INDÚSTRIA 4.0 E A INTERNET DAS COISAS: AVALIAÇÃO DE SEGURANÇA DOS DISPOSITIVOS

Ataide Pereira Cardoso Junior (UNIP)
ataide@unip.br
Jose Benedito Sacomano (UNIP)
sacomano@terra.com.br

Há interesse crescente da academia e indústria sobre Indústria 4.0, com muitas publicações e congressos sobre o tema, contudo a segurança dos dispositivos ligados pela Internet, que permitem a interconectividade digital, apesar de representar a base da Indústria 4.0, tem sido objeto de raros estudos. O objetivo deste artigo é estudar a segurança dos dispositivos que propiciam a Internet das Coisas, com base naquelas utilizadas na Indústria 4.0. Utilizando-se metodologia de pesquisa bibliográfica, identificou-se cinco abordagens para aumentar a segurança dos sistemas e destes dispositivos. A originalidade deste estudo é alertar sobre a relevância da segurança cibernética, e mostrar possibilidades de contramedidas apropriadas para se mitigando os riscos, pois o uso indevido destes dispositivos por pessoas inescrupulosas pode causar ações perturbadoras na vida real, comprometendo os pilares da indústria que vier a adotar o paradigma de produção da Indústria 4.0.

Palavras-chave: segurança, cibersegurança, Indústria 4.0, sistema ciber-físico, IoT

1. Introdução

Um novo paradigma de produção se faz presente, a Indústria 4.0, também denominada a Quarta Revolução industrial, quando o uso de tecnologias digitais, apoiadas na Internet, se fundem aos processos de produção industrial, transformando a indústria convencional (CONFEDERAÇÃO NACIONAL DA INDÚSTRIA - CNI, 2016; EUROPEAN PARLIAMENT, 2015). A Indústria 4.0, é caracterizada pela integração e digitalização entre processos produtivos e produtos, principais *stakeholders* e cadeia de suprimentos em grau progressivo (CHOI et al., 2016; DE MORAIS; MONTEIRO, 2016; SCHLAEPFER, 2015).

Usando a Internet como veículo de troca de informações, um número incomensurável de dispositivos podem ser conectados, trocando informações em tempo real, o que passou a se chamar Internet das Coisas (CNI, 2016). Como a Internet tem papel fundamental para esta conexão, a segurança da informação é encarada com preocupação pelos os profissionais que atuam na área de tecnologia ou tem contato com a tecnologia em seu ambiente profissional. As questões de segurança deveriam ser sempre tratadas com criteriosas análises de riscos e aplicação de frameworks que envolvem além da segurança da informação, a segurança dos processos produtivos, sejam eles eletrônicos ou não.

Como exemplo da falta de segurança cibernética, Hoekstra (2017) afirma haver acessado documentos secretos com informações coletadas pela Agência de inteligência Central dos USA – CIA, através de escuta e capitulação de dados utilizando equipamentos de televisão *Smart* (*Smart TV*), e também telefones *Smart* (*Smartphones*), ocorridas em território norte-americano, abrangendo cidadãos norte-americanos, tudo em nome da segurança nacional, fato não confirmado nem desmentido pela CIA. Segundo Hoekstra (2017), estes vazamentos de informações secretas da CIA mostram como agentes federais norte-americanos aproveitando a falta de segurança cibernética podem *hackear* televisores inteligentes para ouvir suas conversas, mesmo quando estes televisores estiverem desligados, igualmente, *smartphones* podem ser menos seguros do que muitos assumem ser. A CIA pode supostamente penetrar em

uma rede de computadores e deixar impressões digitais, implicando outra pessoa por estas ações (HOEKSTRA, 2017).

Outros exemplo de preocupação com a falta de segurança é a facilidade com que sistemas computacionais são invadidos, assunto de capa da revista *The Economist* de 8 abril de 2017 (COMPUTER SECURITY, 2017), conforme Fig. 1.

