Arquitetura de Baixo Custo para Segurança de Gateways em Internet das Coisas

Douglas Galetti Ribeiro
Universidade Federal do ABC, Santo André, SP – Brasil
douglas.ribeiro@aluno.ufabc.edu.br

João Henrique Kleinschmidt
Universidade Federal do ABC, Santo André, SP – Brasil
joao.kleinschmidt@ufabc.edu.br

Abstract:
IoT devices, in general, are not implemented to be secure and this is leading to consequences that affects the whole society with lack of privacy and malfunction. This project aims to point a proper operating system for IoT devices, mainly gateways, and a low-cost architecture to proper secure them. The architecture consists of a secure operating system, UICC as secure element and use of secure boot. Tests and simulations show the proposed low-cost architecture is reliable and able to detect physical attacks on IoT devices and could be used in high-end devices to protect data privacy and device integrity.

1. Introdução

O interesse em torno da Internet das Coisas (Internet of Things em inglês, ou IoT) vem crescendo exponencialmente e as inúmeras possibilidades de aplicação da IoT colocaram esse recurso no topo da transformação digital nos negócios [1,2]. Estima-se que até 2020 cerca de 50 bilhões de dispositivos estarão conectados a internet, sendo estes capazes de monitorar ambientes e executar tarefas de forma autonoma, sem intervenção humana [4]. Esses aparelhos podem ser responsáveis pelo transporte de pessoas, fornecimento de energia, sistemas médicos, transporte público entre outros, e vunerabilidades poderiam causar sérias consequências a esses sistemas, que incluem privacidade de dados violada, perdas econômicas, danos físicos ou colocar a vida de pessoas em risco.

Apesar da segurança em IoT ser um tema de importância, estima-se que cerca de 70% dos dispositivos contém vulnerabilidades. Um dos motivos do valor dessa taxa é a proliferação de plataformas IoT únicas e específicas do dispositivo, pois resultam em sistemas operacionais mal projetados em nível de *hardware* e *software* sem uso de elementos básicos de segurança [4]. As vulnerabilidades não são incomuns e afetam diferentes tipos de dispositivos presentes na Internet das Coisas. Dentre eles, um equipamento muito utilizado e de grande importância é o *gateway*.

Um dos motivos de seu uso frequente é que dispositivos de baixa complexidade, como os sensores e atuadores, coletam dados, mas não possuem poder de processamento para analisá-los. Também possuem um sistema de comunicação que visa a eficiência energética e limita-os ao uso de protocolos de frequências de baixo alcance [5]. Neste cenário, o *gateway* faz a intermediação entre esses dispositivos e a nuvem, ou seja, um sistema ou banco de dados onde as informações serão armazenadas e analisadas. Dessa maneira, ele não expõe os dispositivos IoT diretamente a internet, mas limita-os apenas a rede interna local.

Apesar de um *gateway* exercer funções de controle e comunicação de dispositivos IoT, ele é afetado dos mesmos problemas que estes, com vulnerabilidades em *software* e *hardware*. Pouco exploradas, as vulnerabilidades de *hardware*, relacionadas ao ataque físico ao dispositivo, são comuns e as soluções demandam altos custos com o uso de elementos seguros proprietários que adicionam segurança na camada física do aparelho. Esses custos muitas vezes inviabilizam a implementação segura do dispositivo e muitas vezes a segurança fica em segundo plano, consequentemente, vulnerabilidades não são tratadas de forma adequada.

O objetivo deste artigo compreende o uso de um sistema operacional seguro que possa ser utilizado em um *gateway* para segurança em nível de *software*; o uso de elemento seguro para segurança em nível de *hardware*; e inicialização segura para garantir a integridade do dispositivo. Propõe a implementação de arquitetura de baixo custo e realiza simulações para validação da proposta.

2. Fundamentação Teórica

A segurança em IoT é um dos muitos desafios existentes para que ocorra a adoção e desenvolvimento desses dispositivos. Esses objetos possuem vulnerabilidades únicas e variam segundo a atividade que realizam, mas compartilham de problemas semelhantes: (i) diferentes tipos de sistemas operacionais; (ii) não há padronização em termos de segurança do dispositivo; (iii) muitos protocolos são de uso proprietário; (iv) arquiteturas heterogêneas e

segurança física comprometida; (v) a integridade de software, com uso de atualizações, não é garantida; (vi) segurança da informação armazenada não é garantida considerando-se confidencialidade, autenticidade e integridade [2]. Em grande parte, esses fatores determinam as razões que tornam os dispositivos IoT vulneráveis a ataques diversos, mesmo aqueles com poder alto de processamento, chamados de *high-end devices* ou *Class 2* [7].

