TIM Lecture Series

Building Trust in an IoT-Enabled World

Jeremy Watson, John Marshall, Mike Young, Peter Smetny, and David Mann

> *"New technologies create wonderfully innovative products, but also create new vulnerabilities and new means of attack. Increasingly, the attacks are network-borne, targeting software and stored information through hacking, malware, or denial-of-service attacks. To address these vulnerabilities, we need to develop systems and software with fewer vulnerabilities and greater resistance. Certainly, trying to bolt on security to existing systems is recognized as not being terribly effective. We need to take a systems view."*
>
> Jeremy Watson
> President of the Institution of Engineering and Technology (IET)

Overview

The Internet of Things (IoT) covers a wide spectrum of human endeavour, and there are great concerns about the safety, security, and robustness of systems and networks that will enable this massive connected environment. To share insights about the increasingly important topic of trust and security in the IoT, the first TIM lecture of 2017 was jointly organized by the IET Ottawa Local Network and Carleton University's TIM Program (timprogram.ca) in Ottawa, Canada.

David Mann, Director and Chief Security Officer at inBay Technologies (https://inbaytech.com/) and Chairman of the IET Ottawa Local Network introduced the four presentations, each of which offered a different perspective on building trust in an IoT-enabled world:

1. IET Initiatives in Cybersecurity and the IoT
   (Jeremy Watson – IET)

2. Trust as a Service
   (John Marshall – InBay Technologies)

3. Wireless Security in the IoT
   (Mike Young – Bastille)

4. WannaCry Ransomware and IoT Security
   (Peter Smetny – Fortinet)

The event was held at Carleton University on May 30th, 2017, where it was hosted by the Technology Innovation Management program as part of the TIM Lecture Series. TIM lectures provide a forum to promote the transfer of knowledge from university research to technology company executives and entrepreneurs as well as research and development personnel.

1. IET Initiatives in Cybersecurity and the IoT

Speaker: Jeremy Watson CBE, President, Institution of Engineering and Technology (IET; theiet.org)

Jeremy Watson introduced the IET's vision and mission, including the scope and nature of the organization's influence throughout the world. With over 167,000 members in 150 countries, the IET takes a multidisciplinary approach in all of its initiatives, which include:

- Informing the public and the wider engineering community.
- Offering professional registration and career development to IET members.
- Providing professional advice to governmental bodies, including calling on the UK government to make cybersecurity a priority.

TIM Lecture Series – Building Trust in an IoT-Enabled World

Jeremy Watson, John Marshall, Mike Young, Peter Smetny, and David Mann

- Providing trusted e-learning for engineers at all career levels through the IET Academy (www.theiet.org/resources/academy/).

- Bringing science, technology, engineering, and mathematics to life in schools through the IET Faraday Program of educational resources, challenges, and events (faraday.theiet.org).

In setting the scene for the IET's initiatives in relation to cybersecurity and the IoT, Watson outlined the diverse and pervasive applications of the IoT in households (e.g., smart thermostats, white goods, televisions), building management systems (e.g., sensors and access controls, heating and cooling systems), industrial and utilities control systems (e.g., sensors and actuators), medical and hospital equipment (e.g., patient monitors and patient information recording), transport (e.g., condition monitoring and asset location), and retail. All of these areas will be affected by the IoT, which highlights the vital role of cybersecurity in the IoT, particularly with respect to the following risks:

- Information theft of personal data or patterns relating to building occupancy and utilization.

- Perturbation of operations, such as hacking into control networks to perturb asset operation. The denial of a physical service could occur, for example, by shutting down an air conditioner in a server room.

- Corruption of falsification of sensor data, for example, by spoofing a building management system or stealing energy by hacking smart meters.

- Falsification of information leading to supply chain or product provenance issues.

