POLYTECHNIQUE MONTRÉAL

WORLD-CLASS ENGINEERING

# Analyzing TLS Use on IoT Devices

Corentin Thomasset , David Barrera
École Polytechnique de Montréal, Montréal, QC, Canada

IoT TLS ANALYZER

## Introduction

### Why TLS?

- TLS is a widely deployed protocol used to secure online communications.
- The protocol itself is actively maintained, and its robustness and security are improved upon regularly.
- TLS is a complex protocol that can be painful to correctly configure and maintain for non-experts [1].

**Potential configuration flaws with critical impact on user security and privacy.**

### Why IoT Devices?

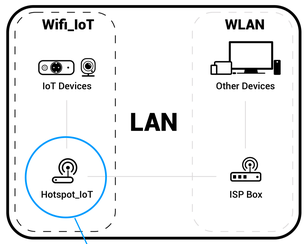
- IoT devices are known to be poorly secured [2].
- IoT devices have been targeted by hackers for large scale attacks.
- Similar analyses lead on Android apps highlighted several misconfigurations on implementations where TLS is used for API calls [3].

**IoT devices could present misconfigurations in their TLS implementations.**

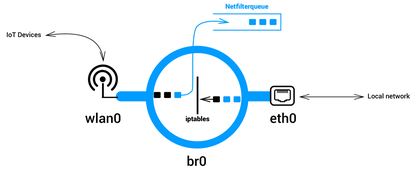
## Methodology

### Network integration

Our solution integrates directly into SOHO networks without interfering with other devices by providing a dedicated Wi-Fi hotspot for IoT devices.




**Packet capture**

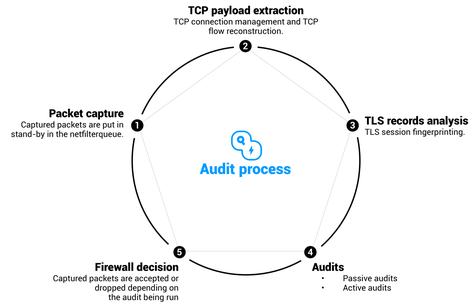


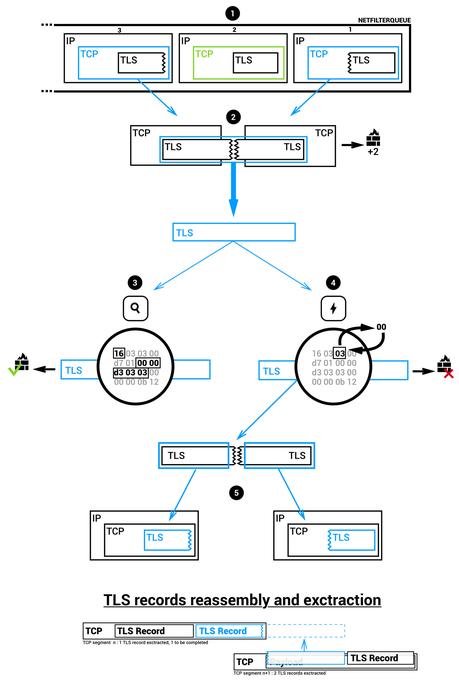

### Packet flow

Packets are intercepted using iptables and netfilterqueue (1). TCP streams are reassembled (2) and the TLS payload is extracted and processed by our analyzer. Contrary to passive audits (3), active audits need to modify packets (4). The modified TLS payload is split between the new packets and original ones are dropped by the firewall to prevent duplicates (5).

