Embedded Cryptography: Syllabus

January 16, 2020 / 4:00 PM - 5:00PM EST

Important Links

Workshop Hackpack

Pre-workshop checklist, and resources to explore during and after the workshop.

Hack the North 2020++ Event Schedule

Check this out to stay up-to-date on activities, workshops, and other key happenings this weekend.

Motivator

When designing a system that is going to intermittently communicate with a server there is a need for a way to authenticate the client device connection requests. While there are existing authentication systems such as TLS/SSL these systems are designed for devices that are more resource rich when compared to existing embedded architectures.

This workshop aims to introduce participants to the use of cryptography in authentication and will go over a basic authentication framework which allows for extension to suit the needs of other projects.

Prerequisite Knowledge

In order to get the most out of this workshop you should be comfortable with the following concepts:

- C programming language
- Memory allocation (static vs dynamic)
- Function callbacks

Learning Outcomes

This is what you will walk away from the workshop able to do:

- Understand the fundamentals of implementing a token based authentication system to securely connect with a server
- Good embedded software design practices
- Understand that implementing your own crypto is a terrible idea outside of academic experimentation

Timeline (1 hour)

Time	Module	Description
10 min.	Fundamentals of authentication	Describe the requirements for something to be authenticatable Non repudiation Difficulty of forging
5 min.	Fundamentals of cryptography	Asymmetric and symmetric ciphers Digital signatures
5 min.	Break	
5 min.	Introduction to arduino crypto library and networking library	Main functions
20 min.	Implementing the components	Overview of code structure, mainly focus on the addition of the cryptographic functions and what each step does
5 min.	Q&A	
5 min.	Closing Remarks	