Internet das coisas: Desafios na Segurança e Privacidade

Ana Luísa Carneiro, Ana Rita Peixoto, Leonardo Marreiros

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal
e-mail: {a89533,a89612,a89537}@alunos.uminho.pt

Resumo A Internet das Coisas (IoT) tem-se tornado cada vez mais parte da sociedade, de forma a melhorar a qualidade de vida do utilizador. Através da mesma, objetos físicos do quotidiano conseguem estar conectados à Internet e auxiliar em tarefas do dia-a-dia. Contudo, devido à complexidade da sua rede e à diversidade de dispositivos ligados a esta, surgem questões relacionadas com a segurança e privacidade dos dados que estão a ser recolhidos. Através de dispositivos IoT, podemos ser rastreados sem o nosso conhecimento e pelo menos parte da nossa informação pode ser deixada no ciberespaço. É necessário estar consciente destes ataques à privacidade e segurança e desenvolver ou utilizar medidas de proteção contra o uso malicioso de informação recolhida através de dispositivos IoT.

1 Introdução

A Internet das Coisas (também conhecida por IoT – *Internet of Things*), apesar de importante e benéfica para a sociedade, levanta várias questões relacionadas com segurança e privacidade dos dados que estão a ser transmitidos e armazenados nas redes IoT. A falta de proteção nestas redes e dispositivos IoT pode levar a roubo de informação e identidade dos utilizadores ou a danos de hardware e software nos próprios dispositivos. Isto leva-nos a evidentes questões e problemas de segurança e privacidade. Será que podemos confiar nos fabricantes de dispositivos com este tipo de tecnologia? Será que a informação que pode ser recolhida por estes aparelhos está a ser tratada da melhor forma? Ou será que está a ser usada para o proveito das empresas ou com intuitos maliciosos?

A presente pesquisa irá primeiramente analisar o conceito da IoT e as suas características. De seguida iremos apresentar quais os principais problemas de segurança e privacidade nas redes IoT. Finalmente iremos abordar e analisar medidas na prevenção de falhas de segurança assim como quais os protocolos a serem tomados.

2 O que é a Internet das Coisas?

A Internet das coisas é um conceito que se refere à interconexão digital de objetos, cujo objetivo é tornar os nossos dias mais seguros e eficientes. É uma rede de objetos capaz de reunir e transmitir dados. Através de sensores (*sensing devices*) como RFID, raios infravermelhos, GPS, *Bluetooth* e *Scanners* a laser, que permitem identificar o dispositivo, consegue-se conectar qualquer objeto com internet para comunicação de dados e serviços formando assim uma "super autoestrada de informação" (*"Information Super highway"*).

Assim, a IoT é uma rede de dispositivos que comunicam entre eles através do IP, sem interferência humana, ou seja, *"Material objects connected to material objects in the internet"*[2].

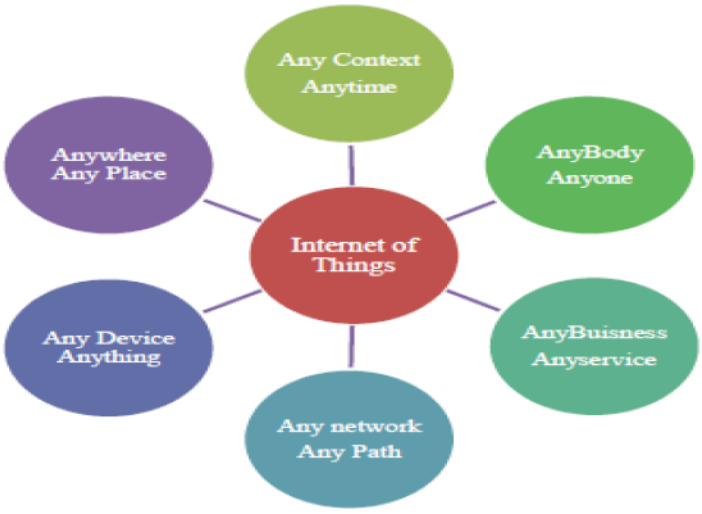

Figura 1. Definição da Internet das Coisas.[4]

Atualmente, muitos dos dispositivos eletrónicos utilizados diariamente fazem parte da IoT. A título de exemplo, um *smartwatch* que seja capaz de transmitir dados com um carro, ou um frigorífico que consiga comunicar com uma mercearia.

