Identificação de Ameaças relacionadas a Medidores de Glicose

Fernando Homem da Costa[1], **Lucila Maria de Souza Bento**[2] **e**
Noemi Rodriguez[1]

[1]Departamento de Informática – Pontifícia Universidade Católica do Rio de Janeiro
Caixa Postal 38097 – CEP 22451-900 – Rio de Janeiro – RJ – Brasil

[2]Laboratório de Informática – Instituto Nacional de Metrologia, Qualidade e Tecnologia
Av. Nossa Sra. das Graças, 50 – Duque de Caxias – RJ – Brasil

nandohdc@gmail.com, lmbento@inmetro.gov.br, noemi@inf.puc-rio.br

Abstract. *Given the COVID-19 pandemic, the advancement of telemedicine demonstrates that the use of technologies is indispensable for performing diagnostics, monitoring and remote treatment of patients in distant locations. Given that they are medical services that include critical devices, a possible breach of the security of these devices has extreme consequences and should therefore be identified and avoided. Although the literature presents a variety of information about smart devices, the same is not true of glucose meters and the safety assessment process for these devices. This article proposes a methodology to understand the architecture and functionalities of glucose meters, the threats to which glucose meters are subject, and the vulnerabilities that can be exploited by malicious agents. The proposed model, which uses the STRIDE and attack tree methods, identifies threats linked to the meter with a focus on three types of threats: physical, networks and software.*

Resumo. *O avanço da telemedicina, devido ao cenário de pandemia do COVID-19, demonstra que o uso de tecnologias é indispensável para realização diagnósticos, monitoramento e tratamento remoto de pacientes em locais distantes. Por serem serviços médicos que incluem dispositivos críticos, uma possível violação de segurança desses dispositivos têm consequências extremas e devem, portanto, ser identificadas e evitadas. Apesar da literatura apresentar uma variedade de informações sobre alguns dispositivos inteligentes, o mesmo não ocorre com os medidores de glicose e o processo de avaliação de segurança dessa classe de dispositivos. Neste sentido, o presente trabalho propõe uma metodologia para conhecer a arquitetura e funcionalidades dos medidores de glicose e com essas informações compreender as ameaças às quais os medidores de glicose estão sujeitos e, consequentemente, as vulnerabilidades que podem ser exploradas por agentes maliciosos. O modelo proposto, com o uso dos métodos STRIDE e árvore de ataque, identifica as ameaças vinculadas ao medidor com foco em três tipos de ameaças: física, redes e software.*

1. Introdução

O avanço da tecnologia e a evolução dos microcontroladores, sensores e conexões de rede possibilitaram que objetos presentes no nosso dia a dia sejam dotados de capacidade computacional e de comunicação, e se conectem em rede criando a chamada de Internet

das Coisas (IoT). Essa evolução tecnológica também transformou os sistemas de saúde e possibilitou aos dispositivos médicos adquirirem inteligência e mobilidade, facilitando o acesso à informação, tanto por parte do paciente quanto dos profissionais da saúde, permitindo diagnósticos rápidos, monitoramento e o tratamento do paciente a distância e de forma personalizada. De acordo com a Gartner [Laurence Goasduff 2020], estima-se que o número de dispositivos inteligentes em uso na área da saúde no final de 2020 será de 360 milhões, um crescimento de 28,57% em relação a 2019.

Entretanto, alguns dos principais desafios que já vem sendo enfrentados em IoT com relação à questões de segurança da informação e privacidade, ganham ainda mais ênfase em sistemas críticos, como da área de saúde, pois qualquer falha, ausência de controles de segurança ou exposição de dados sensíveis pode prejudicar seriamente o funcionamento destes, podendo, até mesmo, causar a perda de vidas humanas. Um exemplo que mostra claramente o poder destrutivo de um incidente de segurança da informação na área da saúde refere-se ao incidente ocorrido em 2018 no Reino Unido [Matthew Field 2020], no qual um malware infectou vários hospitais e criptografou seus dados. Esse incidente gerou um caos momentâneo no sistema de saúde inglês, dificultando o atendimento aos pacientes e impedindo o funcionamento dos dispositivos médicos que dependiam dessas fontes de dados. O incidente chama atenção para um ponto importante: a necessidade de considerar e implementar requisitos de segurança da informação no ambiente computacional de organizações da área e no projeto e implementação de dispositivos médicos inteligentes, principalmente aqueles que podem ser usados de maneira autônoma pelo paciente para acompanhamento de doenças crônicas, como é o caso dos medidores contínuos de glicose [Chunxiao Li et al. 2011]. Estes são utilizados em ambientes não monitorados e, por isso, ficando sujeitos a diferentes tipos de abuso por parte de agentes maliciosos.

Um medidor contínuo de glicose faz parte de um sistema de infusão contínua de insulina (ou sistema de insulinoterapia) que também possui uma bomba de insulina, um controle remoto e um dispositivo para armazenamento de *logs* [Chunxiao Li et al. 2011]. O medidor de glicose é composto por um sensor descartável colocado sob a pele para medir o nível a glicemia do usuário e um transmissor que é conectado ao sensor para enviar os dados para a bomba de insulina e um dispositivo de armazenamento. A bomba de insulina é responsável pela administração autônoma de insulina por infusão subcutânea. O controle remoto controla e programa a bomba de insulina, permitindo ao usuário administrar ou interromper o processo de adição de insulina. O dispositivo de armazenamento é um componente em que todos os dados coletados a partir do medidor e, possivelmente, da bomba de insulina são armazenados e disponibilizados para visualização. No presente trabalho, o termo medidor de glicose será usado para se referir ao conjunto formado pelo medidor e o dispositivo de armazenamento.

