~ Keynote Speaker ~

Dr. Debabrata Nayak, CSO, Huawei Telecommunications India

Title: Building a secure and resilient cyber specific 5G ecosystem is the need of hour

Abstract:

As vertical industries are thriving —Vehicle Network, Internet of Things (IoT), AR/VR, and high speed railways, just to name a few —they all demand fast yet ubiquitous network access to gain a new momentum. The rise of new business, new architecture, and new technologies in 5G will present new challenges to security and privacy protection. In 5G business environment, security is a necessary enabler for continuity of the business. Users already realize that security and privacy are important, and they could be aware of the security/privacy service provided to them. It is believed that the extent and strength of the security mechanisms provided correlate with the perceived security level, at least in the long run. Perception is closely related to trust, hence negative changes may happen very quickly (e.g. because of front-page news about observed attacks). In the 5G context, users may already have some perception of provided security level based on experience with earlier generations. To provide continuity of perceived security, it is important that security and privacy features that exist in earlier generations are also present in 5G, although the actual technical security mechanisms may be different. On the other hand, it is clear that it is not sufficient just to provide the same security features as in the legacy systems because there may be new security requirements and challenges. 5G systems are going to be service-oriented. This implies there will be a special emphasis on security and privacy requirements that stem from the angle of services.

In traditional mobile communications networks, the primary goal is to enrich people's life through communication. Users may communicate by text messages, voice calls, and video calls, or surf Internet or access app services using smart phones. However, 5G is no longer confined to individual customers. It's not simply about having a faster mobile network or richer

functions in smart phones. 5G will also serve vertical industries, from which a diversity of new services are going to system. In the context of vertical industry, security demands could vary significantly among services. For instance, mobile Internet of Things (IoT) devices require lightweight security while high-speed mobile services demand high efficient mobile security. The network based hop-by-hop security approach may not be efficient enough to build differentiated end-to-end (E2E) security for different services. As IoT is gaining momentum, more people will be able to remotely operate or "talk" to networked devices, for instance, instructing facilities at a smart home to get up. Therefore, there is a need of a more stringent authentication method to prevent unauthorized access to IoT devices. For example, biometric identification could be part of the authentication in smart homes.

Biography:

Dr.Debabrata Nayak has completed his PhD in wireless security from IIT Bombay. And has been working on security domain in last 21 years. He has been working in Huawei Telecom as Chief Security Officer. Oobtained Masters degree from NIT Rourkela, specialized in Elliptic Curve Cryptography and Internet security. And rated as Topper. Covering wide areas such as Security system Performance evaluation, Design of secure cryptographic system, Wireless Security policy design and implementation. He designed Security solution for INFINET (Indian Financial Network for RBI).IPv6 migration of INFINET.IPv6 Security for Indian financial network with C-DoT ,Leading IPv6 migration and security strategies in Huawei platform development for various products, cloud security, Currently guiding Enterprise security, Consumer security and Mobile broadband security(MBB). Working on privacy of user content. Spoke more than 100 conferences in India and abroad on network security ,Information security ,Cyber security.

He has presented 62 papers in international conferences and technical journals. He was active member of STIG (DoD) . He has worked with Motorola as Senior Security Architect, Reserve Bank of India as Information Security officer, and with Tata Elxsi as Security expert. He has extensively worked on LTE Security and WiMax Security. He was consultant to various financial institutes for implementation of standards such as BS7799 and ISO 17799. He was also involved in Ministry of Communication and IT of India for Secure mCheque project in IDRBT.Recently presented 10 Cloud computing security Paper in ITU,CJK korea, China and various international conference India like ASSOCHAM Cyber security conference,wireless vitae,Nasscom DSCI.

He was the Head of Patent /innovation Huawei India, He is the member of CII Innovation group.He is a Chairman of Global ICT Forum of India SIG.He is Co-Chairman for Assocham Cyber Law and IT act 2012 and also Co-chair continuing, Chairman for Huawei Senior security Expert Management Committee, 2012 International Association for Cryptological Research member, Motorola information assurance forum for 3 year, WiMax Forum (GWRG Group), LTE Forum (BWA Group), 3GPP SA3 Security, Cloud Security Alliance, IEEE Security and privacy and Cryptology Research Society of India , and Key member in ITU SG17 Security (Cybex- deals country specific Security), He is a member of Security Working group of TEC (DOT) NWG 17, He is a member of Assocham National security Group. Currently founding member in TSDSI cyber security group. And a certified lead Auditor of ISO 27001 :2013 from British standard Indtitute (BSI)