joint Test Action Group
- Industry standard for verifying designs and testing printed circuit boards (PCB)
- Defines a debug port
- Allows Tapping into the operating PCB via a TAP (test access port)
- Daisy-chained to allow access to multiple components
- Allows debugging of firmware code
- Allows boundary scans

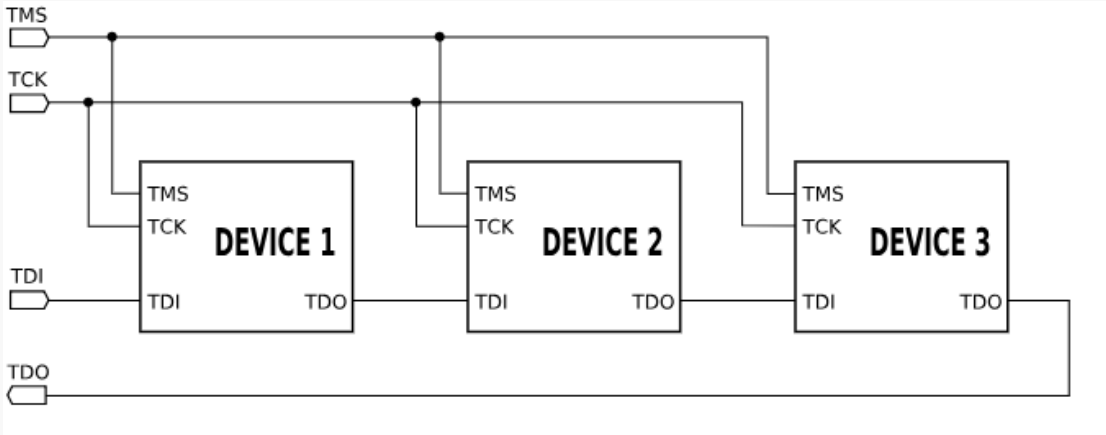


JTAG

What is JTAG

- **TDI**
  - Test Data In
- **TDO**
  - Test Data Out
- **TCK**
  - Test Clock
- **TMS**
  - Test Mode Select
- **TRST**
  - Test Reset (Optional)

- **Switch device state with TMS**
- **Device can have control registers**
  - IR – Instruction Register
  - DR – Data Register



JTAG

How is JTAG used

- **Extract or upload code/data**
- **Modify memory contents**
- **Affect device operation on the fly**
- **Read specific pins on a device**

JTAG

What can I get as an attacker with JTAG

- **Download firmware**
  - For Analysis
- **Upload firmware**
  - Tampering
  - Backdoor
- **Debugging**
  - Bypass security features
- **Full Compromise**
  - Pivoting

- **Specific engagement**
- **As part of a larger initiative**
  - Pen Test
  - Red Team

JTAG

Identifying Pinouts

- **TAP (Test Access Port)**
- **Daisy chained between chips**
- **Main challenge leveraging JTAG is determining connections**
- **Methods of determining JTAG pins**
  - Visual
  - JTAGEnum
  - Jtagulator

JTAG

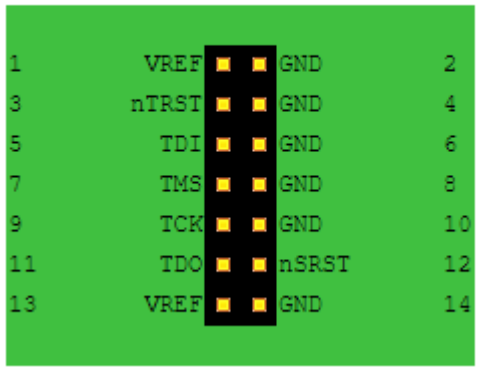
Identifying Pinouts - Visual

- **Sometime you might get lucky and see a labeled JTAG header**
- **Sometimes you might find information online**
- **Sometimes you maybe able to leverage datasheets and tracing**
- **Sometimes it's not so easy**

