

A photograph of the Aurora Borealis (Northern Lights) in shades of green and blue, reflected in a calm lake. A large rock is visible in the foreground. The sky is dark with stars, and the overall scene is serene and natural.

# Software Analysis, Testing and Reverse Engineering Capabilities

# Technical Capabilities

- **Software Analysis, Testing and RE**
- Wireless Testing and RE
- Semi/Systems Testing and RE
- Digital Media/Video Testing and RE



# Testing & Reverse Engineering Scope

- Package RE
- Process RE
- Circuit RE
- Teardown
- Device identification
- Functional testing
- Code extraction
- Decompile
- Disassembly
- Algorithm analysis
- Mobile OS
- Embedded OS
- Cloud software
- System software
- Connectivity
- Mobility
- Security
- Location
- Media



# Outline

- Software Expertise
- Software Reverse Engineering Process
- Examples of recent projects

# Software Experts

Team of experts with development experience at all software levels and for various applications:

- Firmware/Embedded Systems
- Security & Encryption
- System-level software
- Application software
- Operating systems
- Cloud computing
- Source Code



# Software Analysis, RE and Testing Experience

- Firmware Extraction and Analysis:
  - Connectivity: Ethernet, USB, WiFi
  - Memories: DDR, Flash
  - Audio and Video encoders
  - DSP engines
  - Processor cores
- System and App Software Analysis:
  - Range of programming languages from Assembly to Java, Python, etc...
  - Networking: variety of communications protocols
  - Databases: Oracle, Informix, DB2, SQL, MySql
  - User interfaces
  - Drivers: wired and wireless controllers, flash controllers



# Software Analysis, RE and Testing Experience

- Operating systems internals and applications:
  - Range of operating systems: VxWorks,
  - Linux, OSx, Android, Windows, etc...
- Security:
  - PKI, Fraud detection, Secure e-mails
  - Authentication Systems, Smart Card, Biometrics



# Types of Analyses

- **Static Analysis**
  - Analysis without code execution (Effective in producing evidence)
  - Analysis of both source code and compiled code
  - Use of use cutting edge tools like Ghidra, IDA Pro, and BinaryNinja to analyze the binaries.
- **Dynamic Analysis**
  - Analysis through code execution (Effective in showing actual code being implemented)
  - Monitor and “hook” the running code to more intricately understand the inner workings of the application under investigation.
  - Use of a number of tools to gather run-time data
- **Binary Dissection**
  - Use of tools like Wireshark and Scapy to observe and model network communications.
  - Tools for decrypting of communications between a device and a cloud
  - Bus monitoring tools and logic analyzers to observe digital communications between components.





# Approach at Accessing Firmware/Software and Analysis

- **Consider Accessibility of firmware/Software**
  - Is the source code available (e.g. Publicly available Android source code)
  - What are other techniques available to access the firmware
    - Extraction of Flash content via HW or SW mechanisms (e.g. Runtime mechanisms, Routing, etc...)
- **Extract the firmware content from Flash device using selected mechanism**
- **Prepare extracted firmware for analysis**
  - Bit flip, decryption, disassembly, de-compilation, etc ...
- **Analysis of de-compiled firmware**



# Recent Firmware Analysis Projects

- Set Top Box analysis
- Secure world (TrustZone) in cell phones, TVs, laptops and tablets
- Garbage Collection of processes in cell phones, TVs, laptops and tablets
- Embedded systems booting sequence analysis for network switch products
- User authentication module of a client – server secure application
- Qualcomm Hexagon DSP analysis
- Android phone firmware analysis for noise cancellation

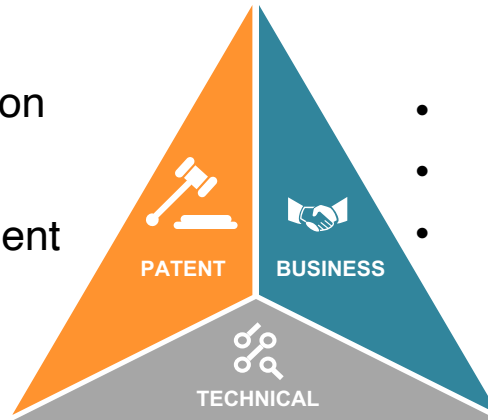
# Example Projects

- Example 1: Secure World (TrustZone) in TV
- Example 2: Garbage Collection of processes in TV
- Example 3: Analysis of baseband chip functionality on a smartphone through a combination of hardware and software/OS testing and data sheet analysis
- Example 4: Tracing a path of video data in a system which simultaneously stores and displays video data
- Example 5: Analysis of a DSP disassembly code to find links between functions of interest

# The TechPats™ Advantage

## Full Service Partner

- Licensing & Litigation Support
- Portfolio Management



- Industry Knowledge
- Strategy Expertise
- IP Transactions, Valuation

- Dedicated Technical & IP Experts
- Hands-on Product Experience
- State of the Art Reverse Engineering and Testing Labs