L&T Technology Services

SECURITY CONSIDERATIONS for Internet Of Things

Ajit Jha | Sunil M C

www.lnttechservices.com

Table of Contents

EXECUTIVE SUMMARY

Security is one of the foremost concerns raised by different stakeholders in Internet of Things which has the potential to slow down its adoption. While security has always been a concern since the computers started connecting to each other, the impact was limited to stealing money and intellectual property. But Internet of things adds a completely new dimension to this where the devices performing critical tasks, if insecure, can be manipulated to the devastating effects. The impact could be on public safety, environment, productivity and many others.

The IP Security protocols already take care of many of the concerns. But the nature of IoT devices and IoT architecture creates its own challenges in securing every IoT Solution. Some new security propositions are already there to work within these architectural constraints. The security requirement of the solution also has direct correlation with the cost and time to market. Moreover, every solution has its own business requirements which may or may not be so stringent. So every IoT solution does not require the whole suite of IoT security protocols.

This paper examines the security challenges for internet of things and suggests some security options and approach that can be used for IoT solutions.

INTRODUCTION

Attacks on cyber physical systems focus on critical devices or systems; they provide huge amount of publicity leading to reputation damage, panic, leading to the treasure-trove, i.e. information and more dangerously-playing with human safety; which means more money for attackers through ransoms, espionage, sabotage, etc. Therefore, impetus must be given to security when speaking about smarter environments and technologies such as IoT.

If the foundation is strong then a structure will be able to reasonably withstand hurricanes. Same is the case with information security defense-in-depth strategy, even for IoT, thereby reducing the risk of information misuse, tampering & disclosure and most importantly in safeguarding human lives.

Of late, IoT and related security researches, attacks are grabbing the limelight in the technology space, what with, lifesaving medical devices, software enabled cars, smart grid infrastructure getting into the thick of “internet of” things. These are at the forefront of discussions in conferences like the Black Hat and other non-security forums. And why not, this proves a point that technology is increasing at a rampant pace and getting more and more complex behind the scenes and to top it, countermeasures are often reactive in nature.

The need of the hour is to take a step back - when such life impacting technologies are pushed to the market for cashing in on the “cool” aspects of technology - and integrate security at every stage, because, in most of the cases, security is an afterthought in almost all boardroom discussions. Although, things are changing due to regulatory compulsions where a governing agency enforces compliance, which is good, however, compliance does not always equal security and I am sure you will agree with us.

Although IoT is fairly nascent with intense rate of adoption, a lot of standards bodies have begun work on security of and around IoT, however, we still see a lot of ifs and buts in terms of pinning down the security requirements for such a disruptive notion. There are a lot of legacy devices involved along with smart devices, however, we still say disruptive because it leverages technologies such as cloud and mobility.

IoT SECURITY – COMMON CONCERNS

With this, we come to the question as to what could be considered during the security requirements stage when it comes to designing an IoT or M2M solution. Well, no doubt this is a complex setting and a nightmare as far as security is concerned, however, there has to be a start with respect to building-in security into solutions and platforms, i.e. within each of the components that make IoT.

This needs to be thought through in terms of the safety of human lives, system availability, confidentiality & integrity of information, privacy protection and monitoring & managing all of these and much more.

Hence, we need to bake security in, right from planning to design through to the implementation and monitoring phase, taking a risk based approach. This begins with identifying the assets/components and value of those components, because we cannot effectively protect something which we do not know it exists. Having said that, we can break-down IoT into various components per figure 1

Device or Equipment	Physical devices, endpoints, e.g sensors, ECU's, smart meters, washing machines, etc. get connected to other devices, endpoints across networks to collect/ provide information about themselves and their associated environment.
Gateway or Hub	Enables these devices get equipped to connect to the outer world via Ethernet, RFID, wireless, Bluetooth, etc.
Network or Transport channels	Facilitates the connectivity and transmission of information from devices/ gateways, e.g IP network, GSM/CDMA, satellite networks, etc.
Facilitation	Provides the ability for the devices to send data/ information across gateways/network for further storage, processing, analysis, e.g cloud computing, big data, etc.
Consumerization on or Application	Allows end user/ customers to consume such information on to their smart devices like tablets, smart phones/Televisions, laptops, etc.

Iot Components breakdown

As is the case with all technologies, there comes along a flurry of questions, queries, uncertainties; security is one such concern. However, before discussing security considerations, let us appreciate some of the security challenges and risks that are posed by the advent of IoT.