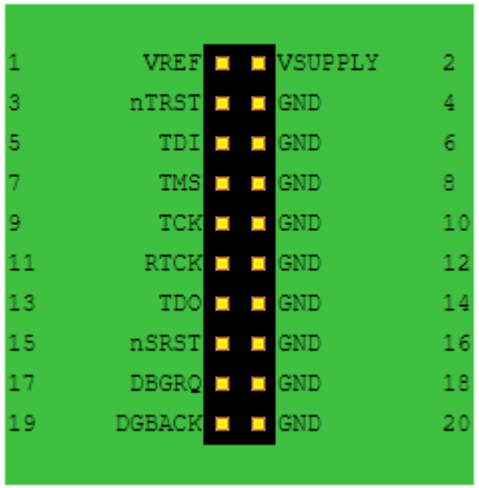
JTAG

Identifying Pinouts - Visual

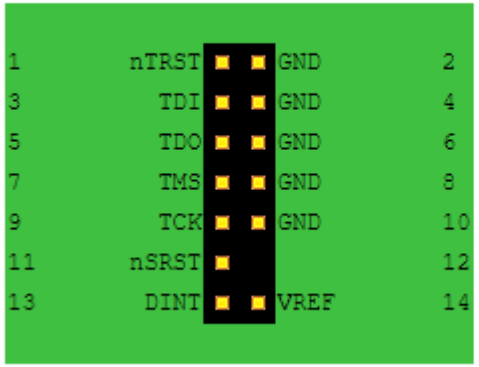
ARM14 JTAG header pinout



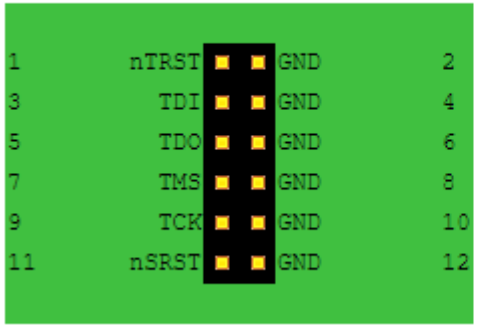
ARM JTAG header pinout



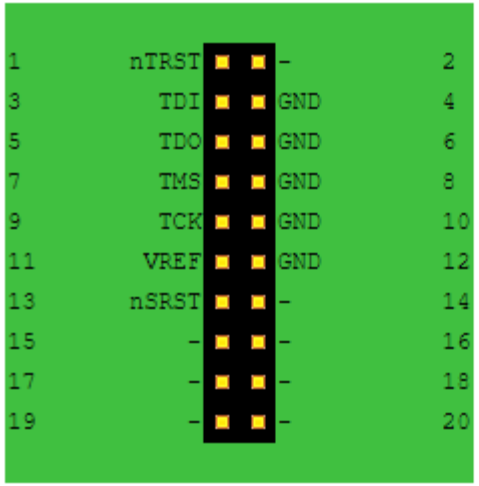
MIPS EJTAG JTAG header pinout



Linksys WRT54G / WRT54GS JTAG header pinout



Toshiba MIPS JTAG header pinout



JTAG