Next, Watson introduced the PETRAS Hub (petrashub.org), a research hub for cybersecurity and the Internet of Things, and for which he is Director and Principal Investigator. PETRAS brings together nine world-leading universities and dozens of international partners to collaborate on inter- and multi-disciplinary projects based on the following principles:

- Use an integrated approach of collaborative social and physical science expertise.

- Remove barriers to the beneficial adoption of IoT.

- Address generic knowledge gaps through case study approaches covering major sectors.

- Use innovative methodologies including "in the wild" and citizen science.

- Engage users by defining research agendas, participation in research, and matched funding.

For further reading on this topic, please see:

- *Code of Practice for Cybersecurity in the Built Environment*
tinyurl.com/ycc2osxh

- *Engineering Secure Internet of Things Systems*
dx.doi.org/10.1049/PBSE002E

- *The Internet of Things: Making the Most of the Second Digital Revolution* (The Blackett Review)
tinyurl.com/plqn3xk

- PETRAS Hub
petrashub.org

2. Trust as a Service

Speaker: John Marshall, Principal Software Engineer, inBay Technologies (inbaytech.com)

The second speaker, John Marshall, introduced the idQ Trust as a Service offering by inBay Technologies, which is designed to help overcome a lingering problem that takes on heightened importance with the IoT: identity assurance. Unsecured networks and weak passwords are commonplace, and the increasing frequency of data breaches means that the risk of compromised credentials is high and widespread. Marshall argued that a root cause is the underlying paradigm of the password model: a password is a secret, but that secret is not as safe as most people tend to think. Passwords are typically transmitted across networks, stored by service providers, reused for multiple services, easily forgotten, and may not even be secret at all (e.g., default passwords). Also, attackers can use dictionary attacks and brute force approaches mean that a password can be discovered in minutes or hours.

Instead, inBay Technologies proposes a paradigm shift: we should stop transmitting secrets across the network, we should stop sharing secrets with service providers,

TIM Lecture Series – Building Trust in an IoT-Enabled World

Jeremy Watson, John Marshall, Mike Young, Peter Smetny, and David Mann

and we should adopt a strong authentication model. Using this new paradigm, idQ Trust as a Service uses a Trust-Relationship Code, which consists of a hardware component (chip/trusted platform module), a service component (provisioned by the service provider), and a personal component (runtime information from the user). The user and their mobile device *trust* each other based on a local authentication factor, such as a PIN or a fingerprint, which is only used at run-time and is not stored on the mobile device nor is it shared with service providers. Instead of transmitting usernames and passwords to the service providers, idQ uses algorithm-based network authentication. Based on digital signatures, a challenge is triggered that can only be answered by a trusted user–device pairing. There is no propagation of users secrets or attributes across the network.

Marshall next showed examples of how this new paradigm can be applied to the IoT in the future: by enabling user-to-device authentication (e.g., for devices in the field) and device-to-device authentication, to protect data repositories, and for authorizing updates and provisioning. inBay Technologies is currently exploring these applications to better secure the IoT through the idQ Trust as a Service approach.

3. Wireless Security in the IoT

Speaker: Mike Young, Senior Wireless Security Engineer, Bastille (bastille.net)

Bastille describes itself as providing "security for the Internet of Radios", because the security vulnerabilities in the IoT have less to do with the "things" themselves than the radios embedded within them. Equally, Bastille recognizes that most enterprises think of "wireless" as equivalent to "Wi-Fi" without considering (or monitoring) the vast number of other protocols operating invisibly in their airspace.

As Mike Young described, companies spend substantial time and money securing the perimeter of their networks with firewalls, intrusion detection, exfiltration detection, etc. while often ignoring the many gigabytes of data leaving the premises via radio signals, for example through company phones, personal phones, hotspots, rogue cell towers, radio-ready infrastructure, GSM listening and surveillance devices, and IoT devices. Indeed, "covert wireless" devices are already infiltrating enterprises today, and many seemingly mundane devices are vulnerable as entry points, even including wireless mice and keyboards.

