
**Automotive**
Security

Bozeman, MT : Seattle, WA : Portland, OR : Rescue, CA : Tokyo, JP : Brisbane, AU : Mobile, AL
Ulm, Germany : Manchester, UK : Waterloo, ON, CA : Stockholm, Sweden : Italy

ADAS

Infotainment

Autonomous

TLS over CAN bus

Cloud Services connectivity

FIPS for Military Grade Vehicles

Body Controllers

Brake Controllers

Automotive Gateways

OBD-II

# We Secure **Automotive** by **Securing Data**

Replacement part verification

Transmission controllers

Key Fobs

Automotive Gateways

Apps for Entry

Lidar/Radar

Telematics ECU’s

Firmware updates

ECU Secure Boot

# Exciting Company Growth

wolfSSL

Founded in Bozeman, MT (2004)

**2,000+ OEM Customers**

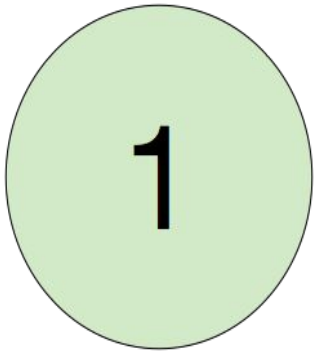
**2+ BILLION**

secure connections!

**15 years Securing Automotive Designs**

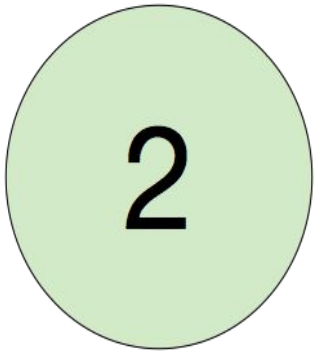
# Three Main Areas of Focus

## Data in **Transit**



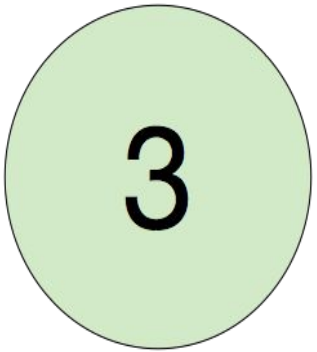

- Secured with **SSL/TLS, SSH**
- Possible Transfer Mediums: TCP, UDP, Bluetooth, Serial, CAN,etc

