# A Internet das coisas e a segurança do mundo real

Bruce Schneier, *especialista em segurança de tecnologias de informação, fellow do Berkman Center dUniversidade Harvard, membro do conselho da Electronic Frontier Foundation e membro do conselho do Centro de Informação sobre Privacidade Eletrônica*

## Data da publicação:

Data da publicação: Outubro de 2016

Histórias de desastres envolvendo a Internet das Coisas estão na moda[1]. Incluem carros (com ou sem motorista), a rede de energia, barragens e sistemas de ventilação de túneis. Uma especialmente vívida e realista, uma ficção sobre o futuro próximo publicada no mês de junho de 2016 no New York Magazine descrevia um ciberataque a Nova York envolvendo ataques de hackers a veículos, ao sistema de abastecimento de água, a hospitais, elevadores e à rede elétrica. Nessas histórias, milhares de pessoas morrem. Estabelece-se o caos. Enquanto alguns desses cenários exageram a destruição em massa[2], os riscos individuais são todos reais. E a segurança de computadores e redes tradicional não está preparada para lidar com eles.

A segurança da informação clássica é uma tríade: confidencialidade, integridade e disponibilidade. Em inglês essa tríade é frequentemente referida pela sigla CIA ("confidentiality, integrity, and availability"), que, convenhamos, cria alguma confusão no contexto da segurança nacional. Mas basicamente as três iniciativas que podem ser feitas com seus dados são furtá-los (confidencialidade), modificá-los (integridade) ou bloqueá-los impedindo que você os use (disponibilidade).

Até agora as ameaças da Internet têm sido largamente sobre confidencialidade. Estas podem ter consequências custosas; uma amostragem estimou que as violações de dados custam uma média de US$ 3,8 milhões cada[3]. Elas podem ser constrangedoras, como o furto de fotos de celebridades do iCloud da Apple em 2014 ou a violação do portal Ashley Madison em 2015. Eles podem ser prejudiciais, como quando o governo da Coreia do Norte furtou dezenas de milhares de documentos internos da Sony ou quando hackers roubaram dados de cerca de 83 milhões de contas de clientes do banco JPMorgan Chase, ambos em 2014. Elas podem até mesmo afetar a segurança nacional, como no caso da violação de dados do Escritório de Administração de Pessoal do governo dos EUA, presumivelmente pela China em 2015.

Na Internet das Coisas, as ameaças à integridade e disponibilidade são muito piores que as ameaças à confidencialidade[4]. Uma coisa é se a fechadura inteligente de sua porta permite bisbilhotagem para saber que está em casa. Outra coisa bem diferente é se a fechadura pode ser violada por hackers para permitir que um ladrão abra a porta – ou impeça o dono da casa de abrir a porta[5]. Um hacker que pode bloquear o controle de seu carro, ou assumir o controle do mesmo, é muito mais perigoso do que aquele que pode escutar suas conversas ou rastrear a localização do seu carro.

Com o advento da Internet das Coisas e de sistemas ciberfísicos em geral, estamos dando à Internet mãos e pés: a capacidade de afetar diretamente o mundo físico[6]. Ataques contra dados e informações agora passam a ser também ataques contra pessoas físicas, aço e concreto.

As ameaças de hoje incluem queda de aviões através de ataques a redes de computadores[7], e desativação remota de veículos, seja quando estão desligados e estacionados ou enquanto eles estão em alta velocidade na estrada[8]. Estamos preocupados com manipulação de contagens em urnas eletrônicas[9], canos de água congelados devido a ataques a termostatos[10], e assassinato remoto através de ataques a sistemas médicos[11]. As possibilidades são quase literalmente infinitas. A Internet das coisas poderá permitir ataques não podemos sequer imaginar.

