Challenges in Phone Forensics

About the Speaker

- 23 books (2 more in progress)
- Over 40 industry certifications
- 2 Masters degrees
- D.Sc. in Cybersecurity ***in progress***
- 13 Computer science related patents
- Over 25 years experience, over 15 years teaching/training
- Helped create CompTIA Security+, Linux+, Server+. Helped revise CEH v8
- Created ECES, created OSFCE
- Frequent consultant/expert witness
- Frequent speaker/presenter including: Defcon, Hakon India, Hakon Africa, SecureWorld, ISC2 Security Congress, AAFS, IAFSL, etc.
- Conducts security related training internationally

www.chuckeasttom.com

chuck@chuckeasttom.com

Areas of concern phones

- Proliferation of Models
- Data Protection
- Proliferation of Apps
- Limitations of Tools
- JTAG/Chip-off
- IoT

Actual cases

- Adam Howe took a "selfie" photo of himself at the scene of a church burglary. This evidence led to a search of the suspect's property, which turned up the stolen goods from the church.
- A cell phone was accidently dropped near the scene and was used to identify the alleged perpetrator. In 2013, cell phone pictures led to an arrest in a burglary of a Jared jewelry store. The alleged thief discarded clothing and accidently dropped his cell phone behind a nearby 7-11. The cell phone photos positively ID'd him

Actual Cases

- Derrick Lee, Jr. is charged with entering an apartment with a gun. He is accused of robbing and shooting the residents while in the apartment. It appears while allegedly committing the robbery, Mr. Lee was carrying a stolen cell phone. The GPS records for the phone confirm Mr. Lee was at the apartment at the time of the robbery and shooting

Models

iPhone: iOS one operating system, but each version is more difficult to extract from. Now using the iTunes backup is an effective work around.

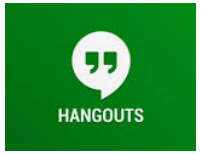
Android: Less secure/difficult to extract from, but many variations in both hardware and the operating system specific.s

Data Protection

- iPhone encryption
- Longer pass codes
- Third party encryption
- Encrypted apps

Proliferation of apps

- Facebook
- Twitter
- Instagram
- Whatsapp
- LinkedIn
- ClassMates
- Kick
- WeChat
- Stack
- Stride
- Kakao Talk
- Line
- Viber
- Hangouts
- Textra SMS
- Line
- XFinity Connect
- Marco Polo
- Skype
- Google Voice



Tools

Cellebrite

XRY

Magnet

Oxygen

Black Bag

Mobile Edit

Paraben

NIST

NIST Special Publication 800-101 Guidelines on Mobile Forensics

Tool Classification System

Level 1: Manual Extraction

Level 2: Logical Extraction

Level 3 methods: Hex Dumping/JTAG

Level 4: Chip-off

Level 5: Micro Read methods using high powers microscopes to view physical state of gates.

JTAG

Joint Test Action Group (JTAG)

Tools

- RIFF

- ORT Box

- Easy JTAG Box

- Octopus Box

- Medusa Box

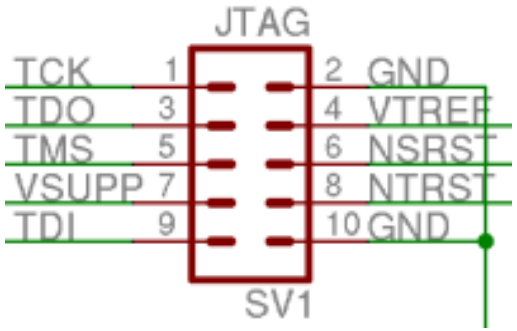
IEEE 1149.1

- The standard was adopted in 1990 by the IEEE as Standard 1149.1
  - Joint Test Action Group (JTAG)
  - Intended for testing boards and devices
- Describes a serial 4-wire (5th is optional)
- Many of today's key components contain Boundary-Scan
  - Microprocessors, FPGAs, DSPs, etc.

How does it work?

"In order to perform a JTAG recovery, one must connect the appropriate JTAG pins (Image 1 below) to the memory flasher. Once the board is powered on, the flasher software can then a full memory dump of the NAND flash. This takes a significant amount of time. The connections can then be broken and the phone can be reassembled.