Figura 1 – Preocupação com segurança cibernética em capa da revista

Fonte: *The Economist* (08 abr. 2017)

Estes exemplos procuram demonstrar a fragilidade a ataques em sistemas eletrônicos, cuja base da segurança da informação tem elos fracos. A tecnologia, os métodos, o sistema e o homem, todos individualmente ou em conjunto, formam a base clássica de análise de riscos que compõem os frameworks de segurança que existem hoje.

O objetivo deste artigo é estudar a segurança dos dispositivos que propiciam a Internet das Coisas, com base nos empregados na Indústria 4.0.

2. Metodologia

A metodologia utilizada foi pesquisa bibliográfica, que tem por base a pesquisa em referências publicadas em periódicos científicos e sites técnicos especializados (MARTINS; THEÓPHILO, 2009).

Utilizou-se a base de dados *Science Direct*, onde foram pesquisados artigos publicados nos últimos seis anos, usando as seguintes palavras-chave: segurança, Internet das Coisas e Indústria 4.0. Como critério de exclusão dos artigos, foram eliminados todos os artigos que não tivessem por foco a Indústria 4.0 e/ou Internet das Coisas, sendo também excluídos os artigos que estavam relacionados às áreas médicas e biomédicas. Também foram utilizados sites técnicos especializados em segurança cibernética nacionais e internacionais.

3. Revisão da literatura

Robôs têm sido muito utilizados na manufatura para agilizar as linhas de produção e melhorar a eficiência do sistema produtivo. Com o crescimento do número de dispositivos interconectados, trocando informações, o que se convencionou chamar Internet das Coisas, e da inteligência artificial, robôs (máquinas autónomas) estão tornando-se mais flexíveis, cooperativos e começando a interagir uns com os outros, juntamente com os seres humanos (LORENZ, 2015).

3.1 Internet das Coisas e Internet dos Serviços

A Internet das coisas ou *Internet of Things* (IoT, da sigla em inglês) pode ser definida como uma infraestrutura global de informação e sociedade, possibilitando serviços avançados interligando objetos - as coisas (físicas e virtuais) (*Internet of Things Global Standards Initiative* – ITU, 2015). A Internet dos Serviços pode ser entendida como um sistema que faz uso sistemático da Internet para novas formas de criação de valor no setor dos serviços (TERZIDIS; OBERLE; KADNER, 2012).

A Internet dos Serviços deverá gerar uma quantidade grande de novos serviços, disponíveis aos consumidores em todos os setores, e esses serviços deverão resultar no crescente aumento da Internet das Coisas.

3.2 Sistemas ciberfísicos

A Indústria 4.0 introduziu sistemas ciberfísicos na manufatura e serviços. Sistemas ciberfísicos são integrações de computação, rede e processos físicos (ASARE; BROMAN, 2012). Os sistemas ciberfísicos são a tecnologia que permite a extração de informações em tempo real, análise de dados, transmissão de dados e tomada de decisão, permitindo atuação remota, por usar a Internet (WIESNER; HAUGE; THOBEN, 2015).

4. Segurança cibernética

O crescimento dos sistemas ciberfísicos dentro Indústria 4.0 implicam em maior necessidade de cuidados com a segurança cibernética, já que um maior número de sistemas pode ficar vulnerável. A segurança cibernética visa a dar proteção contra roubo ou dano ao hardware empregado na Tecnologia da Informação - TI, bem como ao software e aos dados armazenados nos sistemas (HUXTABLE; SCHAEFER, 2016).

Para aumentar a segurança do sistema, cinco abordagens foram identificadas na literatura pesquisada.

