Implementation of various cryptographic algorithms for the purpose of use in passive RFID systems

Team Lead: Dr. Dhiman Saha, Prof. Brejesh Lall

Team Member: Dr. Pabitra Pal, Ahaan Dabholkar, Satanu Maity and Manas Wadhwa

Introduction:

With the advent of 5G networks capable of handling huge bandwidths and massive amounts of data transferred over the air, it is expected that a large number of IoT devices would join the already dense mesh of interconnected devices. These devices would be very constrained in their computational capabilities and power consumption rates and their primary role would be to transmit collected data to an authorized endpoint. As such the security requirements of such devices are very different from the ones required by generic computing systems and would need to be tailored to fit their limited abilities.

Problem Statement

Have a PoC ready to go with standard lightweight protocol support and deploy a use case.

Software and Hardware Requirement

- Board – Rpi
- Communication–XMPP
- Authentication – PRESENT (as per ISO/IEC 29192) & PKI Primitive
- Implementation – Edge/Gateway/Server

Problem details:

Here we propose an initial prototype of an authentication library built into the networking stack of an IoT device (in this case an ESP32). While the traditional protocol, for communication, has always been HTTP, we aim to mitigate the parsing and header size overheads of this protocol by instead using the much lighter and faster XMPP pub–sub protocol. For the security layer built on top of this stack, traditional RSA–AES would be too considered too “heavy” in terms of computational and memory requirements. We propose replacing it with a lightweight alternative such as RSA–PRESENT which would lead to a smaller codebase and a less memory–intensive mode of operation while providing reasonable guarantees of security. For devices (comms modules) with highly constrained downlink speeds, this would lead to smaller size communications and hence higher throughput.

Why people choose our protocol

- Lighter and faster protocol for communication with a huge number of IoT devices.
- Light–weight in terms of computational and memory requirements:
- Easy installation of the library in the communication module:

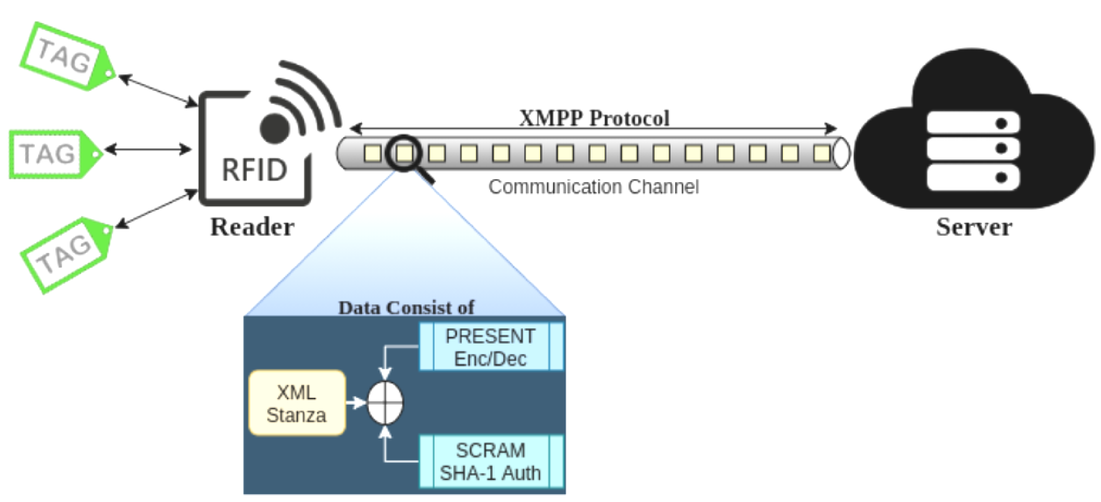
Deliverables:

- An authentication library built into the networking stack of an IoT device (in our case an RPi).
- Detailed report on the benchmarking results of the library in comparison to a vanilla HTTP server using RSA–AES authentication when a bunch of active clients are connected to the server and subscribed to a particular service.

Use Case:

A prototype for the client–server authentication using the authentication library.

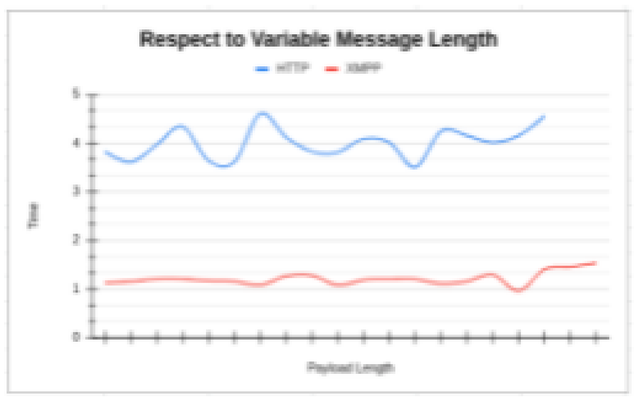
Basic Block Diagram



Client Server Communication

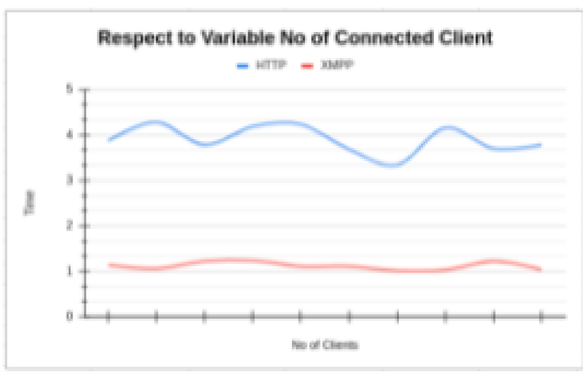
Benchmarking results when compared against a vanilla HTTP server

Experimental Results: Server runs on own machine using docker and client run on different machine but in the same network (LAN: both machines connected in same mobile hotspot).



Round Fixed to 1000

Payload Length Fixed to 100



Round Fixed to 1000, and
Payload Length Fixed to 100