Avaliação de Risco em um Laboratório Remoto IoT

Victor T. Hayashi[1], **Felipe V. de Almeida**[1], **Andrea E. Komo**[1]

[1] Escola Politécnica – Universidade de São Paulo (USP)

{victor.hayashi,felipe.valencia.almeida,andrea.komo}@usp.br

Abstract. *The use of remote laboratories is an alternative to maintain practical activities in laboratory disciplines, even in the remote offering caused by the COVID-19 pandemic. However, in addition to the adoption of various tools for remote work and study, during the period of social distancing, a growing concern with security was observed. In this article, a risk assessment for improving the security of a remote laboratory used in offering a digital electronics laboratory course between September and December 2021 is presented, resulting in a specification using MQTT instead of the HTTP protocol.*

Resumo. *O uso de laboratórios remotos é uma alternativa para manter as atividades práticas em disciplinas de laboratório, mesmo no oferecimento remoto provocado pela pandemia de COVID-19. Contudo, além da adoção de diversas ferramentas para trabalho e estudo remoto, durante o período de distanciamento social foi observado uma preocupação crescente com a segurança. Neste artigo, é apresentada uma avaliação de risco para melhoria da segurança de um laboratório remoto utilizado no oferecimento de uma disciplina de laboratório de eletrônica digital entre setembro e dezembro de 2021, resultando em uma especificação que utiliza MQTT ao invés do protocolo HTTP.*

1. Introdução

A adoção de inovações está diretamente ligada a disparidade de quão útil ela é versus quais os seus riscos percebidos. Considerando a difusão de inovações [Models 2009], para que uma nova inovação possa ser adotada pela grande maioria, há diversos aspectos que podem contribuir positivamente ou negativamente. Por exemplo, a utilidade percebida impacta positivamente a adoção, pois potenciais adotantes têm uma motivação maior para se arriscarem e testarem a nova tecnologia. Já o risco percebido impacta negativamente a adoção, conforme percebido em relação à adoção de aplicativos móveis para acesso a serviços bancários [Dash et al. 2014]. Desta forma, ataques que levam à perda de controle, eventos de indisponibilidade e o vazamento de dados podem impactar negativamente a adoção de novas tecnologias, como as ferramentas para colaboração remota.

Assim, ao se considerar a oportunidade de usar tecnologias de Internet das Coisas (IoT, do inglês *Internet of Things*) para viabilizar um laboratório remoto de eletrônica digital para fomentar atividades laboratoriais mesmo em período de distanciamento social, considerar o aspecto de segurança é necessário, porém também é um grande desafio, pois há desafios resultantes da heterogeneidade e restrições específicas (e.g., banda, processamento, memória, energia) que limitam o uso de mecanismos de segurança tradicionais. Neste artigo, é apresentada uma avaliação de risco para melhorar aspectos de autenticação e controle de acesso de um laboratório remoto utilizado em uma disciplina de laboratório

de eletrônica digital. São destacadas discussões sobre a usabilidade para os estudantes e outros requisitos que devem ser considerados em conjunto com os requisitos de segurança para a especificação de uma solução viável.

O texto está organizado da seguinte forma: a seção 2 apresenta os trabalhos relacionados, enquanto a seção 3 descreve o método adotado. A seção 4 discute o estudo de caso para um laboratório remoto de eletrônica digital. As considerações finais da seção 5 concluem o artigo.

2. Trabalhos Relacionados

É possível identificar na literatura diversos trabalhos voltados para a análise de segurança em ambientes IoT. A seguir são apresentados alguns destes, sendo os três primeiros de caráter mais geral enquanto os dois últimos possuem maior afinidade com o trabalho aqui proposto devido ao contexto dos laboratórios remotos.

Há uma proposta de um *framework* para identificar dispositivos maliciosos em uma arquitetura IoT utilizando Microsoft Azure, OpenStack e a ferramenta python *pytbull*, com a execução de ataques reais neste ambiente virtual, de tal forma que os resultados obtidos serviram como validação, pois foi possível identificar os dispositivos maliciosos [Sohal et al. 2018]. Considerando os desafios de garantir os requisitos de segurança em um ambiente IoT, uma abordagem guiada por testes de segurança (*Test Driven Security Approach*) é proposta. Assim como no trabalho anterior é proposto um *framework*, porém neste o foco é utilizar uma plataforma de segurança também desenvolvida pelos autores denominada Sablo, com o propósito de intensificar a realização de testes no ciclo de vida de um projeto IoT [Săndescu et al. 2018]. Um *gateway* genérico de monitoramento e controle (MCG - *Monitoring and Control Gateway*) que permite realizar testes em dispositivos para casas conectadas é proposto. Os autores conseguiram identificar diversas falhas de segurança nos dispositivos analisados, apontando como um desafio a ser tratado nos próximos anos com a difusão crescente de dispositivos para este nicho [Aloul et al. 2020].