The attack surface has increased	Extensive leverage of open networks e.g. internet, public cloud, etc. Sensors. Web application. USB , Wireless, Bluetooth, Zigbee, GSM, etc.
Legacy systems (out of date OS/software) no longer supported by OEMs	Software updates, security patches mostly become a forgotten concept on legacy devices especially where vendor no longer provides support making them entry points for sabotaging customer networks leading to DOS attacks , malware infliction points, ransomware, etc.
Unidentified, unauthorized and invalidated devices	Unique identification of user, devices; authentication and access control of devices which may not have an OEM supplied unique ID - these could lead to identity spoofing, phishing, rogue devices, impersonation, etc.
Unauthorized remote access	Remote diagnostics/monitoring, remote maintenance of devices, equipment carries the risk of interception and tampering, in not using secure communication thereby leading to MITM (man in the middle) attacks.
Sensitive data exposure	Sensitive or personal information like patient data on EHR/EMR if they are connected to ECG, ventilator, etc., GPS location of a vehicle to target a person, etc., - sniffing , eavesdropping, waylaying
Extensive dependence on software and applications	Most of the attacks are targeted towards application, especially web application - Injections , XSS , CSRF etc.

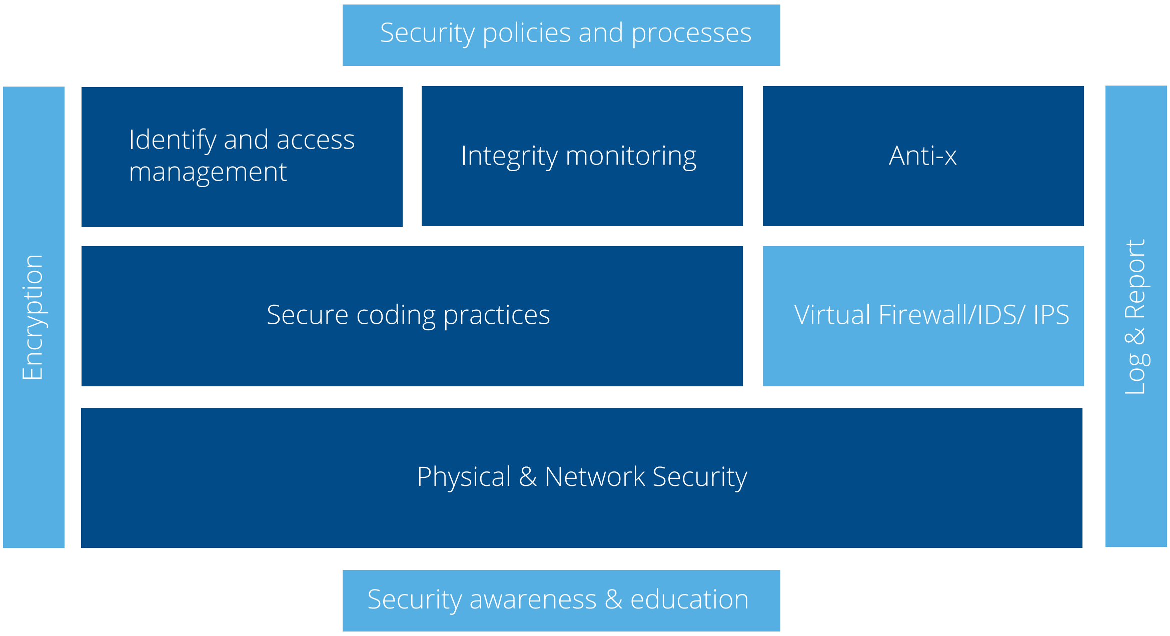
SECURITY FOR IoT – APPROACH AND CONSIDERATIONS

Having seen the various components that make up an IoT, we not only believe that each of these components need to be secured individually, moreover, they also need to work together as one seamless protected environment complimenting one another and completely transparent to the end customer.

Each of the component in IoT environment forms a link in a complex chain. As such it becomes each components' responsibility to implement the basic CIA triad in order to strengthen the over security posture of the environment. CIA triad of confidentiality, integrity, and availability is at the heart of information security. A tried and tested method to cover these aspects is to employ a SSDLC model of development so that security is incorporated in all stages of the life cycle.

We also believe that security must be embedded in stages into any platform or service so that the basic areas are addressed to begin with, proceeding to other security features in a phased manner. This facilitates the business in terms of time to market; however, the business must take an informed decision on their risk appetite i.e. how much risk they are willing to accept & which features to enable depending on the product roadmap. We believe in a layered approach towards security, more often termed as defence-in-depth approach, depicted in the figure 6 below.