Os maiores riscos são provenientes de três coisas: sistemas controlados por software; interconexões entre

sistemas; e sistemas automáticos ou autônomos. Vejamos cada um deles:

**Software de controle**
A Internet das coisas é o resultado de existir um computador em todos os dispositivos. Isso nos dá um enorme poder e flexibilidade, mas também traz inseguranças. À medida que mais coisas estão sob controle de software, tornam-se vulneráveis a todos os ataques já mencionados contra computadores. Mas devido a que muitas dessas coisas são de baixo custo e de longa duração, muitos dos sistemas de atualizações e correções que ocorrem rotineiramente para computadores e smartphones não funcionam. Atualmente, a única maneira de corrigir ou atualizar o software da maioria dos roteadores domésticos é jogá-los fora e comprar novos. E a segurança obtida com a substituição do seu computador ou telefone celular a cada poucos anos não vai ser viável com seu refrigerador ou o termostato de sua casa: na média, um refrigerador é substituido a cada 15 anos[12], e o termostato provavelmente nunca vai ser trocado. Uma pesquisa recente da Universidade de Princeton encontrou 500 mil dispositivos inseguros na Internet[13]. Esse número está prestes a explodir.

**Interconexões**
À medida que os sistemas são interligados, as vulnerabilidades em um podem levar a ataques contra outros. Já vimos contas do Gmail comprometida através de vulnerabilidades em refrigeradores inteligentes Samsung[14], redes hospitalares comprometidas através de vulnerabilidades em dispositivos médicos[15], e os sistemas da empresa Target invadidos devido a uma vulnerabilidade no seu sistema de ventilação e ar condicionado[16]. Sistemas contêm externalidades que afetam outros sistemas de modos imprevisíveis e potencialmente prejudiciais. O que aparenta ser benigno para os projetistas de um sistema pode tornar-se prejudicial quando ele é combinado com algum outro sistema. Vulnerabilidades em um sistema podem propagar-se a outros sistemas, e o resultado é uma vulnerabilidade que ninguém percebeu e ninguém é responsável pela mitigação. A Internet das coisas vai tornar muito mais corriqueira a ocorrência de vulnerabilidades exploráveis. É matemática simples. Se 100 sistemas estão interagindo, isso significa cinco mil interações e cinco mil vulnerabilidades potenciais resultantes dessas interações. Se 300 sistemas estão interagindo, isso resulta em 45 mil interações. Mil sistemas: 12,5 milhões de interações. A maioria delas vai ser benigna ou desinteressante, mas algumas serão muito prejudiciais.

**Autonomia**
Nossos sistemas de computação são cada vez mais autônomos. Eles compram e vendem ações, ligam ou desligam o aquecedor, regulam o fluxo de eletricidade através da rede e – no caso de veículos sem motorista – pilotam automaticamente viaturas a seus destinos. A autonomia é interessante por várias razões, mas de uma perspectiva de segurança ela significa que os ataques podem ter efeito imediato, automático e amplo. Quanto mais nós removemos os seres humanos do controle, ataques mais rápidos podem ocorrer e mais perdemos a capacidade de usar dispositivos inteligentes que nos ajudariam a perceber falhas antes que seja tarde demais.

Estamos construindo sistemas que são cada vez mais poderoso e cada vez mais úteis. O efeito secundário decorrente é que eles são cada vez mais perigosos. Uma única vulnerabilidade forçou a Chrysler a chamar para reparos 1,4 milhões de veículos em 2015[17]. Estamos acostumados a computadores sendo atacados em massa – basta lembrar das infecções por virus em grande escala a partir da última década - mas não estamos preparados para a possibilidade de isso ocorrer em todas as coisas ao nosso redor.

Os governos estão começando a preocupar-se. No ano passado, tanto o diretor da Inteligência Nacional (DNI) dos EUA James Clapper[18] e o diretor da NSA Mike Rogers[19] testemunharam perante o Congresso, alertando para essas ameaças. Ambos acreditam que somos vulneráveis.