Há diversas recomendações e procedimentos para armazenar dados em um *data warehouse* para atender aos interesses de um laboratório remoto. Os autores apresentam um foco nos sistemas de gerenciamento de informação de laboratórios (LMS - *Laboratory Management System*) [Pálka and Schauer 2015]. Também é proposto um conjunto de diretrizes para atender requisitos tanto de segurança de dados quanto de tolerância a falhas nos laboratórios remotos. É aplicada a norma VDI/VDE 2182 voltada para a segurança em automação industrial porém adaptada para atender ao domínio dos laboratórios remotos. Um ciclo composto por 8 etapas é definido, e cada etapa é apresentada com base em um estudo de caso de um laboratório remoto denominado DigiLab4U [Uckelmann et al. 2021].

Mesmo que as duas últimas propostas estejam relacionadas com o cenário de laboratório remoto, estas se atentam a diretrizes e em sistemas de gerenciamento. O presente artigo busca aplicar uma avaliação de risco para analisar as propostas de contramedidas em um laboratório remoto, atentando à escolha de qual protocolo de comunicação seria o mais indicado.

3. Método

O método utilizado para a avaliação de segurança consiste nos seguintes passos:

1. **Domínio do Problema**: entendimento do domínio do problema, considerando a proposta de valor do sistema para suas principais partes interessadas;
2. **Definições**: definição dos principais componentes do sistema;
3. **Modelagem do Sistema**: descrever como os componentes do sistema interagem para suportar as funcionalidades, e identificar as vulnerabilidades;
4. **Modelagem do Atacante**: modelar o atacante descrevendo suas motivações, capacidades e recursos disponíveis;
5. **Premissas**: destacar premissas para o uso de mecanismos de mitigação de ataques, descrevendo também premissas sobre o funcionamento do sistema, seu ambiente, e sobre o atacante;
6. **Requisitos de Segurança**: descrever as principais propriedades de segurança desejadas para o sistema;
7. **Avaliação de Risco**: detalhar alguns cenários de ataques que exploram as vulnerabilidades descritas, e realizar a avaliação de risco para priorizar os ataques com maior probabilidade e maior impacto associados;
8. **Contramedidas**: descrever as contramedidas (e.g., controle de acesso).

4. Avaliação de Risco

Esta seção apresenta a avaliação de risco realizada para melhoria de aspectos de segurança de um laboratório remoto de eletrônica digital. As seguintes partes interessadas e componentes são considerados:

Definição 1 (Aluno)**.** *O aluno está em sua residência e possui acesso à Internet por meio de conexão cabeada ou WiFi.*
Definição 2 (Administrador)**.** *O administrador pode ser um professor ou monitor, e está em sua residência com acesso à Internet por meio de conexão cabeada ou WiFi.*
Definição 3 (Técnico)**.** *O técnico está no laboratório para fornecer o suporte necessário para administradores e alunos.*
Definição 4 (FPGA)**.** *Placa didática Field Programmable Gate Array (FPGA) usada nos experimentos do laboratório remoto. Possui alto custo associado.*
Definição 5 (Interface Móvel IoT)**.** *É a interface móvel usada pelo aluno para compilação, carga e teste do seu projeto na placa FPGA do laboratório.*
Definição 6 (Dispositivo IoT)**.** *O dispositivo IoT ESP8266 é utilizado para interação com a placa FPGA e está instalado no laboratório. Possui conexão WiFi e está conectado à Internet por meio de rede WiFi presente no laboratório.*
Definição 7 (Plataforma IoT)**.** *A plataforma IoT fornece serviços de criação de projeto, monitoramento e controle de dispositivo IoT pela Interface Móvel IoT, e está implantada em um ambiente de computação em nuvem.*
Definição 8 (Plataforma Acesso Remoto)**.** *A plataforma de Acesso Remoto fornece acesso remoto dos alunos e administradores aos computadores do laboratório.*
Definição 9 (Computador do Laboratório)**.** *É o computador para acesso remoto do aluno ao laboratório, usado para a compilação e carga do projeto do aluno na placa FPGA.*
Definição 10 (*Webcam*)**.** *Há uma webcam para visualização da placa FPGA presente no laboratório. É utilizada em experimentos para que os alunos visualizem os resultados de suas interações, além do feedback existente na Interface Móvel IoT.*

Definição 11 (Computador Administrador)**.** *É o computador na residência do professor.*
Definição 12 (Computador Aluno)**.** *É o computador usado pelo aluno em sua residência.*

