Internet of Things Security

Sheeba Backia Mary Baskaran

NEC Technologies India Pvt. Ltd., India
E-mail: sheeba.mary@india.nec.com

Received 19 December 2018;
Accepted 04 January 2019

Abstract

The emergence of the Internet of Things (IoT) with its sprawling set of technologies and use cases paves way for diversified and new service providers to develop a plethora of connected products and services for a go-ahead business and enrich lives of individuals. As the new service providers may be unaware of the threats their services face and the emerging categories of first time connected devices, IoT services, use cases and the network types comes along with a new threat landscape there is a huge possibility for even a Zero-day exploits. The provision of wide area connectivity to an ever-widening variety of IoT services will increase the whole ecosystem's exposure to fraud and attack. As the security issues are a significant inhibitor to the deployment of many new IoT services and attackers are showing ever greater interest in this area, this research article presents an overview of the threat vectors to the IoT ecosystem and the expected security features with Security-as-a-Network Service (SENSE) and other solutions that need to be in place to thwart the evolving security threats.

Keywords: Internet of Things, Network security threat, Communication security, LTE, 5G and SENSE.

Journal of ICT, Vol. 7_1, 21–40. *River Publishers*
doi: 10.13052/jicts2245-800X.712

1 Overview of IoT Security

The various security threats posed by the IoT devices, services and end users that need to be considered in the robust IoT security design is discussed in this section along with an overview of various IoT security standards and framework which drives the IoT security development. The human and digital experiences is no longer placed side-by-side, they are bound ever tighter by the new IoT way of life and use cases as shown in Figure 1.

Unless protected, digital security now directly impacts the physical world more than ever. Further the IoT creates ever greater databases of knowledge, shared experiences, and explosions of innovation with its persistent connectivity. The technologies that drive this connectivity must be secured, to enforce the privacy, reliability, and Quality-of-Service (QoS) necessary to ensure that this great utility and basic need is kept available. In some cases, the service provider may not have developed a service that has connected to a communications network or the internet before and they may not have integrated with skills and expertise to mitigate the risks posed by enabling internet connectivity within their devices. As adversaries understand the technology and security weaknesses, they will quickly take advantage

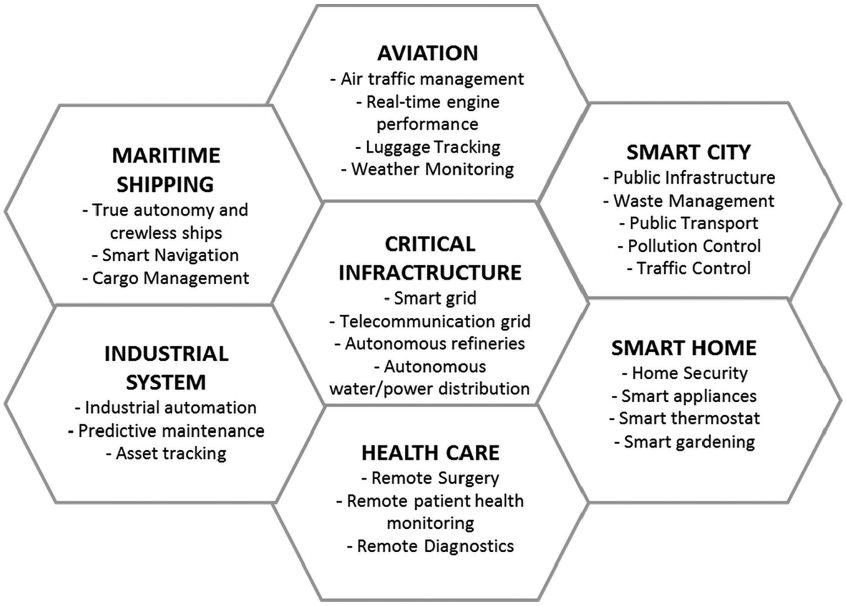


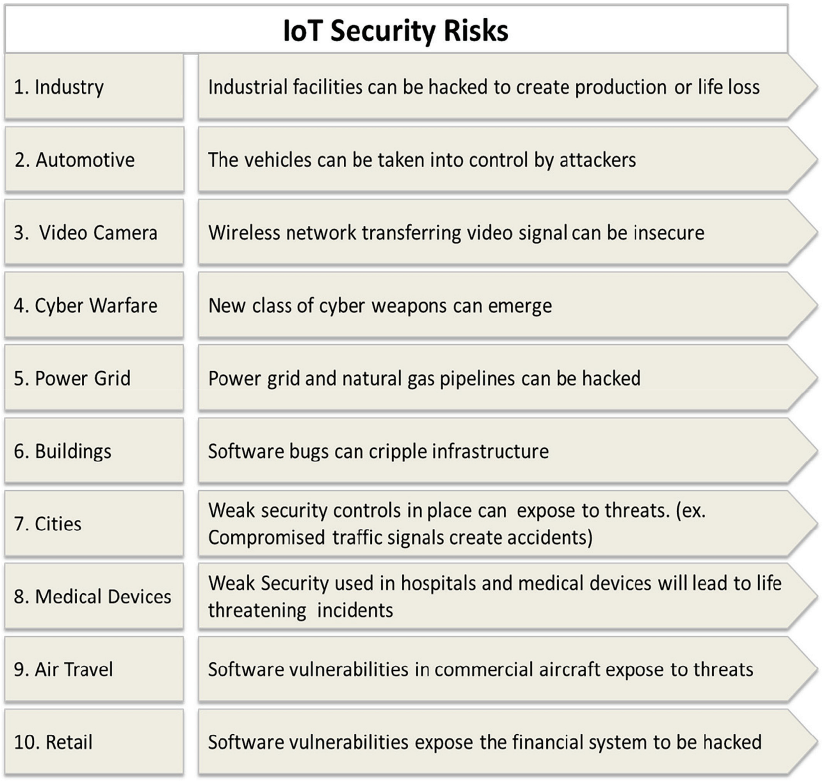
Figure 1 Example of IoT Use cases.