Bastille's wireless and IoT scanning and malware prevention systems are designed to help enterprise security teams to assess and mitigate the risk associated with the growing "Internet of Radios". Bastille's software and security sensors "bring visibility to devices emitting radio signals (Wi-Fi, cellular, wireless dongles, and other IoT communications) in an organization's airspace. The technology scans the entire radio spectrum, identifying devices on frequencies from 60 MHz to 6 GHz. This data is then gathered and stored, and mapped so that users can understand what devices are transmitting data, and from where in corporate airspace. This provides improved situational awareness of potential cyber threats and post-event forensic analysis."

4. WannaCry Ransomware and IoT Security

Speaker: Peter Smetny, Systems Engineering Director, Fortinet (fortinet.com)

Peter Smetny first discussed the recent WannaCry ransomware attack (wikipedia.org/wiki/WannaCry_ransomware_attack), which infected hundreds of thousands of computers within a single day: May 12, 2017. The ransomware targeted Windows-based systems, encrypting a user's data and demanding a ransom to be paid in Bitcoin. WannaCry spread with a worm-like mechanism that scanned for vulnerable systems then gained backdoor access using code leaked from the United States National Security Agency (NSA) to target vulnerable systems from Windows XP to Windows 10 then install and execute a copy of itself. The particularly unique aspects were the worm behaviour, the vulnerability of systems that had not been updated despite the availability of effective patches, and the user of leaked NSA exploits within the ransomware.

The infection spread to over 150 countries and more than 230,000 systems. Many industries were affected, although key among them were healthcare and education, because these industries often run legacy software and may be slow to apply updates to their systems. However, the attack ultimately was not as damaging to users or as lucrative for the attackers as it might have been. Fortunately, a security researcher, Marcus Hitchens, discovered and closed a "kill switch" capability within the worm that dramatically slowed further propagation of the ransomware. Soon, most systems had been updated and were no longer vulnerable, although variants of the ransomware (without the kill switch) also appeared quickly.

TIM Lecture Series – Building Trust in an IoT-Enabled World

Jeremy Watson, John Marshall, Mike Young, Peter Smetny, and David Mann

Smetny then offered short- and long-term recommendations for protection and recovery from similar attacks. In the short-term, he encouraged individuals and organizations to:

1. Patch systems and review patching processes.

2. Test backups.

3. Reinstall operating systems, preferably a proper reinstallation and not a restore process.

4. Regularly run a full anti-virus scan of all systems.

5. Disable Windows' Server Message Block (SMB) if not used.

6. Periodically run a vulnerability scan.

Over the mid-to-long term organizations should:

1. Establish a Next-Generation Firewall (NGFW) Perimeter.

2. Set up an Internal Segmentation Firewall (ISFW).

3. Implement Security Information and Event Management (SIEM) for threat hunting via hashes and to monitor infection spread.

4. Recognize the need for sandboxing for zero-day attacks.

5. Evaluate their protection strategy.

6. Include a self-audit capability on the Next-Generation Firewall.

7. Make full use of threat intelligence.

Smetny concluded the lecture by describing Fortinet's Security Fabric, which is designed to cover an organization's entire attack surface to reduce risk and increase visibility and operational efficiency, and FortiGuard, a comprehensive suite of antivirus, antispyware, intrusion protection, and web content filtering capabilities that draws upon global intelligence and threat sharing. To address the complexities of the IoT, Fortinet adds capabilities around "learning" and "managing", which help organizations to not only identify but also categorize and protect the devices in their environment. These capabilities enable organizations to quickly make a determination about whether an IoT device should be trusted or untrusted, define what segments of the network it should be allowed to access or can access it, and further lock down segments and communications to industrial IoT with new protocol and application controls. Thus, organizations can leverage the IoT as a business enabler while protecting such devices (and the organization from them), even when the devices are not inherently secure.

