Internet das Coisas: Segurança e Privacidade

No âmbito de Sistemas de Comunicação e Redes

2º ano de Licenciatura de Ciência da Computação

Catarina Quintas (A91650), David Machado (A91665), Inês Presa, (A90355)

Universidade do Minho, Departamento de Ciências, 4710-057 Braga, Portugal

Abstract. A Internet das Coisas tem a vindo tornar-se bastante relevante. Cada vez mais existem dispositivos IoT, quer sejam *smart TVs*, *smartwatches* ou campainhas inteligentes. Estes dispositivos facilitam o dia-a-dia, mas também acarretam riscos de segurança e de invasão de privacidade. Neste trablho foi conduzida uma análise das implicações dos IoT na segurança e privacidade do utilizador.

Keywords: Internet das coisas (IoT), Segurança, Privacidade

1 Introdução

A internet das coisas, também conhecida como IoT (do inglês *Internet of Things*), trata-se de um conceito que foi introduzido em 1999 por Kevin Ashton. Este apresenta-se como a rede de dispositivos que estão conectados entre si, recolhendo e partilhando informações para executar determinadas funções com o mínimo de intervenção humana. Exemplos desta tecnologia estendem-se desde relógios que registam batimentos cardíacos, carros automáticos até aspiradores-robôs. [1]

Este é um conceito de tal forma indissociável dos tempos de hoje que se estima que no final do ano 2019 haveriam aproximadamente 9.7 biliões de dispositivos conectados e até ao ano de 2030 este número aumentará para os 24.1 biliões**.** [3]

2 Internet das Coisas

A história da internet das coisas surgiu em 1999, pelo criador Kevin Ashton quando apresentou um sistema de sensores que conectavam o mundo físico com a internet enquanto trabalhava em identificação por rádio frequência (RFID) que permitia que informações fossem transmitidas de maneira independente através da frequência de rádio, sem a necessidade de uma rede de fios ou de um leitor.

De uma forma simplificada, o termo Internet das Coisas consiste na interação de 2 mundos: o digital e o físico. Assim, está compreendido neste conceito, qualquer

tipo de aparelho físico, que convencionalmente não é considerado um computador, ao qual se incrementa um sensor e a capacidade de recolher e partilhar dados pela rede. Consequentemente, com o armazenamento e processamento dos dados recolhidos é possível que esses dispositivos nos proporcionem informações úteis e fidedignas (exemplo de um carro que nos informa sobre o estado do trânsito), ou até mesmo executem e/ou adaptem a sua resposta em função do meio (um carro que executa uma travagem de emergência na deteção de um obstáculo).

Alguns exemplos de dispositivos IoT são frigoríficos inteligentes, aspiradores automáticos, sensores de irrigação para a agricultura, *smartwatches* com GPS e medição dos batimentos cardíacos, lâmpadas com ligação *wi-fi*, carros autónomos, entre muitos outros exemplos. O seu uso está de tal forma generalizado que tem impacto em todos os segmentos da sociedade e contribui positivamente ao nível da segurança, saúde, agricultura, indústria, transportes, energia, entre outros sectores.

2.1 Existem 4 modelos básicos de comunicações de IOT:

Device to Device. Este modelo consiste na comunicação direta entre 2 ou mais dispositivos entre si, trocando dados e informações para cumprir a função desejada, sem ter a intervenção de intermédios. Esses dispositivos podem comunicar de várias formas tais como: tipos de redes, redes IP ou a Internet. Também podem usar protocolos como *Bluetooth*, *Z-Wave* ou *ZigBee* para estabelecer comunicações diretas entre os dispositivos em questão. Geralmente, *Device to device* é utilizado em aplicações de sistemas de automação das nossas casas pois estes necessitam de uma baixa taxa de dados para enviarem informações entre si. Alguns dos dispositivos IoT que recorrem a este modelo são lâmpadas, interruptores de luz, termostatos e fechaduras de portas.

Device to Cloud. O modelo de comunicação de dispositivo para *cloud*, o dispositivo conecta-se diretamente a um serviço de *cloud* da Internet para estabelecer trocas de dados e controlar as mensagens. Essa comunicação pode ser feita através de *Ethernet* com fio tradicional ou conexões *Wi-Fi*, permitindo assim uma conexão entre o dispositivo e a rede IP, que por fim se ligará ao serviço da nuvem. Um dos exemplos mais populares é a *Samsung SmartTV*, esta televisão usa uma conexão com a Internet para transmitir à Samsung as informações de visualização do usuário em questão e também para ativar os recursos de reconhecimento de voz integrados na TV.