if the vulnerabilities are exposed. Compromised devices may exfiltrate data, attack other devices, or cause disruption of services.

Whilst many service providers, such as those in automotive, healthcare, consumer electronics, education and municipal services, may see their particular security requirements as being unique to their market, this is generally not the case. Almost all IoT services are built using endpoint device and service platform components that contain similar technologies to many other communications, computing and IT solutions [6]. An endpoint device is an Internet-capable computer hardware device on a TCP/IP network that can refer to desktop computers, laptops, smart phones, tablets, thin clients, printers or other specialized hardware such POS terminals, smart meters etc. The endpoint can also refer to any configuration of low complexity devices, rich devices, and gateways that connect the physical world to the digital world in novel ways. In addition to this, the threats these different services face, and the potential solutions to mitigate these threats, are usually very similar, even if the attacker's motivation and the impact of successful security breaches may vary as shown in Figure 2. In general, irrespective of the use cases and services, when a device in an IoT ecosystem is compromised, the attackers can take control, steal information and disrupt services.

Few Endpoints such as TVs, webcams, home thermostats, remote power outlets, sprinkler controllers, hubs for controlling multiple devices, door locks, home alarms, scales and garage door openers were on the list of tested devices, and all of them could be controlled from a mobile gadget; in some cases, cloud service would be available [6]. A security research by HP highlights that 90% of these devices collects personal information, while 70% communicate over the network without any form of encryption. Moreover, 80% did not offer the user the possibility to enable strong passwords, forcing them to rely on a weak one by today's industry standards. Given all these risks, it is clear that all devices composing the IoT should be subject to proper security assessment and standards regulating protection measures [1, 13]. For the IoT to evolve effectively, the following security challenges inherent to its growth need to be taken care by both service providers and network operators [5].

- Availability: Ensuring persistent connectivity between endpoints and their respective services.
- Identity: Authenticating endpoints, the end-user operating the endpoint, and the services.
- Privacy: Preventing the potential harm to end-users by protecting the subscription, subscriber (user location) and service related information (user data).



IoT Security Risks	
1. Industry	Industrial facilities can be hacked to create production or life loss
2. Automotive	The vehicles can be taken into control by attackers
3. Video Camera	Wireless network transferring video signal can be insecure
4. Cyber Warfare	New class of cyber weapons can emerge
5. Power Grid	Power grid and natural gas pipelines can be hacked
6. Buildings	Software bugs can cripple infrastructure
7. Cities	Weak security controls in place can expose to threats. (ex. Compromised traffic signals create accidents)
8. Medical Devices	Weak Security used in hospitals and medical devices will lead to life threatening incidents
9. Air Travel	Software vulnerabilities in commercial aircraft expose to threats
10. Retail	Software vulnerabilities expose the financial system to be hacked

Figure 2 Internet of Things security risks.

- Security: Ensuring that system integrity and its service can be verified, tracked, and monitored and ensuring the confidentiality of the communications involved.

IoT security standards and frameworks [3] includes contributions from IEEE, the IETF, MITRE, the OWASP, and dozens more on “Industrial Internet of Things (IIoT)” [14], Industrial Internet Consortium, NIST Framework for Improving Critical Infrastructure, Cybersecurity [5], NIST – Considerations for Managing IoT Cybersecurity & Privacy Risk [6], OWASP – IoT Security Guidance [7], GSMA-IoT Security Guidelines [8] etc.

The organization of the paper is as follows. Initially the background study on the promising technologies of IoT in presented in Section 2, further a case by case analysis on threat vectors is presented in Section 3. Section 4 discussed the critical security requirements that can set up a secured IoT ecosystem. Section 5 discusses the possible potential IoT security solutions in place and Section 6 outlines the expectations over various security enhancements. Section 7 discusses the potential way forward to provide a complete IoT security solution through Security-as-a-Network Service and finally Section 8 concludes with information on various standardization activities focusing towards the deployment of IoT security.

