A SECURED CERTIFICATE RENEWAL SCHEME FOR CONSTRAINED IoT DEVICES

Department of Computer Science and Engineering
PES University, RR Campus, Bengaluru – 560085.

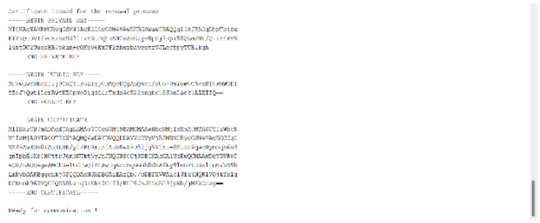
Problem Statement

The secure certificate renewal scheme for constrained IoT devices. This project aims to secure Class 2 constrained devices by establishing a Key Distribution Centre that distributes secure keys to the network's IoT devices for safe and secure communication.

We also design a new certificate-based security scheme where we identify, authenticate, and provide security to the constrained IoT devices in the network by providing secure keys along with the certificate for encryption and decryption of data for communication. We also renew and revoke the certificates when required. We also identify the most efficient lightweight encryption algorithms suitable for constrained devices and implement them in our project.

Result and Discussion

- Registration of a node for the secure certificate



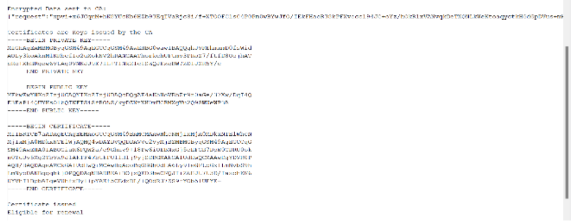
```
Certificate issued for the renewal process
-----BEGIN PRIVATE KEY-----
[illegible]
[illegible]
[illegible]
-----END PRIVATE KEY-----

-----BEGIN PUBLIC KEY-----
[illegible]
[illegible]
-----END PUBLIC KEY-----

-----BEGIN CERTIFICATE-----
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
-----END CERTIFICATE-----

Ready for communication !
```

- Renewed certificate



```
Encrypted Data sent to CA:
{"request":"[illegible]

Certificates and Keys issued by the CA
-----BEGIN PRIVATE KEY-----
[illegible]
[illegible]
[illegible]
-----END PRIVATE KEY-----

-----BEGIN PUBLIC KEY-----
[illegible]
[illegible]
-----END PUBLIC KEY-----

-----BEGIN CERTIFICATE-----
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
-----END CERTIFICATE-----

Certificate issued
Eligible for renewal
```

Dataset and Features / Project Requirement / Project Features

[1] IoT device authentication
[2] Establishing connection between node and Certificate Authority
[3] Certificate Creation
[4] Certificate Issue
[5] Certificate renewal
[6] Certificate Revocation
[7] Sending Data

Design Approach/Method

Waterfall Model: The waterfall model is a classical model used in system development life cycle to create a system with a linear and sequential approach.

- The reason for choosing this model is that our problem statement is stable, well understood and the requirements are very well documented, clear and fixed.
- Each phase must be completed before the next phase can begin and there is no overlapping in the phases.

Background

IoT networks are deployed with many devices and can be used for various operations. These devices produce, collect and process huge amounts of data.

In today's world as more and more IoT devices are used, the transfer of data across the internet is vast and these devices are operated in an uncontrolled and hostile environment. Therefore, securing these devices should be a key feature of an IoT network and should be considered critical.

Most of the IoT devices are battery powered and have limited computational power, low memory processing cycles and low bandwidth. So, the risk of a hacker stealing personal information and hacking the device is very high.

The key security and privacy challenges in IoT devices are authentication, identification, and device heterogeneity. Integration, scalability, ethics communication mechanisms, commercial strategies, and surveillance are all major concerns.

Summary of Project Outcome

The secure certificate renewal scheme for constrained IoT devices mainly contains the following four main phases:

1. Registration of nodes or devices
2. Generating the certificate
3. Renewing the certificate
4. Revoking the certificate

`

Conclusion and Framework

This methodology proposes a unique certificate renewal scheme for constrained devices in IoT network by generating x509 certificate which uses EC secp256r1 algorithm to generate the keys.

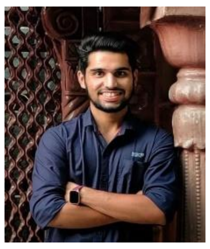
The certificate is signed with SHA256 algorithm to protect it from various attacks. The IoT nodes are ready for communication only when the certificate is valid and issued by the CA.

References

[1] Rehman, A., Rehman, S.U., Khan, I.U., Moiz, M., & Hasan, S. (2016). Security and Privacy Issues in IoT. *Int. J. Commun. Networks Inf. Secur., 8.*

[2] Albarqi, Aysha & Alzaid, Ethar & Alghamdi, Fatimah & Asiri, Somaya & Kar, Jayaprakash. (2015). Public Key Infrastructure: A Survey. Journal of Information Security. 06. 31-37. 10.4236/jis.2015.61004.

[3] Gu, Hongxiang & Potkonjak, Miodrag. (2018). Efficient and Secure Group Key Management in IoT using Multistage Interconnected PUF. 10.1/3218603.3218646

Member1:	Member2:	Member3:	Member4:	Guide:
				
Manideep PR PES1UG19CS258	Nithesh A PES1UG19CS306	Nagesh BS PES1UG20CS816	Navya C PES1UG20CS818	Mr. Vadiraja A Associate Professor, PESU