SocIoTy: Practical Cryptography in Smart Home Contexts

Paper Review By: Rishi Raj Gautam

18th November, 2024

Abstract

Summary

1 Introduction

what is Socioty
what is Context-Security Cryptography

2 Background And Motivation

- expensive?
- Security of HMAC / 2FA
- At-Home cryptography and its design
- PRF

2.1 Use Cases and examples

- Vpn (auth)
- Health machine data (config and auth)
- Journalists data (enc)

2.2 Security Assumptions

Description Examples

- Scenario 1
- Scenario 2

3 SOCIOTY

Description based on At-Home Cryptogrpahic Solution

3.1 Components

- Authorized device
- Remote Service
- Storage For Encryption
- IOT devices

3.2 Operations

- Authentication
- Encryption

3.3 Deployment

- Devices to use
- Network Structure
- Execution of TDRF
  - Runtime evaluation for different IOT devices
  - Implementation Tools
    - Rust
    - ECC Curve25519
    - Devices
    - Microbenchmark
    - End-to-End Deployment
    - Observation
    - Obstruction For Commercial Deployment

4 Related Work

Comparision Table

5 Conclusion

We present SocIoTy, an at-home cryptography system designed with non-technical users in mind.