2 The Backbone of IoT Ecosystem

For the IoT to evolve at its expected pace, endpoint devices must be able to constantly communicate with each other, end-users, and back-end services. While there have been a myriad of technologies that offer connectivity solutions for IoT, none shape the future of IoT better than mobile networks. The mobile industry has developed and standardised a new class of low power wide area (LPWA) technologies that help network operators to tailor the cost, coverage and power consumption of connectivity for specific IoT applications [3]. Motivated by a vision of a digital society with billions of devices communicating over cellular radio access technologies, 3GPP Standardizes LPWA solutions operating in licensed spectrum bands such as Extended Coverage GSM for Internet of Things (EC-GSM-IoT), Long Term Evolution Machine Type Communications Category M1 (LTE MTC Cat M1, also referred to as LTE-M) and Narrowband IoT (NB-IoT) to address the diverse requirements of the IoT market. Moreover, standardisation by 3GPP helps technologies to reach large scale due to the number of companies that implement these standards. The standardised LPWA technologies possess several characteristics such as low power consumption (to the range of nanoamp) that enables devices to operate for 10 years on a single charge, low device unit cost, improved outdoor and indoor coverage, secure connectivity and strong authentication, optimised data transfer (support for small, intermittent blocks of data), simplified network topology and deployment, integrated unified/horizontal (IoT)/ Machine-to-Machine (M2M) platform, network scalability for capacity upgrade to make them particularly attractive. LPWA devices deployed in remote physically inaccessible locations for more than 10 years will need to implement long-term security features; it may also be desirable to deploy security patches remotely.

The various challenges that will come in the way of IoT include the Identity, privacy and security challenges. Every endpoint within an IoT product or service ecosystem, must be capable of securely identifying itself to its peers and services. Privacy must be designed into products from the ground up, to ensure that every action is authorized and every identity is verified while guaranteeing that these actions and the associated meta-data are not exposed to unauthorized parties. The privacy measures implemented in 5G (Transmission of concealed Subscription unique permanent identifier on air) can ensure privacy when IoT devices communicate over 5G [11]. Finally to meet the security challenge, the internet and communication security gaps more evident in embedded systems and in cloud services – the two primary components in IoT technology must be addressed.

3 The Threat Landscape and the Threat Vectors

This section presents an overview of the critical threat landscape and threat vectors which impacts the IoT security.

3.1 IoT Threat Landscape

Following Are critical threat landscape and best practices that need to be considered while designing IoT security solutions.

The usage of IoT technology in future will attract more potential for cyber-attacks and fraud. Some of the reasons which make IoT devices vulnerable to Cyber Risk include the following [TR 33.861] [9]:

- The LTE eNB does not support integrity protection for the user plane. If the infrequent or frequent small data is not integrity protected between the UE and network, then an attacker can modify the small data or even inject fake small data packets on behalf of the IoT device or the network on the air interface.
- If integrity protection of small data is not provided by the lower layers, then any modification of the small data or any replayed small data can't be detected by the lower layers, in order to avoid the delivery of the small data to the application layer for further processing. There will be more offline endpoints (e.g. homes, transports, manufacturing units etc.) that connect to online and will become vulnerable to e-Threats.
- Encryption of NAS signalling is optional to use in NAS layer. If the infrequent or frequent small data is not encrypted, an attacker can eavesdrop on the small data sent on the air interface.
- Distributed Denial-of-Service (DDoS) attacks towards the 5G core network include both large number of signal packets (e.g. NAS signalling messages) and user plane packets sent by compromised Cellular IoT (CIoT) devices overloading the network. This kind of attack can lead to DoS or at least throughput degradation caused by congestion to

legitimate UEs whose traffic shares the same core network links. For instance, access to the crucial core network functions (e.g. Access and Mobility Management Function (AMF)) could be denied to normal UEs by one or more compromised UE(s) repeatedly initiate(s) authentication procedures in a short period.

- In IoT scenarios, many IoT devices will be deployed densely where attackers can hijack these IoT devices which deployed approximately in same location to launch DoS attack on the control/user plane against the gNB by sending a large number of bogus packets to gNB. This attack could exhaust gNB resources, thus it cannot provide its fundamental function of internet access.
- Maliciously the RRC signalling exchanged before AS security activation can be used to cause DoS attack to gNB. For example, attackers may compromise a large number of IoT devices to send access request messages repeatedly, send mass number of Random Access to gNB in a short time to occupy preamble to cause other normal IoT devices fail to access. Attack may also construct malicious RRC signalling to attack gNB.
- After As security activation, IoT devices can be used maliciously to send a large number of signalling or user plane packets to gNB, for example, send massive RRC signalling or UP data such as, RRC re-establishment/RRC resume/User plane packets etc. to cause gNB exhaust the process resource to make the gNB deny service.
- Since the nature of CIoT device communication is a short burst, AS level attack surface is much less compared to normal UEs which need a sustained connection and complete AS security. For such CIoT devices, if application level security is enabled, encryption may not be a critical need between the UE and the gNB. But to avoid any packet injection or manipulation integrity may be enabled at the radio layer. There is a need to balance the resource availability such as computing power, battery consumption and security threat for CIoT UEs at the radio level. Hence a range of AS security options (encryption vs integrity) need to be supported at the AS layer.
- Because of the networked nature of IoT (i.e., that each connected endpoint uses data from other connected objects/endpoints) there is also the risk that a malfunction could lead to catastrophic system failure.
- IoT solution is being implemented by some of the Technology, Media and Telecommunication companies on top of existing systems or collaborating with their customer or partner system. These standalone