Em 2019, a International Diabetes Federation (IDF) estimou que 463 milhões de pessoas no mundo com idade entre 20 e 79 anos viviam com diabetes e que esse número pode chegar a 629 milhões de pessoas em 2048 [International Diabetes Federation 2020]. No Brasil, a IDF estimou que esse número fica perto de 16,8 milhões de pessoas. Outro dado importante é que a maioria dos diabéticos usa medidores de glicose e um número cada vez maior deles usa um sistema de infusão contínua de insulina para terapia [Chunxiao Li et al. 2011]. Com isso, pode-se concluir que quanto maior o número de pessoas diabéticas, maior será a demanda por dispositivos médicos inteligentes que

auxiliem no tratamento, evidenciando a importância destes dispositivos para a sociedade.

Dadas as circunstâncias e as estimativas citadas, o estudo de aspectos de segurança relacionados a medidores de glicose pode ser visto como um tema de pesquisa relevante e de grande impacto para a sociedade. Deste modo, o presente trabalho tem como principal objetivo identificar as ameaças relacionadas aos medidores de glicose, a fim de contribuir para a definição de um processo de análise de segurança dessa classe de dispositivos e com a elaboração de projetos desses dispositivos que adotem medidas para mitigação das ameaças identificadas, incrementando os níveis de segurança dos mesmos. Para alcançar este objetivo, o trabalho propõe um metodologia que inclui a modelagem da arquitetura dos medidores de glicose e a utiliza como entrada para modelar as ameaças relacionadas a esses dispositivos, com o uso dos métodos de modelagem de ameaças STRIDE e árvore de ataque [Shostack 2014].

2. Trabalhos Relacionados

O trabalho de [Chunxiao Li et al. 2011] apresenta o funcionamento do ciclo de insulina, que engloba o monitoramento de glicose e o sistema de administração de insulina. O trabalho também descreve os ataques passivos e ativos contra o sistema de administração de insulina, incluindo os cenários de ataque com base nas violações identificadas. Os autores também apresentam duas mitigações para os cenários enumerados.

Em [Burleson et al. 2012], os autores abordam os principais desafios de se projetar dispositivos médicos implantáveis seguros, incluindo a bomba de insulina e seu ciclo. O trabalho descreve os princípios de *design* para segurança desses dispositivos, destacando as dificuldades relacionadas a segurança na sua concepção. Além disso, no trabalho são esboçadas medidas defensivas que podem ser implementadas.

No trabalho de [Yaqoob et al. 2019] é apresentada uma visão geral do modelo de rede de dispositivos médicos para entender os problemas de segurança associados, seguida por vetores de ataque e recursos de comunicação com tecnologias. Também são examinadas as deficiências de segurança presentes em dispositivos médicos e suas comunicações com outras tecnologias, com ênfase nas áreas demonstradas e aplicáveis a ataques cibernéticos. Além disso, o trabalho analisa pontos fracos de políticas que aumentam os problemas de segurança em dispositivos médicos.

Embora não tenham sido encontrados trabalhos na literatura que trate diretamente de segurança e modelagem de ameaça voltados a medidores de glicose, existem diferentes trabalhos [Chowdhury and Mackenzie 2014, Sándor and Sebestyén-Pál 2017, Wang et al. 2015] que aplicam modelagem de ameaças no contexto de IoT e evidenciam a importância do uso desta técnica para enfrentar as problemáticas de segurança nestes ativos. Um exemplo de uso de modelagem de ameaças em um contexto mais próximo do cenário abordado no presente trabalho foi proposto por [Cagnazzo et al. 2018]. Nesse trabalho, os autores discorrem sobre modelagem de ameaças em sistemas de saúde móveis e a importância de tal ferramenta para mapear possíveis falhas de segurança. Os autores utilizam os métodos STRIDE [Shostack 2014], para identificar as ameaças, e DREAD, para avaliar os riscos associados a cada ameaça específica, além de apresentar possíveis estratégias de mitigação para cada situação observada.

3. Metodologia utilizada

Os diferentes aspectos de segurança precisam ser tratados considerando as características do contexto de uso do dispositivo. Com isso, a metodologia descrita na presente seção visa fornecer uma visão abrangente sobre a arquitetura e funcionalidades dos medidores de glicose, para que, a partir dessas informações seja possível compreender as ameaças às quais os medidores de glicose estão sujeitos e, consequentemente, as vulnerabilidades que podem ser exploradas por agentes maliciosos.

A metodologia proposta, cujo fluxograma é mostrado na Figura 1, é dividida em três etapas. A primeira etapa consiste na modelagem da arquitetura do medidor que visa identificar os componentes, comunicação entre os componentes, funcionalidades comuns, pontos de interação com usuários e as tecnologias utilizadas. A segunda etapa corresponde a modelagem de ameaças e utiliza como entrada a arquitetura do medidor obtida na etapa anterior. A terceira e última etapa envolve a identificação/exploração de vulnerabilidades com base nas ameaças identificadas, a fim de verificar se as ameaças mapeadas foram consideradas (e mitigadas) no design do medidor.

Figura 1. Visão geral da metodologia utilizada

As seções a seguir apresentam um detalhamento de cada uma das atividades mostradas na Figura 1.

