TIM Lecture Series Three Collaborations Enabling Cybersecurity

Deborah Frincke, Dan Craigen, Ned Nadima,
Arthur Low, and Michael Thomas

> *“Cybersecurity is a huge global issue. And no one organization can solve these problems by itself. We need collaborative approaches. We need to partner. We need ecosystems. We need to bring together our very best. And it's going to take time.”*
>
> Dan Craigen
> Science Advisor
> Communications Security Establishment

Overview

The TIM Lecture Series is hosted by the Technology Innovation Management (TIM; timprogram.ca) program 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 third TIM lecture of 2015 was held at Carleton University on May 14th, and was presented by several speakers, each representing different collaborations to enable cybersecurity. In the keynote presentation, Deborah Frincke, Director of Research for the National Security Agency/Central Security Service (www.nsa.gov) in the United States, described the NSA's Research Directorate and its efforts to create breakthroughs in mathematics, science, and engineering that support and enable the wider organization's activities.

Next, Dan Craigen, Science Advisor at the Communications Security Establishment in Canada and a Visiting Scholar at the Technology Innovation Management program of Carleton University in Ottawa, Canada, launched the newest title in the "Best of TIM Review" book series (timbooks.ca), which he co-edited along with Ibrahim Gedeon, Chief Technology Officer at TELUS (telus.com). The book features 15 of the best articles on cybersecurity published in the TIM Review, selected and introduced by the co-editors, and with a foreword from Eros Spadotto, Executive Vice President of Technology Strategy at TELUS. *Cybersecurity: Best of TIM Review* is available for purchase from Amazon (amazon.com/dp/B00XD3O6L0/) in ebook format for Kindle. All proceeds support the ongoing operation of the TIM Review.

Finally, representatives from three companies – Denilson, Crack Semiconductor, and Bedarra Research Labs – described their approaches to collaboration and challenging cybersecurity problems.

Summary

Part I: An introduction to the Research Directorate of the National Security Agency

As Director of Research for the NSA, Frincke leads the only full-spectrum in-house research organization in the United States intelligence community, although its research activities extend beyond the organization through collaborations, linkages, and partnerships with industry, academia, and other government agencies, both within and beyond the United States. The NSA's overall objectives are to:

- defend the vital networks of the United States
- advance the goals of the United States and its alliances
- provide guidance to national decision makers

The Research Directorate engages with leading industries, universities, and national laboratories to both advance core competencies and to leverage work in overlapping disciplines. Through the NSA's Technology Transfer Program, the Directorate licenses and shares internally developed technologies with industry, academia, and other government agencies. As examples of such work, Frincke provided an overview of some of the NSA's laboratories and research centres, including:

1. Laboratory for Physical Sciences
(College Park, Maryland; www.lps.umd.edu)

2. Laboratory for Telecommunication Sciences
(College Park, Maryland; www.ltsnet.net)

3. Center for Advanced Study of Language
(College Park, Maryland; www.casl.umd.edu)

4. Research & Engineering
(Emmerson III, Lavel, Maryland)

5. Laboratory for Analytic Science
(Raleigh, NC). For details, see the summary of the July 2014 TIM Lecture by David J. Harris (timreview.ca/article/813).

6. The Science of Security online community and network of "lablets" (cps-vo.org/group/SoS)

Finally, Frincke shared some key lessons learned through the activities of the Research Directorate:

1. It is important for a research organization to look ahead, but it must also assess the past and present. A key challenge is to plan for a future where there is an ever-more capable adversary. However, we must also assess technologies that are mature or perhaps past their primes, make decisions about whether or not to continue investing in those technologies, and determine what past activities can be drawn upon for further research.

2. Research must consider the transition paths for new technologies, including research, training, and assistance with culture change. When facing the challenge of managing transitions from the Research Directorate to other directorates, one approach is to embed researchers in missions, which enables learning for new research and transitioning new technology, processes, culture, etc.

3. There is a tendency to always want to "add"; however, doing "new" work means dropping something "old". We try to move on from research that is not coming along fast enough or identify technology that is sufficiently mature that it can be brought out of the NSA for further development.

4. The diversity of classified and unclassified information, research, and devices within the NSA creates a balancing act this is all at once a physical problem (e.g., buildings), a people problem (e.g., access), a technology problem (e.g., security), and a culture problem (e.g., people).

5. We try to invest two-thirds of our efforts into what "the customer" says they want and one-third into what they do not yet know they need or say they do not want, including new, radical innovations.

6. We use strategic forecasting to understand "the outside world", the capacities and capabilities of the adversary, what is happening globally, technology, and investment trends/patterns. We need to make investment decisions along each of these dimensions: how much to invest and when.

Part II: Book launch

Dan Craigen introduced the fourth book in the Best of TIM Review series (timbooks.ca), which was launched at this event. The book stems from five issues on Cybersecurity published in the TIM Review:

1. July 2013 (timreview.ca/issue/2013/july)

2. August 2013 (timreview.ca/issue/2013/august)

3. October 2014 (timreview.ca/issue/2014/october)

4. November 2014 (timreview.ca/issue/2014/november)

5. January 2015 (timreview.ca/issue/2015/january)

These issues represent various research efforts and collaborations led by the Technology Innovation Management (TIM; timprogram.ca) program at Carleton University. In outlining the approach used in the TIM program and illustrated in the articles in the book, Craigen emphasized that technology is only a component of the overall solution to the cybersecurity challenges we are facing today. He stressed that we are as much facing a human behaviour problem as a technology problem. And, he called for multiple disciplines to come together (e.g., sociology, psychology, economics, entrepreneurship) to better understand the developing criminal markets and related mechanisms. The key messages were that cybersecurity is a global issue and that we need to partner and collaborate, using an ecosystem approach, because no one organization can solve these problems by themselves.

