TIM Lecture Series

The Internet of Everything: Fridgebots, Smart Sneakers, and Connected Cars

Jeff Greene

> *"Cybersecurity considerations need to be at the forefront of our minds as the Internet of Things moves from expectation to reality.*
>
> Jeff Greene
> Director of NAM Government Affairs & Senior Policy Counsel
> Symantec

Overview

The TIM Lecture Series is hosted by the Technology Innovation Management program (carleton.ca/tim) at Carleton University in Ottawa, Canada. The lectures provide a forum to promote the transfer of knowledge between university research to technology company executives and entrepreneurs as well as research and development personnel. Readers are encouraged to share related insights or provide feedback on the presentation or the TIM Lecture Series, including recommendations of future speakers.

The second TIM lecture of 2015 was held at Carleton University on March 18th, and was presented by Jeff Greene, Director of NAM Government Affairs & Senior Policy Counsel at Symantec (symantec.com). Greene provided an overview of the Internet of Things to compare the hype versus reality and to examine the security implications of connecting myriad physical devices to the Internet and to each other.

Summary

Greene began by sharing examples of new technologies in which privacy concerns, vulnerabilities, and even intrusions that increasingly come from unexpected places, such as trash cans that track pedestrians via smartphones (Satter, 2013), Smart TVs with security gaps through which hackers could view and record users through their webcams (Fink & Segall, 2013), and camera-enabled baby monitors that hackers have been able to control remotely (Hill, 2013). Technologies such as these will become familiar components of the Internet of Things (IoT), or the Internet of Everything, although Greene cautions against defining these terms too closely:

> *"There is no hard and fast definition of the Internet of Things, in part, because it is so new and continues to evolve. Even five or ten years from now, we will likely be calling the IoT something different."*

In the context of the lecture, Greene's view of the Internet of Things is quite broad, and it includes "a whole host of connected endpoints that in some way interact with the physical world, whether sensing, acting, or reacting". This view extends beyond computers and handheld devices – it includes factories, water treatment plants, fitness devices, toys, and so on. And, generally, he finds that it can be helpful to distinguish between the industrial Internet of Things (e.g., heavy machinery, manufacturing, critical infrastructure) and the consumer Internet of things (e.g., appliances, toys, home devices).

Greene argued that, although we see current technologies that will likely contribute to the Internet of Things, we are likely still five to ten years a from realizing it, meaning that we still have a window of opportunity to shape it and ensure that it is as secure as possible. In particular, we must recognize the clash of cultures between the physical world and the IT world that the Internet of Things brings about. For example, manufacturers and critical infrastructure utilities depend on having their systems up and running 24 hours per day, whereas the IT culture assumes systems will be taken down on a regular basis for patching and other maintenance.

TIM Lecture Series – The Internet of Everything

Jeff Greene

Greene's presentation included examples of the intersections between vulnerabilities in the physical and IT worlds and the poor practices that are increasing creating cyber-risks as the Internet of Things evolves. Notably, many of the underlying vulnerabilities do not represent a shortcoming in technical development, but rather point to poor security practices that can be remedied, such as re-using or sharing passwords, hard-coding passwords, and having (or not changing) default passwords. Thus, there are basic steps that can be taken to improve security through behavioural changes, without requiring innovative technological solutions. Equally, there can be greater consideration paid to human behaviour when designing and implementing technical solutions. For greater cybersecurity, this human-behaviour element should also factor into our expectations of how devices will be used. Increasingly, devices are being used in ways or for purposes not intended by their designers. As users, Greene encourages us to focus less on the question "can it be connected?" and ask instead "should it be connected?"

In closing, Greene examined what is being done to assess the risks of the Internet of Things and to develop appropriate policies for its cybersecurity so that we can all enjoy the tremendous benefits that it may bring. As identified by the National Security Telecommunications Security Advisory Committee (NSTAC, 2014) in the United States, there is "a small – and rapidly closing – window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations." Greene reports that this small and rapidly closing window is likely on the scale of two to four years:

> *"Based on our experience with the Internet itself, and its key lesson that security should be part of design, we have only a short time to avoid making the same mistake with the Internet of Things. Cybersecurity considerations need to be at the forefront of our minds as the Internet of Things moves from expectation to reality."*

About the Speaker

Jeff Greene is the Director of Government Affairs for North America and Senior Policy Counsel at Symantec, where he focuses on issues including cybersecurity, the Internet of Things, and privacy. In this role, he monitors executive and legislative branch activity and works extensively with industry and government organizations. Prior to joining Symantec, Jeff was Senior Counsel with the U.S. Senate Homeland Security and Governmental Affairs Committee, where he focused on cybersecurity and Homeland Defense issues. He has also worked in the House of Representatives, where he was a subcommittee staff director on the House Committee on Homeland Security. Previously, he was an attorney with a Washington, D.C. law firm, where his practice focused on government contracts and contract fraud, as well as general civil and criminal investigations. Jeff recently served as the staff co-chair of the "Internet of Things" research subcommittee of the President's National Security Telecommunications Advisory Committee. He is also a Senior Advisor at the Truman National Security Project, where he is on the Steering Committee for the Cyberspace and Security Program. He is co-chair of the Homeland Security Committee of the American Bar Association's Section of Science & Technology Law and is on the Executive Committee of the Information Technology Sector Coordinating Council. He has a BA in International Relations from Boston University in the United States and a JD with Honors from the University of Maryland, also in the United States, where he has taught classes in Homeland Security law and policy.

This report was written by Chris McPhee.

TIM Lecture Series – The Internet of Everything

Jeff Greene

References

Fink, E., & Segall, L. 2013. Your TV Might Be Watching You. *CNN Money*. August 1, 2013. Accessed March 1, 2015: http://money.cnn.com/2013/08/01/technology/security/tv-hack/

Hill, K. 2013. How a Creep Hacked a Baby Monitor to Say Lewd Things to A 2-Year-Old. *Forbes*. August 13, 2013. Accessed March 1, 2015: http://www.forbes.com/sites/kashmirhill/2013/08/13/how-a-creep-hacked-a-baby-monitor-to-say-lewd-things-to-a-2-year-old/

NSTAC. 2014. *Draft Report to the President on the Internet of Things*, November. Washington, DC: Department of Homeland Security, National Security Telecommunications Security Advisory Committee.

Satter, R. 2013. London's Creepiest Startup' Forced to Pull 'Spy' Trash Cans that Could Track London Pedestrians via Smartphones. *National Post*. August 12, 2013. Accessed March 1, 2015: http://news.nationalpost.com/2013/08/12/londons-creepiest-startup-forced-to-pull-spy-trash-cans-that-could-track-london-pedestrians-via-smartphones/

Citation: Greene, J. 2015. TIM Lecture Series – The Internet of Everything: Fridgebots, Smart Sneakers, and Connected Cars. *Technology Innovation Management Review*, 5(5): 47–49. http://timreview.ca/article/898

Keywords: cybersecurity, Internet of Things, IoT, Internet of Everything, Industrial Internet, Consumer Internet of Things, hackers, cyber-attacks