3.1. Modelagem de arquitetura dos medidores de glicose

Conforme já citado, a etapa de modelagem da arquitetura do medidor é composta pela identificação das partes que compõem um medidor, os pontos de interação com o ativo e as tecnologias utilizadas. O processo de identificação das partes que compõem o ativo envolve a identificação dos componentes que fazem parte do medidor (como sensores, atuadores, banco de dados, entidades na nuvem, por exemplo), como é realizada a comunicação entre esses componentes e as principais funcionalidades disponíveis no ativo. A determinação dos pontos de interação com o medidor inclui a identificação dos pontos em que há a interação entre usuários e o medidor, entre o medidor e sistemas externos, ou entre o medidor e quaisquer outros ativos. No processo de identificação das tecnologias adotadas são mapeadas as tecnologias usadas na implementação de cada componente para prover as funcionalidades necessárias àqueles componentes.

3.1.1. Padrões, Normas Técnicas e Guias

Para obter as informações necessárias sobre a arquitetura dos medidores de glicose, foram realizadas diversas pesquisas por padrões, normas técnicas e guias que pudessem apresentar recomendações sobre a implementação, funcionalidades e recomendações de segurança deste tipo de ativo.

No cenário nacional, foi identificada a instrução normativa Nº 24 da [ANVISA 2018], de 17 de maio de 2018, na qual são estabelecidos os critérios para o registro, alteração e revalidação relativos ao desempenho analítico de instrumentos de autoteste para glicose e seus consumíveis, tomando como base a Norma Técnica internacional ISO 15197:2013 [International Organization for Standardization 2013]. Entretanto, tais documentos não fornecem orientações sobre aspectos arquiteturais dos medidores de glicose, versando somente sobre seu desempenho analítico.

No cenário internacional, além da ISO 15197:2013, dois documentos orientativos apresentados pela Food and Drug Administration dos Estados Unidos merecem destaque. O primeiro documento é um relato de um processo de avaliação de medidor de glicose [USFDA 2018] que contém várias normas técnicas e padrões usados na avaliação e que envolvem diversas áreas de conhecimento, como química, biologia e tecnologia. Dentre as referências citadas nesse documento, o mais relevante para o contexto deste trabalho é a IEC 62304:2006 [International Electrotechnical Commission 2006], que é um padrão que se aplica aos processos de desenvolvimento e manutenção de software para dispositivos médicos, podendo tal software ser o próprio dispositivo ou parte integrante de um dispositivo médico final. A IEC 62304 aborda os processos e o ciclo de vida de desenvolvimento do software, mas não faz citação às funcionalidades básicas necessárias aos dispositivos, nem quaisquer aspectos arquiteturais. O segundo documento de destaque [U.S. Food and Drug Administration 2014] apresenta questões relacionadas à segurança cibernética que os fabricantes devem considerar na fase de projeto e desenvolvimento de seus dispositivos médicos, bem como na preparação da documentação desses dispositivos, para aqueles fabricantes interessados em receber autorização para comercializar seus dispositivos no mercado interno do Estados Unidos. Além disso, o documento aborda alguns requisitos básicos de segurança que os medidores de glicose devem implementar para serem aprovados para uso no mercado interno americano. São eles:

- Limitar o acesso apenas a usuários confiáveis
  - Limitar o acesso aos dispositivos através da autenticação de usuários (por exemplo, ID do usuário e senha, cartão inteligente, biométrico);
  - Usar métodos cronometrados automáticos para encerrar sessões no sistema, onde apropriado para o ambiente de uso;
  - Quando apropriado, empregar um modelo de autorização em camadas diferenciando privilégios com base na função do usuário (por exemplo, cuidador, administrador do sistema) ou função do dispositivo;
  - Usar autenticação apropriada (por exemplo, autenticação multi-fator para permitir acesso privilegiado ao dispositivo a administradores de sistema, serviços técnicos ou pessoal de manutenção);
  - Reforçar a proteção de senha, evitando a senha "codificada" ou palavras comuns (ou seja, senhas iguais para cada dispositivo, difícil de mudar e vulnerável à divulgação pública) e limitar o acesso a senhas usadas para acesso privilegiado ao dispositivo;
  - Quando apropriado, fornecer bloqueios físicos nos dispositivos e suas portas de comunicação para minimizar a violação;
  - Exigir autenticação do usuário ou outros controles apropriados antes de permitir atualizações de software ou firmware, incluindo aquelas que afetam o sistema operacional, aplicativos e antimalware.

- Garantir conteúdo confiável
  - Restringir as atualizações de software ou firmware a código autenticado. Um método de autenticação que os fabricantes podem considerar é a verificação de assinatura de código;
  - Usar procedimentos sistemáticos para usuários autorizados para baixar software e firmware identificáveis de versão do fabricante;
  - Garantir a capacidade de transferência segura de dados de e para o dispositivo e, quando apropriado, usar métodos para criptografia.

Embora os documentos apresentados anteriormente sejam importantes para entender alguns aspectos sobre a implementação geral dos medidores de glicose, não foi encontrado nenhum padrão, norma técnica ou guia que apresentasse claramente especificações sobre arquitetura, funcionalidades e requisitos de hardware e software para estes dispositivos. Com isso, foi realizada uma busca pelos principais fabricantes de medidores de glicose no mercado internacional e foram analisadas as documentações de suas produtos[Instruments 2015, Instruments 2014, Technology 2013, Nexperia 2013, Integrated 2010] para entender como esses dispositivos estão implementados. Tais documentos também foram usados na modelagem da arquitetura dos medidores de glicose, detalhada na Seção 4.1.

