IEEE ANTS™ 10th IEEE International Conference on Advanced Networks and Telecommunications Systems
6-9 NOVEMBER 2016 - BANGALORE, INDIA
IEEE ComSoc IEEE Communications Society
IEEE

Workshop Title:

Building Secure IoT Networks (Date: November 9, 2016)

Abstract:

Amidst all the hype and hope of the expected benefits from the Internet of Things (IoT), Security remains its biggest challenge to overcome. IoT is dependent on a wealth of data being collected from numerous devices connected across different interfaces and locations within the Enterprise, while carrying sensitive company or customer information. Any kind of security breach could compromise the organization's customers, workers or even the business itself. It is also critical to securely transport the IoT data to its destination by segregating and isolating data streams based on the source device role, the utility and criticality of these data streams. Security policies defined at any of these levels cannot be static but must be dynamically adaptable to meet the demands of business needs as well as to meet the challenges of continuously evolving threats. A smart and elastic network is required to maximize the much expected value from IoT, to securely connect thousands of these "things" with the highest levels of security including encryption, authentication, traffic segmentation, intrusion detection and remediation.

A majority of devices in today's connected world are out there for very long time. They are running old operating systems which may be vulnerable due to its openness or maybe they never ever got patches. The big threat is not because we expect people hacking into it. But do we know what we don't know?

On the other hand, today's conventional security mechanism may bring false sense of security, analogous to "security theatre". This phenomenon actually makes the system less secure. For example, a "secure" product could have been deployed with great fanfare. 3 years down the line when the product is working as usual, the Firewalls is in place, the Intrusion Detection system in place, it is quite natural to become very complacent. And that brings a false sense of security. This doesn't mean that the system would never have been attacked during this time.

Obfuscation and Segmentation can also play a big role in securing the network and the devices on it. It works on the basic premise that "If you can't see it you can't attack it".

Another aspect we need to look at is that the security architectures revolve mostly around AAA. Here are some of the questions we need to answer:

- Authentication - Should we be all address physical theft, replacing the actual device with a modified device etc.?
- Authorization - Will just policy enforcement work or do we need to come up with a complete new set of authorization-related standard?
- Auditing - What points are audited and how low powered devices can be handled? How big the sample space should be to call it a reliable sample space for auditing?

These are few of the example scenarios where IoT devices and networks need to be secured:

1. Shared networks which need separation of user groups.
2. Shared network where sharing needs to be done between different companies/vendors and network segmentation becomes indispensable.
3. A network extended to another campus where the medium thorough which it is being extended is inherently insecure, e.g., the Internet.
4. IoT enabled devices which are on the move and re-connect to core network frequently either physically or by wireless access.
5. Securing the networks when there is inherent heterogeneity due to devices of diverse type, make and model, following different standards; some of these devices are legacy devices.
6. Security protocols we are trying to adopt/modify/reuse for IoT devices and network from the traditional protocols we use on our PCs connecting to internet are too bulky in terms of compute (and storage) and sometimes come up their own vulnerabilities. What security mechanism can be used in such scenarios?

This session looks at the above mentioned challenges and discusses the enabling technologies and standards. This is followed by discussion on how these standards are going to evolve and should evolve to take care of future needs to IoT networks. Any outstanding issues which are not solved by existing standards are also discussed.

Agenda

Talks (60 minutes):

Talk 1: The complexity of IoT World and Security Challenges

Abstract: The vision of Internet of Things (IoT) is to enable devices to collaborate with each other on the Internet. Multiple devices collaborating with each other have opened up various opportunities in multitude of areas. It has presented unique set of challenges in scaling the Internet, techniques for identification of the devices, power efficient algorithms and communication protocols. Always connected devices have access to private sensitive information and any breach in them is a huge security risk. The IoT systems are often composed of the complex hardware, software and middleware components making it a complex system to manage and secure.

Speaker: Varun M Tayur, Software Developer, Avaya

Varun M Tayur is a software developer with 9 years of experience working on Software Defined Networks (SDN) and Network Management Systems (NMS). He has 5 research publications in the area of IoT – Interoperability. He is pursuing PhD in “Semantic methods for interoperable and dynamic workflow composition in IoT”. He has 4 Applications published on the Android Play Store. His areas of interest include IoT, Cloud, SDN & Android

Talk 2: IoT Device Security

Abstract: Devices across verticals such as Utilities, Industrial , Home Automation, Automobiles and Healthcare are getting smarter with connectivity (Cellular/BT/BTLE/WIFI/NFC/RFID etc.) becoming an integral part. These devices are being exposed to increased vulnerability across connectivity interfaces. Product manufacturers, suppliers and end users are responsible to protect their data, interfaces against un-

authorized access and attacks.

There is need to develop Security validation platform with capability to test, analyze and report vulnerabilities arising from connectivity interfaces of endpoints. Comprehensive assessment of wireless and wireline connectivity interfaces enabling OEM's/Tier 1/vendor assets to be hardened and secured against real-world attacks.

Speaker: Vijayakumar Kabbin, Technology Practice Head, IoT Initiatives, Wipro Technologies

Vijayakumar Kabbin is the General Manager for Embedded products design and Internet of Things in Wipro Technologies. He is instrumental in driving several Internet of Things (IoT) solutions for Industrial & smart city customers. He is also responsible for building computer vision systems using Deep Learning, helping Autonomous car, Smart Drone and Cobotics solutions.

Wipro is a global leader in Engineering R&D services with solutions for manufacturing, media, telecom, technology, healthcare, energy & utilities, banking and retail industries.