O *gateway* faz parte dos dispositivos *high-end*, e é amplamente utilizado para se conectar a outros objetos IoT, tendo se tornado alvo de ataques remotos. Entretanto, esses objetos ficam a maior parte do tempo em lugares não vigiados, e favorece o ataque físico; a comunicação é sem fio, e ataques como "*man-in-the-middle"* são utilizados com frequência; e muitos dispositivos conectados a ele possuem recursos de energia e processamento escassos que impossibilita a implementação de segurança adequada [4,5]. Portanto, o *gateway* tem papel importante em obter os dados de outros dispositivos, além controlar e garantir a atualização remota deles. Se o *gateway* for comprometido, os demais dispositivos conectados a ele estarão vulneráveis. Portanto, o uso de segurança adequada do *gateway* em nível de *software* e em nível de *hardware* é necessária.

O uso de sistemas operacionais projetados para assegurar atualizações constantes, uso de chaves criptográficas e meios para melhorar a segurança para garantir a confidencialidade, integridade e autenticidade do dispositivo, não são suficientes [3], pois atuam em nível de *software*. Muitos ataques são realizados em nível de *hardware*. Há diversos exemplos como a adulteração de um dispositivo através do acesso físico; a extração de chaves criptográficas; alteração do sistema operacional; captura do dispositivo IoT para criar uma réplica que substitua o original; injetar um código malicioso diretamente no dispositivo sem necessidade de acesso remoto [8].

Um elemento seguro, isto é, a combinação de *hardware* e *software*, interfaces e protocolos instalados em um dispositivo, permitiria o armazenamento seguro de dados sensíveis como chaves simétricas e identidade do objeto [9]. A união de *software* e *hardware* é necessária para garantir a segurança adequada do dispositivo. É preciso de: (i) um sistema operacional adequado; (ii) uso de elemento seguro; (iii) inicialização segura para permitir a verificação da integridade do *software* com o uso de informações contidas no elemento seguro [11].

Diferentes sistemas operacionais estão disponíveis no mercado, mas poucos projetados exclusivamente para IoT com foco em segurança. Dentre eles, possível de utilizar em *gateways* e sem custo, o Ubuntu Core. Este sistema operacional possui características de interesse: canal de atualização seguro; atualizações frequentes; regras de interação entre aplicações; garantia de *rollback* em uma atualização má sucedida; e o acesso remoto ao dispositivo com uso de chaves assimétricas é padrão [10]. Dos elementos seguros, o *UICC* (*Universal Integrated Circuit Card*) é, do ponto de vista de segurança, resistente a violação (*tamper-proof)*, característica que o torna útil para armazenamento de informações somente leitura, como chaves públicas [9,10]. O uso da inicialização segura realiza a verificação de integridade e segurança do dispositivo com base em informações contidas no elemento seguro e no sistema operacional.

3. Materiais e Métodos

Para o estudo da segurança em *gateway* foi necessário o uso de um computador capaz de executar virtualização; um Raspbery Pi 3B e um cartão de memória *microSD*. Os métodos se concentram em duas partes: (i) proposta de arquitetura de segurança para um *gateway*; (ii) simulação dessa arquitetura com uso do programa Virtual Box 5.2 para instalação do Ubuntu Core 16 e um computador hospedeiro Linux Deepin 15.6.

3.1. Proposta de Arquitetura de Segurança para um Gateway

O sistema operacional utilizado para a proposta de arquitetura de segurança para um *gateway* foi o Ubuntu Core, pois apresenta características que são requisitos no uso desse tipo de dispositivo IoT, como atualizações regulares, políticas de segurança e privacidade, variedade de protocolos de comunicação disponíveis e portabilidade de aplicações. Testes prévios foram realizados para estudar o sistema operacional e um teste de invasão foi realizado para verificar a necessidade de implementar meios de segurança em nível de *hardware* ao dispositivo. A invasão do dispositivo consistiu da remoção do cartão *microSD* do Raspberry Pi, inserção deste em um computador onde os dados pudessem ser acessados e uma nova chave pública não autorizada foi inserida junto a chave pública original, de maneira a permitir acesso remoto de um usuário não autorizado ao dispositivo.

Verificada a vulnerabilidade existente, para garantia de segurança adicional do dispositivo a ataques virtuais e físicos uma arquitetura é proposta e contém os elementos: (i) sistema operacional Ubuntu Core; (ii) *UICC* como elemento seguro*;* (iii) inicialização segura. Nesta arquitetura, o sistema operacional possui características que garantem o funcionamento seguro das aplicações instaladas com o uso de políticas de segurança e certificados digitais para aplicações. O *UICC* é responsável por armazenar três informações de importância: dois *hash* assinados e uma chave pública utilizada para acesso remoto ao dispositivo. Essa chave faz parte de um par de chaves assimétricas. Os *hash* são gerados a partir de uma função MD5. O primeiro *hash* corresponde ao ID do dispositivo e

o segundo corresponde ao caminho do diretório do *UICC* no dispositivo. Após gerados os *hash*, estes são assinados com a chave privada e os *hash* assinados são armazenados na BIOS do *gateway* e no *UICC* (Fig 1).

