Propondo uma Análise de Risco focada na singularidade da Internet das Coisas

Silvio Beskow[1], **Érico S. Rocha**[1]

[1]Curso Superior de Tecnologia em Segurança da Informação
Universidade do Vale do Rio dos Sinos (UNISINOS)
Porto Alegre – RS – Brasil

segbeskow@gmail.com, ericor@unisinos.br

Abstract. *The Internet of Things connects countless devices exchanging information among themselves. These devices are produced by various manufacturers with restricted computer resources. They are part of a wide range of human daily activities, thus linking diverse multiple digital resources to the physical world. This article is a fragment of a research in progress. Its main objective is to present the reasons that justify the need for improvements in IoT systems risk analysis. To live up to this challenge, it focuses on the purpose of such devices, on their computational capacity, on the infrastructure they require and on possible impacts on users.*

Resumo. *A Internet das Coisas conecta uma infinidade de dispositivos que trocam informações entre si. Esses dispositivos são produzidos pelos mais variados fabricantes e com recursos computacionais restritos. Eles, por sua vez, fazem parte das mais diversas atividades da vida humana, interligando, assim, os mais diversos recursos digitais ao mundo físico. Este artigo é um fragmento de uma pesquisa em andamento. Seu principal objetivo é apresentar as razões que justificam a necessidade de melhorias na Análise de Risco de sistemas IoT. Para realizar esse desafio, apoia o foco no propósito desses dispositivos, na sua capacidade computacional, na infraestrutura que eles necessitam e nos possíveis impactos causados aos seus usuários.*

1. Introdução

A Internet das Coisas (IoT) é uma evolução do sistema de rede atual. São mais dinâmicas, são interoperáveis e autoconfiguráveis. Além disso, são redes constituídas por "coisas" que possuem identidade, atributos físicos e personalidades virtuais. Integram-se à rede através das suas interfaces inteligentes [Vermesan et al. 2011].

"Nesta época de conectividade eletrônica universal, de vírus e hackers, de espionagem eletrônica e fraude eletrônica, não há realmente um tempo em que a segurança não importa" [Stallings 2014]. Estamos vivendo um novo momento no qual o conhecimento humano, herdado e cultivado de muitas gerações, coloca a humanidade sob uma nova perspectiva evolutiva de atividades na rede para troca de informações.

Os desafios da Internet das Coisas, quanto ao volume de dispositivos, aplicativos e pessoas, fomentam estudos sobre como tornar esta rede mais confiável e convidativa aos seus usuários. A motivação desse estudo se estabelece no fato de que

alguns dos dispositivos (de capacidade computacional limitada) que são conectados à rede, não apresentam os requisitos mínimos para a aplicação das tecnologias de Segurança da Informação disponíveis. Nesse contexto, objetiva-se salientar a necessidade de melhorias na Análise de Risco para destacar as singularidades do sistema durante o planejamento desse sistema.

2. Internet das Coisas

A Internet das Coisas começou a receber maior atenção após a popularização das comunicações sem fio. Isso ocorreu pelo volume de dispositivos (coisas como portas, luzes da casa, eletrodomésticos etc.) que que são de uso comum dos seres humanos, ligados das mais variadas formas e para as mais diferentes finalidades.

2.1. Conceito

Os conceitos de IoT propostos por [Singer 2012] tem como base: a) o paradigma que intersecciona os saberes e a tecnologia proposto por [Atzori et al. 2010]; b) a relação entre homens e máquinas, [Greenfield 2010]; c) a posição reativa (conectividade conhecida), e a proativa (entre homens e máquinas e entre máquinas e máquinas), sendo que as comunicações máquina a máquina (M2M) são autônomas, proposta por [Van Kranenburg et al. 2011][1]. Assim, com a reunião desses três conceitos, o autor propõe uma definição operacional da IoT que *"a considera como um paradigma computacional com implicações profundas no relacionamento entre homens e objetos"*[Singer 2012][2].