Craigen highlighted that we lack a science of cybersecurity, although this book highlights several steps being taken in that direction. Developing the science will take time, but it will allow us to develop a holistic, proactive approach to replace our current paradigm, which involves simply reacting to new events as though they are independent and do not share any underlying mechanisms or patterns. As evidenced by the articles in this book, efforts are going on to contribute to the science of security, by adding intellectual capacity through courses and research, and through the application of theory to practical problems in the real world.

The book presents different ways of thinking about cybersecurity problems. The hope is that these articles will contribute to theory and provide practical solutions, but also that they will sow the seeds of future research and discussion in different areas. Based on the five special issues published in the TIM Review from 2013 to 2015, the co-editors selected 15 that they feel provide particularly relevant insights into cybersecurity and, in general, contribute to a theory (or science) of cybersecurity. These articles have been divided into three categories:

1. *Understand:* developing and applying models to examine what is happening today to see if it can enhance our understanding

2. *Technical:* trying to advance our approaches on a technical level

3. *Future:* looking out to where we might be in 10 to 20 years and how we might get there

Craigen then illustrated the diversity of thought in the selected articles and put them into context, as he and Ibrahim Gedeon did in the Preface to the book. *Cybersecurity: Best of TIM Review* is available for purchase from Amazon (amazon.com/dp/B00XD3O6L0/) in ebook format for Kindle. All proceeds support the ongoing operation of the TIM Review.

Part III: Company presentations

In the third and final part of the lecture, representatives of three companies shared their current work and collaborations in cybersecurity:

1. Ned Nadina, CEO of Denilson, introduced his company's secure mobile point-of-sale solution for retail enterprises, stressing that a financial technology company needs cybersecurity from day one. Denilson's solution enables credit card payments through the user's mobile hardware, thereby replacing the need for payment terminals.

2. Arthur Low, CEO of Crack Semiconductor, described a lead project through which his company is collaborating. The project, titled Nebular Trusted Provisioning, seeks to develop high-end protection and authentication for intellectual property relating to microchip design software and tools.

3. Michael Thomas, VP of Engineering at Bedarra Research Labs (bedarra.com), described Ivy, which is Bedarra's interactive analytics research environment. It is "an open, interoperable, and extensible platform that combines powerful server-side analytic processing with modern web-based user interfaces for query and visualization". It enables specialists to build customized test suites to allow domain experts to easily and collaboratively explore, analyze, and visualize large datasets using commodity hardware.

TIM Lecture Series – Three Collaborations Enabling Cybersecurity

Deborah Frincke, Dan Craigen, Ned Nadima, Arthur Low, and Michael Thomas

About the Speakers

Deborah Frincke is the Director of Research for the National Security Agency/Central Security Service in the United States. Dr. Frincke's research spans a broad cross section of computer security, both open and classified, with a particular emphasis on infrastructure defense and computer security education. She has been a member of several editorial boards, including: *Journal of Computer Security,* the *Elsevier International Journal of Computer Networks,* and the *International Journal of Information and Computer Security,* and she co-edits a Board column for *IEEE Security and Privacy*. She is a steering committee member for Recent Advances in Intrusion Detection (RAID) and Systematic Advances in Digital Forensic Engineering (SADFE). Dr. Frincke received her PhD from the University of California, Davis in 1992.

Dan Craigen is a Science Advisor at the Communications Security Establishment in Canada and a Visiting Scholar at the Technology Innovation Management Program of Carleton University in Ottawa, Canada. Previously, he was President of ORA Canada, a company that focused on High Assurance/Formal Methods and distributed its technology to over 60 countries. His research interests include formal methods, the science of cybersecurity, and technology transfer. He was the chair of two NATO research task groups pertaining to validation, verification, and certification of embedded systems and high-assurance technologies. He received his BScH and MSc degrees from Carleton University.

Citation: Frincke, D., Craigen, D., Nadima, N., Low, A., & Thomas, M. 2015. TIM Lecture Series – Three Collaborations Enabling Cybersecurity. *Technology Innovation Management Review,* 5(6): 45–48. http://timreview.ca/article/906

Keywords: cybersecurity, collaboration, NSA, book launch, entrepreneurship, research

Ned Nadima is the Founder and Chief Executive Officer of Denilson, a company that develops mobile payment solutions for retail enterprises. He is currently a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada, and he holds a Bachelor's of Science degree in Commerce and Marketing from the University of Ottawa.

Arthur Low is the founder and Chief Executive Officer of Crack Semiconductor, a supplier of high-performance cryptographic silicon IP used in some of the most demanding security applications. Arthur has a number of patents in the field of hardware cryptography. He has worked for a number of IC startups as a Senior IC designer and Architect and gained much of his fundamental IC design experience with Bell-Northern Research in the early 1990s and with IBM Microelectronics in the late 1990s. Arthur has a BSc degree in Electrical Engineering from the University of Alberta in Edmonton, Canada, and is completing his MSc degree in Technology Innovation Management in the Department of Systems and Computer Engineering at Carleton University in Ottawa, Canada.

Michael Thomas is the Vice President of Development at Bedarra Research Labs, a private industrial R&D lab whose mission is to seek out promising next-generation computing and communication technologies and apply them to creative solutions for emerging business problems. Prior to joining Bedarra Research Labs, he worked as a Software Developer and Release Engineer at Object Technology International. Michael holds a Master of Business Administration degree from Athabasca University in Canada, in addition to a Bachelor of Arts degree from Brock University in St. Catharines, Canada.

This report was written by Chris McPhee.