## Data at **Rest**



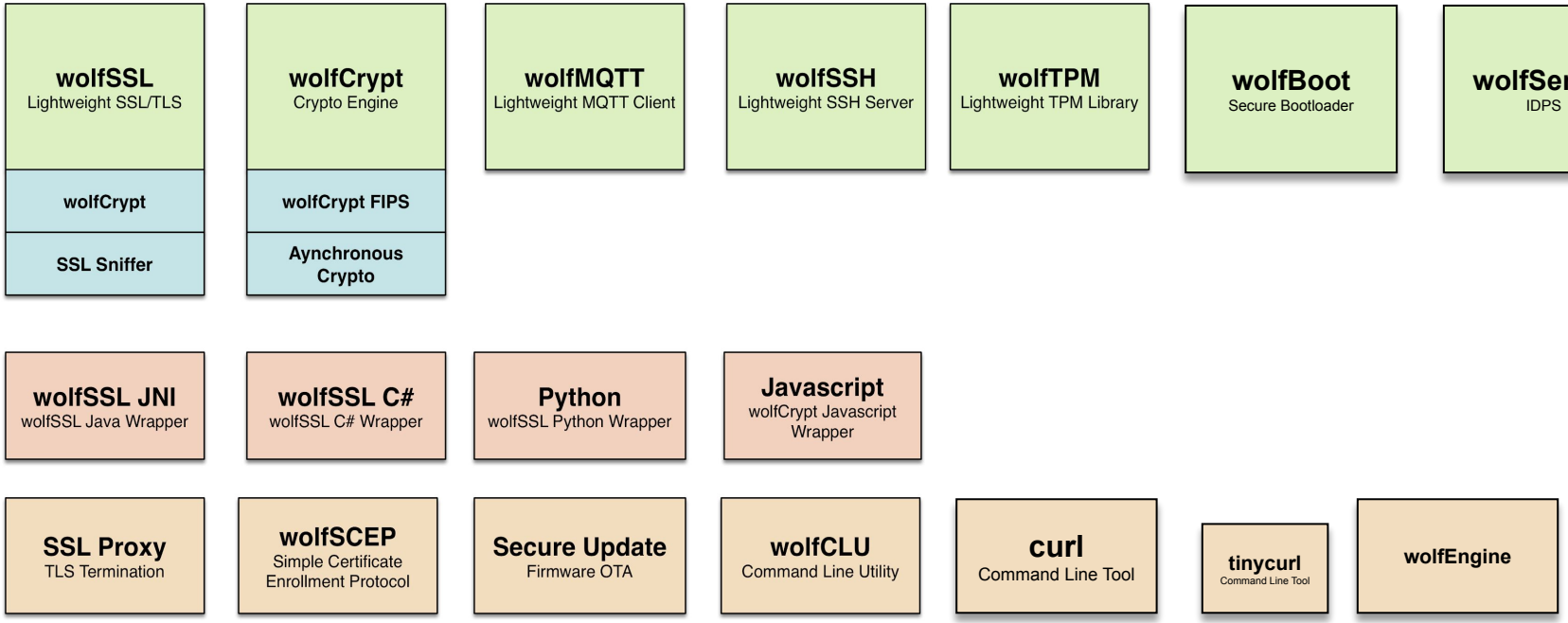

- Secured with **Cryptography**

## **Firmware Updates**




- Secured with **SSL/TLS**, **crypto**, **MQTT**
- Prevent malicious firmware flashing and updates

# wolfSSL Products Used in Automotive




Products are ported to all of the most popular Automotive Operating Systems: QNX, Autosar, Integrity, VXWorks, FreeRTOS, Automotive Grade Linux, Bare Metal etc!!!

# Automotive

- 15+ years experience
- Major customers in Japan, Germany, USA and France
- wolfSSL products are used by all top 10 automotive OEM's

## ECUs



## Telematics



## Infotainment

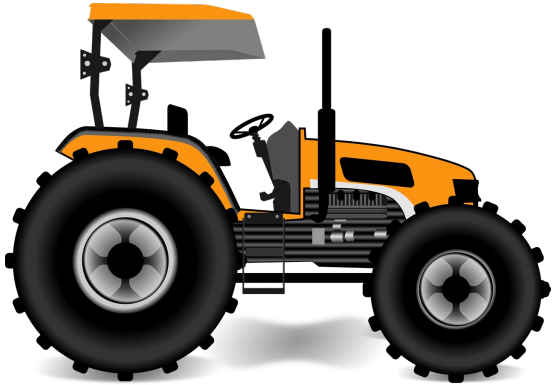

# Increased Complexity and Safety Requires Increased Security

**Simple Old School:**
Still cool…. but no auto break safety, no electronic fuel injections run by an ECU. Less attack vectors but less safety and functionality.

**Current Vehicles:**
Interconnected electronic parts, diagnostics, auto break engagement, many electronic safety enhancement functions. More attack vectors that need secured.

# All Automotive (not just the luxury car)

- wolfSSL products used in military vehicles
- Agricultural and heavy equipment vehicles
- Heavy duty and light weight trucks from Semi trucks to small pickup trucks
- In both the vehicle and the back end servers that may be supporting vehicle operations



# High throughput data verification for V2X.

# Use Case

- Leveraging DSP’s to get the most out of the hardware

- Difficulty of verifying the high volume data stream in a V2X environment
    - V2X environment gets a really high amount throughput - over 16,000 verifications per sec

# wolfSSL Products Used

- wolfCrypt used for signature verification
- Cryptographic Primitives running on a DSP as well as ARM core
- Dispatcher, custom built library for directing which cores a verification runs on and handling a high volume of verification requests
- SM2 public key support implemented for the Chinese Market, in addition to the existing Branpool and NIST implementations

# Specific Engineering Detail

- Performance optimization of caching ECC information for points with repetitive use and sharing that cached information between cores was a challenge
- Investigation into use of hardware acceleration such as HVX on DSP
- Many benchmarks done to investigate trade off of number of threads for parallelism and the point where it negatively impacts performance
- Isolation of processing power to a single core with the help of a dispatcher library and verification of processor usage