Device to gateway. Neste tipo de modelo de comunicação, o dispositivo liga-se a um *gateway* para ter acesso à Internet. Um dos exemplos deste tipo são as pulseiras de exercício físico. O aparelho envia os dados fornecidos pela pulseira para o *gateway* (*smartphone*) através do *Bluetooth* e posteriormente a informação transmitida para a internet por *Wi-Fi* ou pela rede de dados.

Back end Data-Sharing. Como já foi referido, a IoT tem como função de comunicar e transmitir dados entre os dispositivos. Para complementar esse processo foi criado o modelo *Back-end Data Sharing* que possibilita a partilha de informações sobre o clima,

o trânsito, as atividades diárias de cada pessoa e utilizar isto para gerar informações. Por exemplo: Numa quinta, através de sensores conectados são recolhidas características do solo e esses dados são enviados para o Servidor A. Nesse servidor os dados são analisados, gerando recomendações e indicadores para a quinta. Para reunir mais dados os sensores do Servidor A comunicam com mais 2 Servidores, recolhendo informações sobre a meteorologia, histórico das plantações, altura do ano mais favorável para a colheita. Assim através deste das informações fornecidas pelos servidores, os agricultores poderão aumentar consideravelmente as suas produções. [1] [4]

3 Segurança

Fig. 1.

Artigo: *The Independent 15.Jan.2019*

Um automóvel como o Tesla Model 3 é um grande objeto do quotidiano que incorpora em grande escala a Internet das Coisas. A Tesla oferece um carro e 900 mil dólares a quem o conseguir *hackear* [Fig.1], porquê? Este tipo de competições de *hacking* com *white-hat hackers* permitem que a Tesla teste e aperfeiçoe os seus sistemas de segurança, o que está a ganhar grande importância já que os carros cada vez se parecem mais com computadores sobre rodas.

Tal como o Tesla pode ser *hackeado*, também muitos outros objetos do nosso dia a dia apresentam este problema, uma vez que coisas desde lâmpadas e frigoríficos a *pacemakers* estão agora ligadas à Internet. À medida que os dispositivos ligados à Internet aumentam, surgem novas oportunidades para explorar potenciais vulnerabilidades de segurança. Quando associado com a elevada natureza interconectada dos dispositivos IoT, qualquer instrumento conectado online mal seguro pode afetar a segurança e resiliência da Internet globalmente, não só localmente.

3.1 Existem já vários exemplos "famosos" de *hacking* em dispositivos de IoT. Entre estes temos:

O *Hack* Mirai. Este consistiu num programa que infetava computadores e os usava para procurar aparelhos de IoT, tais como máquinas de filmar, e os corrompia, impedindo o seu funcionamento. Uma das vulnerabilidades que foram usadas pelos hackers foi a de aparelhos com passwords "*default*", como 123456, que nunca são atualizadas pelos utilizadores.

O *Hack* dos JEEPs. Neste caso, uma equipa de investigadores da IBM (*Internet Business Machines Corporation*) identificou uma vulnerabilidade no *firmware* de um Jeep SUV que permitia que o *hacker* tomasse controlo total do carro, podendo então fazê-lo acelerar, abrandar e virar.

Os Dispositivos Cardíacos Vulneráveis do Hospital St. Jude. Em 2017, foi confirmado que os pacemakers concebidos pelo St. Jude Medical apresentavam uma grave vulnerabilidade que permitia que hackers acedessem ao dispositivo, podendo desde aí alterar o seu funcionamento, esgotar a bateria e até mesmo administrar choques incorretos ao doente. A vulnerabilidade ocorreu no transmissor que recolhia e partilhava remotamente a informação com o médico. [7][8]

3.2 Problemas de Segurança Específicos de Dispositivos IoT

Recentemente, numa entrevista dada a uma televisão portuguesa, o fundador da Kaspersky disse que já existe sensibilidade para cerca de 90% dos problemas de segurança dos computadores, 50% em relação aos telemóveis e para a IoT... quase nada. Isto leva-nos a questionar quais serão então as particularidades destes dispositivos no que diz respeito à segurança, de modo que, passamos a enumerar:

A simples quantidade destes dispositivos. A quantidade de dispositivos de IoT vai em breve ser uma ou mais ordens de grandeza maior que a dos computadores e telemóveis todos somados. Vão existir literalmente biliões de dispositivos interconectados entre si e a comunicar de forma mais ou menos autónoma.

