Secure Smart Home: Aplicações IoT residenciais seguras utilizando o protocolo TLS

Ana C. S. Rosa, Arielli A. da Conceição, Francisco A. S. do Carmo, Guilherme P. Aquino e Evandro C. Vilas Boas

***Resumo*— Esse trabalho descreve o desenvolvimento de uma aplicação IoT (*Internet of Things*) residencial segura, utilizando o protocolo TLS (*Transport Layer Security*). O projeto integra um aplicativo móvel e módulos de *hardware* para o controle de ar-condicionado, iluminação interna e cortinas. Desenvolveu-se o aplicativo móvel para Android por meio da linguagem Java. Esse aplicativo permite que um usuário controle o ambiente por meio dos módulos de *hardware*. A comunicação entre aplicativo e *firmware* ocorre por intermédio de um *broker* com protocolo MQTT (*Message Queuing Telemetry Transport*). Para prover aspectos de segurança, implementou-se o protocolo TLS, assim como autenticação por usuário e senha.**

Palavras-Chave*— *IoT, segurança cibernética, protocolo TLS.

***Abstract*— This work describes a secure residential IoT (Internet of Things) application development using the transport layer security (TLS) protocol. The project integrates a mobile application and hardware modules, which allows for the control of air conditioning, internal lighting, and curtains. The Android mobile application controls the environment in which the hardware modules are located. Application and firmware communicate through a broker entity using the MQTT protocol (Message Queuing Telemetry Transport). Security aspects were provided by adding TLS protocol and authentication.**

Keywords — Cyber Security, IoT, TLS protocol.

I. INTRODUÇÃO

Internet das Coisas (*Internet of Things*, IoT) se refere à interconexão digital de dispositivos eletrônicos por meio da Internet [1, 2]. Acessam-se e controlam-se remotamente as funções de um dispositivo, provendo o sensoriamento de aspectos naturais e humanos e/ou atuação. Em um ambiente residencial, a IoT provê a conexão à Internet de diversos aparelhos eletrônicos e o controle remoto por meio de *smartphones*, definindo as *Smart Houses*. Expande-se esse conceito para ambientes corporativos (*Smart Offices*), colaborativos e educacionais (*Smart Labs*). A conexão com a Internet torna esses ambientes propícios a ataques que exploram vulnerabilidades de rede (ou comunicação) [3]. Relacionam-se esses ataques ao acesso indevido, à violação de privacidade e à indisponibilidade do sistema. Portanto, deve-se implementar a comunicação segura fim-a-fim. Dentre as possíveis abordagens, considera-se o uso de autenticação e criptografia.

Esse trabalho emprega essas técnicas para desenvolver aplicações IoT residências com comunicação segura fim-a-fim ao projeto *Smart Home* [4]. Na primeira fase do projeto, conceberam-se três aplicações IoT para controle de ar-condicionado e de sistemas de iluminação artificial e natural. Desenvolveu-se um aplicativo móvel para Android, cujo envio de comandos era intermediado por um *broker* com protocolo MQTT (*Message Queuing Telemetry Transport*). A comunicação fim-a-fim não utilizou mecanismo de segurança. Nesse trabalho, aplicarM-se os conceitos no ambiente do Laboratório de Cyber Segurança e Internet das Coisas (Lab. CS&I) do Inatel. Redefiniu-se o aplicativo móvel para atender os novos objetivos e configurou-se um *broker* MQTT próprio. Essas modificações permitiram a implementação de mecanismos de autenticação e de criptografia por meio do protocolo TLS (*Transport Layer Security*) para uma comunicação segura fim-a-fim. Estruturou-se esse trabalho em quatro seções. Na Seção II, apresenta-se o desenvolvimento do projeto, explorando aspectos de *software* e *hardware*. Na Seção III, discute-se a o uso do protocolo TLS para comunicação segura fim-a-fim para as aplicações IoT do projeto. Abordam-se as conclusões e trabalhos futuros, na Seção IV.

Ana C. S. Rosa, Arielli A. Conceição, Francisco A. S. do Carmo, Guilherme P. Aquino e Evandro C. V. Boas, Laboratório de Cyber Segurança e Internet das Coisas (CS&I Lab.), Instituto Nacional de Telecomunicações (Inatel). ana.ac@ges.inatel.br, arielli.a@inatel.br, francisco.assis@inatel.br, guilhermeaquino@inatel.br, evandro.cesar@inatel.br.