Ubiquitous defence-in-depth strategy


Security policies and processes
Encryption
Identify and access management
Integrity monitoring
Anti-x
Log & Report
Secure coding practices
Virtual Firewall/IDS/ IPS
Physical & Network Security
Security awareness & education

Defense-in-depth approach

This approach helps building security in, right from the ground up to monitoring and management allowing the organization to buy more time to plan the defense of their resources, by keeping the potential attacker engaged layer after layer.

Device or Equipment

Physical devices, endpoint, equipment security

- Protecting endpoints or devices(eg. Medical devices) is of utmost importance and organization must adopt means to secure them using various means, for example hardening best practices such as
  - disabling external device connectivity e.g USB drives and allowing their usage only upon approval, review, scanning and on need to know basis
  - disabling direct internet success from sensitive devices/endpoints if not required
  - ensure that unused services are disabled or blocked such as open ports, insecure protocols
  - Secure booting(using keys) and Secure firmware
  - Device authentication support when connecting
  - Applying regular patches on device OS, etc.
  - Secure and authenticated firmware upgrades
  - Connection whitelisting instead of blacklisting
  - Secure key-exchange

Gateway & Network

Gateway security

- Ensure that the IoT/M2M gateway is secured from intrusions and malware by using appropriate mechanisms such as ACLs, IPS, filtering, etc.

Physical and network security

- Facilities should have adequate physical security such as security guards, access cards, visitor logs, CCTV cameras, secure zones, etc. for preventing unauthorized access
- Appropriate security mechanisms should be leveraged for isolating sensitive information bearing segments such as IDS/IPS, firewalls, network ACLs, etc.
- Service provider should obtain and produce assurance certifications such as ISO 27001, SSAE/ISAE SOC reports, privacy seals, etc.

Remote access security

- Allow only strong authentication(e.g MFA) for remote access to privileged users like administrators, clinicians, maintenance personnel for logging in securely from outside the company network
- Usage of secure communication channels such as VPNs- S2S, C2S for regular employees accessing the company network from branch offices or outside locations and disabling that access when no longer needed

Wireless Communications security

- Use of secure configurations when communicating across wireless networks; devices/ sensors to gateways

Enforcing authentications and encryptions

Facilitation

Cloud Security

- Cloud Security & management is an important cog in the wheel and hence needs special attention when it comes to security. Some of the risk mitigation strategies are listed below.
- VMs security needs to be taken care of (e.g Guest OS hardening, patching, updates, etc.)
- Access to the VMs, applications therein needs to have strong control mechanisms
- Data Security within cloud with appropriate technologies and approved encryption algorithms including strong key management procedures need to be thought through
- BC/DR solutions need to be designed like snapshots of VMs and data therein, leveraging regional or offsite backups, having VMs on standby at other cloud services, regions within same cloud provider
- Protecting web facing cloud instances with IDS/IPS, host based firewalls, etc. for malicious traffic detection/prevention
- Log monitoring especially for privileged users and log management integrating logs from multiple and disparate sources with SIEM solutions for correlation and analysis of security incidents

Consumerization or Application	
Application security	Applications(could be web, mobile, cloud, etc.) must be developed with industry standard secure coding practices such as OWASP, SAFECode, SANS/CWE. Etc. to minimize the risk of application related attacks E.g. preventing SQLi, XSS, data leakage, session replay, buffer overflow attacks, etc. Leveraging best practices such as file restrictions(e.g type, size), input validation, etc. Scanning/fuzz testing the applications(dynamic, static, hybrid) for vulnerabilities and taking corrective actions to fix them Employ code signing to assure customers on the authenticity of the software as well as non-repudiation
Integrity monitoring	Critical files must be monitored for any unauthorized alteration or changes, e.g configuration files, traffic must be monitored for any deliberate or accidental changes Appropriate mechanisms like integrity monitoring tools must be implemented to prevent or alert on the above The above must be complemented with strong change approval and review processes.

Table 1 – Security considerations mapped to IoT components

There is another layer apart from the IoT components/layers which is ubiquitous, finds place in each of the above layers irrespective of any component and we can term that as the pervasive layer.

Pervasive		
1	**Identify & understand customer requirements**	Work with customer business, IT & security team to understand business needs, system and environment: Work with customer business, IT & security team to understand business needs, system and environment: customer policies(security & privacy) Regulatory compliance/ industry driven requirements aligned to business objectives(HIPAA, PCI DSS, NERC CIP, EU DPD, US FDA, PIPEDA, etc.) assess security risks
2	**Identity & Access Management(IAM)**	User/ device/endpoint authentication like workstations, medical devices, smart meters, ECU's, etc. Secure provisioning & de-provisioning of devices, users, applications, etc. Integration with existing credentials management system such as AD Securing credentials with salting and hashing Role based access-to device, application, database, network, cloud, etc.