Although this captures a full physical image, it is not normally used as logical means can perform sufficient coverage. Also, any errors in soldering or voltages can destroy the very small PCB connections & the device itself." -Do-It-Yourself Mobile Forensics by Lewis Sykalski

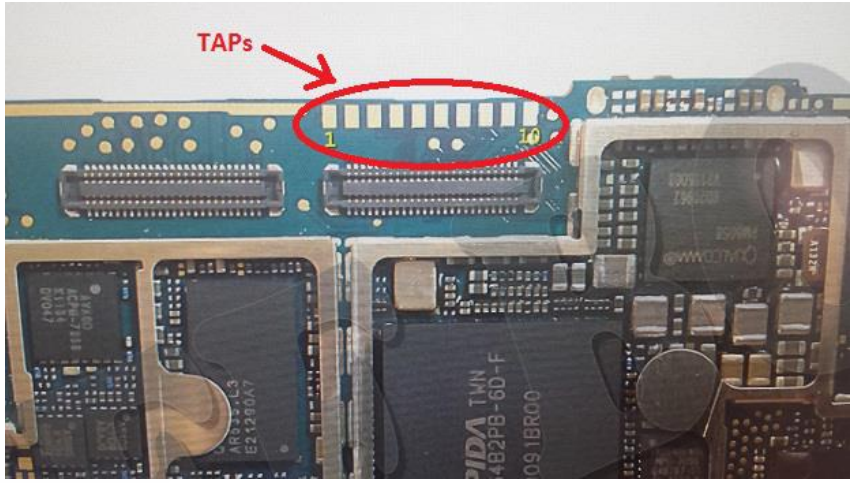


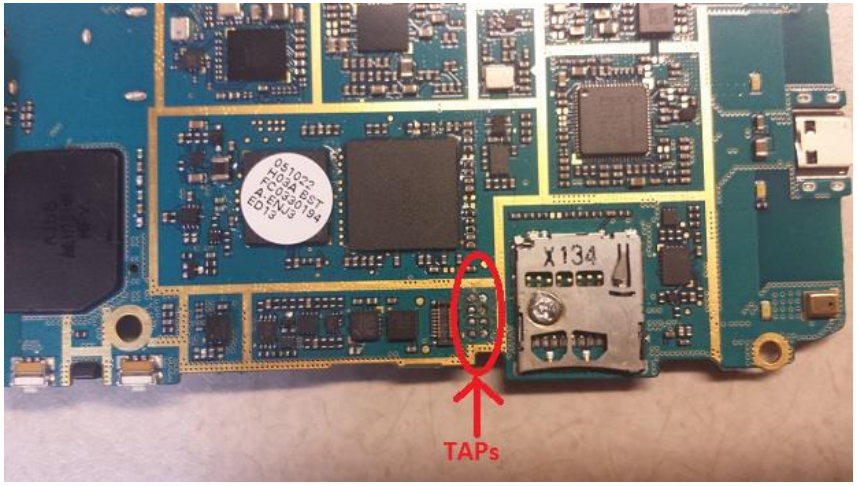
What JTAG can (and can't) do

It can bypass login
It can work on Android and Windows phones
It cannot (at least not now) work in iPhone
It cannot bypass encrypted drives
It is not fast
It is not a phone forensics panacea

What do the TAPs look like?

- **These are generic pictures of TAPs from NIST and AAFS**





IoT

- GPS
- Book Readers
- Smart Devices
- Vehicle Navigation Systems
- Vehicle Entertainment Systems
- Portable Devices
- Drones
- Google Home
- Amazon Echo

Further Reading

- Mobile Device Forensics
  http://www.lawtechnologytoday.org/2016/12/mobile-device-forensics/
- Mobile Forensics Must Keep Up With the Times
  https://www.forensicmag.com/article/2017/06/mobile-forensics-must-keep-times
- Top 3 Challenges in Mobile Phone Forensics
  https://www.linkedin.com/pulse/top-3-challenges-mobile-phone-forensics-aaron-abbe/
- Challenges to Forensics from Anti-Forensics
  https://www.securedatarecovery.com/blog/challenges-forensics-anti-forensics