O facto de grandes quantidades de dispositivos diferentes conterem componentes comuns. Por exemplo, o mesmo *chip* de comunicação por *BLUETOOTH* usado por um grande número de dispositivos. Uma vulnerabilidade deste chip pode colocar em risco todos os dispositivos que o incorporam.

A longevidade dos dispositivos. Estes novos dispositivos têm uma longevidade esperada maior que a normalmente associada a instrumentos de alta tecnologia. Com o tempo surgem novos desafios de segurança e a reconfiguração dos dispositivos pode ser difícil ou mesmo impossível, pelo contrário, os sistemas de computação tradicionais

fazem *updates* durante o "curso de vida" do computador para combater as novas ameaças de segurança.

Falta de possibilidade de *upgrade*. Muitos dispositivos são desenhados intencionalmente sem a possibilidade de fazer upgrades ou com um processo de upgrade complicado, deixando os mesmos eternamente vulneráveis.

Funcionalidades Invisíveis ao Utilizador. Muitas vezes os utilizadores não têm visibilidade de todas as funcionalidades do dispositivo. Isto deixa o utilizador vulnerável, uma vez que o dispositivo pode executar tarefas ou recolher informação indesejadas.

Segurança Física Impossível. Alguns dispositivos podem encontrar-se em locais cuja asseguração da segurança física do objeto seja difícil, deixando-o vulnerável a acesso físico de invasores.

Dispositivos Invisíveis ao Utilizador. Alguns dispositivos são desenhados de modo a não serem notados pelo utilizador. Neste caso, podem ocorrer problemas de segurança no dispositivo que ficam desconhecidos por tempo indeterminado e consequentemente, sem serem resolvidos. Pode também acontecer que a informação esteja a ser recolhida sem que o utilizador esteja ciente.

Surgimento de "*Build Your own Internet of Things*" (BYIoT). Como se pode constatar pelo crescendo das comunidades de Arduino e Raspberry Pi *developers*, a prática de construir o próprio dispositivo IoT está-se a tornar cada vez mais comum. Nestes casos não é certo que os melhores padrões de segurança sejam aplicados.[1]

4 Privacidade

Nesta secção focada em privacidade, vai ser exposta a forma de como são processados os dados, se é utilizada encriptação, se os dados são eliminâveis e casos de atividade imprevista no funcionamento do equipamento. A maioria dos dados aqui expostos são provenientes de uma análise feita pelo *Mon(IoT)r Research Group na Northeastern University.* [9]

4.1 Processamento de Dados

Por processamento de dados entende-se ato de armazenar e interpretar informação recolhida pelo dispositivo. Os dados podem ser armazenados e processados localmente ou ser enviados para um servidor de modo a serem processados remotamente.

Processamento local. Quando os dados estão contidos no equipamento e são processados localmente todo o processo é mais simples e seguro. Se tudo for implementado corretamente (encriptação dos dados no caso de acesso físico e *resets* de fábrica no caso de venda do equipamento) esta é a opção mais segura e benéfica para a privacidade do utilizador.

Processamento remoto. Quando os dados são processados remotamente a privacidade pode estar em risco. Uma vez que os dados ficam definitivamente fora do controlo do utilizador estes podem, posteriormente, ser vendidos a terceiros. Além disso, se a transmissão da informação for insegura pode existir uma fuga de dados privados. Existem dispositivos que conseguem funcionar tanto com ligação a um servidor como sem ela, o que pode implicar, por vezes, perda de funcionalidades.

4.2 Encriptação

Encriptação é o ato de converter dados em código, é algo extremamente importante para proteger os dados dos utilizadores. No entanto, não é uma garantia de privacidade, mas sim, uma camada adicional para suportar a segurança dos dados.