4.1 Balanceamento de riscos

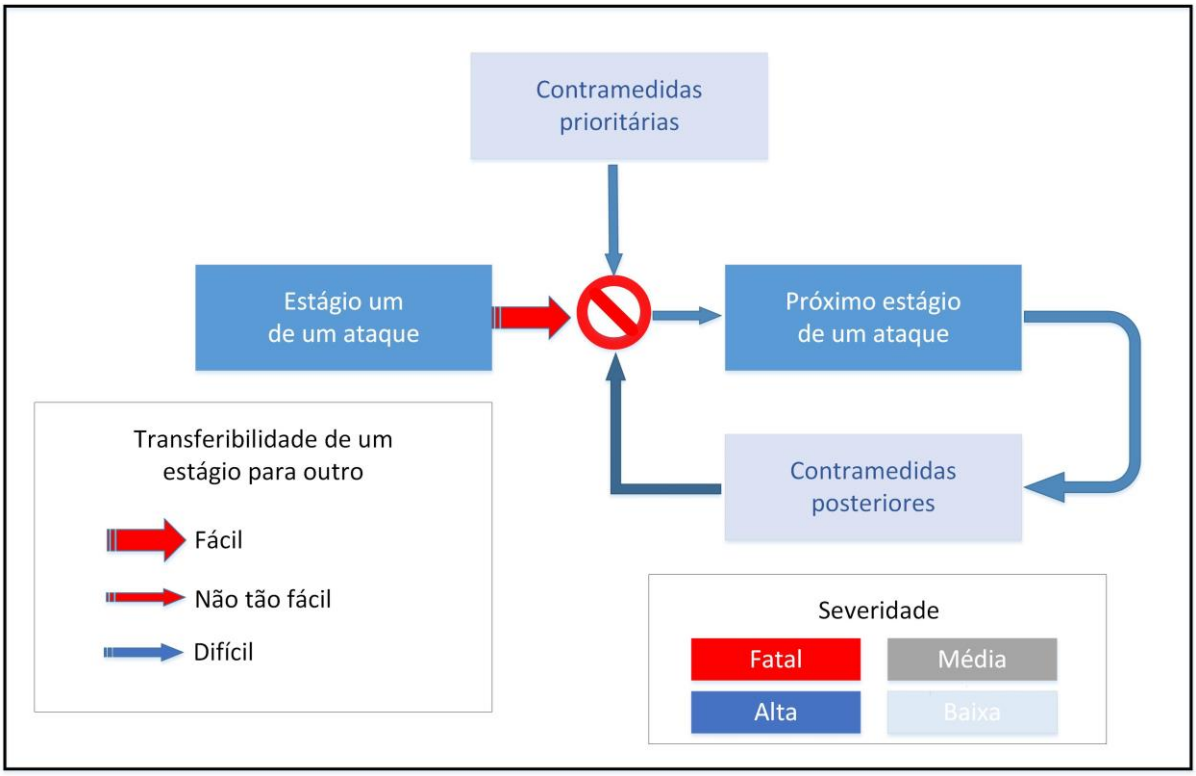
Estabelecer um balanceamento entre risco, segurança e contramedidas, não é uma tarefa simples. Kobara (2016) compara os riscos de segurança ao formato de árvore de ataque, em que um problema é como a raiz, e suas fontes como sendo as folhas. As fraquezas das árvores de ataque são os caminhos mais vulneráveis ao ataque, e contramedidas são os métodos de eficácia a serem empregados nos caminhos a fim de superar essas deficiências. A proposta é melhorar a árvore de ataque tomando-se ações, que devem ser analisadas segundo os seguintes aspectos (KOBARA, 2016):

a) Nível de gravidade de cada estágio ou nó;

b) Possibilidade de transferência de uma fase para outra, e

c) Contramedidas e seus efeitos.