Before taking over Embedded and IoT, Kabbin was the head of Industrial Automation and Internet of Things in 2014. Previously he was handling Global delivery for Embedded Group which included portfolio of services spanning Automotive, Consumer Electronics, Mobile and Medical devices and Industrial Automation in a global delivery model.

Kabbin is also a certified Six Sigma black belt and carries vast experience in application of Six Sigma and Lean methodologies for software in delivery.

Kabbin has an experience of over 25 years in the IT industry. He joined Wipro as a campus recruit in 1987 and has held various responsibilities in R&D, Engineering, customer support, sales, marketing and business management.

Kabbin holds a bachelor degree in Electronics and Communications Engineering from University of Mysore and EGMP from Indian Institute of Management, Bangalore.

Talk 3: IEEE Security Standards which can be applied to IoT

Abstract: This talk briefly discusses the standards which can be applied IoT. This includes already established standards and standards in the works. Few of the standards and technologies which will be discussed area listed below:

- IEEE 802.1x - Port-Based Authentication (Fingerprinting)
- IEEE 802.1Qcj - Automatic Attachment to Provider Backbone Bridging (PBB) services
- IEEE 802.1aq - Shortest Path Bridging
- Tunneling - GRE, VXLAN, Hyper Segmentation, etc.

Speaker: Nishant Krishna, Software Architect, Avaya

Nishant is a Software Architect, Innovator and Inventor with 16 years of experience working on Network Management Systems (NMS), Cloud and Virtualization, Software-Defined Network (SDN) and Internet of Things (IoT) technologies. Nishant has 1 patent

granted and 6 patents filed/pending with US Patent Office in the areas of Network Management Systems, Cloud, Virtualization and SDN Technologies. He participates actively in User Experience (UX) and Wireframing related activities. He is an active member and contributor to numerous technical meetups. He is also a contributor to IEEE conferences and standards, and is a member of subcommittee working on defining standards for IoT and Smart Cities.

His areas of interest include Cloud and Virtualization, SDN, IoT, UX, User Interfaces, Network Security, Cryptography, public speaking and latest tech and gadgets.

Nishant has a Master of Science (MS) in Software Engineering degree from BITS, Pilani, along with many technical certifications.

Panel Discussion (30 minutes)

Theme: Building Secure IoT Networks – Challenges and Solutions

Panel discussion chair: Nishant Krishna

Panelists:

Sashank Dara, Cyber Security Technologist, Security Evangelist and Technical Leader, Cisco

Sashank is a Cyber Security Technologist, Security Evangelist and Technical Leader at Cisco. Sashank has 13 years of industry experience in the areas of Cyber Security and Privacy and has completed M.S from IIIT-Bangalore. Sashank is a prolific speaker and author of 5 US Patents and received numerous corporate awards for security advocacy and technology Innovation. Sashank also published around dozen papers at major conferences out of which he also received Best Research Paper @ IEEE CCEM (2015). He is passionate about research and innovation, especially in the domain of security and privacy, and has great enthusiasm for the use of technology as a tool to transform and benefit society.

Seema Sirivara, Product Manager, Avaya

Seema Sirivara has 18+ years of experience in the networking Industry and currently works as Senior Product Manager at Avaya, India. In her role as Product Manager, she is responsible for defining new Products and Features in the Campus and Data Center Ethernet Switching segment and also responsible for defining a successful Go To Market Strategy.

Prior to working at Avaya, she worked at Infosys where held the role of Lead Designer for several Data Networking products in both the Carrier and Enterprise space across multiple vendors and was responsible for design and implementation of key features and functionalities on routers and switches in both the Wired and Carrier Wireless Space.

Ajit Jha, Delivery Head M2M & IoT, L&T Technology Services Ltd.

Ajit is Delivery Head, M2M & IoT for L&T Technology Services, a niche global company in Engineering R&D. Ajit is a business leader with about 20 years of experience focusing primarily on Product engineering services cutting across industry segments be it Automotive, Semiconductor, Industrial, Transport or Telecoms.

Virendra Gupta, Huawei

Virendra Gupta is Senior Vice President and Business Line Head – 2012 Labs Business line and Network Business Line in Huawei Technologies India Pvt. Ltd., Huawei's largest overseas R&D center focused on developing and delivering telecom, enterprise and consumer domain core platforms, products, end-to-end solutions and services for global market.

His business lines are focused on developing products and platforms in the space of big data, IOT, 5G, Protocols, Database, OSS, SDN/NFV, PAAS, IP operating System. Products and platforms developed in his business line are widely deployed with leading enterprises and operators throughout the world. His business line has also filed more than 70 patents in last 3 years. His team also provides market technical support in OSS, Datacom and Transmission domain to India market.

Virendra has over 26 years of experience in the ICT (IT and communication technology) industry, of which more than 14 years have been with Huawei. He has earlier worked with C-DOT, HP, Hughes Software and Nokia, Finland.

Virendra holds an Engineering Bachelor's Degree in Electrical and Electronics from National Institute of Technology, Jaipur; Masters Degree in Integrated Electronics from Indian Institute of Technology, New Delhi; MBA (Marketing) from University of Delhi, Faculty of Management Studies; M Tech in Computer Science from Dr MGR University, MS in Embedded System Design from Manipal University.

Dr. Thomas Lee Sebastian, Tata Consultancy Services

Being a physicist, Dr. Thomas Lee has been involved in fiber optics and networking for past 13 years. He has designed and developed Light Runner, the world's first WDM training kit. He has been working in the area of SDN for past 4 years and been the project lead for two OpenDaylight projects, Controller Shield and NATApp. He has also involved in Analytical CORD in ONOS project. He has also worked in NFV, OpenStack, Dockers and Network Security. He has been awarded a couple of patents and has published several international journal articles.