3.2. Modelagem de Ameaças

Introduzida inicialmente pela Microsoft como uma etapa de design do SDL (*Secure Development Lifecycle*) de aplicações web [Meier et al. 2003], a modelagem de ameaças tem sido muito usada para incrementar os níveis de segurança de ativos, principalmente depois do surgimento do conceito de "*Secure by Design*" [Deogun et al. 2019], que tem como um de seus princípios manter a superfície de ataque a menor possível. A ideia central da modelagem de ameaças é prover uma metodologia sistemática para a identificação, categorização e classificação de ameaças à segurança da informação associadas a um dado ativo sob análise, onde ameaça é entendida como um evento ou ação que pode resultar em dano a um sistema ou organização.

Nesta etapa, as informações obtidas na etapa de modelagem da arquitetura do medidor são utilizadas como entrada e analisadas em busca de possíveis cenários de ameaças à segurança associados ao ativo. A etapa utiliza dois métodos de modelagem de ameaças: STRIDE e árvore de ataque. O STRIDE é usado para identificar as ameaças, enquanto a árvore de ataque é usada para fornecer uma caminho possível para identificação/exploração de vulnerabilidades a partir das ameaças identificadas. Adicionalmente, é importante observar que como o STRIDE foi concebido para ser utilizado no contexto de aplicações web e as ameaças estão intimamente relacionadas ao contexto. Esse fato poderia induzir a identificação predominante de ameaças associadas ao acesso físico ao medidor de glicose. Por isso, além de descrever os métodos STRIDE e árvore de ataque, também foi apresentada uma sugestão de classificação das ameaças, de acordo com o contexto de exploração, para ser usada junto com o STRIDE, a fim de aumentar as chances de identificar diferentes tipos de ameaças.

3.2.1. STRIDE

Desenvolvido em 1999 por Loren Kohnfelder e Praerit Garg [Shostack 2014], o STRIDE é um método de modelagem de ameaças para auxiliar desenvolvedores de software a

identificar os tipos de ataques aos quais uma aplicação está sujeita. O acrônimo STRIDE representa as iniciais das seguintes categorias de ameaças:

- *Spoofing* (Falsificação) é definido como a ação de fingir ser algo ou alguém, que não seja a própria pessoa ou entidade, para acessar informações sensíveis. Um cenário clássico é o caso de falsificação de endereço de e-mail, em que *spammers*, remetentes dos e-mails, ocultam a origem de seus e-mails, causando problemas para os servidores de e-mail, como devoluções mal direcionadas.
- *Tampering* (adulteração) é a ação de modificar algum dado ou informação em disco, memória, sistema ou aplicação para o qual não se possui autorização. Quando um agente malicioso manipula um arquivo no sistema da vítima e consegue alterar o nome dele, isso corresponde a uma violação da integridade desse arquivo, por exemplo.
- *Repudiation* (repúdio) é o ato do usuário (legítimo ou não legítimo) negar ou rejeitar alguma ação que foi executada. Essa ameaça está fortemente relacionada à falta de evidências que provem o autor da ação. Um caso de repúdio conhecido é de um atacante modificando o fluxo de dados através da rede para os *logs* serem preenchidos com informação enganosas.
- *Information Disclosure* (exposição de informações) é caracterizada por permitir que pessoas tenham acesso a informações que elas não possuem autorização para acessar. Os cenários que abrangem essa ameaça vão desde exposição de *banner* de serviços até encontrar chaves criptográficas em discos ou em memória.
- *Denial of Service* (negação de serviço) é uma ameaça que tem por objetivo esgotar recursos de um sistema, tornando-o indisponível para os usuários legítimos. Por exemplo, um atacante pode preencher todo o disco de armazenamento de um ativo de modo a impossibilitar que um usuário legítimo o utilize.
- *Elevation of Privilege* (elevação de privilégio) acontece quando um usuário consegue executar uma ação que ele não está autorizado a realizar. Um exemplo desse cenário seria uma aplicação móvel que permite que um usuário, que não possui privilégio de administrador, possa trocar a senha de outro usuário sem que ocorra a validação de quem está trocando a senha e de qual usuário.

Logo, o acrônimo do STRIDE representa as ameaças que negam algumas propriedades que um sistema deveria ter, a saber, autenticidade, integridade, não repúdio, confidencialidade, disponibilidade e autorização.

3.2.2. Árvore de ataque

As árvores de ataque (ou *attack trees*, em inglês) têm como objetivo fornecer uma maneira formal e organizada de descrever a segurança de ativos, com base em ataques diversos. Para tal processo de modelagem, um ataque contra um ativo é representado por meio de uma estrutura em árvore, tendo o objetivo apresentado como nó raiz e as folhas como as diferentes maneiras de atingir o objetivo definido [Shostack 2014]. Essa forma de organizar o pensamento sobre as possíveis ameaças facilitam a identificação de falhas de segurança que podem afetar o projeto. O processo permite a criação de uma única árvore para todo o projeto (ou ativo), ou a divisão da árvore em várias árvores distintas, possibilitando utilizar o método de forma única ou geral. As etapas desse método

são [Shostack 2014]: 1) Escolher uma representação; 2) Criar um nó raiz; 3) Criar filhos; 4) Avaliar a integridade; 5) Podar a árvore; 6) Verificar a apresentação.