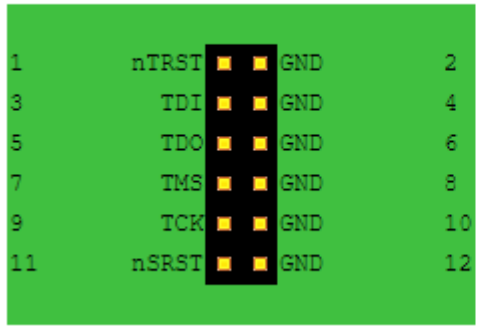
Identifying Pinouts - Preparation

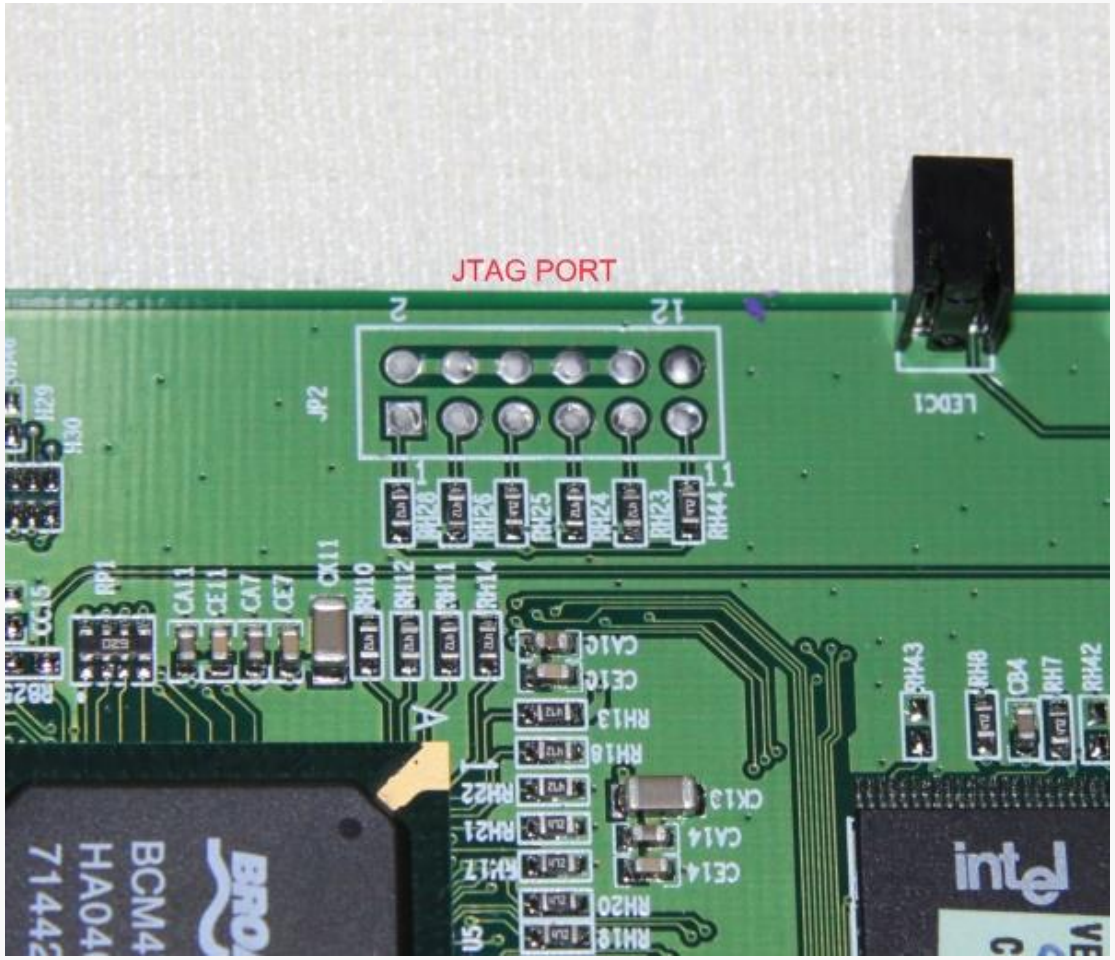
- **Add headers**
- **Clips**
- **Identify target voltage**
  - Lookup datasheet
  - Measure VCC /GND
- **Precautions**
  - Ensure there is a shared ground between the target and your enumerating device
  - Connect to target with power off
  - Power on dongle first then target