legacy systems which were earlier unconnected are vulnerable targets for hacking.
- Infrequent updates to IoT devices after installing them will leave them vulnerable.
- Some IoT devices do not have the ability to receive patches to update security settings
- Most of IoT platform comes with default ID and password.

The large number of diverse devices connected to the network will increase network vulnerability and potentially become targets of hacking and denial-of-service attacks due to security pitfalls existing in the radio access network as shown in Figure 3 [12]. The requirement to handle possibly billions of DNS requests per second, for example, may impact network performance and availability for many service providers. DDoS attacks and advanced persistent threats (APTs) could have devastating effects on network availability. The main security concern for service providers is outages caused by DDoS and botnet attacks. Service providers recognize that security threats exist across their network domains, with the top area of concern in the data center. But they also understand that devices, the RAN, the core network (4G EPC), (5G Core),

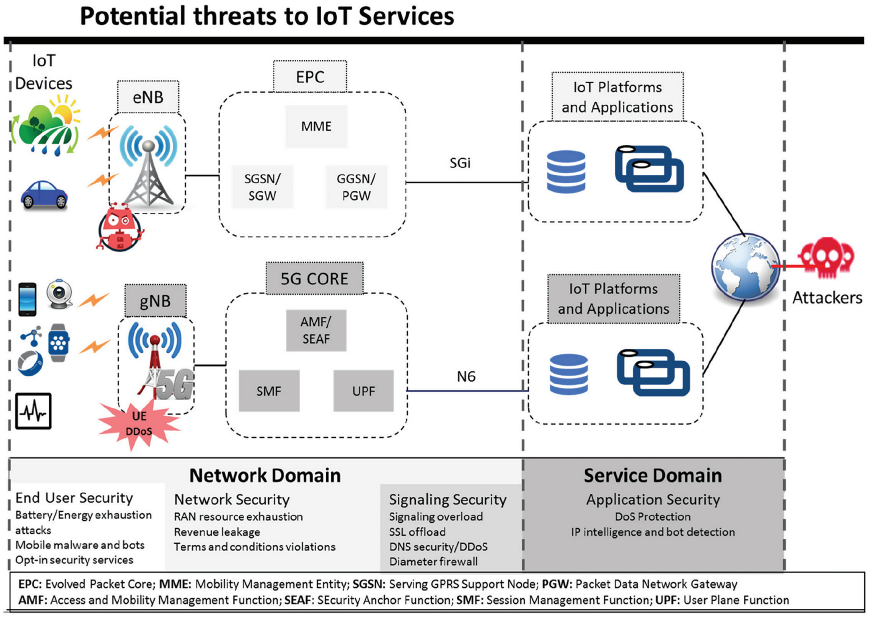

Potential threats to IoT Services
IoT Devices
eNB
EPC
MME
SGSN/ SGW
GGSN/ PGW
SGi
IoT Platforms and Applications
gNB
5G CORE
AMF/ SEAF
SMF
UPF
N6
IoT Platforms and Applications
UE DDoS
Attackers
Network Domain
End User Security
Battery/Energy exhaustion attacks
Mobile malware and bots
Opt-in security services
Network Security
RAN resource exhaustion
Revenue leakage
Terms and conditions violations
Signaling Security
Signaling overload
SSL offload
DNS security/DDoS
Diameter firewall
Service Domain
Application Security
DoS Protection
IP intelligence and bot detection
EPC: Evolved Packet Core; MME: Mobility Management Entity; SGSN: Serving GPRS Support Node; PGW: Packet Data Network Gateway
AMF: Access and Mobility Management Function; SEAF: SEcurity Anchor Function; SMF: Session Management Function; UPF: User Plane Function

Figure 3 Potential threats to IoT services.

the IMS, and the Gi-LAN must be protected to ensure seamless, end-to-end network security.

Keeping a watch on these basic threat landscape and security measures will ensure privacy of end consumers and they will build a long lasting confidence in such devices, services and companies, hence, ensuring secure IoT ecosystem ahead in the connected world of the IoT.