A IoT possui diversas características. Para além de permitir a comunicação utilizador-dispositivo e dispositivo-dispositivo, também é possível que este tipo de dispositivos tenham inteligência associada e garantam a segurança na vida do utilizador. Por exemplo, um carro pode informar ao utilizador o estado atual dos seus pneus, no caso de se tratar de um *smart car*, evitando um possível acidente.

A IoT também tem a capacidade única de informar o seu estado atual a outros dispositivos conectados nas redondezas, facilitando a comunicação entre humanos e máquinas. Além disso, os dispositivos IoT podem poupar muita energia e utilizá-la de forma eficiente, por exemplo, no uso de luzes automáticas que se ligam quando sentem movimento.

3 Problemas de segurança e privacidade na Internet das coisas

Os dispositivos IoT não só monitorizam o utilizador, mas também colecionam e transmitem informação sobre o mesmo. Assim, torna-se complicado proporcionar uma transmissão segura dos dados dos utilizadores. Para além disso, como a maioria da transmissão acontece em espaço aberto (através de ondas eletromagnéticas, por exemplo) existe uma maior suscetibilidade a ataques e dificuldade de manter segurança e privacidade na rede.

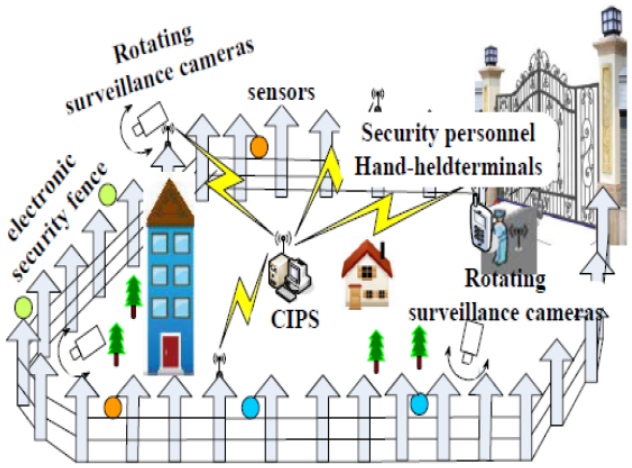

Figura 2. Exemplo de uma rede IoT. [4]

3.1 Segurança

No que toca à segurança em dispositivos da Internet das coisas, existem diversos aspetos importantes. Ao proporcionar uma vasta rede de conexão entre objetos, é necessário que a rede IoT tenha a capacidade de proteção contra ataques externos que podem atacar os sensores, a rede de comunicação de informação ou então as diversas aplicações das IoT.

É necessário ter em consideração os ataques que interferem, monitorizam ou perturbam informação que chega aos sensores através de canais *wireless*, pois podem aceder à rede de controlo dos sensores e assim danificá-los ou retirar-lhes informação. Exemplos deste tipo de ataques são a captura do nodo, nodo falso, SCA, entre outros. Um outro ataque muito recorrente e perigoso é o ataque DOS (*Denial of Service*), que invalida um sensor através do consumo dos seus recursos, forçando reiniciar o dispositivo. Assim, o sensor deixa de conseguir realizar as suas funcionalidades e até pode mesmo danificar o dispositivo e interferir com toda a rede IoT.

No que toca à rede, esta desempenha um papel importante para fornecer uma maior capacidade de interconexão, eficiência e maior qualidade de serviço nos dispositivos IoT. Assim, os ataques têm maiores consequências quando aplicados à IoT devido à sua vasta e complexa rede. Além destes ataques, existem também problemas de compatibilidade de IP (entre a internet e IoT) e de tráfego de informação devido ao elevado número de terminais em redes IoT [1].

Em relação às aplicações IoT, como não há *standards* na criação das mesmas, torna-se complicado criar um sistema de segurança fiável e compatível. Assim, cada aplicação, como é destinada a ambientes e funcionalidades diferentes, possui problemas distintos. Os dispositivos IoT que tem falta de segurança podem colocar todo o sistema IoT em risco. Pontos de baixa segurança são entradas para *cyber*-ataques, que podem levar à violação de dados. São exemplos desses ataques os *trojan* ataques (cavalo de tróia), vírus, vulnerabilidades de *Software*, entre outros.

3.2 Privacidade

A privacidade dos utilizadores e dos seus dados foi identificada como sendo um dos maiores desafios a ser abordado nos dispositivos IoT.