JTAG

Identifying Pinouts - Preparation

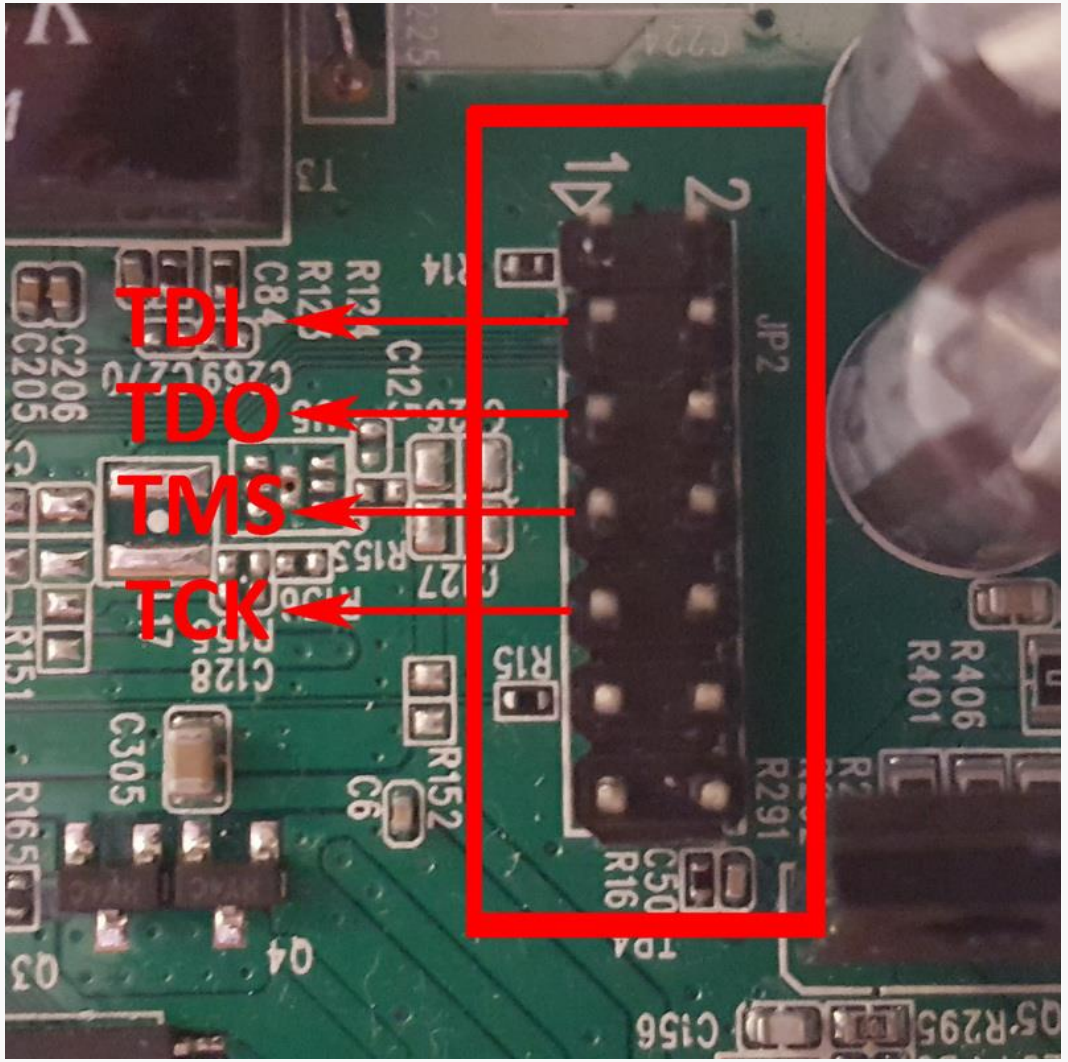
Linksys WRT54G / WRT54GS JTAG header pinout