O conceito de que IoT é uma rede dinâmica, composta de coisas físicas e virtuais, únicas, interoperáveis, autônomas, e que tornam as redes inteligentes por serem compostas por dispositivos inteligentes, foi proposto pela Strategic Reserch Roadmap da Cluster of European Research Projects on the Internet of Things. Essas "coisas inteligentes" podem ou não necessitar de intervenção humana e são capazes de conectar o mundo real e o virtual. Possuem a capacidade de manipular os dados com os quais interagem, assim é necessário observar as questões de privacidade e segurança[Vermesan et al. 2011][3].

Com base nessas definições, propõe-se que a IoT incorpore os aspectos de segurança em suas variadas definições da seguinte forma: objetos inteligentes, privados, que interoperem por meios seguros, com dados suficientes e limitados para realizar as tarefas as quais são designadas e consentidas por seus proprietários.

3. Segurança da Informação

A Segurança da Informação tem sua base na tríade: confidencialidade, integridade e disponibilidade (CID). A partir dessa tríade, ela se aprofunda em todas as áreas que tenham a informação como ativo a ser protegido.

Destaca-se que a segurança inter-redes já é uma tarefa que exige um grande esforço técnico e do negócio. Então, pode-se imaginar se tudo e todos estiverem

[1]Retirado do trabalho The Internet of Things, p.9.
[2]fragmento retirado ipsis litteris p.5.
[3]Interpretação e resumo do autor de fragmento de texto lido em, p.6.

interconectados? Este fato já é uma realidade em expansão hoje, onde os esforços para a proteção de todos os usuários, seus dados e suas múltiplas interconexões já encontram seus desafios específicos [Stallings 2014].

4. Referencial Teórico

No trabalho *Internet of Things (IoT): Smart and Secure Service Delivery*, a IoT é definida como uma rede que apresenta uma diversidade de dispositivos conectados, com benefícios e vulnerabilidades. Afirma que os serviços para a IoT estão sendo desenvolvidos e implementados sem considerar a segurança [BERTINO et al. 2016]. Sustenta a necessidade do planejamento organizacional e seguro dos sistemas IoT.

O artigo *Managing the risk of the Internet of Things*, define IoT como uma rede composta de dispositivos de capacidade computacional limitada. Entende-se aqui, aqueles objetos corriqueiros, de uso diário (ex.: exemplo uma cafeteira) e que não são considerados computadores. Todavia, a Internet das Coisas faz uso da computação tradicional enviando ou recebendo dados como, por exemplo, um medidor de temperatura enviando e recebendo dados de um servidor na nuvem [Sorebo 2015]. A proposta do artigo é trabalhar com uma Gestão de Risco mais focada no impacto futuro e não na vulnerabilidade. Para tanto, afirma que é preciso, em um primeiro momento, definir qual o propósito de uso do dispositivo IoT. Depreende-se que ele pode ser usado para vários objetivos distintos e variar o tipo de risco em decorrência do seu propósito. Assim, uma linha desse processo seria: definir o uso, verificar as estruturas de suporte necessárias, analisar as restrições técnicas dos dispositivos, verificar o alinhamento com os objetivos do negócio e estimar o seu valor operacional.

Irshad (2016), avaliou sistematicamente e revisou os frameworks de Gerenciamento de Segurança da Informação relacionados à Internet das Coisas. Incentiva a definição de uma estratégia de governança com foco na segurança dos seus ativos [Irshad 2016]. Seu estudo é relevante para o presente artigo por apresentar uma Arquitetura IoT relacionando as camadas e os tipos de tecnologias. Também se pode salientar a questão do enquadramento adequado dos dispositivos.

Rob Clyde, um dos diretores do conselho da *Information Systems Audit and Control Association* (ISACA), assinalou o potencial que a IoT e a Realidade Aumentada têm de se tornarem uma fonte sem precedentes de valor e oportunidade, bem como o potencial de risco para a segurança das informações. Acrescentou que indivíduos e empresas precisam acelerar seus esforços para desenvolver essas tecnologias, ao mesmo tempo que aprendem a gerenciar os seus riscos. Esse aprendizado é de grande importância para que não comprometa a capacidade de inovação das empresas [ISACA 2016]. O diretor ressalta que não deve haver simplesmente um não uso da tecnologia em função das suas fraquezas, mas um esforço de gerência para minimizar os riscos. Nesse caso, tem-se mais uma referência à gestão de segurança como uma alternativa.