A IoT possui uma elevada conexão de dispositivos em que muitos deles podem armazenar o histórico de saúde do indivíduo, compras efetuadas, localização, finanças, negócios, entre outros. Assim, ao aceder a um dispositivo, pode ser possível aceder a muitos outros. Alem disso, através de manipulação não autorizada de *hardware* / *software* é possível que informação do histórico de um utilizador vaze do dispositivo ou então que as funcionalidades desse dispositivo sejam utilizadas de forma ilegal [7].

A título de exemplo destacamos o dispositivo *MyQ Garage* que permite ao utilizador abrir e fechar a sua garagem através do seu *smartphone*, pode ser utilizado por assaltantes que poderiam ganhar acesso ao dispositivo e usá-lo para encontrar, abrir e fechar o portão e, deste modo, ter oportunidade para assaltar a casa [6].

Para além disso, também é relevante realçar a importância de ter sistemas de vigilância bem protegidos. Por exemplo, um intruso pode reprogramar uma câmara de vigilância de modo a aceder à sua informação, comprometendo a segurança do indivíduo. Também se deve ter especial atenção à privacidade dos utilizadores durante a comunicação. Devem ser implementados mecanismos que permitam aos utilizadores comunicar sem que haja extravio de informação que pode ser utilizada para fins políticos por governos, ou ser utilizada por setores privados como empresas de marketing. O facto de muitos dispositivos transmitirem informações em redes sem criptografia representa um risco ainda maior de privacidade [5].

É importante referir que as falhas existentes na proteção de dados e privacidade dos utilizadores podem ter origem noutros aspetos. Por exemplo, verifica-se atualmente que muitos utilizadores adotam senhas fracas e simples que constituem uma autenticação insuficiente e tornam o dispositivo mais suscetível a ataques.

A falta de privacidade pode ainda surgir à medida que objetos dentro da IoT coletam e agregam fragmentos de dados relacionados com o seu serviço. Por exemplo, a compra regular de diferentes tipos de alimentos pode divulgar a religião ou informações de saúde acerca do comprador. [9]

4 Como garantir a segurança e privacidade na Internet das coisas

A Internet das coisas conecta e partilha informação acerca de objetos vivos e inanimados. Tudo desde dispositivos médicos até dispositivos de casa, são conectados e fazem parte da IoT. A proteção de dispositivos IoT é um processo complexo e multifacetado.

As medidas a garantir a segurança e privacidade em dispositivos IoT devem-se focar em: proteção da privacidade, controlo de acesso, autenticação do utilizador, camada de comunicação de segurança, integridade dos dados, confidencialidade dos dados e disponibilidade a qualquer altura.[4]

4.1 Segurança

Existem diversas medidas para manter segurança nas redes IoT. Tal como foi expresso na secção 3, existem vários ataques que podem vir a acontecer aos sensores e aos seus constituintes (nodos). É por isso necessário que haja acesso controlado aos sensores, verificação de que todos os seus nodos funcionam corretamente e manutenção constante dos mesmos.

No que toca às medidas de segurança a serem aplicadas aos dispositivos IoT é necessário ter em atenção que cada aplicativo é diferente e requer proteções distintas. Contudo, existem medidas comuns que podemos tomar de forma a evitar ataques informáticos, tais como reforçar a importância da utilização de produtos antivírus e *firewalls*. O uso destes produtos é importante para manter um aplicativo protegido e consequentemente toda a rede IoT.

Um dos problemas mencionado na secção 3 foi a incompatibilidade entre a rede internet e a IoT no que toca aos endereçamentos IP. Por isso criou-se o protocolo *6LoWPAN*, uma vez que o IP atual (IPv6) não é suficiente para suportar funcionalidades das redes IoT. Assim, é possível fazer com que se consiga usar endereços atuais em redes IoT. [3]

Para além deste protocolo, também existem diversos outros a serem aplicados aos sensores, redes e aplicações para manutenção da segurança como por exemplo: protocolos de gestão (*Key Managment*, etc), algoritmos de chaves secretas, deteção de intrusos, protocolos na segurança de transmissão de informação, protocolos de autenticação e acesso controlado, entre outros.

4.2 Privacidade

Uma das formas de melhor lidar com a privacidade em dispositivos IoT é implementar medidas eficazes no combate a ataques de roubo de informação e entidade.

No que toca ao roubo de identidade, uma das principais medidas a tomar é por exemplo reforçar a autenticação nos aplicativos, isto é, quando é pedido ao utilizador que faça autenticação através de um *login*, essa informação pode ser desviada ao ser transferida para o site ou aplicativo. Fortalecer essa transferência pode evitar roubos de identidade.