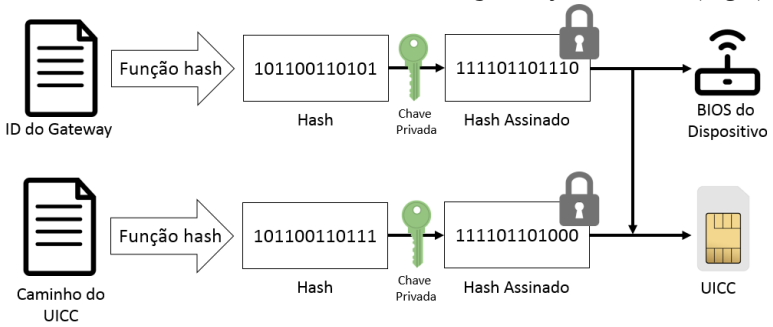

Fig. 1. Representa a criação de *hash* assinado e seu armazenamento. O *hash* do ID do dispositivo é assinado e armazenado na BIOS do dispositivo e no *UICC*. A *hash* do caminho do *UICC* do sistema operacional é assinado e armazenado apenas no *UICC*.

Quando o dispositivo é inicializado, a BIOS é executada e esta fará as validações do ID do dispositivo e do caminho do diretório onde está contida a chave pública, neste caso, UICC. A primeira validação consiste em utilizar a chave pública contida no elemento seguro para decriptografar o *hash* do ID do dispositivo presente também no elemento seguro e assim verificar a correspondência deste *hash* com o *hash* presente na BIOS. A segunda validação é semelhante, porém compara se o caminho do diretório do UICC atual é o mesmo provisionado no elemento seguro UICC (Fig. 1.b). Se ambas as validações ocorrem com sucesso, a BIOS inicia o sistema operacional, caso contrário desliga o dispositivo.

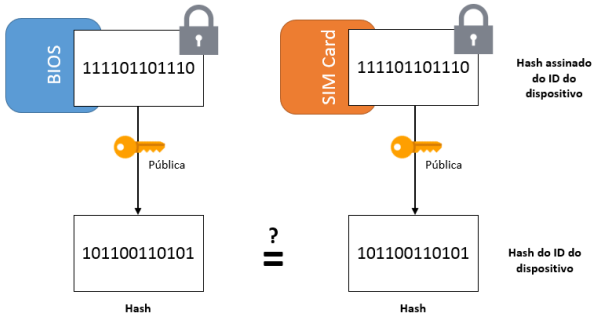

Fig. 2. O processo de inicialização segura corresponde a verificação do *hash* assinado presente na BIOS com o hash assinado presente no *UICC*. Se ambos forem iguais, a assinatura é válida. Processo semelhante ocorre com o caminho do *UICC* definido no sistema operacional.

3.2. Simulação da Arquitetura de Segurança para um Gateway

Com o uso de virtualização, o Ubuntu Core é instalado em uma máquina virtual. Nas configurações do dispositivo é modificado o diretório padrão da chave pública para o diretório correspondente ao *UICC*. Os *hash* e as chaves assimétricas são gerados pelo sistema hospedeiro e inseridos neste diretório, configurado para ser somente leitura. O sistema hospedeiro simula a BIOS. Ele responsável pelo processo de verificação dos *hash* e inicialização da máquina. Essa verificação é realizada como mencionado anteriormente, entretanto, o hospedeiro monta o Ubuntu Core virtualizado, procura pelo *UICC* e realiza as etapas de verificação. Se validadas, aciona o programa Virtual Box e inicia o sistema operacional virtualizado. Durante a simulação, houve uma tentativa de inserção de uma nova chave pública não autorizada no dispositivo. Também a mudança de diretório do *UICC* para outro com o intuito de burlar a inicialização do dispositivo para que este utilizasse uma chave pública indevida e permitisse acesso não autorizado no dispositivo.