II. *SMART HOME:* APLICAÇÕES IOT RESIDENCIAIS

O projeto *Smart Home* automatiza e controla por meio de aplicativo móvel a temperatura, a iluminação artificial e a natural de um ambiente residencial ou similar (escritórios ou laboratórios). Para implementação, considerou-se o ambiente do Laboratório CS&I, integrando três sistemas ou módulos, como visto na Figura 1. O sistema de controle do ar-condicionado permite que o usuário gerencie as funções de refrigeração ou ventilação do ambiente. O sistema de controle de iluminação artificial provê acesso aos relés que determinam o fornecimento de corrente elétrica para o conjunto de lâmpadas. O sistema de iluminação natural comanda a abertura das cortinas por meio de motores. A comunicação entre o aplicativo móvel e os sistemas ocorre por intermédio de um *broker* MQTT.

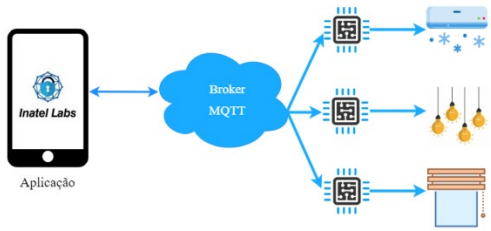


Fig. 1. Diagrama em blocos do projeto *Smart House*.

Desenvolveu-se o aplicativo móvel para sistema Android, utilizando a linguagem de programação Java e ambiente de desenvolvimento integrado Android Studio. O aplicativo é a interface do usuário e permite controlar os três sistemas por meio do envio de comandos através de botões ou fala. Na Figura 2, apresentam-se as telas do aplicativo. O sistema de controle de ar-condicionado é composto pelo aplicativo móvel e um módulo de *hardware*, que integra um microcontrolador ESP8266, um diodo LED emissor de infravermelho (IR) e um resistor de 220 Ω. O sistema de controle de iluminação artificial também emprega um microcontrolador ESP8266 para o controle de oito

relés, como visto na Figura 3. Alimentam-se as lâmpadas por meio da rede elétrica de 127 V do Laboratório, controlando essa alimentação por meio de relés de 5 V. Devido à diferença entre a voltagem de alimentação do ESP8266 (3 V) e dos relés (5 V), empregam-se fontes de alimentação distintas para suprir as necessidades energéticas do módulo de controle de iluminação artificial. O sistema de controle de iluminação natural permite regular a luminosidade externa que adentra ao Laboratório por meio do controle de cortinas. Para isso, emprega-se um módulo de *hardware* composto por um terceiro microcontrolador ESP8266, um circuito em ponte H e um motor de vidro elétrico.

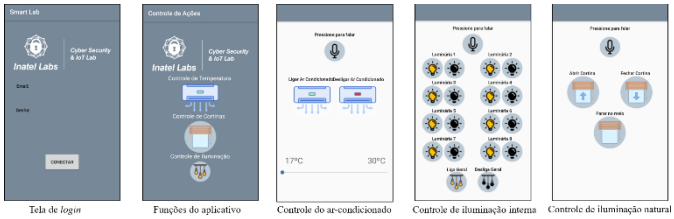


Fig. 2. Aplicativo móvel.

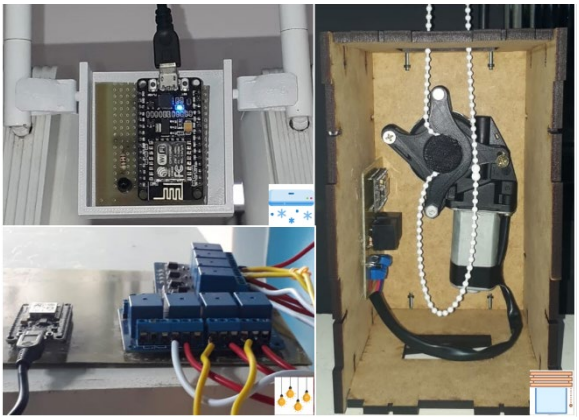
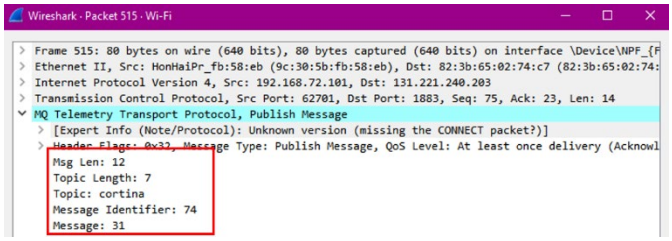


Fig. 3. Módulos de *hardware* instalados no Lab. CS&I.