### Audit process

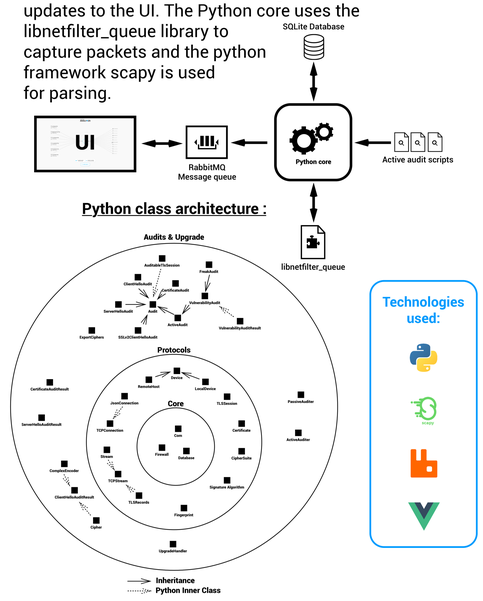
Passive audits are run on TLS handshake records and report potentials issues by analyzing negotiated parameters. Active audits modify fields in TLS records to test the client / server reaction to detect vulnerabilities.




## Soft. Architecture

The python core captures packets and runs analyses. The web UI is designed for the user to easily follow analysis status and reports. The UI and Python Core interface use RabbitMQ Message queue for real time updates to the UI. The Python core uses the libnetfilter_queue library to capture packets and the python framework scapy is used for parsing.




**Technologies used:**

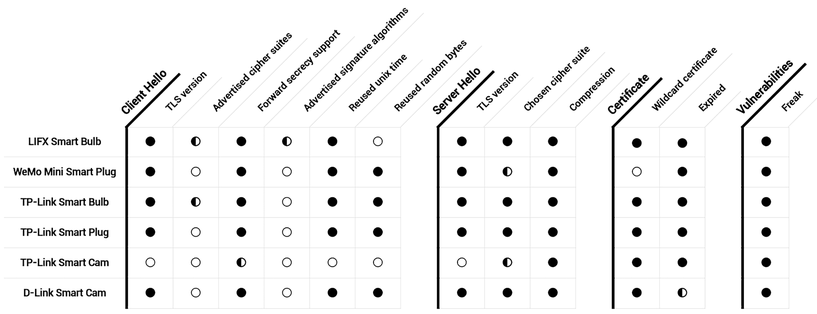
## Objectives

**Develop a methodology to automate TLS analysis on home IoT devices to identify vulnerable implementations.**

### Analysis features :

- **Threat detector:** Identify devices vulnerable to known TLS flaws and presenting misconfigurations.
- **Black box tests:** No modifications on devices are needed.
- **Active audits:** Analyzer can intercept / block / modify packets.
- **Fully automated:** Analyses are run without needing any user intervention.
- **Low profile analysis:** Could be deployed in a home environment to monitor IoT devices without interfering in a noticeable way with their behavior.

## Conclusion




**All tested devices fail to adhere to best security practices**

**Should IoT devices follow the same TLS recommendations as web servers / clients ?**

**Our analysis has shown that:**

- Most of tested IoT devices conforms to minimum security requirements but are unnecessarily vulnerable. Fixes require manufacturers to issue firmware updates.
- All devices advertise a large set of cipher suites when no backwards compatibility is needed (few API endpoints controlled by the manufacturer). For IoT devices, supporting old cipher suites extends the attack surface.

**Why this is problematic:**

- Negotiation and support of weak cipher suites can lead to attacks where a MITM attacker is able to decrypt the connection. This is problematic for devices that can leak sensible information about habits & presence.
- IoT devices are known to be hard to keep up to date. Conforming to minimum security today means vulnerable in near future.

**Future work & improvements:**

- We aim to develop a complete solution to protect vulnerable home IoT devices [4]. This TLS analysis module is part of a larger project for IoT traffic monitoring.
- Improve stability and develop more active audit scripts.

## References

[1] Jeremy Clark and Paul C. van Oorschot. SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements. IEEE S&P 2013

[2] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, Blase Ur. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). USENIX Security 2018.

[3] A. Razaghpanah, A.A. Niaki, N. Vallina-Rodriguez, S. Sundaresan, J. Amann, P. Gill - Studying TLS Usage in Android Apps. ACM CoNEXT 2017

[4] D. Barrera, I. Molloy, H. Huang - IDIoT : Securing the Internet of Things like it's 1994. Technical Report arXiv: 1712.03623