SEGURANÇA NO CONTEXTO DE INTERNET DAS COISAS

Fabíola Maria Kretzer – 16100725
Aluna da da disciplina INE5414 – Redes de Computadores I
do Departamento Informática e Estatística da Universidade Federal de
Santa Catarina
Florianópolis, 12 de Agosto de 2017

Resumo

Será abordado sobre uma tecnologia que está cada vez mais presente no cotidiano das pessoas, a Internet das Coisas(IoT). É uma revolução tecnológica com a finalidade de que cada vez mais equipamentos como eletrodomésticos e meios de transporte sejam conectados a Internet e até mesmo a outros dispositivos, como smartphones e computadores. Mas a IoT traz enormes desafios para sua implementação no mundo real. Um desses desafios é a questão de segurança e privacidade. Com isso, este artigo busca ressaltar os principais problemas e comentar possíveis soluções.

1.Introdução

1.1.Motivação

Com a queda de preços de sensores, vem ocorrendo a popularização dos serviços de armazenamento remoto e a big data. A facilidade de acesso à esses recursos também tem fortalecido uma tendência que está cada vez mais presente em nossas vidas: o IoT (Internet of Things). Como o ser humano está sempre evoluindo, há a busca constate por tecnologias para melhorar a qualidade de vida do ser humano, mas a segurança não evoluiu, e as pessoas devem tomar muito cuidado na utilização desses dispositivos, pois podem se tornar perigosos e acabar com a privacidade das pessoas que as utilizam.

1.2.Justificativa

A IoT tem causado causado muitas transformações na vida das pessoas e das empresas, que cada vez mais estão interligadas com a Internet das Coisas, isso significa que mais informações pessoais e de negócios serão passadas na nuvem e, com isso, surgem novos riscos de segurança e tipos de ataques. Assim com o aumento da automatização de serviços essenciais, dados pessoais são transferidos para os dispositivos com acesso a internet, aumentando a vulnerabilidade e precisando aumentar a segurança na medida com que as informações na nuvem cresce.

1.3.Objetivos

1.3.1.Objetivos específicos

A Internet das Coisas é um novo paradigma que envolve muitas muitas aplicações e possui um impacto muito grande na privacidade da pessoas. Assim, objetivo desse artigo é entender as vulnerabilidades e desenvolver ideias e aplicações que podem melhorar a segurança dessa tecnologia.

1.3.1.Objetivos gerais

- Apresentar dificuldades em solucionar as vulnerabilidades em IoT.
- Apresentar ideias atuais e futuras para aumentar a segurança na Internet das Coisas.

1.4.Organização do artigo

O presente artigo encontra-se organizado da seguinte forma: na seção 2 serão discutidos os principais conceitos de Internet das Coisas com enfase na parte de segurança e de algumas dificuldades atuais. Na seção 3 serão apresentados alguns trabalhos correlatados com o tema deste artigo.

2. Conceitos básicos

Nas próximas subseções são apresentados alguns conceitos abordados no contexto do artigo.

2.1. Internet das Coisas (IoT)

Internet das Coisas é um conceito tecnológico que interliga objetos do cotidiano das pessoas com a internet. Tem como finalidade facilitar a vida das pessoas, fazendo com que tarefas diárias possam ser feitas com a ajuda de um dispositivo. As aplicações podem envolver desde a área da saúde, até organização pessoal. É um conceito que está sendo capaz de mudar o jeito como o ser humano vive, pensa e trabalha. Funciona com o uso de sensores inteligentes e software que transmitem dados por rede, assim várias coisas estão conectadas e se comunicam umas com as outras e também com o usuário, possibilitando a troca de informações via internet. A alguns anos atrás poderia se pensar que era apenas uma utopia ou um delírio de alguns pesquisadores que defendiam esse assunto. Mas vem evoluindo muito e hoje já é realidade em muitas partes do mundo. Como em casas inteligentes que tem uma conexão entre vários eletrodomésticos, e possui software responsável por gerenciar toda a casa e ainda podem estar conectados com outros lugares, tornando-se uma cidade inteligente,

que por exemplo, avisa o supermercado que a geladeira está vazia, para entregar mais comida ou que avisa o caminhão do lixo que a lixeira está vazia, para ir coletar, e muitas outras coisas simples do cotidiano que podem ser automatizadas.