# Secure Firmware Update

# Use Case

- Retrieving and authenticating a new firmware update
- Phone in to backend server with wolfSSL + cURL
- Heightened security using CAAM on i.MX device
- CAAM Driver supports both

  Hardware Encryption and

  Secure Key store on QNX

# wolfSSL Products

- cURL
- wolfSSL
- wolfCrypt
    - Integrated with CAAM Driver for key storage retrieval

# Specific Engineering Detail

- Leveraged i.MX6 device and vastly improved security by using the CAAM
- Uses black encrypted keys with ECC ephemeral keys during TLS connections
- Red Vs Black Blobs
- Running with QNX
- Performance of sign/verify with black encrypted keys is close to an optimized unencrypted operation

| Algorithm | Software Only avg ms | QNX CAAM (black keys) avg ms | SP ASM avg ms |
|---|---|---|---|
| ECC [ SECP256R1] 256 key gen | 69.733 | 4.917 | 3.138 |
| ECDHE [ SECP256R1] 256 agree | 69.27 | 5.68 | 7.095 |
| ECDSA [ SECP256R1] 256 sign | 73.06 | 7.17 | 4.22 |
| ECDSA [ SECP256R1] 256 verify | 50.84 | 9.29 | 7.655 |
| ECC [ SECP256R1] 256 encryption | 69.47 | 5.935 | 7.275 |
| ECC [ SECP256R1] 256 decryption | 69.54 | 5.955 | 7.285 |

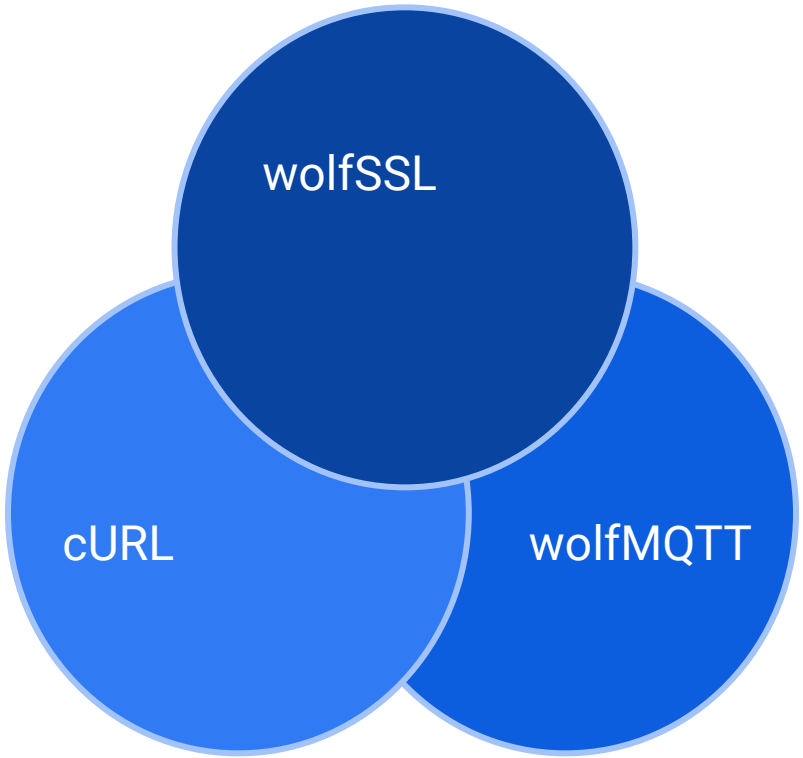
# TLS 1.3 to Connect Car to the Backend

# Use Case

- Heavily Used MQTT, LibcURL
    - Used cURL for HTTP Proxy
- Complex Network Topologies to Communicate with the Backend