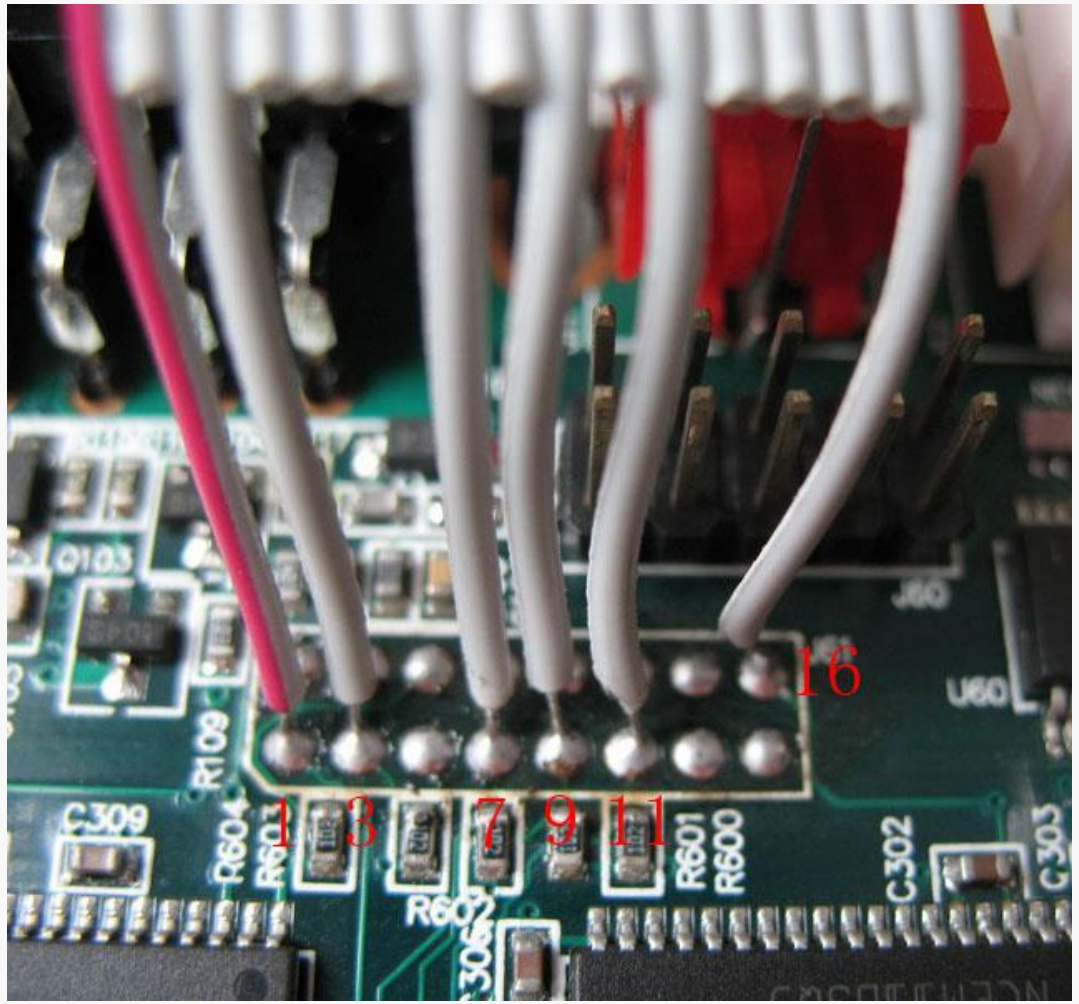
JTAG

Identifying Pinouts - Preparation



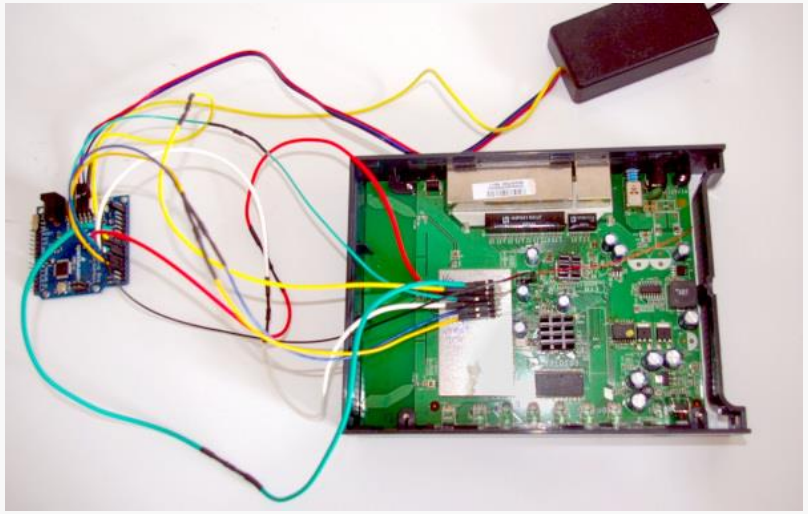
JTAG

Identifying Pinouts - Preparation



JTAG

Identifying Pinouts -JTAGEnum

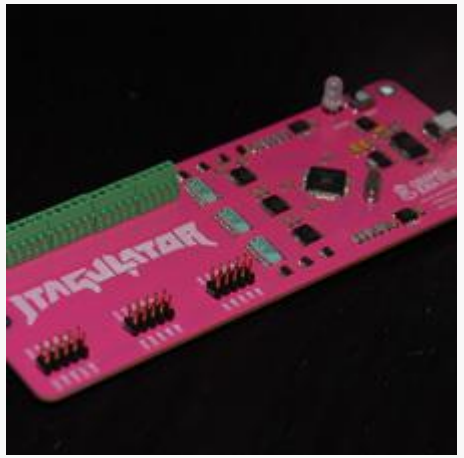


- **Free Tool Created by Nathan Andrew Fain (Cyphunk)**
- **Runs on Arduino (JTAG.ino)**
  - Teensy++ Can do up to 46 pins
- **Now runs on Raspberry PI (JTAGenum.sh)**
- **Both have minimal configuration that can be tweaked directly in the scripts**
- **Mark sure your device support the power level of your target (3.3v vs 5v)**
- **Can also identify UART pinout**
- **Works sometimes**

JTAG

Identifying Pinouts - Jtagulator

- **Open source tool created by Joe Grand (Grand Idea Studio)**