Antes de elaborar uma árvore de ataque, deve-se escolher qual o tipo de representação ela terá, podendo ser divida em duas categorias: "AND" ou "OR". As árvores "AND" são aquelas em que o estado de um nó depende de todos os filhos imediatamente abaixo dele. Para as árvores do tipo "OR", um nó é verdadeiro se algum de seus filhos são verdadeiros. Ao representar uma árvore é recomendado deixar explícito de qual tipo ela pertence. A Figura 2 representa um cenário de exemplo de uma árvore "AND"em que a meta é autenticar-se como usuário legítimo no sistema e, para isso, é necessário obter um usuário e senha válido. Já a Figura 3 apresenta um exemplo de uma árvore "OR" em que apenas um deles precisa ser válido. Ou seja, esse exemplo diz que é possível interceptar a comunicação entre um usuário legítimo e o servidor de *back-end* e obter uma credencial válida, como também é possível realizar um ataque de força bruta de *login* e encontrar credenciais de um usuário legítimo.

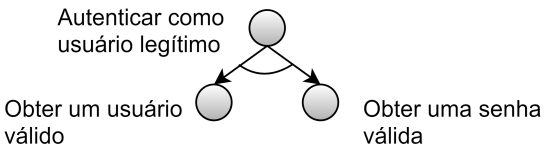

Figura 2. Árvore de Ataque AND

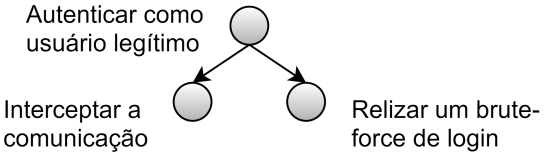

Figura 3. Árvore de Ataque OR

Durante a criação de um árvore de ataque deve-se estabelecer qual será o objetivo a ser atingido. O nó raiz pode ser um componente do ativo que será analisado ou uma meta de um agente malicioso. Caso o nó raiz seja um componente, os filhos devem indicar o que pode dar errado para o nó. Se o nó raiz for um objetivo de uma agente malicioso, os filhos devem considerar as ações a serem executadas para atingir esse objetivo. Cada ação alternativa para alcançar o objetivo expresso na raiz deve ser inserida como um filho.

3.2.3. Classificação das ameaças

A definição de medidor de glicose apresentada na Seção 1 permite dividir as ameaças em três categorias, de acordo com o contexto de exploração. Tais categorias podem ser usadas em conjunto com as categorias do método STRIDE para tornar mais claro o meio de persistência da ameaça. São elas:

- Ameaças físicas: compostas por ataques direcionados ao hardware do medidor;
- Ameaças de rede: compostas por ataques que visam explorar características do meio de comunicação usado pelo medidor;
- Ameaças de software: relacionadas, principalmente, a exploração de vulnerabilidades que possam existir tanto nos softwares embarcados nos componentes do medidor quanto em ativos externos que se comunicam com o medidor.

De maneira simplificada, pode-se entender que as ameaças de software estão relacionadas as ameaças de rede e físicas, pois um agente malicioso será capaz de explorar as ameaças identificadas nessas duas últimas categorias se não foram implementadas medidas de mitigação para tais ameaças nos softwares embarcados nos componentes do medidor. Deste modo, a partir das ameaças de rede e físicas identificadas pode-se utilizar o

método de árvore de ataque para analisar e identificar as vulnerabilidades correspondentes a uma dada ameaça.

3.3. Identificação/Exploração de vulnerabilidades

A última etapa da metodologia proposta consiste em verificar se as ameaças identificadas com a modelagem de ameaças estão presentes no medidor de glicose. Em outras palavras, essa etapa consiste em tomar como referência um medidor de glicose e avaliar se as ameaças identificadas na etapa anterior podem ser exploradas. Entretanto, como o presente trabalho visa modelar as ameaças a segurança dessa classe de ativos, a exploração de vulnerabilidade ficará em aberto para realização em trabalhos futuros.

4. Identificação de ameaças

A seguir são apresentados os detalhes da aplicação da metodologia proposta na Seção 3 na identificação de ameaças relacionadas aos medidores de glicose.

4.1. Características dos medidores de glicose

Com base na análise dos documentos descritos na Seção 3.1.1, foram identificadas as informações relevantes para modelar a arquitetura geral dos medidores de glicose, por meio do reconhecimento das características listadas anteriormente, a saber, os componentes do ativo, os pontos de interação com o ativo e as tecnologias utilizadas. Assim, os principais componentes identificados foram os seguintes:

- Sensor: responsável pela leitura (medição) de glicemia. O sensor pode se comunicar com dois tipos de dispositivos: um leitor ou um smartphone. O sensor utiliza NFC (*Near Field Communication*) para estabelecer conexão com o leitor e o smartphone, sendo essa a única maneira de coletar dados do sensor.
- Leitor: dispositivo responsável por capturar os dados do sensor (por meio de NFC) e apresentar os dados ao usuário. O leitor possui interface USB para atualização do firmware por meio de um computador, interface Bluetooth para comunicação com smartphones, NFC, memória para armazenar uma determinada quantidade de coletas, display para visualização dos dados; fonte de alimentação (bateria) e software para processamento dos dados de medição.
- Aplicativo móvel: pode ser instalado em um smartphone. Realiza a captura dos dados de medição a partir do sensor (por meio de NFC) ou a partir do leitor (por meio de Bluetooth) e disponibiliza os dados para visualização pelo usuário.

A Figura 4 ilustra como é realizada a comunicação entre os componentes do medidor de glicose.