3.2 IoT Threat Vectors

The main threat vectors that could impact the IoT evolution include Ransomware which could be the primary threat. The attackers Disrupt one or more IoT devices, their control plane, or their cloud aggregation point, and holding them hostage is an easier and faster way to make money than compromising a large number of devices quietly to siphon data. Already IoT devices were being held for ransom in the power distribution and health care verticals. The next potential threat is Hacktivism. Hackers can launch DDoS attacks by infiltrating and leveraging thousands or millions of unsecured devices. Hacktivism can cripple infrastructure, down networks, and as IoT advances into our everyday lives, those attacks may very well put real human lives in jeopardy. And even if hackers can compromise gateways and core IoT networks in order to reveal and exploit sensitive personal and corporate information. Few examples includes taking control and altering voting machine tallies, opening valves at a dam, or overriding safety systems at a chemical plant where the potential for catastrophic damage is real. There can also be Nation-state attacks on critical infrastructure, where attackers can damage or disrupt the military or economic capabilities of one country. The attacks are mainly been on SCADA systems, which are a type of IoT device. The IoT control plane could be the prime target as device-level attacks are certainly common, but difficult to scale. Attacking one autonomous car, connected valve, or smart door lock does not provide much in the way of payoff. As a result, attackers will often prefer going after the control plane for IoT devices. Control planes have some level of privileged access to monitor processes and change settings on multiple devices. While security efforts have been focused on IoT devices themselves, less effort has been applied to the systems that control those devices. The expected scale of most important IoT device deployments means that their control planes will be complex, with a very large attack surface. Attackers can disturb the integrity of messages in the control stream, or can compromise the controller itself because of weak authentication or stolen credentials. Next IoT aggregation can be the prime target. Instead of attacking multiple devices and slowly gathering data in small increments, the main system can be taken control. Instead of trying to hold cars for ransom one by one, take over an entire car dealer's worth of cars through their maintenance systems. Credentials and authentications systems are again the weak points. Of course, most IoT device aggregation points will be in the cloud, so cloud vulnerabilities and threats apply, too.

One of the major threat is IoT Request Forgery. An attacker usually will not crack through layers of enterprise-grade security to get targeted data. They seek the path of least resistance. While many IoT devices might not be privy to sensitive information, attackers can simply keep sending bogus requests to vulnerable devices until they get what they are after. Wearables being the significant population in an IoT ecosystem, the wearable malwares need to be considered. When smartphones and tablets first entered the market, very few people considered the possibility that they might become attractive targets for malicious software. Most businesses now acknowledge the threat of mobile malware. And with mobile malware an acknowledged threat, one cannot help but look at the possibility that wearable devices could end up being an attack vector, too. A pair of smart glasses or a fitness tracking watch could easily serve as a point of entry for savvy attackers, and wearable malware represents just as much of a risk as its mobile cousin. Botnets have the potential to grow larger – and smarter – than ever before. Routing information in IoT networks can be spoofed, altered, or replayed, in order to create routing loops, attract/repel network traffic, extend/shorten source routes, etc. Few types of routing attacks includes sink hole attack, selective forwarding, worm hole attack, Sybil attack etc. Devices in an IoT ecosystem rely on software that might contain severe bugs and/or bad design choices. This makes the things vulnerable to many different types of attacks, depending on the criticality of the bugs, e.g., buffer overflows or lack of authentication. This can be considered as one of the most important security threat (For example Mirai, the botnet that took down servers across the US East Coast at the end of 2016 is one of the largest and complex botnets of its kind). Mirai is only the beginning. Botnets are only going to grow larger and more complex as time goes on [1, 17].

4 IoT Security Requirements

IoT and 5G service offerings tout greater revenue opportunities with emerging use cases driving the need for higher speeds and lower latency, but also brings with it, the associated security implications. Three main security objectives for IoT networks includes protection of IoT network from attackers, protection of IoT applications and thus, the things and users and finally the protection of the rest of the Internet and other things from attacks that use compromised information or device as an attack platform. The security requirement at various stages for a secure IoT communication is discussed below.

4.1 Network Level Security Requirements

Until vendors adopt security standards and frameworks voluntarily, and the government enforces security requirements, IoT users can take a stand against IoT threats using the following network-level security approaches [3–6]:

- Continually update the network configurations, capabilities, and rules to listen and detect new devices on the network.
- Discover all connected devices on the network including IoT, Shadow IoT, Rogue IoT, and Bring Your Own IoT device (BYO-IoT).
- Use network security that understands and addresses the broad array of IoT device abilities and protocols.
- Segregate the IoT devices on a separate network.
- Develop a knack for using Network Access Control (NAC) that defends IoT without frustrating end users.

4.2 LPWA Security Considerations that Apply to IoT Services

Regardless of the type of LPWA application, there is a minimum set of security-related requirements for all, such as:

- Secure provisioning of device identity, network authentication credentials and communication cryptographic keys.
- Physical protection of device identity, network authentication credentials and communication using cryptographic keys.
- Strong mutual authentication of the device and network.
- Strong (and efficient) cryptography to provide secure communication channels.