- **Build it yourself or buy pre-made**
- **Purpose built**
- **Adjustable voltage from 1.2v to 3.3v**
- **Can do up to 24 pins**
- **Can also identify UART pinout**
- **More reliable**



JTAG

Interfacing with JTAG

- **What to do once you figured out the pinout**
- **urJTAG**
- **OpenOCD**

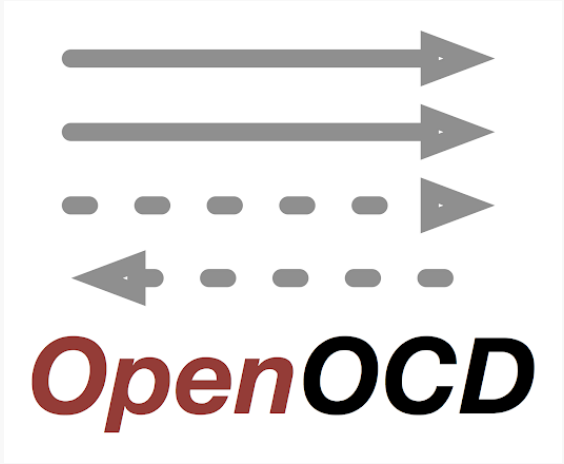
JTAG

Interfacing with JTAG - urJTAG

- **Simpler solution**
- **Allows read/writing firmware (readmem/flashmem)**
- **Does not allow debugging**
- **BSDL files (.bsd) are used to define interfaces**
  - Uses VHDL syntax
  - Can be downloaded from http://bsdl.info/
- **“cable” command to configure your connection**
- **“detect” command to see devices on the chain**
  - Leverage BSDL files