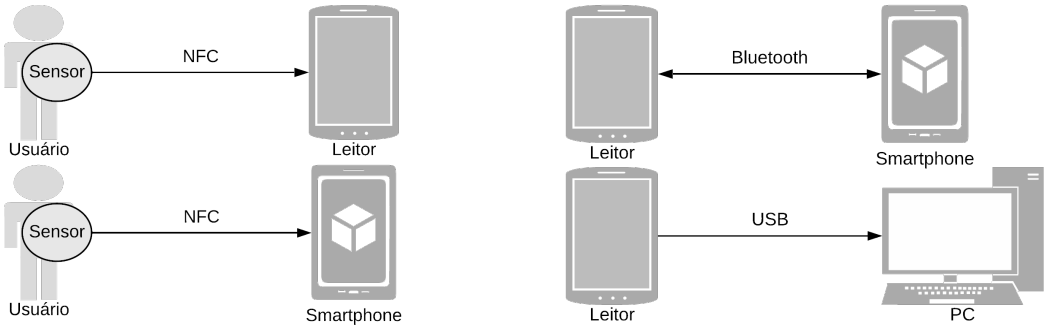

Figura 4. Comunicação entre os componentes do medidor

Diante dos componentes listados anteriormente, foi realizada a correlação entre as funcionalidades de hardware e software, extraídas dos documentos apresentados na Seção 3.1.1, a fim de identificar os pontos de interação do dispositivo com os usuários e outros sistemas. Os principais pontos de interação observados são:

- Atualização do firmware por meio da interface USB;
- Transferência dos dados de medição via Bluetooth entre leitor e smartphone;
- Transferência dos dados de medição do sensor para leitor e smartphone via NFC;
- Aplicativo móvel instalado em smartphone para consulta dos dados de medição;
- Botões e display presentes na interface física do leitor.

A partir do pontos de interação, a identificação das tecnologias que normalmente são utilizadas na implementação dos componente do medidor de glicose foi direta. Deste modo, as principais tecnologias identificadas são sensor de leitura de glicemia, linguagens de programação para desenvolvimento do aplicativo móvel (geralmente Java, Swift e Kotlin), sistema operacional no qual o aplicativo móvel é executado (Android e iOS), protocolo Bluetooth, protocolo USB, protocolos NFC.

4.2. Modelagem de ameaças

Esta seção apresenta os resultados da etapa de modelagem de ameaças apresentada na Seção 3.2. A modelagem de ameaças foi realizada utilizando o método STRIDE associado a categorização das ameaças propostas na Seção 3.2.3, o que permitiu analisar os medidores de glicose a partir de três pontos de vista: análise do ativo físico, análise dos meios de comunicação com o ativo e interação via aplicativo móvel. Assim, as ameaças identificadas estão relacionadas ao dano à saúde do usuário e são detalhadas a seguir:

Capturar leituras de glicemia: Um agente malicioso pode realizar a obtenção dos dados de leitura de glicemia do usuário do medidor de glicose, interceptando a comunicação entre os componentes do medidor. Por exemplo, enquanto o usuário estiver próximo do agente malicioso, o mesmo pode tentar interceptar a comunicação entre o sensor fixado no corpo da vítima e seu smartphone.

Negação de serviço: Um agente malicioso pode ocasionar uma negação de serviço entre os componentes do medidor, com o objetivo de prejudicar a transmissão e a leitura dos dados de glicemia por parte do usuário. Por exemplo, um agente malicioso pode estar nas proximidades da vítima e utilizar um dispositivo sem fio para gerar interferência na comunicação entre os componentes do medidor.

Injeção de leituras de glicemia falsas: Um agente malicioso pode se aproveitar dos esquemas de comunicação entre os componentes do medidor (Figura 4) para injetar leituras de glicemia falsas, a fim de induzi-lo a ministração incorreta de insulina. Por exemplo, o agente malicioso pode assumir uma posição estratégica, *Man-in-the-middle*, para realizar injetar leituras de glicemia falsas no leitor.

Adulteração do firmware: Um agente malicioso pode realizar uma cópia do firmware original do leitor da vítima e realizar adulterações no código, com objetivo de assumir o controle do dispositivo. Por exemplo, o agente malicioso pode se aproveitar de momentos em que o leitor esteja fora do alcance do usuário para realizar a cópia e, futuramente, a troca pelo firmware adulterado.

As árvores de ataque que fornecem caminhos possíveis que podem ser seguidos por um agente malicioso para identificação/exploração de vulnerabilidades a partir das

ameaças identificadas são mostradas na sequência. Deste modo, a Figura 5 apresenta a árvore de ataque para a ameaça capturar leituras de glicemia. A árvore ilustra que um agente malicioso pode tentar capturar os dados de glicemia do usuário por meio de dois caminhos distintos. No primeiro, um agente malicioso pode obter os dados por meio da interceptação do tráfego entre os componentes do medidor. Para esse processo, o atacante pode utilizar uma ferramenta de captura de tráfego (*sniffer*). Essa ferramenta possibilita analisar o tráfego da comunicação interceptada. Após isso, ele pode fazer uma requisição legítima e observar o reação da aplicação a requisição através do *sniffer*. No segundo caminho, um agente malicioso pode se utilizar do acesso físico a porta USB do leitor para montar a estrutura de diretórios presente no leitor e realizar uma navegação pelos diretórios até encontrar os arquivos que contém os dados de medição de glicemia.

A árvore de ataque relacionada a ameaça de negação de serviço é ilustrada pela Figura 6, na qual um agente malicioso pode se aproveitar da comunicação entre sensor, leitor e aplicativo móvel para negar o serviço de visualização de dados para um usuário legítimo. Para tanto, o agente malicioso precisa estar nas proximidades da vítima e conseguir interceptar o código de pareamento do leitor com o smartphone. Em seguida, a partir do código interceptado, ele irá estabelecer uma conexão entre o leitor da vítima e e um dispositivo e enviará ao leitor inúmeras requisições legítimas a fim de sobrecarregá-lo, até que esse último se torne inoperável. Outra situação de negação de serviço possível é por meio de um dispositivo que realize bloqueio de sinal. Esse dispositivo é usando para gerar interferência (ou ruído) na comunicação sem fio entre os componentes do medidor, impossibilitando a transmissão de dados entre eles.