Segundo o autor Rolf H. Weber (2010), a Internet das coisas (IoT) é uma internet global emergente baseada na arquitetura da informação que facilita a troca de bens e serviços em redes de suprimentos globais. E tem o objetivo de fornecer uma infraestrutura de modo a facilitar o intercâmbio de “coisas” de forma segura e confiável. Pode-se dizer que o amadurecimento dessa nova tecnologia deve-se ao fato do barateamento de sensores, que é a base para um sistema inteligente funcione.

2.2 Computação em nuvem

A computação em nuvem refere-se à utilização da memória e da capacidade de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet. O armazenamento de dados é feito em serviços que poderão ser acessados de qualquer lugar do mundo, a qualquer hora, não havendo necessidade de instalação de programas ou de armazenar dados. O acesso a programas, serviços e arquivos é remoto, através da Internet - daí a alusão à nuvem.(Wikipédia)

Figura 1 – Esquemático de computação em nuvem

Fonte:<https://pt.wikipedia.org/wiki/Ficheiro:ComputaC3%A7%C3%A3o_em_nuvem.svg>

Mesmo sem perceber as pessoa estão utilizando a computação em nuvem, seja utilizando um serviço online como e-mail, jogos e vídeos ou armazenando arquivos. Há alguns anos atrás, a aposta era a de que ninguém mais precisaria instalar programa algum em seu computador para realizar desde tarefas básicas até trabalhos mais complexos, pois tudo seria feito pela internet.(Danilo Amoroso)

2.3 Segurança em IoT

A segurança em IoT está ligada a proteção dos dados de seus usuários. Na medida do aumento no uso de Internet das Coisas, mais informações pessoais e de negócios são passadas na nuvem. Assim, surgem cada vez mais problemas relacionados a segurança desse novo paradigma, pois essa tecnologia cresceu mas a segurança que está ao redor dela, não.

Para o autor Paulo Gaona-García, a necessidade de criar redes que interagem com dispositivos ligados à internet, privacidade e a proteção de dados é substancial. Portanto, a segurança da informação é um aspecto bem conhecido, devido a dispositivos conectados à internet estarem crescendo rapidamente, o que representa um aumento de exposição nos dados no rede.

Seema Nath e Subhranil Som também ressaltam questão de que a confidencialidade dos dados privados dos usuários devem ser assegurados, uma vez que os dispositivos também esta gerenciando informações confidenciais.

Um dos problemas diz respeito à “atribuição de tags a objetos que pode não ser conhecida por usuários, e pode não haver um sinal acústico ou visual para chamar a atenção do usuário do objeto. Por isso, indivíduos podem ser seguidos sem que eles saibam disso e deixar seus dados ou, pelo menos, seus vestígios no ciberespaço. Mais agravando o problema, não é mais apenas o estado que está interessado em colecionar os respectivos dados, mas também atores privados, como empresas de marketing.”(Rolf H. Weber ,2010)

3. Trabalhos Correlatos

3.1 Primeiro trabalho correlato

Os autores Gaona-García, Montenegro-Marin, Prieto e Nieto (2017) apresentam em seu artigo “Analysis of Security Mechanisms Based on Clusters IoT Enviroments” uma análise da revisão sistemática de artigos sobre Internet das Coisas (IoT), aspectos de segurança como privacidade e controle de acesso e também analisa questões de segurança que devem se abordados e identificados nesse novo paradigma. Também é apresentado o estado da arte com enfase em segurança da Internet das Coisas, alguns aspectos envolvidos, análise de alguns conceitos e segurança no desempenho. É relatado neste artigo um sistema de segurança que propõe neutralizar vulnerabilidades no IoT utilizando PKI que permitem autenticação de identidade baseada em uma chave pública combinada,

dando solução para a quantidade excessiva de autenticações. Ao analisar o reconhecimento de impressão digital, foi proposto um modelo com três camadas; sensor, transporte e aplicação, permitindo assim poder analisar cada camada de forma separada. É proposto também um sistema RFID ligada com uma memória junto com um micro-chip, com o objetivo de receber sinais e devolver com alguns sinais à mais. Atualmente uma das medidas chave na a segurança em IoT a proteção de informações que viajam através da Internet. Na maioria dos casos, esta informação viaja através de redes sem fio ou através de redes públicas, que são vulneráveis a serem atacadas. Se o canal de comunicação não estiver adequadamente protegido por criptografia os dados, podem serem fáceis para um invasor realizar ataques. Assim, as pessoas que atacam a rede podem obter toda a informação que querem e ainda alterar o comportamento ou o desempenho do dispositivo. Para o futuro, estão previstos a cara caracterização de problemas envolvendo Internet das Coisas para que agentes inteligentes possam realizar a identificação adequada dos problemas que acontecem com mais problemas e assim facilitar a identificação de segurança e melhorar a sua implantação na resolução de problemas.

