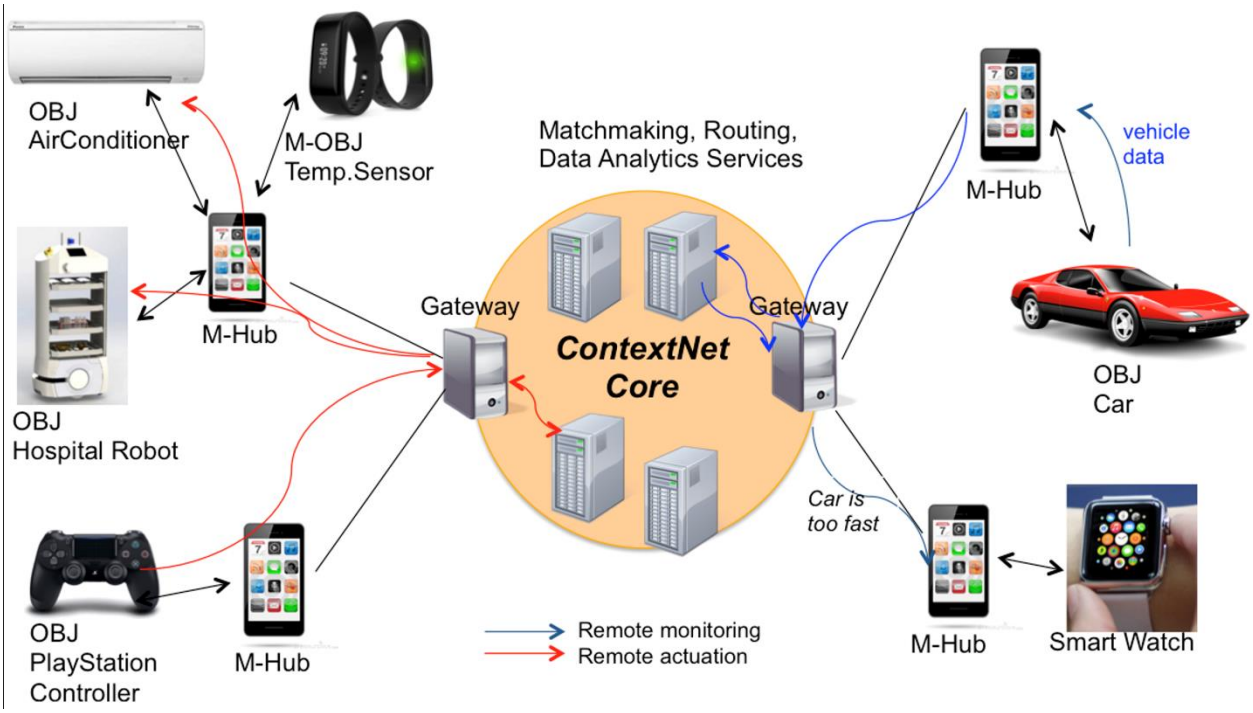
Framework EdgeSec - Especificação

Projeto Final de Programação – Gabriel Cantergiani

Contexto e motivação

Este projeto consiste no desenvolvimento de um framework de comunicação segura para ser utilizado em sistemas IoT heterogêneos e móveis. Apesar este trabalho se basear fortemente em um outro projeto de pesquisa que traz o conceito de um framework de segurança genérico e flexível aplicável em diversos sistemas IoT, o foco do desenvolvimento será no contexto dos middlewares de IoT ContextNet e Mobile Hub. Estes middlewares são constituídos pelos seguintes componentes: nós de processamento em nuvem (ContextNetCore), dispositivos móveis atuando como gateways (Mobile Hub), e dispositivos/sensores IoT captando e gerando dados em tempo real (Smart Objects). A imagem a seguir ilustra a arquitetura e os principais componentes do ContextNet.