Em *Identity Transformed as Internet of Things Invades the Workplace*, o *Chief Information Officer* (CIO), de uma certa organização, solicita um *pentest* à uma organização terceira que comprometa um computador da empresa explorando uma falha de segurança de um teclado wireless conectado a esse computador. O artigo propõe que os dispositivos que estão no espaço de trabalho devem ser identificados

[Lemos 2017]. A existência de uma política de segurança eficaz depende de uma análise de risco tão profunda, quanto mais pervasivos são os dispositivos que poderão ser conectados à rede da organização.

5. Problemas e Desafios Gerais da IoT

Os problemas básicos de segurança na IoT estão na limitação de hardware (processamento, armazenamento e energia) e na interpolaridade dos diversos dispositivos. Abaixo são destacados alguns agravamentos:

- Cada dispositivo apresenta um risco potencial e pode tornar-se um vetor de ataque [BERTINO et al. 2016];
- Falta de identificação dos dispositivos IoT nas organizações;
- A capacidade das redes e a transmissão de dados com relação à segurança dos protocolos de rede e aplicações nos dispositivos IoT [Heer et al. 2011];
- A grande capacidade de processamento, gerenciamento e distribuição de chaves que são exigidas para implementar a criptografia;
- Falta de uma padronização para um desenvolvimento sustentável [Atzori et al. 2010];

Devido à ampla variedade de dispositivos, de fabricantes, às restrições de hardware [Sorebo 2015] e algumas estruturas de redes, destacam-se os desafios considerados importantes:

- Capacidade de adequação padronizada de comunicação entre diversos dispositivos e diferentes fabricantes, chamado de Interpolaridade;
- Desenvolvimento de criptografia leve e um sistema adequado de gerenciamento e distribuição de chaves;
- Reflexão sobre "autoria, propriedade e privacidade das informações" [Singer 2012];
- Capacidade de aderir a conformidade com a legislação [Ziegeldorf et al. 2014];
- Privacidade e segurança, sem inviabilizar a troca de dados entre os dispositivos [Guo et al. 2011];
- Estrutura que permita aos proprietários da informação definirem o seu apetite de risco em relação à **privacidade e a segurança**, deixando-os conscientes dos produtos e serviços IoT que estão consumindo [Vermesan et al. 2011].

6. Problema e Desafio Específicos

Defende-se que uma forma de enfrentar os problemas da IoT está na gestão dos seus riscos. Segundo Sorebo (2015), o problema está no fato de que a gestão de risco tradicional está embasada em como os dispositivos são usados. Mesmo na tentativa de compreender as ameaças e, por conseguinte, propor controles, pode-se apontar em distintas direções e ainda assim não conseguir lidar de forma efetiva com o desenvolvimento contínuo de novos dispositivos e suas novas ameaças [Sorebo 2015].

O autor propõe que se tenha um esforço maior de concentração nos impactos catastróficos que o uso de um dispositivo em uma determinada tarefa poderia causar e não nas vulnerabilidades do mesmo. Para isso, propõe deslocar o foco do como os dispositivos são usados, para focar em quais as tarefas eles irão executar. Um exemplo

disso é um sensor de temperatura em um local público mandando informações de uso comum para internet e o mesmo sensor em uma siderúrgica mandando informações de uso privado para internet. Assim, afirma ainda que iniciando uma análise pelo caso de uso, o objetivo comercial pretendido já se destacará. Também havendo mudança de tarefa desse dispositivo, é evidente que o risco deverá ser reavaliado [Sorebo 2015].

O desafio é propor uma melhoria nos frameworks de análise de risco existentes que contemple todas as questões ímpares que envolvem a IoT, seus dispositivos e estrutura, com base nos estudos do artigo de Sorebo (2015).

7. Justificativa

Bertino et al. (2016) conclui no seu artigo que os sistemas IoT apresentam uma grande quantidade de vulnerabilidades e afirma que há um risco potencial dos seus dispositivos. Ressalta a necessidade da pesquisa e do desenvolvimento necessários para mitigar ameaças, a fim de evitar e resolver as vulnerabilidades.

