

The Center for Cyber Defenders

Expanding computer security knowledge



DUF

Digitally Unclonable Function

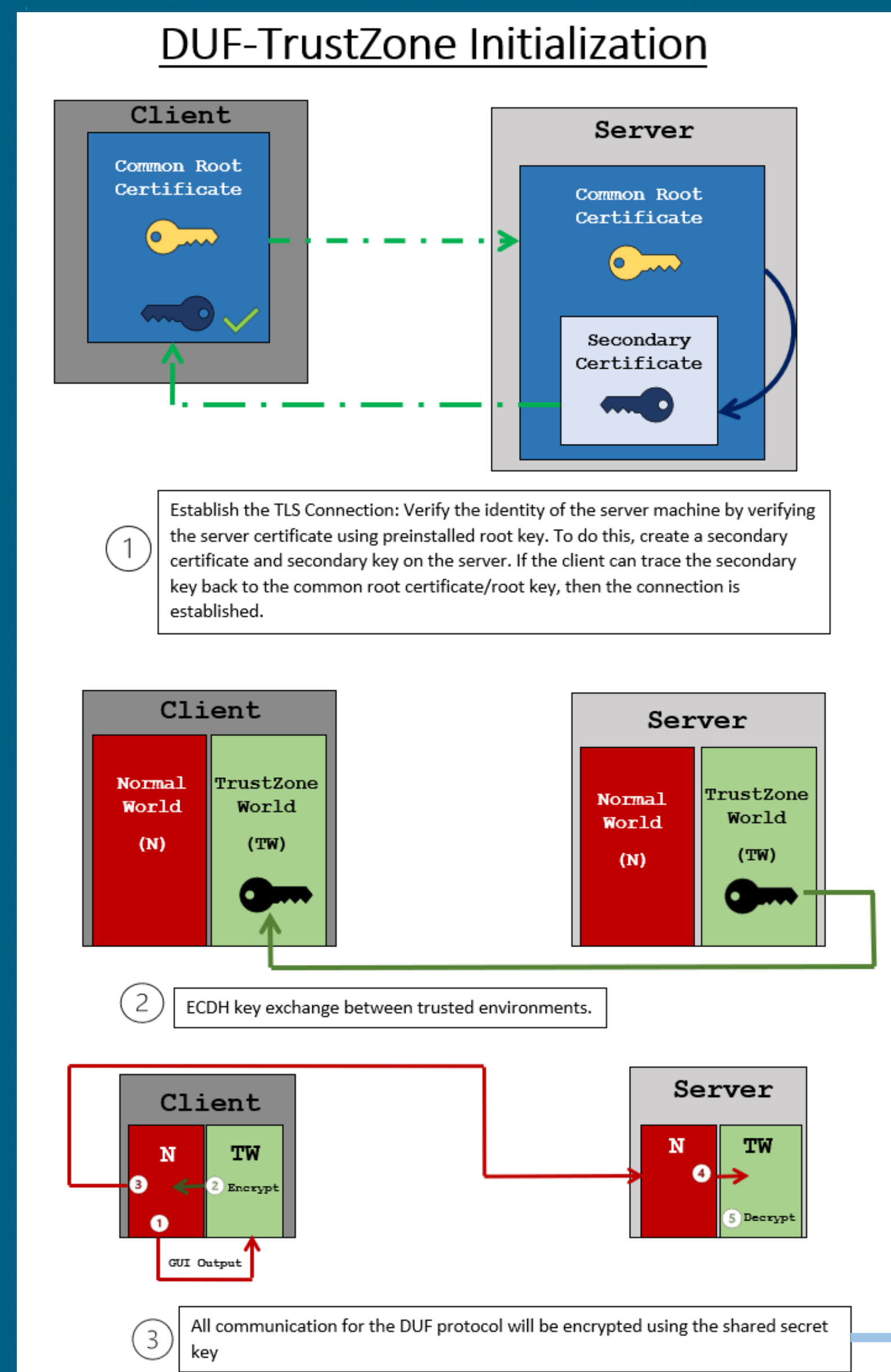
Hannah Ballard and Friedrich Doku

Mentor: Adrian Chavez

Problem Statement

- IoT is a rapidly growing infrastructure with a projection of 27 billion connected IoT devices in 2025. As these devices are making their way into our cars, homes, and work places the number of security concerns increase and as such, it's important that we protect IoT devices from attackers. One major area of concern is Over-the-air (OTA) updates. With billions of IoT devices a non-secure OTA update can leave many devices compromised, even without the user's knowledge.
- To secure OTA updates we introduce the DUF protocol. The DUF protocol is built on top of ARM TrustZone which can be used to securely verify software packages and secure transfers between servers and IoT devices.