Para ser eficaz devem ser usados algoritmos seguros para o armazenamento e transmissão de informação. É importante para prevenir que tanto o acesso físico ao equipamento, como um ataque MitM*(Man in the Middle)* ou uma análise do tráfego da rede não ponha em risco os dados.

4.3 Comportamentos inesperados

Existem vários relatos de equipamentos com comportamentos inesperados desde *Alexa's* que começam a funcionar inesperadamente durante conversas privadas (*creepy*), como campainhas inteligentes que gravam vídeo sempre que detetam movimento. Estes comportamentos são preocupantes visto que podem ser gravadas conversas privadas ou rotinas de entrada/saída da casa.

Com gigantes tecnológicos como a Google a defender que analistas humanos ouçam gravações do Google Home (*recordings*) e com a Amazon a montar uma rede de vídeo vigilância para uso policial com as suas campainhas inteligentes, todas as precauções com privacidade e liberdades individuais devem ser reforçadas. [12][13]

5 Conclusão

O conceito de Internet das Coisas tem em vista um mundo no qual biliões de objetos interconectados possuem inteligência artificial, internet e capacidades de deteção e atuação.

Este conceito dá asas a um mundo revolucionário, de progresso, eficiência e oportunidade, totalmente interconectado, com um potencial de adicionar biliões em valor à indústria e à economia global. Por outro lado, com a evolução abrupta de uma

realidade híper-conectada, surgem novos desafios relativamente à segurança e privacidade.

Em suma, há uma necessidade de ultrapassar os obstáculos, procurando soluções que simultaneamente maximizem os benefícios e reduzam os riscos.

Referências

1. Rose, K., Eldridge, S., Chapin, L.: (2015) *The Internet Of Things: An Overview*
2. 24 top internet- of things (IOT) examples you should know, https://builtin.com/internet-things/iot-examples, Consultado em: 2020/10/16.
3. IoT Device Security Issues and Why They Exist, https://www.iotforall.com/security-issues-in-iot-devices-and-why-they-exist, Consultado em: 2020/10/18.
4. Communication Models in Internet of Things: A Survey, http://www.ijste.org/articles/IJSTEV3I11049.pdf, Consultado em: 2020/10/17.
5. Tesla is challenging hackers to crack its car, and it is putting ~$1 million on the line, https://electrek.co/2020/01/10/tesla-hacking-challenge/, Consultado em: 2020/10/13.
6. TESLA HACKING COMPETITION OFFERS $900,000 AND FREE CAR IF SOMEONE CAN HIJACK MODEL 3, https://www.independent.co.uk/life-style/gadgets-and-tech/news/tesla-model-3-hacking-competition-pwn2own-prize-elon-musk-a8728376.html, Consultado em: 2020/10/13.
7. The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History, https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities, Consultado em: 2020/10/13.
8. 5 infamous IoT hacks and vulnerabities, https://www.iotsworldcongress.com/5-infamous-iot-hacks-and-vulnerabilities/, Consultado em: 2020/10/13.
9. Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach, https://moniotrlab.ccis.neu.edu/wp-content/uploads/2019/09/ren-imc19.pdf, Consultado em: 2020/10/17.
10. Privacy leaks Extracting data from used smart home devices, https://youtu.be/Iit4SmzQ2Uo, Consultado em: 2020/10/15.
11. Effects of the Factory Reset on Mobile Devices, https://www.researchgate.net/publication/315370004_Effects_of_the_Factory_Reset_on_Mobile_Devices, Consultado em: 2020/10/17
12. Has Alexa snapped? Why your Echo sometimes does creepy things, https://www.zdnet.com/article/has-alexa-snapped-why-alexa-sometimes-laughs-or-does-other-creepy-things/, Consultado em: 2020/10/17.
13. Company admitted voice assistant is sometimes triggered by accident and recordings could be sent to workers for analysis, https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-home-recordings-listen-privacy-amazon-alexa-hack-a9002096.html, Consultado em: 2020/10/17.
14. The 9 most important applications of the Internet of Things (IoT), https://www.fracttal.com/en/blog/the-9-most-important-applications-of-the-internet-of-things, Consultado em: 2020/10/17
15. An Overview of Security Issues Relating to the Internet of Things, https://www.researchgate.net/publication/334603508_An_Overview_of_Security_Issues_Relating_to_the_Internet_of_Things, Consultado em: 2020/10/17