A arquitetura de segurança EdgeSec foi proposta como uma solução para trazer mecanismos de autenticação, autorização e sigilo nas trocas de dados dentro dos middlewares mencionados. Após a sua elaboração teórica, e posteriormente, sua implementação e utilização prática, a arquitetura EdgeSec se mostrou uma solução viável, apesar de algumas necessidades de melhorias. Dentre os pontos fracos da implementação existente está o fato de os mecanismos de segurança serem fortemente acoplados a dispositivos e protocolos específicos, como a tecnologia BLE e os protocolos criptográficos MD5 e RC4. Apesar de funcionar para os dispositivos testados, um smartphone Android e um microcontrolador ESP32, esta solução não é compatível com outros tipos de dispositivos que podem vir a se conectar com o sistema ContextNet, ou com outro sistema IoT no qual o EdgeSec esteja sendo utilizado. Para isso, seria necessário reestruturar e refazer grande parte da implementação já realizada.

Esta dificuldade foi a principal motivação para o desenvolvimento de um framework genérico, que seja capaz de integrar diferentes implementações e possibilitar o uso dos mecanismos de segurança do EdgeSec em diversos dispositivos IoT, protocolos e tecnologias.

Finalidade

O framework tem a finalidade de ser usado por desenvolvedores e fabricantes de dispositivos IoT que queiram integrar diferentes tipos de dispositivos em uma mesma arquitetura, sem precisar se preocupar com questões de compatibilidade entre protocolos. O framework pretende fornecer interface genéricas de comunicação segura dentro de uma arquitetura IoT, e atuar como intermediador de todas as trocas de dados entre processadores na nuvem e dispositivos inteligentes nas pontas. Isso possibilitará o acoplamento de qualquer novo dispositivo a partir da criação de plugins que implementem as operações especificadas pelas interfaces. Como já foi mencionado, o framework será inicialmente desenvolvido com foco na arquitetura dos middlewares de IoT ContextNet e Mobile Hub, permitindo que eles sejam utilizados como um sistema de comunicação segura unificado para dispositivos IoT variados.

Escopo

Este projeto representa uma evolução da arquitetura EdgeSec, e pretende se utilizar do que já foi desenvolvido anteriormente, adaptando e transformando a implementação. Além

disso, o desenvolvimento completo deste framework, e de forma mais flexível e não acoplada ao ContextNet, é um objetivo para a tese de Mestrado, e por tanto, nem todas as funcionalidades estarão inclusas no projeto desta disciplina. A seguir são listadas as características que **fazem parte do escopo deste projeto**:

- Elaboração de interfaces genéricas que define os métodos e atributos necessários de serem implementados por plugins para que novos dispositivos/protocolos possam ser utilizados e integrados na troca de dados segura do EdgeSec.

- Adaptação da lógica básica de autenticação do Mobile Hub para classes e métodos genéricos. Isto inclui a criação de novas classes e métodos que são agnósticos de protocolo e tecnologia, executando os passos básicos para autenticar um dispositivo e trocar dados de forma criptografada entre diferentes dispositivos.

- Adaptação dos módulos implementados no item anterior, transformando-os em um pacote/biblioteca que possa ser importado e incorporado no código do Mobile Hub e no código de dispositivos IoT. Esta adaptação irá constituir o núcleo (core) do framework.

- Implementação de plugins utilizando os protocolos já existentes na implementação atual do EdgeSec (BLE, HMAC-MD5 e RC4). Estes plugins servirão como prova de conceito, comprovando o funcionamento correto do framework e a integração adequada de plugins externos. Eles irão se utilizar das lógicas já existentes, porém as isolando de forma a serem específicas para os protocolos e dispositivos em questão.