All 3GPP technologies share similar network architectures and provide similar transport layer security mechanisms and constraints. Confidentiality protection and integrity of subscriber traffic for mobile backhaul protection is the key for IoT security. Several other security mechanisms required for IoT security as specified by TS 33.501 [11] includes Device/network mutual authentication; Securing of communication channels; Ability to support “end-to-end security” at the application level; and Secure provisioning and storage of device identity and credentials.

5 Security Solution in Place for IoT Ecosystem

The challenge of availability can be significantly addressed as the global addressable market for LPWA devices is large, as around 1.4 billion connections can be expected by 2020, with some industry watchers forecasting 5 billion by 2022. To address the challenge of identity management, the mobile industry is typically associated with the removable SIM card, the GSMA has created a SIM based solution called the 'Embedded SIM Remote Provisioning Architecture' and 'Embedded UICC Remote provisioning architecture [2] which is appropriate for use in IoT to enable in-depth component level integration into endpoint devices, reduced production costs and the management of connectivity via Over-The-Air (OTA) platforms to enable the connectivity of the IoT endpoint devices for their whole lifetime.

Identity technologies, such as the Embedded SIM, are designed as trust anchors that integrate security by default. They are manufactured to withstand attacks such as, glitching, side-channel analysis, passive data interception, physical tampering, identity theft etc. An excellent advancement to this already security hardened technology is that new generations of these trust anchors incorporate an important addition to the IoT landscape. These technologies will be dual use. They will not simply verify the security of the network, they will also be capable of securing application communications and the application itself, similar to traditional computing trust anchors. This dual use capability will be further augmented by the integration of mobile industry security specifications such as those provided by 3GPP GBA [15], OMA, oneM2M and others. oneM2M defines requirements, architecture, API specifications, security solutions and interoperability for IoT technologies. It creates a service layer that can run on any IoT device hardware and software. The oneM2M security architecture comprises security functions layer, security environment abstraction layer, and secure environment layer. The main security functions specified for IoT includes access Management through authorization, authentication and access Control. The sensitive data handling can be supported through sensitive functions protection and secure Storage. Further the security association establishment includes secure connection via secure session establishment, secure connection via object security and security administration (including remote security provisioning). Finally the privacy of the subscribers is ensured using identity Protection [16]. These security functions and technologies will help to securely provision devices in the field, securely enable over-the-air firmware updates, and manage device capabilities and identity. Instead of application engineers building complex technologies that they themselves have to manage, the network operator, who already manages the network identity, can perform this on behalf of the application. This not only reduces the engineering complexity, but the business's daily management requirements.

The challenge of Privacy and Security can be addressed as with the capabilities of the SIM, the mobile industry has developed resilient protocols, processes, and monitoring systems to enable security and reduce the potential for fraud and other malicious activities. For example, 3G and 4G technologies use mutual authentication to verify the identity of the endpoint and the network. This process helps ensure that adversaries are unable to intercept communications. There are a wide range of security solutions available for the Internet domain that supports IoT communication such as IKEv2/IPsec [18], Transport Layer Security (TLS) [19], Datagram Transport Layer Security (DTLS) [20], Host Identity Protocol (HIP) [21], PANA [22], Kerberos [23], Simple Authentication and Security Layer (SASL) [24], and Extensible Authentication Protocol (EAP) [17]. An IoT network access can be secured using the SIM and other technologies such as, GBA, EAP-SIM, 5G AKA [11], EAP-AKA' [11], EAP TLS, or any other EAP methods for authentication and key exchange. By using these technologies, the SIM can be provisioned with a session security key that can be used in communications with application network peers over well-known protocols. This process can diminish the potential for adversaries to manipulate the application protocol to compromise the devices or service. Thus, it is possible to secure both the network and the application with this model.

Further the LTE standardization considers enhancements to the current system to support the CIoT. The User Data via MME is Control Plane CIoT EPS optimisation specified, where the user data is sent to or from the UE that uses an RRC connection established using the control plane [10]. The 3GPP 5G standardization is currently analysing the security aspects of infrequent and frequent small data transmission. The security for inter-RAT mobility to/from NB-IoT or modifications in the EPC-5GC interworking security specific to CIoT is also under study [TR 33.861] [9]. Enterprise, service providers and network operators focusing on consumer IoT devices and services, should have security solutions and plans in place from the very initial design stages, so that security will not be a concern when it is deployed.

