Veículos autônomos são riscos gigantescos à segurança e a defesa dos sistemas precisa antecipar-se aos ataques*

Zach Aysan, cientista especialista em cibersegurança dedicado à defesa de melhor qualidade de vida nas cidades; membro da iniciativa comunitária CityAction em Toronto, Canadá

Data da publicação:

Dezembro de 2018

(*) [1]

Em janeiro de 2018 publiquei minhas preocupações sobre como vários veículos autônomos poderiam ser controlados simultaneamente via ataque cibernético[2]. (Para quem não leu, aqui está a essência: devido à natureza do tipo tudo-ou-nada de certas classes de ataque cibernético, carros autônomos e outros sistemas autônomos podem ser utilizados por agentes hostis para criar um ataque em massa coordenado.) Está na hora de uma atualização.

Em uma sessão de perguntas e respostas a portas fechadas na conferência de hackers de software DEF CON[3], Elon Musk disse que um ataque em massa era um "cenário de pesadelo" da Tesla e anunciou que a empresa abriria seus módulos de segurança para que os fabricantes trabalhassem juntos para garantir um futuro autônomo seguro. (Mais tarde, ele anunciou a iniciativa de código aberto de segurança no Twitter.[4]) O anúncio de Musk é um ótimo começo que deixa-me animado, já que uma iniciativa de código aberto é o passo mais importante para garantir a segurança de veículos autônomos. Mas houve outros desenvolvimentos também.

Em uma conferência de segurança cibernética ofensiva no início deste ano, Matt Tait, ex-especialista em segurança da informação do GCHQ[5], foi o principal palestrante. (Os advogados sabem que Tait é um colaborador do blog Lawfare[6] e hackers o conhecem como @pwnallthethings – é divertido e estranho quando os mundos colidem.) Um dos comentários finais de Tait foi que agora há múltiplas ameaças estratégicas mundiais de um ciberataque em massa.

Os planejadores militares chamam de ameaças estratégicas as armas nucleares e outras armas de destruição em massa porque elas afetam o planejamento militar em relação à estratégia de defesa nacional. Tait usou o exemplo específico de uma atualização do Windows alterada por hackers, que poderia acabar com cadeias complexas de logística ou paralisar a rede elétrica. O mesmo tipo de ameaça estratégica também existe para dispositivos autônomos. Tait então implorou aos seus colegas pesquisadores em cibersegurança que fossem cuidadosos com as conseqüências de suas ações. Para ilustrar isso, ele exibiu uma nuvem de cogumelos como a imagem de fundo da apresentação.

O que nos traz ao presente. Bruce Schneier é o profissional de cibersegurança mais conhecido do mundo e, durante décadas, tem sido considerado um pensador equilibrado, sóbrio e cuidadoso. Em setembro, Schneier lançou um novo livro intitulado Click Here to Kill Everybody[7]. Nele, o autor aborda o perigo do tudo-ou-nada de certas classes de ataques cibernéticos e menciona especificamente o risco de um ataque cibernético em massa a veículos automotores computadorizados.

Portanto, a má notícia é que o risco de um ataque cibernético bem sucedido a um único sistema é agora catastrófico. Mas a boa notícia é que as pessoas agora estão começando a prestar atenção. Em 2018, o governo canadense anunciou aumentos de gastos para defesa cibernética, aumentou o financiamento para a divisão de crimes cibernéticos da Polícia Montada Real Canadense e destacou uma interação maior com membros do setor privado na criação de ciber-reservistas e forças ciberespeciais associadas.

Todos estes são desenvolvimentos encorajadores. Mas regular dispositivos autônomos é muito complicado para os canadenses atacarem sozinhos. Os países centrais precisam liderar um esforço internacional em regulamentações para dispositivos ciberfísicos. O senador Ben Sasse, o congressista James Langevin e alguns outros líderes dos EUA entendem que esse é um problema real e urgente, e precisamos que seus colegas se juntem a eles. Legisladores e funcionários devem ler o livro de Schneier para entender melhor essa crescente ameaça e trabalhar com parceiros do setor privado, enquanto ainda temos tempo.
--

1 Tradução adaptada do original em inglês em https://www.weeklystandard.com/zach-aysan/driverless-cars-could-become-wmds, publicada com autorização.

2 https://www.weeklystandard.com/zach-aysan/terrorists-could-use-teslas-to.... Versão em português na *poliTICs*: https://politics.org.br/edicoes/terroristas-poderiam-usar-teslas-para-no...

3 https://www.defcon.org

4 https://twitter.com/elonmusk/status/1028351047478042624

5 https://www.gchq.gov.uk

6 https://www.lawfareblog.com/contributors/mtait

7 https://www.schneier.com/books/click_here

Categoria:

- poliTICs 28