# wolfSSL Products

- wolfSSL
- wolfMQTT
- cURL



# Specific Engineering Detail

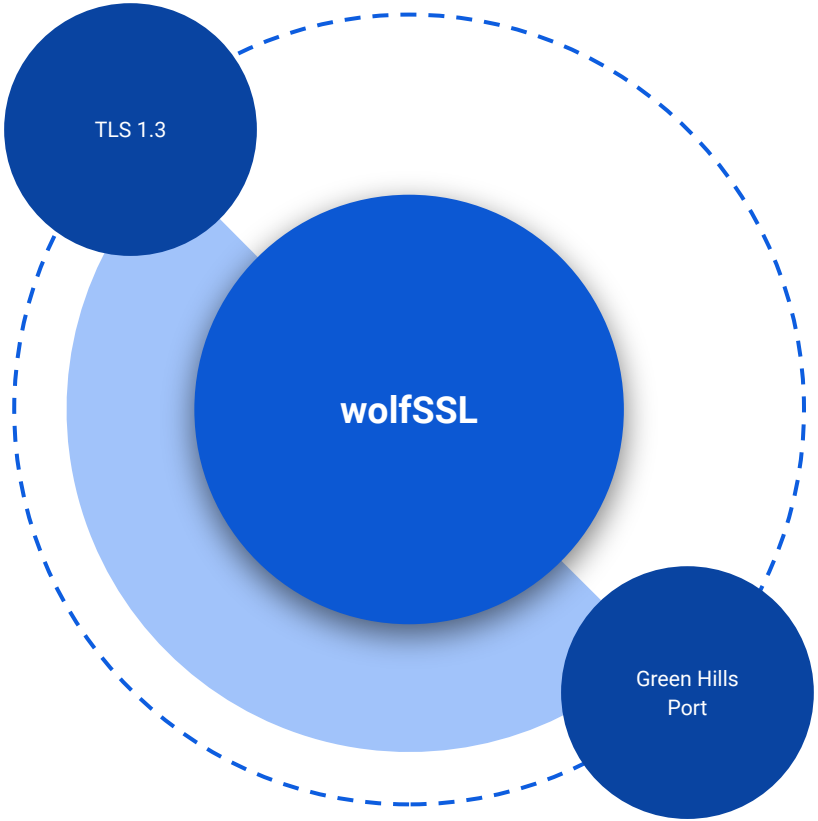
- Made use of MQTT v5
- Resolved issues due to multi threaded use cases with wolfMQTT and minor behavior fixes with wolfMQTT
- Support with integration and setup

# ADAS/autonomous driving

# Use Case

- Use for connection to map
- Updates navigation
- Aids a system used for an enhanced version of cruise control

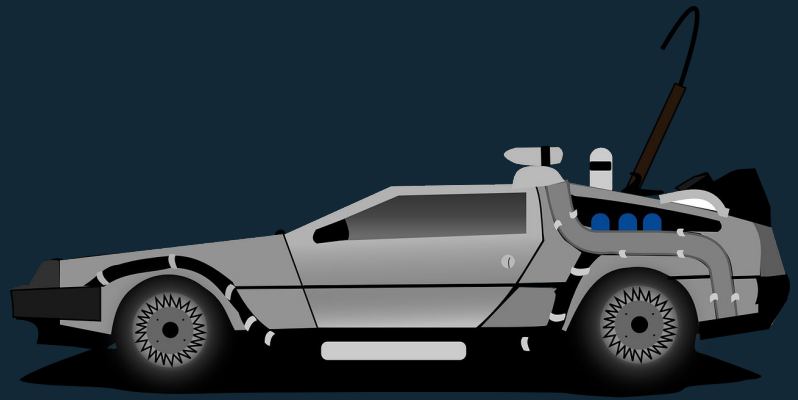
# wolfSSL Products



# Specific Engineering Detail

- Porting to an ST Telemaco board with a7 core
- Made use of hardware crypto
- Some misra c work was done on specific files