6 IoT Security Outlooks and Best Practices

Evidently, the security measures and good practices need to considered to eliminate the vulnerabilities in IoT ecosystem. ENISA has suggested in, "Baseline Security Recommendations for IoT", potential technical measures to preserve and protect the security of information in IoT [12]. Applying those technical measures should take into account the particularities of the IoT ecosystem such as scalability, namely given the huge number of involved devices certain measures might need to be carried out at the level of specialised architectural components, e.g. gateways. On top of the network security backed by the 3GPP standardization and information security highlighted by ENISA, some additional best practices have to be considered while defining the IoT security solutions. That includes restrictions to default credentials where the default admin/password to allow users log in to their new IoT devices need to be restricted. All vulnerable entry points need to be locked. As often, consumer devices have hardware boards with test points, serial port connectors, etc., which can be used as a back door by the attackers to take control of the device. Removing such access ensures no voiding of security at hardware level. Disable SSH/Telnet based logins of Linux-based IoT devices, if this facility is not required by end user. Confidentiality of IoT communication is the more important aspect of security. For instance the room temperature data are usually unencrypted and if control signals start floating from device to the Internet unencrypted, these devices can be controlled by cloned signals from attackers. So it is required to always have an encrypted communication over SSL/TLS. Over-the-air software/firmware upgrades have to be secured. It is nearly impossible to recall millions of devices to manually patch security vulnerabilities. Updates should be made ensuring authenticity of source by using certificate exchange methods or similar. High Level Interface such as Cloud interface, Web app, and mobile app communication must be encrypted, patched to all known vulnerabilities and protected against attacks, like cross site scripting and SQL injections. To reduce the footprints of large volume of data stored in the cloud by IoT devices, they are commonly left logically unencrypted or non-hashed, which will lead to security threats. Data volume restrictions can be added. For instance, a connected weather station may only be allowed to send 100 MBs of data in a day. This could prevent it being used as a botnet to launch massive DDoS attacks. The other main aspect is the RF security IoT devices that communicate using non-TCP/IP based protocols, like Zigbee, BLE, LoRA [4] etc. are found in devices like fitness bands, smart watches etc. These are often taken for granted, as they are not directly connected to Internet, but, rather, use a gateway. However, the data can be sniffed over radio frequencies using RF explorers or software defined radios, so encryption on data produced by these devices is also essential. DDoS leading to signalling storm imposes a severe risk on the home location register/subscriber system (HLR/HSS) or Unified Data Management (UDM). 3GPP TS 23.122 [8] defines an Extended Access Barring (EAB) service to address this issue. Network Operators can be able to restrict network access to the endpoint/IoT devices configured for EAB, in addition to common and domain-specific access control mechanisms. The UICC or the endpoint devices can be configured for EAB. Network security gateways also need to be configured to "sinkhole" intentional DoS or DDoS attacks [5]. Adopting these security measures will enable a secured communication among IoTs and end users using the IoT service.

7 Security-as-a-Network Service (SENSE) – The Way Forward

Security-as-a-Network Service (SENSE) can be one of the potential way forward to meet the dynamic IoT security issues. SENSE uses the latest networking and information technologies combined with other technological enhancements towards provisioning of security for all stages of products and services. SENSE strives to automate and integrate the security services, security operations, security tools and security technology for Physical (Vehicle-to-Everything (V2X), IoT, 4G etc) and Virtual networks (NFV, 5G etc); which can take spontaneous action for the security events and manage the security controls as forward, faster and secure. For the SENSE to meet out the dynamic security requirements of an IoT ecosystem various fundamental security requirement in a granular level has to be finely designed into the IoT cloud and service which can be customised on demand when there arises a completely new security issue because of a Zero-day exploit or due to an un-common vulnerability. The core security requirements that will form as the basis of SENSE includes security hardening, access management, security audit, secure logging, security policy management and enforcement, communication security, security monitoring, secure credential provisioning and storage, vulnerability assessment (periodic and event-driven), network function security, identity management, security controls, secure clean-up, secure storage protection, secure remote management, physical security, secure update and patching, secure initiation, secure boot-up, secure migration etc. Any IoT security solution that can meet these security requirements can secure any end device, a network function device supporting end-user communication throughout their life-cycle starting from design, supply chain, production, delivery, deployment, usage, maintenance and retirement. A well-designed and implemented SENSE has the potential to offer a complete solution for the IoT security.

8 Summary

The major threats to the IoT ecosystem such as the DDoS, Botnet, impersonation, privacy threats and other advanced persistent threats can jeopardise both the physically and virtually connected world. Systems that contain critical information need to be separated and secured from more heavily abused public-facing systems. IoT security requires an end-to-end approach; Encryption is an absolute must; Security analytics will play a significant role in IoT security solutions; It's imperative for today's digital businesses to balance the business benefits that IoT-connected products can deliver with the recognition that these same devices have become an attractive attack plane for hackers and cybercriminals seeking to cause disruption and exfiltrate sensitive data. Overall, this simple technology IoT can be easily compromised if it is deployed "as such". Yet, with a few fast, simple, and cost-effective security features supported by the SENSE is one of the way forward that can assure IoT to have years of longevity in the communication era.

References

[1] The National Security Agency's review of emerging technologies "The Next Wave", https://www.nsa.gov/Portals/70/documents/resources/everyone/digital-media-center/publications/the-next-wave/TNW-21-2.pdf, Last accessed: 07 Jan 2019.

[2] GSMA, "Remote Provisioning Architecture for Embedded UICC", https://www.gsma.com/newsroom/wp-content/uploads/SGP.02_v3.2_updated.pdf, Last accessed: 07 Jan 2019.

[3] GSMA Whitepaper, "3GPP Low Power Wide Area Technologies", https://www.gsma.com/iot/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper. pdf, Last accessed: 07 Jan 2019.