Domínio do Problema: os laboratórios remotos tiveram grande difusão na pandemia do COVID-19 como forma de viabilizar as aulas práticas e respeitar os protocolos de distanciamento social, sendo uma alternativa ao ensino por meio de simulação, também muito adotado neste contexto. A arquitetura de um laboratório remoto é dividida em duas partes. A primeira delas consiste em um aparato experimental relacionado a determinada disciplina e ao seu conjunto de experiências. Em uma disciplina relacionada a engenharia elétrica por exemplo, o aparato experimental pode ser composto por resistores, capacitores, indutores, além de dispositivos IoT, como microcontroladores e componentes SoC (*System on a Chip*). A segunda parte é uma interface de acesso, que tanto o aluno quanto o professor utiliza para interagir com o aparato experimental. Esta interface possui uma miríade de possibilidades de implementação, desde utilizar soluções já disponíveis comercialmente, como por exemplo o AnyDesk, que realiza uma conexão remota com uma máquina, até implementações específicas para uma disciplina, utilizando requisições HTTP ou então o protocolo MQTT no contexto de IoT.

Modelagem do Sistema: o modelo do sistema é apresentado na Figura 1. O acesso remoto dos alunos por meio de seus computadores é autorizado pelo administrador por meio de seu computador. O Computador do Laboratório é acessado remotamente, e possibilita compilação e carga para a placa FPGA, além da visualização pela *Webcam*. O aluno pode interagir com a placa FPGA usando a Interface Móvel IoT, que está integrada a uma Plataforma IoT, que é a responsável por transportar os comandos até o Dispositivo IoT que interage com a placa FPGA. O Técnico se encontra no laboratório para prestar suporte se necessário.

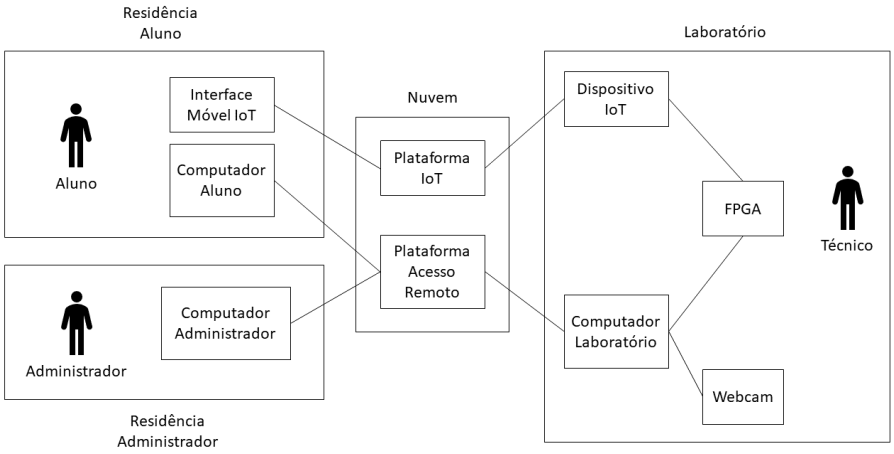

Figura 1. Modelo do sistema de laboratório remoto considerado

Modelagem do Atacante: o atacante considerado é um aluno mal intencionado, reprovado no oferecimento anterior da disciplina. Sua motivação para realizar o ataque é sua insatisfação com sua reprovação, que acredita que não foi justa. Como foi aluno do oferecimento anterior, possui conhecimento sobre o funcionamento do sistema.

As seguintes premissas foram consideradas:

Premissa 1 (Credencial Mestre Acesso Remoto)**.** *A credencial para acesso remoto aos computadores do laboratório é conhecida apenas pelos técnicos e administradores.*
Premissa 2 (Comunicação HTTP)**.** *A comunicação utilizada inicialmente na plataforma IoT é HTTP, baseada em um token de acesso estático.*
Premissa 3 (Credencial Interface Móvel IoT)**.** *A credencial para acesso ao aluno pela Interface Móvel IoT é do tipo usuário-senha conhecido apenas pelo usuário, porém reutilizada em outras plataformas.*

A modelagem motivou a especificação dos seguintes requisitos:

Requisito 1 (Integridade dos equipamentos do laboratório)**.** *Os equipamentos FPGA, computador do laboratório e Webcam devem ter sua integridade garantida.*
Requisito 2 (Disponibilidade)**.** *O sistema deve estar disponível em 99% das vezes.*