TIM Lecture Series – Building Trust in an IoT-Enabled World

Jeremy Watson, John Marshall, Mike Young, Peter Smetny, and David Mann

About the Speakers

Jeremy Watson CBE is President and Fellow of the IET and Professor of Engineering Systems and Vice-Dean (Mission) in the Faculty of Engineering Sciences, based in the Department of Science Technology, Engineering and Public Policy at University College London. He is also Chief Scientist and Engineer at the Building Research Establishment (BRE). Until November 2012, Jeremy was Chief Scientific Advisor for the Department of Communities & Local Government (DCLG). He worked as Arup's Global Research Director between 2006 and 2013. Jeremy was awarded a CBE in the Queen's 2013 Birthday honours for services to engineering. An engineer by training, Jeremy has experience as a practitioner and director of pure and applied research and development in industry, the public sector, and academia. He has held research and technical management roles in industry and universities plus voluntary service with the DTI and BIS. His interests include interactions in, and the design of, socio-technical systems, emerging technology identification, development and deployment, and strategic innovation processes. Jeremy is a Chartered Engineer, a Fellow of the Royal Academy of Engineering, a Fellow of the Institution of Civil Engineers. He is a former Board member of the UK Government Technology Strategy Board (Innovate UK), and he is a founding trustee and Chair-elect of the Institute for Sustainability. He chairs the Natural Environment Research Council (NERC) Innovation Advisory Board and BuildingSMART UK, and until recently, served on the Council of the Engineering & Physical Sciences Research Council (EPSRC).

John Marshall is Principal Software Engineer at inBay Technologies in Kanata, Canada. He has over 20 years of experience as a software architect and technical leader developing real-time embedded telecommunications software, with a passion for improving software development. Previously, he worked as a Senior Software Engineer at Avaya and Software Architect for Nortel Networks. He holds a Bachelor's degrees in Computing Science from the Technical University of Nova Scotia in Halifax, Canada, and in Mathematics from Dalhousie University, also in Halifax.

Mike Young is a Senior Wireless Security Engineer at Bastille in New York, United States. He founded the Connecticut ISSA chapter and is currently a board member of the New York Metro ISSA. He has worked at Verizon, Verisign, RSA Security, and many security startups. He gave a speech on "Applying PKI" at the NSA in Fort Meade, Maryland. Mike received his Bachelor's degree in IT Management from Fordham University in New York, and he holds a Master's degree in IT Management from the University of Virginia in Charlottesville.

Peter Smetny is the Systems Engineering Director at Fortinet in Ottawa, Canada. As a technical architect, Peter has extensive experience in systems infrastructure design and implementation. He offers vast experience as a network/security architect, with a wide range of network devices, protocols, applications, operating systems, as well as integration, best practice, and design knowledge. His success is attributed to a demonstrated sense of accomplishment, leadership, dedication and initiative. Peter holds a Bachelor of Engineering degree from Carleton University in Ottawa, Canada.

David Mann is Director and Chief Security Officer of inBay Technologies in Kanata, Canada. He is a visionary innovator and calculated risk-taker with expertise in creating and leading new business ventures. He is a former Nortel executive, where amongst many achievements he nurtured the development of Entrust, a pioneer digital security company, leading to its $700+ million IPO. David actively engages in executive mentoring and advising Canada's leading researchers in the futures of cybersecurity, web network evolution, and the rapidly changing market of smart web-based applications. David is the Chair of several not-for-profit organizations, including the IET Ottawa Local Network, and he is an honorary member of the Canadian Association for the Advancement of Science.

This report was written by Chris McPhee.

Citation: Watson, J., Marshall, J., Young, M., Smetny, P., & Mann, D. 2017. TIM Lecture Series – Building Trust in an IoT-Enabled World. *Technology Innovation Management Review*, 7(6): 50–54. http://timreview.ca/article/1084

Keywords: cybersecurity, Internet of Things, IoT, trust, wireless, WannaCry, ransomware