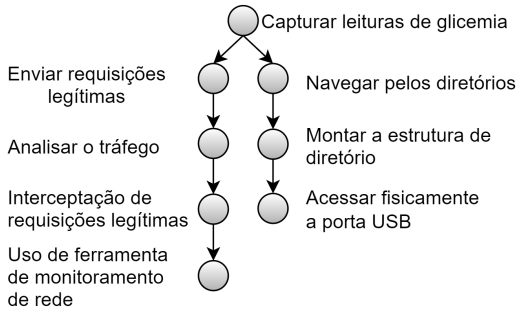

Figura 5. Ameaça: Capturar de Leituras de Glicemia

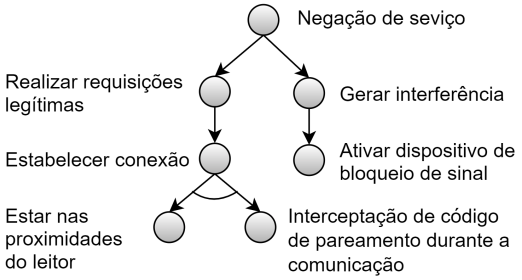

Figura 6. Ameaça: Negação de Serviço

A Figura 7 relata a ameaça que está relacionada a injeção de leituras de glicemia falsas. No ramo mais à esquerda da árvore, um agente malicioso pode utilizar de uma ferramenta de monitoramento de rede para analisar a comunicação entre os componentes do medidor e interceptar requisições legítimas e entender como estão estruturadas. Depois, ele pode montar requisições maliciosas e envia-las, realizando a injeção de leituras de glicemias falsas. O ramo central da árvore é inicializado pelo agente malicioso assumindo uma posição estratégica em relação aos esquemas de comunicação relatados na Figura 4. Essa posição estratégica está vinculada com o objetivo de executar o ataque *Man-in-the-middle* para que, assim, o agente malicioso possa adulterar os parâmetros em requisições legítimas e realizar a injeção de leituras de glicemia falsas. Em outro cenário é efetuada a substituição do sensor vinculado ao leitor da vítima. Um agente malicioso realiza a troca do sensor original por um malicioso, que enviará informações não legítimas,

fazendo com que a vítima tenha acesso a informações falsas disponibilizadas no leitor. No ramo mais à direita é realizada a interceptação do código de pareamento durante a comunicação entre o leitor e aplicativo móvel (smartphone). Nesse cenário, o agente malicioso irá utilizar de uma ferramenta de monitoramento para analisar a comunicação entre o leitor e o smartphone, com objetivo de obter o código de pareamento. Após isso, o agente malicioso poderá vincular o seu aplicativo ao leitor da vítima, possibilitando o envio de requisições maliciosas e a injeção de leituras de glicemia falsas.

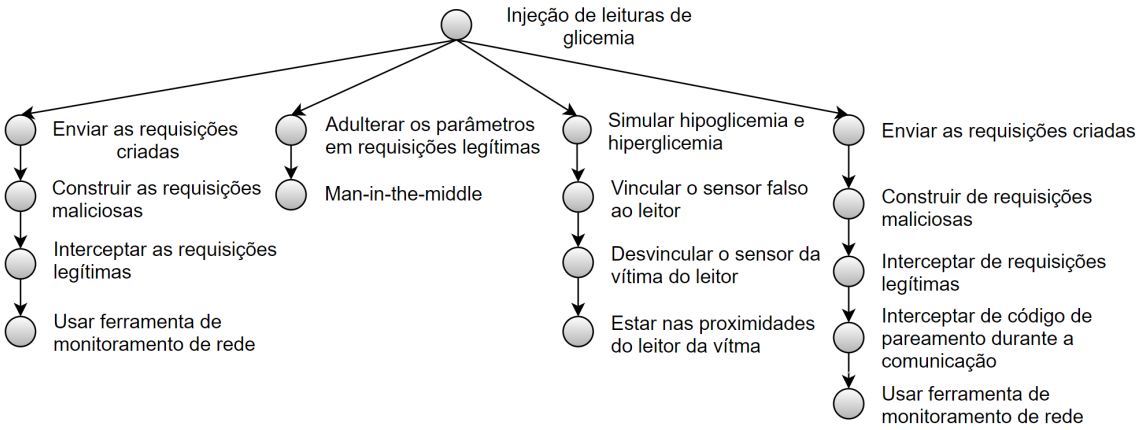

Figura 7. Ameaça: Injeção de Leituras de Glicemia

Na Figura 8 é retratada a ameaça de adulteração de firmware. Nesse cenário, um agente malicioso precisa que o leitor esteja fora do alcance de vítima para que ele possa realizar o acesso físico via USB. Com o acesso, o agente malicioso realiza a cópia do firmware original, executa o processo de engenharia reversa a fim de conhecer mais sobre as funcionalidades disponibilizadas pelo software, realiza alterações no código para que o beneficiem e instala a versão adulterada no leitor da vítima (por meio da interface USB), que não tem noção das atividades maliciosas que estão executadas em seu leitor. Similar a ameaça de adulteração de firmware também pode ser listada a ameaça de identificação de funcionalidades do software por parte de um fabricante de medidores concorrente. O fabricante concorrente pode ter o interesse de obter o código embarcado nos componentes do medidor para conhecer os detalhes de projeto a fim de obter vantagens competitivas, o que pode resultar em perdas financeiras para o fabricante do medidor considerado.