# NTP (network time protocol) for Autosar



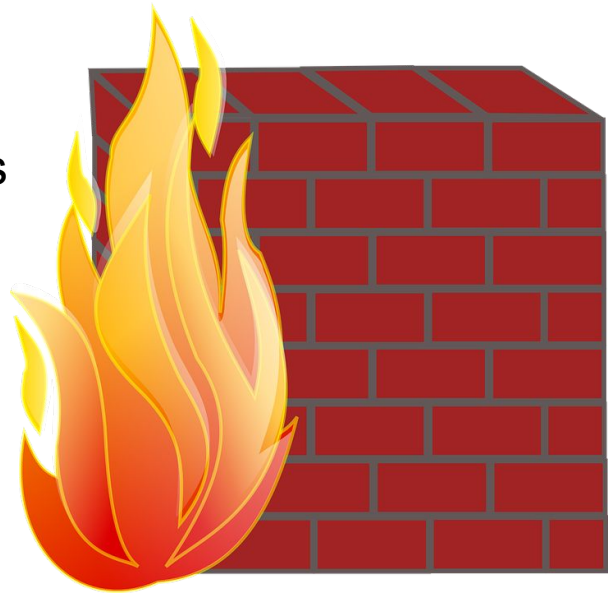
# Timestamping Events for smart cars

- Ecosystem Time Sync
  - Example:  Brakes have the same time reference as machine vision systems!
  - Maintaining Constant sub millisec time in the vehicle
  - Cryptographically Secure Reference Time
- Critical but Simple Facility
- Why do we need NTP on a Car?
  - Sync of Subsystems in Smart Car Apps
  - Forensic Reconstruction of Events

# How wolfSentry Fits Into Automotive

# wolfSentry:  Identify and Mitigate network intrusions

- wolfSentry
  - Firewall: Filtering Bus Traffic
  - IDS: Monitoring Bus Traffic to notify on Anomaly Detection
  - IDPS: Dynamically Respond to Block Bus Spam
  - Driver and manufacturer alerts through callbacks



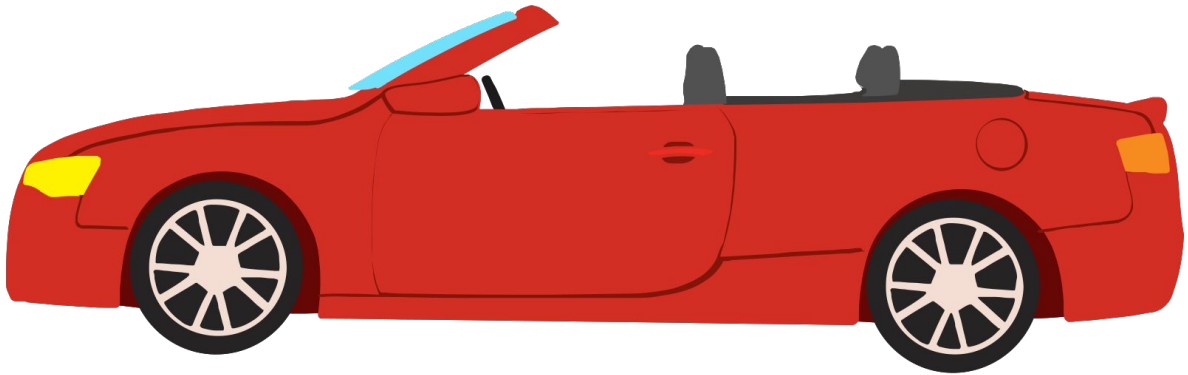
# ISO 21434

- wolfSentry IDS
  - Designed for embedded devices
  - Dynamic rule generation, Transactional rule changes on-the-fly
  - Record and / or react to events
- wolfSSL
  - Secure transmission of event data
  - Secure general communications between microcontrollers / servers
- wolfBoot
  - Secure firmware updates

# New: TLS Over CAN

# TLS over CAN

- CAN (controller area network)
- Authenticate, Encrypt, Integrity
- Use top industry standard for intra-car security



# TLS over CAN - How to Implement in Practice

- wolfSSL ISO-TP wrapper with variable minimum packet delay
  - Allows the bus to be available for other packets
  - Eliminates the 8byte CAN max packet size
  - Adaptable for CAN FD
- TLS 1.3 for reduced round-trip handshakes
- Simple callback interface
  - Platform agnostic CAN bus wrapper