O Protocolo de Comunicação Seguro (*Secure Communication Protocol*) pode ser a abordagem adequada para quando queremos protocolos que visam a proteção de identidade dos utilizadores. Durante a transferência de dados, os pseudónimos (identidade na rede dos utilizadores) podem ser encriptados, a fim de diminuir a vulnerabilidade da comunicação.

A IoT é basicamente um repositório de cada aspeto da vida de uma pessoa e como forma de reduzir ao mínimo os riscos de roubo de informação quando esta se encontra armazenada nos dispositivos deve-se tentar ao máximo reduzir a quantidade de informação armazenada para a que seja só necessária. Em caso de obrigatoriedade, devem ser apenas armazenadas informações pessoais que sejam necessárias para o correto funcionamento do dispositivo e/ou da aplicação. Ocultar a identidade real ligada aos dados armazenados, Pseudonimização e/ou a Anonimização, podem também ser usadas como métodos preventivos.

Os utilizadores devem ser capazes de controlar e escolher quais os dados que são coletados, quem os está a coletar e quando é que isso ocorre. O consentimento fornecido pelos utilizadores aos dispositivos IoT deve ser informado e livremente dado. Isto não só reduz o mal associado às violações de dados, mas também minimiza o risco dos mesmos serem usados de forma ilegítima.

Contudo, é preciso ter em consideração que os dados que são enviados a outros dispositivos ou sensores devem ser tratados com o fim a que se destinam. Caso não haja aceitação explícita e o conhecimento do titular dos dados, os seus dados pessoais nunca devem ser divulgados a terceiros. É por essa razão que o Sistema de Gestão de Direitos Digitais (DRM), tem como função controlar o consumo de meios comerciais e defendem contra a redistribuição ilegal de dados.

A principal forma de proteger a informação enviada pela rede é através da criptografia de mensagens. A encriptação é feita nas saídas de informação dos sensores e das aplicações. Este método de proteção de dados permite que a informação não seja desvendada caso seja intercetada por terceiros, tal como pode acontecer nos casos de roubo de identidade acima explicados. Nas entradas dos dispositivos ou aplicações a mensagem pode ser desvendada através de uma chave (desencriptação).

5 Conclusão

Com a realização deste trabalho, conseguimos reparar que as tecnologias IoT são já uma grande parte da sociedade e desempenham um papel fundamental no mundo conectado à Internet, contudo antes de ser considerado seguro e confiável para milhões de consumidores, as ameaças de segurança às redes IoT devem ser reconhecidas e devem ser tomadas medidas por *developers* e fornecedores, bem como pelo governo e agências reguladoras. Ataques devem ser intercetados, dados autenticados, acesso controlado e privacidade dos clientes (pessoas singulares e coletivas) garantida. Medidas tecnológicas e sociais devem ser implementadas de forma mutuamente benéfica, de modo a permitir aos vendedores controlar os seus inventários e garantindo aos consumidores que seus dados não serão desviados. Esforços educativos são necessários para garantir aos utilizadores que os seus dados estão realmente seguros, através do uso de serviços que visam a proteção dos dispositivos de cada um [8]. Finalmente, somos da opinião de que devem ser criadas medidas do foro legal tais como leis e políticas de forma a proteger a informação e dados dos utilizadores.

Referências

1. Kai Zhao, Lina Ge: A Survey on the Internet of Things Security (2013)
2. GAN Gang, LU Zeyong, JIANG Jun: Internet of Things Security Analysis.
3. Jorge Granjal, Edmundo Monteiro, Jorge Sá Silva: Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues (2015)
4. J. Sathish Kumar, Dhiren R. Patel: A Survey on Internet of Things: Security and Privacy Issues (2014)
5. Rolf H. Weber: Internet of Things – New security and privacy challenges (2010)
6. Sachchidanand Singh, Nirmala Singh: Internet of Things(IoT): Security Challenges, Business Opportunities Reference Architecture for E-commerce (2014)
7. Marie-Helen Maras: Internet of Things: security and privacy implications
8. Sivarama Subramanian, Varadarajan Vellore Gopal, Marimuthu Muthusamy: RFID Privacy Issues and Technical Challenges
9. Miyako Ohkubo, Koutarou Suzuki, Shingo Kinoshita: Security and Privacy Challenges of IoT-enabled Solutions