Avaliação de Risco: a maior vulnerabilidade considerada é a comunicação HTTP com um *token* de acesso estático. Este *token* é utilizado para o monitoramento e controle do Dispositivo IoT que interage com a FPGA. Para obter este *token*, o atacante precisa obter acesso momentâneo ao computador do laboratório, que mantém este *token* armazenado para configurar o Dispositivo IoT para a conta do aluno legítimo que está acessando o Computador Remoto no momento. O possível ataque possui alta probabilidade e impacto médio, impactando o requisito de disponibilidade, resultando em risco alto. Outra vulnerabilidade ocorre na autorização do uso do Computador do Laboratório pelo Administrador ao Aluno. A única verificação de identidade realizada é a validação do nome do aluno. Contudo, um atacante pode personificar um aluno legítimo se souber seu nome. O possível ataque tem alta probabilidade e impacto baixo, resultando em risco médio. O roubo da credencial do aluno pode ocasionar sua personificação em outras plataformas devido ao reuso da senha, contudo isso não está relacionado à motivação do perfil de atacante considerado. Já o roubo da credencial mestre de acesso remoto pode levar ao comprometimento de todos os computadores do laboratório, já que esta credencial é usada para acesso remoto em todos os computadores. A probabilidade do possível ataque é baixa e seu impacto é alto, resultando em risco médio.

Contramedidas: a comunicação do Dispositivo IoT e Interface Móvel IoT com a Plataforma IoT poderia ser criptografada com o uso de criptografia simétrica, ou então um mecanismo de autenticação baseado em desafio resposta baseado em números aleatórios poderia ser utilizado. Uma alternativa mais simples é utilizar o protocolo MQTT ao invés do HTTP, integrado com mecanismo de autenticação básico baseado em usuário e senha com restrições de tópico (i.e., relacionadas a um controle de acesso mais granular). O procedimento de autorização de uso de um Computador do Laboratório pelo Administrador ao Aluno pode ser realizada em conjunto com uma validação em videoconferência com imagem e som em tempo real do aluno, que deve confirmar o nome utilizado e só realizar a requisição quando o professor autorizar. Os alunos podem ser instruídos a usarem uma senha que não é utilizada em outras plataformas, e a credencial de acesso aos computadores pode ser diferente para cada computador, além da implantação de mecanismos de gerenciamento de credenciais como a troca periódica de senha. Como principais

sugestões estão o uso do protocolo MQTT com autenticação baseada em usuário e senha e restrições de tópicos para um controle de acesso mais granular ao invés da comunicação HTTP no curto prazo. Além disso, a validação em tempo real do aluno por videoconferência para acesso remoto deve ser implantada em conjunto com políticas de gerenciamento de senhas do acesso remoto e da Interface Móvel IoT. O uso de mecanismos de acesso a máquinas virtuais por meio de SSH (Secure Shell) pode suportar um controle de acesso mais granular, porém aspectos de usabilidade podem ser prejudicados.

5. Considerações Finais

Este artigo apresentou uma avaliação de risco para o laboratório remoto considerando a aplicação de tecnologias de IoT para suportar o ensino remoto de forma segura, tanto pela perspectiva sanitária quanto na visão de segurança da informação.

A especificação resultante de laboratório remoto com uso do protocolo aberto MQTT também considerou aspectos de usabilidade dos usuários. Espera-se que esta especificação contribua para a construção de laboratórios remotos para disciplinas de Engenharia Elétrica (e.g., eletrônica digital, eletrônica analógica).

Referências

[Aloul et al. 2020] Aloul, F., Zualkernan, I., Shapsough, S., and Towheed, M. (2020). A monitoring and control gateway for iot edge devices in smart home. In *2020 International Conference on Information Networking (ICOIN)*, pages 696–701. IEEE.

[Dash et al. 2014] Dash, M., Bhusan, P. B., and Samal, S. (2014). Determinants of customers' adoption of mobile banking: An empirical study by integrating diffusion of innovation with attitude. *Journal of Internet Banking and commerce*, 19(3):1–21.

[Models 2009] Models, P. (2009). Diffusion of innovations.

[Pálka and Schauer 2015] Pálka, L. and Schauer, F. (2015). Safety of communication and neural networks for security enhancement in data warehouse for remote laboratories and laboratory management system. In *2015 6th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–8. IEEE.

[Săndescu et al. 2018] Săndescu, C., Grigorescu, O., Rughiniş, R., Deaconescu, R., and Calin, M. (2018). Why iot security is failing. the need of a test driven security approach. In *2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pages 1–6. IEEE.

[Sohal et al. 2018] Sohal, A. S., Sandhu, R., Sood, S. K., and Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Computers & Security*, 74:340–354.

[Uckelmann et al. 2021] Uckelmann, D., Mezzogori, D., Esposito, G., Neroni, M., Reverberi, D., Ustenko, M., and Baalsrud-Hauge, J. (2021). Guideline to safety and security in federated remote labs. *International Journal of Online & Biomedical Engineering*, 17(4).