JTAG

Interfacing with JTAG - OpenOCD

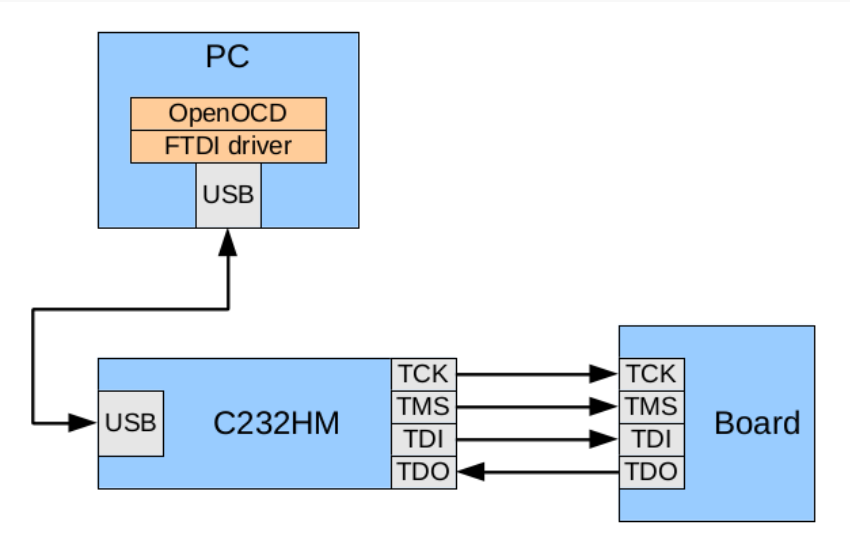


- **Open On-Chip Debugger (OpenOCD)**
- **Extensive features**
- **Supports reading/writing to flash memory**
- **Supports live debugging using GDB**
  - ARM7, ARM9, Cortex-M3, XScale, Intel Quark and others
- **Uses .cfg files to interface with hardware**
- **Runs as a server on port 4444 by default**
- **When debugging, GDB listens on port 3333 by default**
  - gdb-multiarch (build of GDB that supports many architectures)
  - target remote localhost:3333

JTAG

Interfacing with JTAG – Hardware

- **Many dongles available**
- **FTDI FT2232 chip used in many solution**
  - USB to JTAG (and more)
  - FT**2**232**H**
    - High Speed (480Mbps)
    - 2 Channels so UART and JTAG can be used at the same time



JTAG

Interfacing with JTAG – Analysis Tools

- **Binwalk**
  - Inspects a firmware images to look for known file types
  - Will identify headers, compressed kernels, file systems, etc
  - You can then extract and use these files
  - Signature based and not always accurate
- **Firmware Mod Kit**
  - Automates deconstruction and reconstruction of firmware
  - Decompress/compress
  - Update headers
  - Rebuilds/resize file systems

JTAG

Interfacing with JTAG – Analysis Tools

- **Firmwalker**
  - Search extracted or mounted firmware file systems
  - Looks for
    - Passwords
    - Certificates
    - Configuration files
    - Keywords
    - Web servers
    - Common binaries
    - etc

Handling IoT Growth

Handling IoT Growth

Organizations

- **Define and implement an IoT policy**
- **Manage IoT inventory**
- **Vendor management program**
- **Regular scanning and penetration testing**
- **Network Segmentation**

Handling IoT Growth

Implementers

- **Don't expose debug interface (UART, JTAG, etc)**
  - Or at least make it as difficult as possible to identify and connect to
- **Validate firmware**
- **Run services with least privileges**
- **Don't assume code running on the device is running in a trusted environment**
- **Do not use default credentials**
- **Ensure you have a solid update mechanism in place**
- **Use encryption correctly**
- **Have a 3rd party test the full solution**

Conclusion

Conclusion

Recap

- There are many types of IoT/smart devices on the market
- IoT is going thru a massive growth
- Security is weak in IoT
- Lots of opportunities for IoT security testers
- IoT security testing is an aggregate of other types of testing and more
- IoT security testing can be difficult
- Many things can be done to reduce risk by both users and implementers

Conclusion

Final Words

- **Pay attention to IoT**
- **Want to connect?**
  - mchamberland@trustwave.com
  - @SecurityWire on Twitter
- **Salamat at Paalam!**


Trustwave®
Smart security on demand