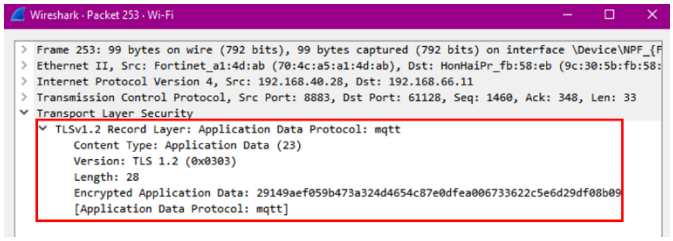
III. *Secure Smart House*

Para prover a conexão segura entre o aplicativo e o *broker*, incluíram-se bibliotecas do pacote Paho Java MQTT Client, que implementam o protocolo TLS durante a comunicação. Encapsulou-se a conexão MQTT em um *Android-Service* que é executado no plano de fundo do aplicativo móvel, mantendo-o ativo quando o aplicativo está alternando entre diferentes atividades. Ao se conectar com TLS, o MQTT necessita de um certificado válido que seja confiável por meio da cadeia de confiança do dispositivo móvel. Para que a conexão seja bem-sucedida, definem-se os caminhos para o armazenamento do certificado, tornando-os explícitos no código no momento de acesso. Para implementar a segurança nas conexões do microcontrolador ESP8266 com a Internet e com o *broker*, utilizam-se as bibliotecas WifiClientSecure. e MQTT.h, pois oferecem suporte ao protocolo TLS. Instalou-se no microcontrolador o certificado de autenticação e incluiu-se no código um arquivo ".h", que contém os principais parâmetros de acesso TLS, como a chave pública e o *fingerprint* (impressão digital).

Para demonstração, utilizou-se a ferramenta Wireshark para monitorar o tráfego de dados de uma versão do projeto sem uso do protocolo TLS e uma segunda, que o implementa. Na Figura 4(a), visualiza-se o tráfego de informações em texto claro, expondo os comandos trocados entre as entidades do projeto. Na Figura 4(b), intercepta-se o tráfego de dados da versão com protocolo TLS em texto cifrado. Nesse segundo cenário, tem-se comunicação segura fim-a-fim entre as entidades.



(a) Comunicação sem uso de protocolo TLS.



(b) Comunicação com uso de protocolo TLS.

Fig. 4. Análise de tráfego de mensagens na rede entre entidades do projeto *Smart House* e *Secure Smart House*.

IV. Conclusões

Este trabalho apresentou o desenvolvimento de aplicações IoT residenciais empregando o protocolo TLS e autenticação para prover comunicação segura fim-a-fim. Desenvolveram-se três sistemas para controle de ar-condicionado, de iluminação artificial e de iluminação natural do Laboratório CS&I do Inatel. Além disso, projetou-se uma aplicação móvel como interface de usuário para envio de comandos aos módulos de *hardware*. Em relação à segurança, implementou-se o protocolo TLS e também autenticação com usuário e senha para troca de mensagens entre clientes e *broker* MQTT. Durante os testes, validaram-se o uso do protocolo TLS e aplicativo, observando as modificações em ambiente real. A implementação do protocolo TLS implica em um aumento de tráfego de dados entre as entidades do projeto. Contudo, instalaram-se esses módulos em ambientes que possuem fontes de energia que dispensam o uso de bateria, viabilizando o projeto. Como trabalhos futuros, visa-se aplicar conceitos de inteligência artificial para reduzir a intervenção humana e tornar o Laboratório CS&I inteligente.

Agradecimentos

Os autores agradecem ao Instituto Nacional de Telecomunicações - Inatel, por prover os meios necessários a realização desse trabalho de IC.

Referências

[1] Simone Cirani *et al*., *Internet of Things: Architectures, Protocols and Standards*. 1th. John Wiley Sons Ltd, 2019.

[2] IA. Al-Fuqaha *et al*., "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.

[3] H. Tschofenig e E. Baccelli, "Cyberphysical Security for the Masses: A Survey of the Internet Protocol Suite for Internet of Things Security," in *IEEE Security & Privacy*, vol. 17, no. 5, pp. 47-57, Sept.-Oct. 2019.

[4] A. C. S. Rosa *et al*., "Controle de Dispositivos Residenciais utilizando IoT," in XXXII Congresso de Iniciação Científica do Inatel – Incitel 2020, Santa Rita do Sapucaí, MG, Brasil: Instituto Nacional de Telecomunicacões, pp. 58–62, 2020.