A Avaliação de Ameaças Mundiais feita pelo DNI em 2015 coloca o desafio desta forma: “A maior parte da discussão pública sobre as ameaças cibernéticas concentrou-se na confidencialidade e oferta da informação; a espionagem cibernética enfraquece a confidencialidade, ao passo que os ataques de negação de serviço e as ações de destruição de dados enfraquecem a oferta de produtos e serviços. No futuro, no entanto, poderemos ver também mais operações cibernéticas para alterar ou manipular informação eletrônica, a fim de comprometer a sua integridade (ou seja, precisão e confiabilidade) em vez de apagá-la ou bloqueá-la. A tomada de decisões governamentais, de executivos, investidores ou outros será prejudicada se eles não podem confiar nas informações que estão recebendo”[20].

A edição de 2016 da Avaliação do DNI constatou: “As operações cibernéticas futuras quase certamente darão uma ênfase maior nas ações de manipulação ou alteração de dados para comprometer sua integridade… que poderão afetar a tomada de decisões, reduzir a confiança em sistemas ou causar efeitos físicos adversos. A adoção mais ampla de dispositivos de Internet das coisas e inteligência artificial – em ambientes como sistemas

de saúde e serviços públicos – só irá agravar esses efeitos potenciais”[21].

Especialistas em segurança estão trabalhando em tecnologias que podem mitigar grande parte desses riscos, mas muitas soluções não poderão ser implantadas sem o envolvimento dos governos. Isso não é algo que o mercado pode resolver. Tal como no caso da privacidade dos dados, os riscos e as soluções são técnicos demais para a compreensão da maioria das pessoas e organizações; empresas podem procurar esconder de seus clientes, seus usuários e o público a insegurança de seus próprios sistemas; as interconexões podem tornar impossível relacionar os violadores de dados com os danos resultantes; e os interesses das empresas muitas vezes não coincidem com os interesses do público[22].

Os governos precisam desempenhar um papel maior: estabeler normas, fiscalizar a conformidade, estimular a implementação de soluções em empresas e redes. E, nos EUA, mesmo que o Plano de Ação Nacional de Cibersegurança do governo federal tenha alguns pontos corretos, está longe de ser suficiente, até porque muitos de nós desconfiam de qualquer solução liderada pelo governo. A próxima pessoa a ocupar a presidência dos EUA será provavelmente forçada a lidar com um desastre na Internet em grande escala que poderá inclusive matar muita gente. Espero que ele ou ela responda com tanto o reconhecimento do que o governo pode fazer que a indústria não pode, como com a vontade política de fazer isso acontecer.

--

1. https://motherboard.vice.com/tag/The+Internet+of+Hackable+Things
2. https://www.schneier.com/essays/archives/2005/09/terrorists_dont_do_m.html
3. https://securityintelligence.com/cost-of-a-data-breach-2015
4. https://www.schneier.com/blog/archives/2016/01/integrity_and_a.html
5. https://www.wired.com/2016/05/flaws-samsungs-smart-home-let-hackers-unlo...
6. https://www.schneier.com/blog/archives/2016/02/the_internet_of_1.html
7. http://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft
8. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
9. https://www.schneier.com/blog/archives/2004/11/the_problem_wit.html
10. http://www.networkworld.com/article/2905053/security0/smart-home-hacking...
11. http://www.informationweek.com/partner-perspectives/bitdefender/hacking-...
12. http://homeguides.sfgate.com/expected-life-refrigerator-88577.html
13. https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet...
14. http://www.networkworld.com/article/2976270/internet-of-things/smart-ref...
15. http://www.meddeviceonline.com/doc/medjacking-how-hackers-use-medical-de...
16. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-comp...
17. https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-b...
18. http://www.scmagazine.com/intelligence-committee-hosts-cybersecurity-hea...
19. http://thehill.com/policy/cybersecurity/254977-officials-worried-hackers...
20. http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINA...
21. http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf
22. https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html

Categoria:

- poliTICs 24