Approach

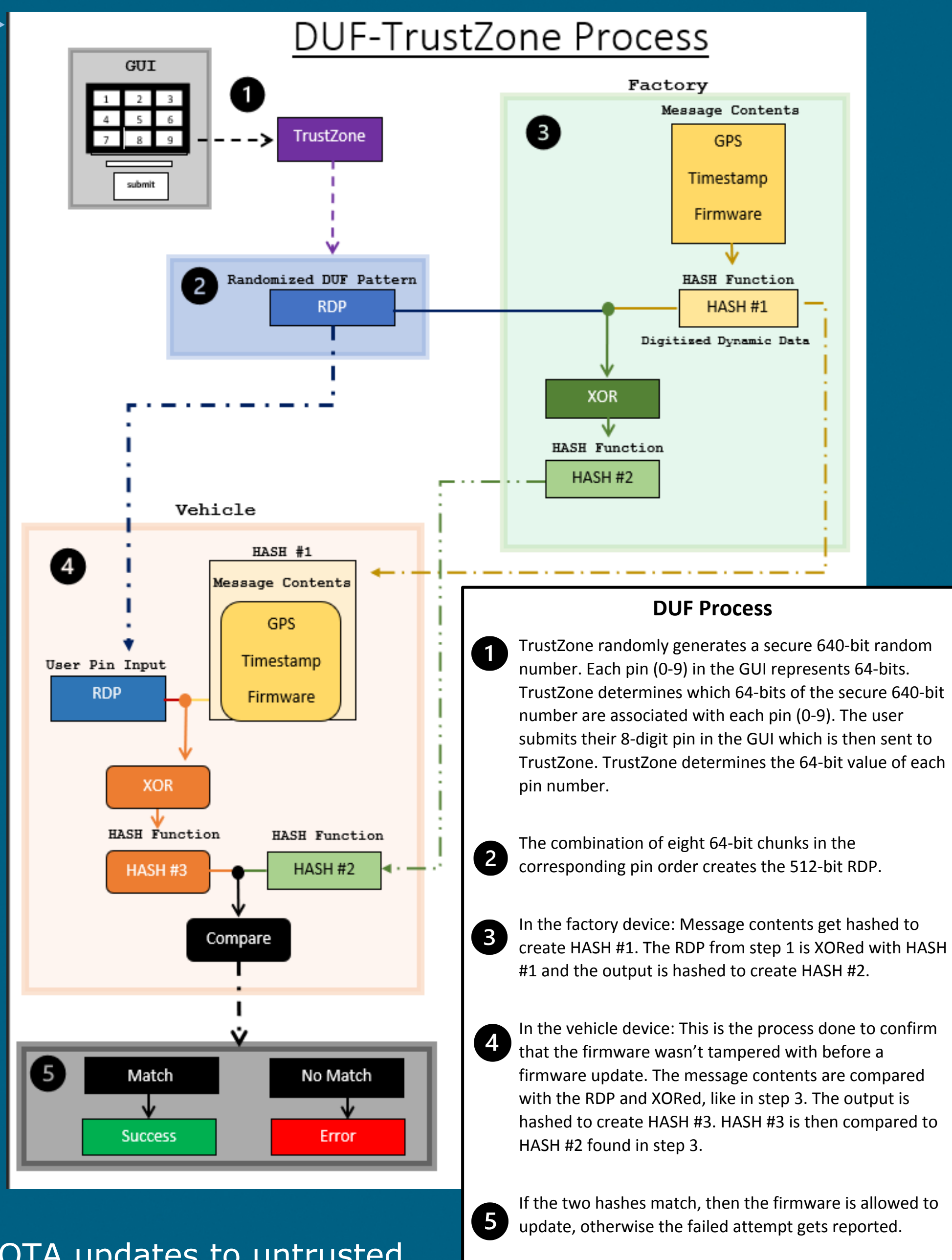


Results

- Completed:
The DUF protocol implemented with TrustZone is running successfully on QEMU
- In Progress:
Working toward implementing a GUI to allow the user to create their own RDP
- Next Steps:
Get the QEMU implementation and the GUI working in hardware



(Potential Hardware: Rock Pi 4 Plus Model B Rockchip RK3399(OP1))



Benefits

- We propose a novel architecture that allows secure OTA updates to untrusted IoT devices.
- This architecture prevents potentially malicious unsecure applications already running on the IoT device from altering the software package.