Projeto de Formatura – Turmas 2017

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia Elétrica – Ênfase Computação

Tema:

Sistema de IoT com Segurança

MOTIVAÇÃO

Observamos uma tendência cada vez maior de transformar objetos e ferramentas do cotidiano em dispositivos inteligentes, com conectividade à Internet. Isso possibilita uma amálgama de funcionalidades e facilidades nos mais diversos aparelhos domésticos. Entretanto a conexão sem fio traz riscos de segurança. Dispositivos inteligentes estão se difundindo para aplicações críticas, como o controle de sistemas a gás, temperatura e inclusive monitoramento e intervenção para pacientes. Com essa proliferação de dispositivos torna-se necessário garantir os maiores níveis de segurança para que esses projetos resultem em produtos que tragam conforto e minimizem riscos aos seus usuários.

PROJETO

O objetivo é propor uma arquitetura segura para o funcionamento de uma "Smart Home". A Arquitetura consiste de 3 entidades:

1) Dispositivos com conexão Wi-Fi.
2) Controlador central da residência.
3) Servidor Web para gestão das residências.

O sistema busca concentrar o processamento e fluxo dos dados no controlador central, o que além de tornar a arquitetura mais escalável, traz benefícios de segurança como resistência maior contra ataques e maior poder de detecção de intrusão.

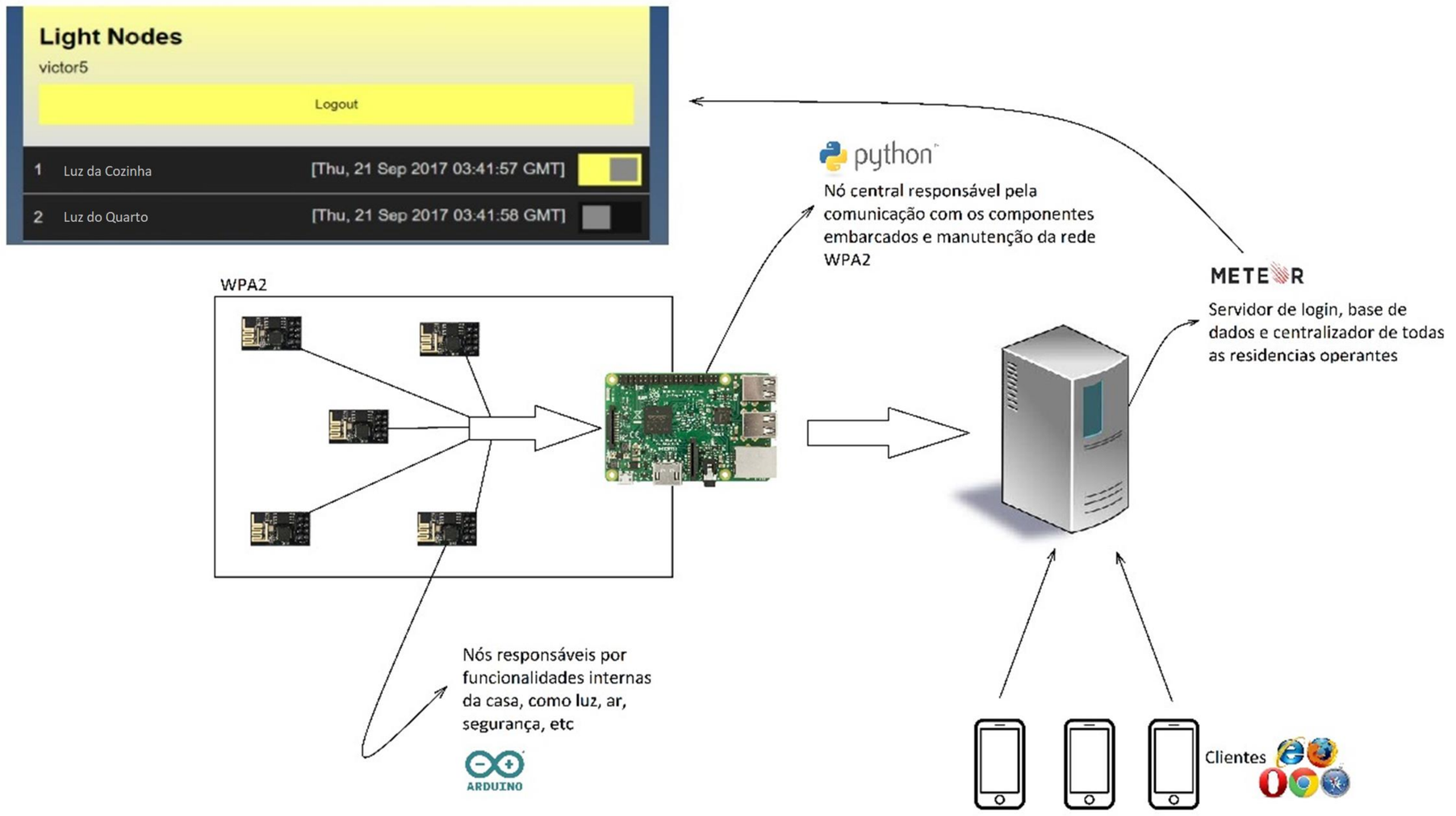
Segurança da Rede Local

O foco do projeto é na segurança dos dispositivos inteligentes da casa, que possuem limitações de processamento e memória.
A arquitetura de segurança local consiste de duas camadas principais de segurança: o isolamento dos nós de baixa capacidade de processamento de redes externas, por meio de uma rede WPA2 gerada internamente e sem acesso à internet, e em segunda instância a adoção de criptografia simétrica e outras tecnologias que visam assegurar a confidencialidade, integridade e autenticidade da mensagem.

Tecnologias	Objetivo
Identificador da mensagem	Prevenir ataques replay
AES-256-CBC	Garantir confidencialidade das mensagens
HMAC-SHA-256	Garantir Integridade e Autenticidade das mensagens
WPA2	Isolamento da rede local da Internet. Resistência contra Invasão da rede local.

CONCLUSÃO

Em vista dos ataques recentes a estruturas IoT e grande variedade de ameaças que descobrimos durante nossa pesquisa, assim como a aproximação da criptografia quântica à nossa realidade, a análise de uma estrutura mais robusta e segura é fundamental para a viabilidade de sistemas embarcados no controle de funções sensíveis e interconectadas no nosso cotidiano. A arquitetura desenvolvida é suportada por dispositivos com baixos recursos computacionais e os testes realizados cumprem com elevados requisitos de segurança, sendo resistente mesmo quando um atacante possui acesso à rede sem fio.



Integrantes: Diego Sulzbeck Villalobos - 8041904 (diego.villalobos@usp.br)
Victor Taddeo do Val – 8041797 (victor.val@usp.br)
Rafael Ehrich Pontes Ferreira – 8041223 (repferreira94@gmail.com)

Professor Orientador: Prof. Dr. Reginaldo Arakaki
Co-orientador: Marcelo Pita; Leandro Souza