Embora os esforços empregados por todas as partes interessadas na sua segurança e confiabilidade, a IoT é um problema de segurança em expansão. Um exemplo disso é o caso da planta de uma indústria química que usa sensores para monitorar reações usadas na fabricação de produtos sem a segurança adequada [Irshad 2016]. Ou ainda, a falha de segurança em um teclado wireless [Lemos 2017].

O esforço de estudar melhorias para a análise de risco em IoT está na importância de conhecer as limitações dos dispositivos e antecipar os seus possíveis impactos negativos no negócio. Há uma diversidade imensa de fabricantes, de hardware, de software, de infraestrutura, cada um com a sua singularidade, o que justifica o empenho em rever a prática atual da análise de risco tradicional.

8. Conclusão

Com base nos estudos realizados e nas dificuldades destacadas em diversas literaturas, acredita-se que gerenciar os riscos é uma importante ferramenta de segurança no projeto de sistemas da Internet das Coisas. Pensando nos desafios gerais da IoT, os problemas com relação à segurança e a privacidades ainda necessitam de desenvolvimento. Por essa razão, o desafio específico desse trabalho buscará preencher essas lacunas com melhorias aos frameworks existentes ou metodologia de base ágil de avaliação de riscos para sistemas IoT.

Ela deverá contribuir para a melhor visualização das capacidades técnicas dos dispositivos, de modo a equacionar os objetivos do negócio, as expectativas das partes interessadas e a legislação, respectivamente. A questão que se destaca hoje, com relação à IoT, principalmente da Segurança da Informação em dispositivos e ambientes restritos, prolonga-se por anos, conforme os trabalhos estudados até o momento. Assim, a Internet das Coisas poderá ser implementada com maior segurança através de uma análise de riscos ímpar, que atue sobre o propósito dos dispositivos que compõe o sistema e seus possíveis impactos futuros.

Referências

Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15):2787–2805.

BERTINO, E., KIM-KWANG RAYMOND, C., GEORGAKOPOLOUS, D., and NEPAL, S. (2016). Internet of things (iot): Smart and secure service delivery. *ACM Transactions on Internet Technology*, 16(4):22:1 – 22:7.

Greenfield, A. (2010). *Everyware: The dawning age of ubiquitous computing*. New Riders.

Guo, B., Zhang, D., and Wang, Z. (2011). Living with internet of things: The emergence of embedded intelligence. In *Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*, pages 297–304. IEEE.

Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., and Wehrle, K. (2011). Security challenges in the ip-based internet of things. *Wireless Personal Communications*, 61(3):527–542.

Irshad, M. (2016). A systematic review of information security frameworks in the internet of things (iot). In *High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th International Conference on*, pages 1270–1275. IEEE.

ISACA (2016). Isaca survey shows us consumers see value in augmented reality, but confidence in internet of things knowledge takes a dive. *Business Wire (English)*.

Lemos, R. (2017). Identity transformed as internet of things invades the workplace. *Information Security*, pages 8 – 12.

Singer, T. (2012). Tudo conectado: conceitos e representações da internet das coisas. *Simpósio em tecnologias digitais e sociabilidade*, 10.

Sorebo, G. (2015). Managing the risk of the internet of things. *Control Engineering*, 62(9):DE27–DE30.

Stallings, W. (2014). *Cryptography and Network Security: Principles and Practice, International Edition: Principles and Practice*. Pearson Higher Ed.

Van Kranenburg, R., Anzelmo, E., Bassi, A., Caprio, D., Dodson, S., and Ratto, M. (2011). The internet of things. *A critique of ambient technology and the all-seeing network of RFID, Network Notebooks*, 2.

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Jubert, I. S., Mazura, M., Harrison, M., Eisenhauer, M., et al. (2011). Internet of things strategic research roadmap. *Internet of Things-Global Technological and Societal Trends*, 1:9–52.

Ziegeldorf, J. H., Morchon, O. G., and Wehrle, K. (2014). Privacy in the internet of things: threats and challenges. *Security and Communication Networks*, 7(12):2728–2742.