Figura - 2 Exemplo de uma árvore de ataque



Fonte: Adaptado de Kobara (2016)

4.2 Mecanismos de autenticação

Huxtable e Schaefer (2016) propõe para a melhoria da segurança, o fortalecimento no mecanismo de autenticação de dispositivos IoT com o gateway interno e este com os serviços em nuvem, através de protocolos web com extensões de segurança e a habilitação de criptografia na camada de aplicação. Estas medidas fortalecem o laço de integridade e confidencialidade dos dados transacionados entre os dispositivos ciberfísicos usando a infraestrutura interna e caminhos até o serviço de nuvem pela Internet (HUXTABLE; SCHAEFER, 2016).

Atualmente vários dispositivos usam outros dispositivos intermediários, como celulares, para transferir dados via protocolo web com extensões de segurança. Isso não seria viável no futuro, em função do crescente número de dispositivos conectados na web. Existe uma necessidade de diminuir ou até mesmo remover esses dispositivos intermédios e alcançar diretamente a web usando mecanismos de mediação dos dados com extensões de segurança na camada da aplicação para chegar aos serviços de nuvem (GAURAV et al., 2015).

Gaurav et al. (2015) afirma que muitos dispositivos IoT conectados à nuvem comprometem sistematicamente a eficiência do processo de transações como um todo, e ainda mais associados a algoritmos de criptografia na camada de aplicação web, gerando nova preocupação com a rapidez com que os códigos são criptados e decriptados. Este fato está relacionado aos componentes físicos de rede integrados nos dispositivos IoT, por exemplo placas de baixos recursos representam alguns desafios, que poderiam ser superados usando algoritmos de criptografia mais simples.

4.3 Defesa e contra ataques

Schlaepfer (2015) estuda técnicas de defesa e contra ataque a dispositivos Internet das Coisas em diversos ambientes, incluindo a Indústria 4.0, classificando a possibilidade de ataques à segurança dentro de cinco áreas de observação: (1) desconfiança da vulnerabilidade das redes locais, (2) desconfiança generalizada do ambiente, (3) excesso de privilégios de aplicativos, (4) falta de autenticação ou autenticação fraca na camada de aplicativos e (5) falhas de implantação. Para cada área problema, deverá ser realizada uma investigação detalhada sobre a sua prevalência, severidade e causas, bem como estabelecidas estratégias de defesa, e técnicas de alinhamento para proteção contra as ameaças. Os ataques e defesas devem ser analisados com base em várias propriedades, tais como: canal de comunicação de rede, modelo de ameaça, invisibilidade e modificações necessárias para defesa (ZHANG et al., 2017).

Zhang et al., 2017 identifica a necessidade de se aprofundar na compreensão da mecânica das plataformas dos vários aplicativos emergentes, para estudo das suas vulnerabilidades,

sugerido também analisar as ameaças decorrentes do ambiente físico, tais como trabalhar na autenticação de voz e controlar esta autenticação de forma mais efetiva (ZHANG et al., 2017).

4.4 Comunicação maquina a maquina

Segundo Asare e Broman, 2012 o alto volume de dispositivos conectados exige cada vez mais o uso de comunicação máquina-máquina; assim no ápice correremos o risco de não ter mais controle direto sobre com quem, ou o que nossos dispositivos estarão se comunicando. Desta forma, a crescente presença de dispositivos on-line permite novos métodos de ataque e novas superfícies de ataque para que criminosos e hackers possam explorar, expondo graves questões de segurança e privacidade. Já são conhecidas inúmeras técnicas de ataque e defesa, e fica evidente o fato de dispositivos que são ligados em rede serem submetidos a sérias ameaças, que poderiam ter consequências significativas no mundo real, mais um dos muitos desafios dos aspectos de segurança a dispositivos Internet das Coisas (ZHANG et al., 2017).