[4] Migrating an Internet of Things (IoT) Sensor Design to LoRaWAN, https://info.semtech.com/migrating_sensor_design_white_paper_download, Last accessed: 07 Jan 2019.

[5] GSMA, "IoT Security Guidelines for Network Operators", https://www.gsma. com/iot/iot-security-guidelines-for-network-operators/, Last accessed: 07 Jan 2019.

[6] GSMA, "IoT Security Guidelines for Endpoint Ecosystems", https://www.gsma. com/iot/iot-security-guidelines-for-endpoint-ecosystem/, Last accessed: 07 Jan 2019.

[7] GSMA, "IoT Security Guidelines for IoT Service Ecosystems", https://www.gsma. com/iot/iot-security-guidelines-for-iot-service-ecosystem/, Last accessed: 07 Jan 2019.

[8] 3GPP TS 23.122, "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[9] 3GPP TR 33.861, "Study on evolution of Cellular IoT security for the 5G System".

[10] 3GPP TS 33.401, "3GPP System Architecture Evolution (SAE); Security architecture".

[11] 3GPP TS 33.501, "Security architecture and procedures for 5G system".

[12] ENISA, "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures", November 2017, https://publications. europa.eu/en/publication-detail/-/publication/c37f8196-d96f-11e7-a506-01aa75ed71a1, Last accessed: 07 Jan 2019.

[13] William M.S. Stout and Vincent E. Urias (Sandia National Laboratories), "Challenges to Securing the Internet of Things", 2016 IEEE International Carnahan Conference on Security Technology (ICCST).

[14] NIST – Industrial Internet Consortium, "Industrial Internet of Things Security Framework", https://www.iiconsortium.org/IISF.htm, Last accessed: 07 Jan 2019.

[15] 3GPP TS 33.220, "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[16] ONEM2M TS-0003-V3.8.0, "Security Solutions", April 2018.

[17] O. Garcia-Morchon (Philips IP&S), S. Kumar (Philips Research), M. Sethi (Ericsson), "State-of-the-Art and Challenges for the Internet of Things Security", Network Working Group, Dec 2018, https://tools.ietf.org/id/draft-irtf-t2trg-iot-seccons-13.html, Last accessed: 07 Jan 2019.

[18] C. Kaufman (Microsoft), P. Hoffman (VPN Consortium), Y. Nir (Check Point), P. Eronen (Independent), T. Kivinen (INSIDE Secure), RFC7296, "Internet Key Exchange Protocol Version 2", 2014.

[19] E. Rescorla (Mozilla), RFC8446, "The Transport Layer Security (TLS) Protocol Version 1.3", 2018.

[20] E. Rescorla (RTFM Inc.), N. Modadugu (Google Inc.), RFC6347, "Datagram Transport Layer Security Version 1.2", 2012.

[21] R. Moskowitz, Ed. (HTT Consulting), T. Heer (Hirschmann Automation and Control), P. Jokela (Ericsson), T. Henderson (University of Washington), RFC7401, "Host Identity Protocol Version 2 (HIPv2)", 2015.

[22] D. Forsberg (Nokia), Y. Ohba, Ed. (Toshiba), B. Patil & H. Tschofenig (Nokia Siemens Networks), A. Yegin (Samsung), RFC5191, "Protocol for Carrying Authentication for Network Access (PANA)", 2008.

[23] C. Neuman (USC-ISI), T. Yu, S. Hartman & K. Raeburn (MIT), RFC4120, "The Kerberos Network Authentication Service (V5)", 2005.

[24] A. Melnikov, Ed. (Isode Limited), K. Zeilenga, Ed. (OpenLDAP Foundation), RFC4422, "Simple Authentication and Security Layer (SASL)", 2006.

Biography

Sheeba Backia Mary Baskaran received her Ph.D. in Faculty of Information and Communication Engineering from Anna University, Chennai in 2017. She received her M.E. degree in Computer science and engineering from Anna University, Coimbatore and received the B.Tech. degree in Information Technology from Anna University, Chennai. She was a member of NGNLabs Anna University and was a recipient of University Grants Commissions' Maulana Azad National Fellowship from 2013–2016. She is currently working as a Research Engineer with NEC Technologies India Pvt. Ltd., and she has

2 years and 3 months of experience in Research and Development of mobile communication networks and security standardization. She is carrying out her research in Security Solutions for 5G, Vertical Services, Internet of Things, Public Safety network and Common API Framework. Her research interest includes LTE, LTE-Advanced, 5G, IoT Security and MAC layer protocol design. She is a 3GPP SA3 delegate and GISFI member. She contributes to 3GPP SA3 standard Specifications, Global ICT Standardization Forum for India (GISFI) and applied for more than 12 patents in next generation network security. She has authored over 10 publications in international journals (IEEE Access, ACM, Elsevier & Springer) and conferences. She is also a reviewer for IEEE Access and Elsevier journals.