3.2 Segundo trabalho correlato

Segundo os autores Patra e Udai (2016) em seu artigo "Internet of Things—Architecture, applications, security and other major challenges" os equipamentos físicos equipados com sensores atuam no poder da computação. Para ele o conceito de Internet das Coisas é uma noção de "objetos inteligentes" que precisam de sensores conectado à microprocessadores para funcionar. Para os autores esses "objetos inteligentes" estarão no futuro em várias áreas, como a saúde, a automação residencial, o transporte, entre outros, assim estes dispositivos coletam dados, os analisam e iniciam ações, dependendo do ambiente ondo estão instalados. Apesar da IoT trazer muitos benefícios para as pessoas que utilizam esse sistema o artigo discute vários desafios e ameaças de segurança. O estado atual da Internet está passando por uma revolução que trará sob suas redes transparentes de objetos inteligentes interconectados cada a capacidade de reunir informações e interagir com o mundo real e fazer uso da internet existente. Essas coisas inteligentes prestam ajuda e exigem grande quantidade de dados pertencentes ao usuário. Os dados pessoais recolhidos por estes sistemas são habilitadas pelo sensor devido ao monitoramento contínuo do ambiente de implantação que podem representar sérias ameaças à privacidade e à segurança dos usuários. A presença dessas vulnerabilidades no IoT exige atenção imediata dos pesquisadores na busca de métodos para proteger a privacidade dos dados pessoais. Apesar da IoT misturar o mundo real e o virtual de forma perfeita os autores estão preocupados com o aumento da insegurança e das vulnerabilidades nessa tecnologia e afirmam que se continuar a aumentar pode ofuscar muitos os benefícios da Internet das Coisas.

3.3 Terceiro trabalho correlato

Segundo os autores Sicari, Rizzardi, Grieco e Coen-Porisini em seu artigo “Security, privacy and trust in Internet of Things: The road ahead” no cenário da Internet das Coisas a satisfação dos requisitos de segurança e privacidade é fundamental para essa nova tecnologia. Esse requisitos podem incluir confiabilidade dos dados, controle de acesso pela rede IoT, privacidade e confiança dos usuários com os objetos e políticas de privacidade. Para os autores são necessárias medidas flexíveis que são capazes de resolver ameaças de segurança que atacam a rede. A IoT se aproximou das pessoas rapidamente na última década por meio de tecnologias de sistemas de comunicação sem fio como RFID, WiFi, 4G, IEEE 802.15.x, entre outros que se tornou crucial na vida das pessoas. Os autores relatam que no ponto de vista lógico, um sistema IoT pode ser representado como uma coleção de dispositivos inteligentes que interagem em uma colaboração racional para cumprir um objetivo comum. As implementações da IoT podem adotar diferentes arquiteturas de processamento e comunicação, tecnologias e além metodologias de design, com base em seu alvo. Por exemplo, o mesmo sistema IoT poderia aproveitar as capacidades de um rede de sensores sem fio (WSN) que coleta informações do ambiente em uma determinada área e um conjunto de smartphones em cima dos quais aplicativos de monitoramento corre. Os esforços de pesquisa estão voltados para enfrentar os problemas de segurança e privacidade na IoT e das tecnologias de comunicação em geral. Outro campo de pesquisa é o da segurança IoT em dispositivos móveis, que cada vez mais se difundem hoje pelo mundo. Muitos esforços foram (e estão sendo) gastos pelo mundo comunidade científica para melhorar sistemas abordados acima.