4. Resultados

Ao considerar os requisitos de uso em um *gateway* IoT, dentre os sistemas operacionais, o Ubuntu Core apresentou características de interesse em segurança de internet das coisas que contribuem para a segurança em nível de *software* do dispositivo como políticas se segurança e atualizações regulares, e características secundárias relevantes ao projeto como código aberto e ser gratuíto. O acesso remoto indevido é dificultado pelo sistema operacional e contribui para conter ataques remotos, entretanto, a integridade do dispositivo poderia ser afetada com ataques

físicos ao objeto. O *UICC* é de baixo-custo (preço inferiror a R$30,00 com leitor) e possui atributos que podem ser explorados para uso em IoT como resistência a violação de dados. Na simulação, um ataque físico para inserção de uma nova chave pública foi impossibilitado. No segundo ataque, com mudança do diretório do elemento seguro, o dispositivo não foi acionado, pois a BIOS detectou inconsistência nos *hash* do caminho do diretório original e do diretório malicioso.

5. Discussão

As análises e simulações realizadas mostram que o sistema operacional, mesmo que tenha sido projetado para IoT, é incapaz de suprir requisitos de segurança não relacionados a *software*. O ataque físico utilizado para inserir uma nova chave pública no dispositivo e o consequente acesso remoto indevido, corrobora com essa afirmação e com outros estudos sobre o assunto. Fez-se necessário o uso de outros meios para garantia de segurança do *gateway*.

Existem diversas empresas que vendem dispositivos IoT e muitas vezes o investimento para assegurar a integridade destes objetos é alto devido ao elevado custo de utilização de elementos seguros proprietários. O uso do *UICC* como elemento seguro poderia contribuir de forma significativa para que mais empresas implementassem a segurança adequada em dispositivos *high-end*. A simulação da arquitetura proposta serve de evidencia a esse fato e poderia ser adaptada a outros dispositivos do mesmo tipo o que contribuiria positivamente para a inserção de mais dispositivos IoT seguros no mercado a um baixo custo.

6. Conclusões

Implementar um dispositivo IoT, seja um *gateway* ou mesmo um robô, exige o uso de dispositivos com poder de processamento elevado, porém permite o uso de métodos de segurança robustos. Apesar dos esforços realizados para melhoria da segurança em objetos IoT, a implementação adequada, seja em nível de *software* ou *hardware*, é custosa e muitas vezes evitada, o que colabora para que mais dispositivos sejam levados ao mercado consumidor sem a segurança adequada e com vulnerabilidades que podem gerar consequências aos usuários.

A arquitetura proposta é uma simplificação de outras arquiteturas proprietárias e poderia ser implementada em projetos que usam dispositivos considerados *high-end*, principalmente pelo baixo custo de implementação. A escolha do sistema operacional para internet das coisas e elemento seguro de baixo custo alinhado com uso de inicialização segura, proporcionam segurança extra em nível de *software* e *hardware*.

O próximo passo do projeto é implementar essa arquittura em um *hardware*, utilizar o *UICC*, implementar a inicialização segura e realizar novos testes de segurança para medir a eficiência da arquitetura proposta.

Referências

[1] R. H. Weber, "Internet of things – new security and privacy challenges," Computer Law & Security Review, vol. 26, 23-30 (2010).

[2] J. F. Wan, H. H. Yan, H. Suo, and F. Li, "Advances in cyber-physical systems research," KSII Transactions on Internet and Information Systems, 1891-1908 (2011).

[3] O. Bello, S. Zeadally, and M. Badra, "Network layer interoperation of device-to-device communication technologies in internet of things (iot)," Ad Hoc Networks, Special Issue on Internet of Things and Smart Cities: security, privacy and new technologies, vol. 57, 52 – 62 (2017).

[4] A. Todman, "Privacy in the age of big data: recognizing threats, defending your rights and protecting your family," Archives and Records, vol. 37:1, 113-115 (2016).

[5] R. Shujaee and Prof. M. Nasiruddin, "Optimization of A Smart IOT Gateway," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 5, Issue 7, 494-501 (2017).

[6] J. Deogirikar and A. Vidhate, "Security Attacks inIoT: A Survey," IEEE International conference on I-SMAC, 32-37 (2017).

[7] O. Hahm, E. Baccelli, H. Petersen and N. Tsiftes, "Operating Systems for Low-End Devices in the Internet of Things: A Survey," IEEE Internet of Things Journal, vol. 3, no. 5, 720-734 (2016).

[8] H. A. Abdul-Ghani and D. Konstantas, "A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model," International Journal of Advanced Computer Science and Applications, vol. 9, 355-373 (2018).

[9] M. Reveilhac and M. Pasquet, "Promising Secure Element Alternatives for NFC Technology," First International Workshop on Near Field Communication, Hagenberg, 75-80 (2009).

[10] D. Forsberg, G. Horn, W. Moeller and V. Niemi,"LTE security," John Wiley and Sons Ltd (2010).

[11] W. Arbaugh, A.D. Keromytis, D.J. Farber and J.M. Smith, "Automated Recovery in a Secure Bootstrap Process," (2012).