CEST
Centro de Estudos Sociedade e Tecnologia
USP
Universidade de São Paulo
Boletim - Volume 2, Número 3, Setembro/2017

IoT e Indústria 4.0

Rodrigo Filev

Os termos internet das coisas e manufatura avançada estão sem dúvida entre os tópicos mais discutidos desta década, e trazem o paradoxo entre a boa aventurança e o sucateamento do homem. A literatura acadêmica e técnica vêm sistematicamente apresentando tecnologias, integração de sistemas, plataformas, segurança e privacidade. A sinergia entre a internet das coisas e a manufatura digital criaram a indústria 4.0 ou manufatura avançada (termo mais amplo), assunto recorrente de diversos fóruns, entre eles o Fórum Econômico Mundial. As consequências destes dois novos paradigmas (IoT e manufatura avançada) são, dentre outras, mudanças profundas nas relações de trabalho e nas questões de privacidade e segurança.

Na esteira da evolução da internet das coisas e da manufatura avançada há diversos desafios globais a serem discutidos e solucionados.

A segurança cibernética já é tema antigo em fóruns de tecnologias e há tempos está presente nas atividades cotidianas; afinal quem nunca se preocupou em atualizar um antivírus do seu computador? Mas os contornos das ameaças atuais de segurança extrapolam em muito as questões puramente cibernéticas por um motivo: se a internet das coisas integra o mundo virtual com o mundo físico de uma forma inédita, e tem como uma das consequências a manufatura avançada, uma ameaça de segurança com origem no mundo virtual pode afetar como a perspectiva física? E a recíproca é verdadeira? No segundo semestre de 2016 uma notícia que poderia passar desapercebida tempos atrás confirmou temores discutidos nos ambientes acadêmico e de negócios: uma empresa de equipamentos médicos anunciou uma falha de segurança em um medidor de glicemia. Através desta falha de segurança um indivíduo poderia alterar as medidas do referido aparelho, o que poderia fazer com que um paciente administrasse quantidades de insulina inapropriadas ao seu organismo. Naturalmente, as consequências podem causar danos severos à saúde.

Numa sociedade IoT (ou Cyber Physical Society) já é necessário proteger um indivíduo de uma falha virtual que pode causar um dano físico. Talvez se pudesse pensar que a solução seja instalarmos firewall nos medidores de glicemia, ou utilizarmos canais de comunicação criptografados, e desta forma resolveríamos o problema. Felizmente o desafio é mais complexo e instigante, pois os dados destes novos sistemas IoT descrevem tanto particularidades dos ambientes quanto detalhes sobre as pessoas que estão nestes ambientes, dados tão íntimos quanto de saúde ou de hábitos privados. Além disto, falhas ou ataques a sistemas IoT podem causar danos materiais não só a um indivíduo, mas a uma comunidade inteira. Em um outro exemplo já houve ataques muito bem documentados a veículos que puderam ser dirigidos à distância por um atacante, tornando o motorista impotente.

Atualmente não se tem mecanismos de segurança que previnam as ameaças à sua privacidade. Paradoxalmente as mudanças nos limites da privacidade trazem serviços novos, surpreendentes e benéficos sob vários aspectos. Para o consumidor, o uso de um determinado serviço gratuito que pede em troca acesso aos dados do indivíduo parece um bom negócio, e até mesmo inofensivo; contudo, o consumidor não se atenta para o fato de que cada um dos aplicativos que ele utiliza, os serviços de uma cidade

inteligente (ainda que limitados) e os dados capturados geram perfis de uso do serviço, os quais certamente procuram representar o cidadão em uma espécie de avatar, ou procura classificar um indivíduo em um estereótipo (persona), ambos os casos para melhor oferecer serviço ao consumidor. Neste cenário, há o risco de um determinado serviço produzir um perfil ou classificar um determinado indivíduo de forma incorreta e até mesmo prejudicial, o que também pode ser considerado uma falha de segurança.

Suponha que um pesquisador ou um profissional da área de segurança trabalhe com um tema sensível, como combate a um crime. Suponha que tal profissional combata crimes sexuais cometidos contra crianças e adolescentes. Suponha também que este mesmo profissional tenha filhos ainda na primeira infância ou pré-adolescentes. Imagine a situação que este profissional vá ao trabalho e deixe o seu smartphone ao seu lado constantemente, conectado à rede sem fio do seu local de trabalho. Cenário absolutamente factível e existente hoje. Algo que acontece é que o fabricante do sistema operacional do smartphone deste profissional informa a rede de dados e a localização em que o mesmo se encontra, e dado a hora do registro e dia da semana não é difícil concluir que o indivíduo está trabalhando. Da mesma forma, se o profissional deve se passar por um predador sexual em uma investigação e usar a internet para se infiltrar em uma determinada comunidade virtual, é possível que o browser registre os acessos do indivíduo, e coletando dados pode inferir que aquele usuário acessa dados sobre pornografia infantil, e como tanto os computadores quanto os smartphones de diversos profissionais estão em uma mesma rede, logo há pelo menos um candidato a ser um predador sexual naquele local. Se o sistema souber que naquele local trabalham profissionais da área de segurança, tudo bem. Contudo, se este profissional estiver em outro lugar qualquer, utilizando um laptop e com o smartphone no bolso, então um sistema IoT pode presumir que o usuário daquele smartphone é um predador sexual; afinal, o uso do laptop mais a proximidade do smartphone indicam um sujeito perigoso. Se esta informação é compartilhada com outros sistemas, algo corriqueiro hoje, o que pode acontecer se este individuo for a uma loja de roupas infantis comprar algo para um de seus filhos? O que o sistema da loja recomendaria? Poderia a loja ser avisada sobre um potencial cliente perigoso?

Este cenário fictício pode ocorrer se não houver mecanismos de gestão de dados que sejam capazes de discernir questões sensíveis. Imagine situação similar na manufatura avançada, onde se deseja produzir produtos personalizados para qualquer indivíduo. Suponha a indústria de medicamentos que poderá produzir um determinado remédio na dosagem apropriada para o organismo do consumidor. Esta indústria provavelmente precisará de dados da genética de um individuo, e sem um controle de privacidade adequado, o risco de segurança potencial que tais dados possuem não está claro, mas os impactos estimados são tremendos.

Na esteira da evolução da internet das coisas e da manufatura avançada há diversos desafios globais a serem discutidos e solucionados, e não podemos nos dar ao luxo de não ter voz ativa em tais questões. Embora privacidade e segurança estejam sendo discutidas do ponto de vista tecnológico parece caber considerar o ser humano como integrado à solução de segurança e privacidade, e não o considerar apenas um usuário, pois questões e valores de ordem pessoal serão fundamentais para que os novos serviços busquem ser seguros.

Rodrigo Filev *é Doutor em Engenharia de Computação pela Escola Politécnica da Universidade de São Paulo e pesquisador do CEST-USP.*

Coordenador: Edison Spina

Este artigo resulta do trabalho de apuração e análise do autor, não refletindo obrigatoriamente a opinião do CEST.