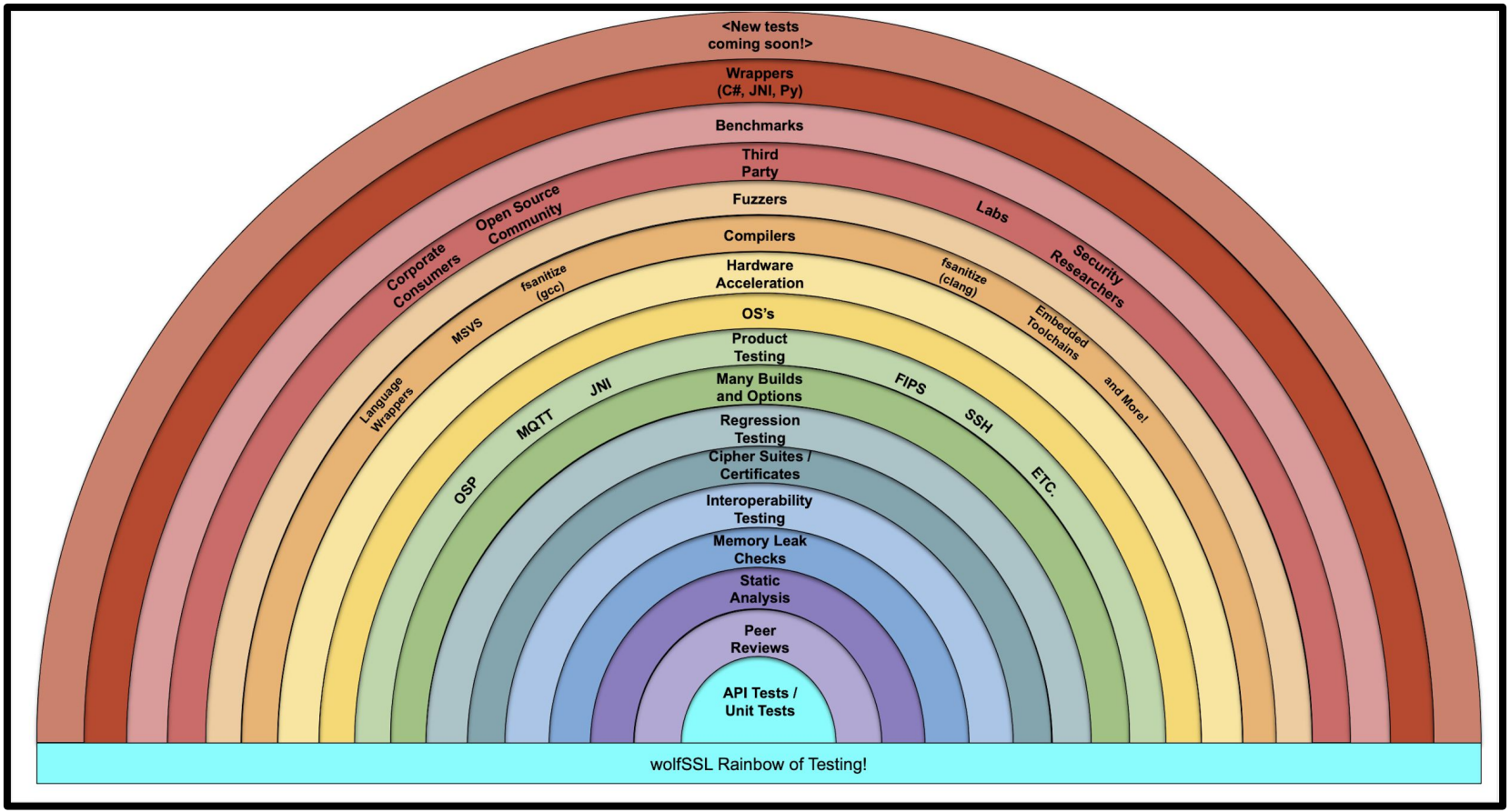
# Testing

# Testing In Order To Avoid Crashes

# Testing and Code Quality

- Benchmark tests on real HW, multiple boards
  - Keeps track of code size vs Boot time
  - Measure memory resources
  - Manually run additional resource collection to update usage figures
- Functional tests running on real STM32F407 target in Amsterdam
  - Covers forward update, rollback
  - SPI flash tests
  - TPM test (using the Infineon TPM module)
  - Testing with combinations of possible DSA+SHA algorithms

# Rainbow of Testing




**Thanks!**
Questions?

**facts@wolfssl.com**

www.wolfssl.com
www.github.com/wolfssl

Bozeman, MT : Seattle, WA : Portland, OR : Rescue, CA : Tokyo, JP : Brisbane, AU : Mobile, AL : Stockholm, SE