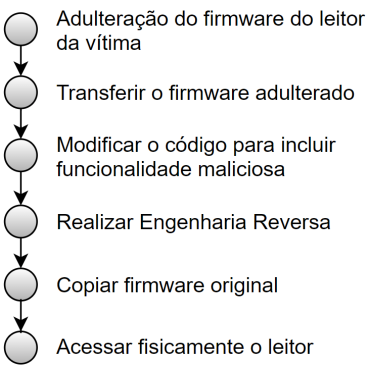

Figura 8. Ameaça: Adulteração de Firmware

5. Conclusão

Neste trabalho, discutimos questões envolvendo o processo de análise de segurança de medidores de glicose. Com a intenção de viabilizar a realização do trabalho, analisamos a presente literatura com enfoque em medidores de glicose. Ainda que tal literatura apresente métodos para tratar outras de classes de dispositivos, tais como marca-passos e bombas de insulinas, a mesma não apresenta diretrizes ou informações de como avaliar a segurança de medidores de glicose. Todavia, por meio da metodologia proposta, foi possível correlacionar informações sobre as funcionalidades básicas dessa classe de dispositivos para obter os requisitos mínimos de segurança e, com base em métodos de modelagem ameaças, foram identificadas diversas ameaças e as ações de ataque que um agente malicioso pode realizar para comprometer a segurança desses dispositivos.

A metodologia proposta serve como um guia para outros trabalhos futuros no que se diz respeito ao processo de identificar ameaças, além de proporcionar um comparativo entre diversos documentos e padrões técnicos de ativos que pertencem a outros ativos de diferentes classes. Ainda sobre trabalhos futuros, existem diversas oportunidades de estudos, como a priorização das ameaças a serem mitigadas, além da avaliação dos riscos associados, dos impactos e das possíveis mitigações provenientes das vulnerabilidades encontradas em testes de segurança realizados a partir do modelo de ameaças proposto.

Referências

ANVISA (2018). Instrução normativa Nº 24, de 17 de maio de 2018. Standard, Agência Nacional de Vigilância Sanitária, Brasil, BR.

Burleson, W., Clark, S. S., Ransford, B., and Fu, K. (2012). Design challenges for secure implantable medical devices. In *DAC Design Automation Conference 2012*, pages 12–17.

Cagnazzo, M., Hertlein, M., Holz, T., and Pohlmann, N. (2018). Threat modeling for mobile health systems. In *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pages 314–319.

Chowdhury, N. M. and Mackenzie, L. (2014). Development of a threat model for vehicular ad-hoc network based accident warning systems. In *Proceedings of the 7th International Conference on Security of Information and Networks*, SIN '14, page 447–458, New York, NY, USA. Association for Computing Machinery.

Chunxiao Li, Raghunathan, A., and Jha, N. K. (2011). Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services*, pages 150–156.

Deogun, D., Johnsson, D. B., and Sawano, D. (2019). *Secure by Design*. O'Reilly.

Instruments, T. (2014). Blood glucose monitor - continuous blood glucose monitor - sensor unit. [Online; accessed 23-July-2020].

Instruments, T. (2015). Microcontrollers in Blood Glucose Meters. Standard, Texas Instruments, United States of America, USA.

Integrated, M. (2010). Important Considerations for Insulin Pump and Portable Medical Designs. Standard, Maxim Integrated, United States of America, USA.

International Diabetes Federation (2020). Demographic and geographic outline. [Online; accessed 06-Abril-2020].

International Electrotechnical Commission (2006). Medical Device Software - Software Life Cycle Processes. Standard, International Electrotechnical Commission, Switzerland, CH.

International Organization for Standardization (2013). In vitro diagnostic test systems — Requirements for blood-glucose monitoring systems for self-testing in managing diabetes mellitus. Standard, International Organization for Standardization, Switzerland, CH.

Laurence Goasduff (2020). Gartner says 5.8 billion enterprise and automotive iot endpoints will be in use in 2020. [Online; accessed 09-Abril-2020].

Matthew Field (2020). Wannacry cyber attack cost the nhs £92m as 19,000 appointments cancelled. [Online; accessed 07-Abril-2020].

Meier, J., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., and Murukan, A. (2003). Chapter 3 – threat modeling. [Online; accessed 21-July-2020].

Nexperia (2013). Glucose Meter Fundamentals and Design. Standard, Nexperia, Netherlands , NL.

Shostack, A. (2014). *Threat Modeling: Designing for Security*. Wiley Publishing, 1st edition.

Sándor, H. and Sebestyén-Pál, G. (2017). Optimal security design in the Internet of Things. In *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*, pages 1–6.

Technology, M. (2013). Glucose Meter Reference Design. Standard, Microchip Technology, United States of Americas , USA.

U.S. Food and Drug Administration (2014). Content of premarket submissions for management of cybersecurity in medical devices. Standard, U.S. Food and Drug Administration, United States of America, USA.

USFDA (2018). Evaluation of automatic class III designation for Dexcom G6 continuous glucose monitoring system. Standard, U.S. Food and Drug Administrationa, United States of America, USA.

Wang, P., Ali, A., and Kelly, W. (2015). Data security and threat modeling for smart city infrastructure. In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pages 1–6.

Yaqoob, T., Abbas, H., and Atiquzzaman, M. (2019). Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review. *IEEE Communications Surveys Tutorials*, 21(4):3723–3768.