4.5 Proteção extensiva dos dispositivos e canais de comunicação

De acordo com a *Internet of Things Global Standards Initiative* – ITU (2015) a segurança deve ser o foco principal da preocupação dos administradores de tecnologia e os usuários finais, o que é um desafio, devido à existência de bilhões de dispositivos na Internet onde novas tecnologias de diferentes fabricantes reivindicam fornecimento de soluções para as ameaças de segurança. Os mecanismos de segurança garantem a exatidão e a integridade dos dados sendo transportado através dos dispositivos de comunicação e dos gateways. A visão de segurança garante o envio dos dados corretamente para o seu destino sem qualquer distorção e moderação aplicada ao longo de sua jornada, da origem ao seu destino. O mecanismo de segurança deve construir uma relação de confiança entre as partes, emissor e receptor dos dados, também ter certeza de que um emissor está falando com o dispositivo receptor correto e vice-versa, ainda usar o canal de comunicação correto através do qual todos os dados confidenciais podem ser enviados (MATHEW; HAJJ, 2017).

Segundo ITU (2015), para proteção das ameaças em ambientes contendo muitos dispositivos, deve-se estar atento ao processo de verificação de identidade das partes envolvidas na

transação dos dados, - emissor e, receptor -, e se possível, também verificar os dispositivos que intermediam esta comunicação, bem como promover ações buscando a permissão para acesso aos dados ou todos os recursos que envolvem o processo de comunicação. A autenticação e identificação mútua são necessárias durante a comunicação, assim apenas duas questões de identificação de cada dispositivo e a autenticação de cada identidade precisam ser resolvidos. A identidade de verificação dos componentes (sensores, no próprio dispositivo, no gateway ou no servidor), e ainda no processo de comunicação são ambas importantes, contudo o grau de dificuldade aumenta quando existe um grande número de dispositivos envolvidos e o método de comunicação ser restrito.

Uma das barreiras é ser muito curto o tempo de vida dos pacotes de dados enviados de um grande número de dispositivos, sendo alterado com relativa frequência, bem como a mesma identidade de emissor/receptor não poder ser fornecida por um longo tempo devido ao temor sobre *hacking*. Quando um objeto - uma "coisa"-, está tentando autenticar neste processo de transmissão de dados, um mecanismo forte de autenticação deve ser usado, ou ainda um token peso criptográfico baixo e uma chave de criptografia privada com certificado. Lembrando que uma URL (endereço completo de origem ou destino) também pode ser associada ao dispositivo (MATHEW; HAJJ, 2017).

5. Considerações finais

A segurança da informação na aplicação de Internet das Coisas deve ser uma preocupação constante em todas as fases da transferência dos dados. Sugerem-se mais estudos para criação de modelos referenciais de ataque e defesa, assim como melhor detalhamento de uma classificação e avaliação dos riscos de segurança. É imprescindível a criação de novos *frameworks* de segurança para mitigar as ameaças existentes e prever situações de risco.

6. Conclusão

A segurança dos dispositivos Internet das Coisas foi avaliada com base em artigos científicos de relevância internacional, fruto de estudos das mais diversas fontes acadêmicas, contextualizando as bases da comunicação de dados com enfoque na cibersegurança física e

lógica, onde são identificados os conjuntos de contramedidas significativas para diversas técnicas de ataque.

Tendo suas restrições estabelecidas, a necessidade de cibersegurança física e lógica no futuro irão se expandir não só no campo da infraestrutura, mas também nos aplicativos, softwares especialistas e na linha base das redes de computadores. Entendendo que o ponto principal é a preservação da integridade, disponibilidade e autenticidade envolvida nas inúmeras formas de comunicação dos dispositivos Internet das Coisas, a proteção dos dados estará ainda mais vulnerável se o agressor obtiver acesso físico a estes.

Espera-se que este trabalho desperte o interesse da academia e da indústria para a necessidade do aprimoramento da segurança cibernética, a fim de que a Indústria 4.0 não se apoie em bases fracas, e venha a entrar em colapso como um todo.

REFERÊNCIAS

ASARE, P.; BROMAN D. **CPS, Cyber Physical Systems**. 2012. Disponível em: <http://cyberphysicalsystems.org/> . Acesso em: 09 abr. 2017.