Além disso, é importante mencionar o que está nos planos futuros de implementação deste framework, mas **não está no escopo deste projeto**:

- Implementação do mecanismo de handshake para negociação de protocolos durante o processo de conexão e autenticação. Este handshake é uma maneira de “combinar” dinamicamente qual será o plugin a ser utilizado quando um novo dispositivo IoT se conecta com o Mobile Hub. Porém, a implementação deste handshake dinâmico é

complexa, e será abordada posteriormente como um complemento ao desenvolvimento inicial. Para este projeto, o handshake será usado somente para troca de IDs, e a decisão de qual protocolo utilizar caberá ao ContextNetCore.

- Implementação de outros plugins que suportem outros tipos de protocolos como forma de testar a utilização do framework na comunicação entre dispositivos que utilizem protocolos distintos.
- Execução do framework em um teste real utilizando o Mobile Hub e um Smart Object como o ESP32. Isso não será possível pois seria necessário alterar a implementação existente no Smart Object para se adequar aos novos mecanismos e interfaces do framework. Este é um objetivo futuro do projeto, mas não seria viável dentro do prazo da disciplina.

Requisitos

Os usuários do framework podem ser desenvolvedores de sistemas IoT que desejem utilizar um mecanismo de segurança para troca de dados, ou fabricantes de dispositivos IoT que desejam que o seu dispositivo se adeque à uma troca de dados segura, permitindo-o ser utilizado de forma mais ampla.

Portanto, os requisitos não são voltados para um usuário leigo do sistema e com a descrição de comportamentos do ponto de vista da interface de usuário. São requisitos mais técnicos diretamente ligados ao fluxo de desenvolvimento de alguém que queira utilizar o framework para trazer mais segurança à algum sistema no qual se está trabalhando.

Requisitos Funcionais

A seguir são listados e detalhados os requisitos funcionais do projeto:

- No Mobile Hub, um usuário deve ser capaz de importar o framework como uma dependência do projeto.
- No Mobile Hub, um usuário deve ser capaz de importar plugins como dependências do projeto.

- Um usuário deve conseguir importar tanto o framework como os plugins de forma separada e independente. Ele deve ser capaz de fornecer plugins compatíveis no momento de configurar o framework.
- Para a correta inicialização do framework, o usuário deve configurar pelo menos três tipos diferentes de plugins: um para a tecnologia de transporte (ex: BLE), um para o protocolo de autenticação (ex: HMAC MD5) e outro para o protocolo de criptografia de dados (ex: RC4).
- O framework deve definir 3 interfaces de plugins diferentes, uma para cada tipo de plugin necessário para a correta configuração. Além disso, deve fornecer uma quarta interface que define os métodos disponibilizados pelo framework para escanear dispositivos, se conectar e trocar dados de forma segura.
- Ao utilizar o framework, o usuário deve ser capaz de trocar dados de forma criptografada entre o Mobile Hub e algum dispositivo IoT que tenha suporte aos protocolos dos plugins escolhidos.
- Os mecanismos de segurança utilizados devem ser transparentes para o usuário que está utilizando o framework.
- Um fabricante deve ter disponível as interfaces com as definições de quais métodos devem ser implementados por cada plugin para que este seja compatível com o framework.
- Ao desenvolver um plugin, um fabricante deve conseguir testar a correta integração do mesmo com o framework.

Requisitos Não Funcionais

A seguir são listados e detalhados os requisitos não funcionais do projeto:

- O framework deverá utilizar o mecanismo especificado no protocolo EdgeSec para calcular e gerar os dados e chaves referentes a cada processo de autenticação, como o OTP (*One-Time Password)* e o pacote de autenticação. Nas partes específicas de protocolo, deverá invocar métodos dos plugins configurados.
- Os plugins utilizados com prova de conceito devem utilizar os protocolos já estabelecidos na implementação existente do EdgeSec, como BLE, HMAC MD5 e RC4.

- As funcionalidades do ContextNetCore, como o processo de autorização, devem ser simuladas dentro um módulo separado e isolado, fornecendo uma interface para integração com o framework.
- O ContextNetCore deve armazenar em variáveis os dados referentes a cada dispositivo registrado, como os gateways autorizados e os protocolos suportados.