3.4 Quarto trabalho correlato

Segundo os autores Ahlmeyer e Chircu (2016) em seu artigo “SECURING THE INTERNET OF THINGS: A REVIEW” a próxima evolução da Intenet das Coisas é conectar bilhões de outros dispositivos para a Internet. Isso permitirá que as empresas coletem dados de seus clientes e produtos para melhorar a qualidade do atendimento e fazer uma maior organização das necessidades da empresa e do cliente, trazendo mais satisfação aos dois. Mas essa facilidade tem um preço, a insegurança. Especialistas na área dizem que apesar de ter grande importância nos negócios, a IoT está atrasada quando se refere na implantação de medidas para a melhoria da segurança dos usuários. Uma análise dos autores, identifica três grandes problemas, a falta se segurança em implementações de IoT, a falta de diretrizes detalhadas e padrões de segurança em TI e a falta de leis e regulamentos referente a Internet das Coisas em nível nacional e internacional. O IoT utiliza tecnologias como identificação por radiofrequência (RFID) e sensores para conectar "coisas" no ambiente à internet. Neste contexto, uma coisa pode ser, por exemplo, o monitor de casa de alguém, um rastreador, um aparelho, uma máquina industrial ou um carro, que pode coletar dados sobre seu desempenho ou localização, salvá-lo e processá-lo localmente ou em um servidor e criar alertas com base em regras pré-definidas, como um carro que alerta o usuário quando a pressão do pneu é muito baixa. As projeções atuais indicam que o número de tais dispositivos conectados à IoT irá aumentar significaticamente, mas a segurança relacionada com essa tecnologia, não. Isso traz

muitos problemas ligados a privacidade. A pesquisa acadêmica futura pode avançar nossa compreensão dos conceitos relacionados a IoT, identificando barreiras técnicas e econômicas. As práticas de segurança da IoT e os desafios de desenvolver e adotar a segurança atualmente estão tentando descobrir maneiras de melhorar a privacidade.

Referências Bibliográficas

[1] GAONA-GARCÍA, Paulo et al. Analysis of Security Mechanisms Based on Clusters IoT Enviroments. 2017.International Journal of Interactive Multimedia and Artificial Intelligence. Disponível em: <http://www.ijimai.org/journal/sites/default/files/files/2016/08/ijimai20174_3_8_pdf_20224.pdf>. Acesso em: Agosto 2017.

[2] Nath, Seema, and Subhranil Som. "Security and Privacy Challenges: Internet of Things." *Indian Journal of Science and Technology* 10.3 (2017). Disponível em: <http://52.172.159.94/index.php/indjst/article/view/110642>. Acesso em: Agosto de 2017

[3] MAHYAR, Taj Dini; SOKOLOV, V. Yu. Internet of things security problems. **Сучасний захист інформації**, n. 1, p. 120-127, 2017. Disponível em: <http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/szi_2017_1_21.pdf>. Acesso em: Agosto de 2017

[4] Goeke, Lisa. "Security Challenges of the Internet of Things." (2017). Disponível em: <https://www.theseus.fi/bitstream/handle/10024/128420/Goeke_Lisa.pdf?sequence=1> . Acesso em: Agosto de 2017

[5] Patra, Litun, and Udai Pratap Rao. "Internet of Things—Architecture, applications, security and other major challenges." *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on*. IEEE, 2016. Disponível em: <https://www.researchgate.net/profile/Udai_Pratap_Rao/publication/308886519_Internet_of_Things_-_Architecture_Applications_Security_and_other_Major_Challenges/links/57f4a16d08ae91deaa5ae4ed.pdf>. Acesso em: Agosto de 2017

[6] Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava. "Security in internet of things: Challenges, solutions and future directions." *System Sciences (HICSS), 2016 49th Hawaii International Conference on*. IEEE, 2016. Disponível em: <http://tarjomefa.com/wp-content/uploads/2016/09/5288-English.pdf>. Acesso em: Agosto de 2017

[7] Ahlmeyer, Matthew, and Alina M. Chircu. "SECURING THE INTERNET OF THINGS: A REVIEW." *Issues in Information Systems* 17.4 (2016). Disponível em: <http://www.iacis.org/iis/2016/4_iis_2016_21-28.pdf>. Acesso em: Agosto de 2017

[8] SICARI, Sabrina et al. Security, privacy and trust in Internet of Things: The road ahead. **Computer Networks**, v. 76, p. 146-164, 2015. Disponível em: <http://tarjomefa.com/wp-content/uploads/2016/07/5009-English.pdf>. Acesso em: Agosto de 2017

[9] WEBER, Rolf H. Internet of Things–New security and privacy challenges. **Computer law & security review**, v. 26, n. 1, p. 23-30, 2010. Disponível em: <https://www.researchgate.net/profile/Rolf_Weber3/publication/222708179_Internet_of_Things_-_New_security_and_privacy_challenges/links/0c96053cab03fee371000000.pdf>. Acesso em: Agosto de 2017

[10]Wikipédia, a enciclopédia livre (2016). Disponível em: <https://pt.wikipedia.org/wiki/Computa%C3%A7%C3%A3o_em_nuvem>. Acesso em: Agosto de 2017.