CHOI, S. S., KANG, G., JUNG, K., KULVATUNYOU, B., MORRIS, K.C.: Applications of the factory design and improvement reference activity model. In: I. A. Nääs et al. (Eds.) **IFIP** 2016: APMS 2016 (2016).

CONFEDERAÇÃO NACIONAL DA INDÚSTRIA – CNI. Desafios para indústria 4.0 no Brasil. Brasília: **CNI**, 2016.

COMPUTER SECURITY. Everything is hackable. **The Economist**. p. 66-68, 8-14 abr., 2017

DE MORAIS, Roberto Ramos; MONTEIRO, Rogério. A indústria 4.0 e o impacto na área de operações: Um ensaio. In: V SINGEP – **Simpósio de Gestão De Projetos, Inovação e Sustentabilidade**. São Paulo, 2016.

EUROPEAN PARLIAMENT. **Industry 4.0 Digitalisation for productivity and growth**. Setembro de 2015. Disponível em: <http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/ EPRS_BRI(2015)568337_EN.pdf>. Acesso em: 14 abr. 2016.

GAURAV; K, GOYAL, P, AGRAWAL, V; RAO, S.L. IoT Transaction Security. In: **5th International Conference on the Internet of Things (IoT)**, p.1-2, 2015.

HOEKSTRA, P. Can Americans trust their spies? - If intelligence agencies can't keep their secrets, they can't credibly assure us they follow other rules. **The Wall Street Journal**. 15 mar. 2017.

HUXTABLE J.; SCHAEFER D. On Servitization of the Manufacturing Industry in the UK, **Procedia CIRP**. v. 52, p. 46-52, 2016.

INTERNET OF THINGS GLOBAL STANDARDS INITIATIVE – ITU**. – IoT-GSI.** 2015. Disponível em: <http://www.itu.int/en/ITUT/gsi/iot/Pages/default.aspx>. Acesso em: 09 abr. 2017.

KOBARA, Kazukuni, 2016. Cyber Physical Security for Industrial Control Systems and IoT. IEICE Transactions on Information and Systems. v.99–D, n. 4, p. 787-795, abr. 2016.

LORENZ, M. **Industry 4.0: The future of productivity and growth in the manufacturing sector**. Boston Consulting Group, 9th April 2015. Disponível em: <http://www.inovasyon.org/pdf/bcg.perspectives _Industry.4.0_2015.pdf>. Acesso em: 09 abr. 2017.

MARTINS, G. A; THEÓPHILO, C. R. **Metodologia da investigação científica para ciências sociais aplicadas**. 2. ed. São Paulo: Atlas, 2009.

MATHEW, A.R.; HAJJ A. A. Secure Communications on IoT and Big Data. **Indian Journal of Science and Technology**, v. 10 (11), |mar. 2017.

SCHLAEPFER, Ralf C. **Industry 4.0 Challenges and solutions for the digital transformation and use of exponential technologies.** 2015. Disponível em: <http://www.industrie2025.ch/fileadmin/user_upload/ch-en-delloite-ndustry-4-0-24102014.pdf. Acesso em: 09 abr. 2017.

TERZIDIS, O.; OBERLE, D.; KADNER, K. **The Internet of Services and USDL**, 2012. Disponível em: < https://www.w3.org/2011/10/integration-workshop/p/USDLPositionPaper.pdf>. Accesso em: 04 abr. 2017.

WIESNER, S., HAUGE, J.B., THOBEN, K-D.: Challenges for requirements engineering of cyber-physical systems in distributed environments. In: S. Umeda et al. (Eds.) APMS 2015, Part II, **IFIP** AICT 460, pp. 49–58 (2015).

ZHANG, N; DEMETRIOU, S, MI, X, DIAO, W, YUAN, K, et al. 2017. Understanding IoT security through the data crystal ball: Where we are now and where we are going to be. **Cornel University Library**, p. 1-19, 2017.