Pervasive		
3	**Data security & Privacy**	Encryption of data at rest(Field/ row level encryption, prevention of unauthorized access to the data store) to ensure confidentiality Security & privacy of data in transit E.g secure transmission of data from device/gateway to cloud, between mobile and cloud, etc. security support in newer/emerging protocols like MQTT which may not have basic security built-in channel or message level encryptions & key management adoption of lightweight secure protocols Integrity of the sensitive information being stored, processed and transmitted must be maintained. Mitigation of repudiation risks for e.g by using digital signatures
4	**Security management**	Ensure that anti-x solutions are deployed and functioning to protect against malwares Patch updates, OS/version upgrades should be regularly employed to avoid known vulnerabilities Conduct vulnerability scans & security testing on an ongoing basis for endpoints, workstations, devices, applications, networks, etc. which form an integral part of IoT solution
5	**Logging and Auditing**	Provide for accountability by enabling logs for tracking access to devices, application, network, etc. and unauthorized changes to files The solution should be able to integrate the logs with customer SIEM solutions for correlation and analysis

Table 2 – Pervasive security layer

One of the critical concern on security comes for the sensors/devices because they have the ability to directly control the things. The IoT sensing devices are connected using diverse communication protocols which use different mechanisms to secure themselves. Some of these mechanisms are listed in table below.

1	**Wi-Fi**	AES, TKIP and WEP encryption WPA and WPA2 EAP-methods for layer 2 authentication
2	**Bluetooth/BLE**	Secure pairing Turning off discoverable mode when not required, enforcing authentication og BT devices For BLE, initial pairing is insecure
3	**Zigbee (802.15.4)**	Link layer encryption with 128 bit AES Trust center for key distribution
4	**6LowPAN**	Secure mode using 802.15.4 link layer encryption Access Control List (ACL)
5	**Weightless**	Encrypted communication link between base station and device
6	**GSM**	Authentication algorithm(A3) to protect from unauthorized service access Cipher Key generating algorithm(A8) embedded in SIM. Temporary Mobile Subscriber Identity(TMSI) to avoid intrusions
7	**3G**	Mutual authentication – Cipher key and integrity key generation Data Integrity User-USIM authentication

IP security Protocols

1	**IKEv2/IPsec**	X.509 certificates for authentication Diffie-Hellman Key exchange for shared session secret Cryptographic key generation using shared secret Establishes a secure tunnel
2	**TLS/SSL**	X. 509 certificate for authentication Asymmetric keys from X.509 used for symmetric key exchange Symmetric key used for data encryption
3	**DTLS**	Datagram TLS(based on TL5)
4	**HIP**	Host Identity Protocol Host identity based on public key(instead of popular IP address/ DNS)

5	EAP	Extensible Authentication Protocol An authentication framework supporting multiple authentication methods Works on Link layer Uses different protocols for EAP messages transmission Supports key delivery and usage mechanisms
6	SSH	A cryptographic network protocol Uses public key cryptography for mutual authentication Creates a secure channel for data

Table 3 – Secure protocols for Sensing devices

CONCLUSION

Security is critical to the internet of things and needs to be taken care of at every stage because we are not just dealing with financial transactions which can be tackled through penalties in case there is a data breach. Here we are talking of systems whose infiltration could lead to loss of lives or cause massive disruption to the society.

IoT is a worthwhile amalgamation of business agility and technology, however, it is imperative that any rendezvous which relates to IoT takes a holistic risk based approach not only aligned to business objectives but also take into account the probable impact it may have on human lives. Within this, Security is an enabler for a business to be conducted in a secure manner which is transparent and works behind the scenes. Security in a solution provides reasonable assurance to the business that the end customer's as well as their interests are safeguarded from potential threats.

Hence, the IoT shall use well-defined standards for security which talk with safety standards catering to diverse industries and enables businesses to think and act in a pragmatic way.

REFERENCES

1. http://cache.freescale.com/files/32bit/doc/brochure/PWRARBYNDBITSMTM.pdf

2. http://www1.cnnic.cn/ScientificResearch/LeadingEdge/wlw1/

3. http://en.wikipedia.org

4. http://en.wikipedia.org/wiki/Internet_of_Things

5. http://www.forbes.com/

6. http://www.hhs.gov/

7. https://www.hslu.ch/

8. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6188257

9. http://www.mercurynews.com/

10. https://www.pcisecuritystandards.org/index.php

11. http://postscapes.com/internet-of-things-market-size

12. http://www.rfidjournal.com/articles/view?4986

13. https://tools.ietf.org/html/draft-garcia-core-security-06

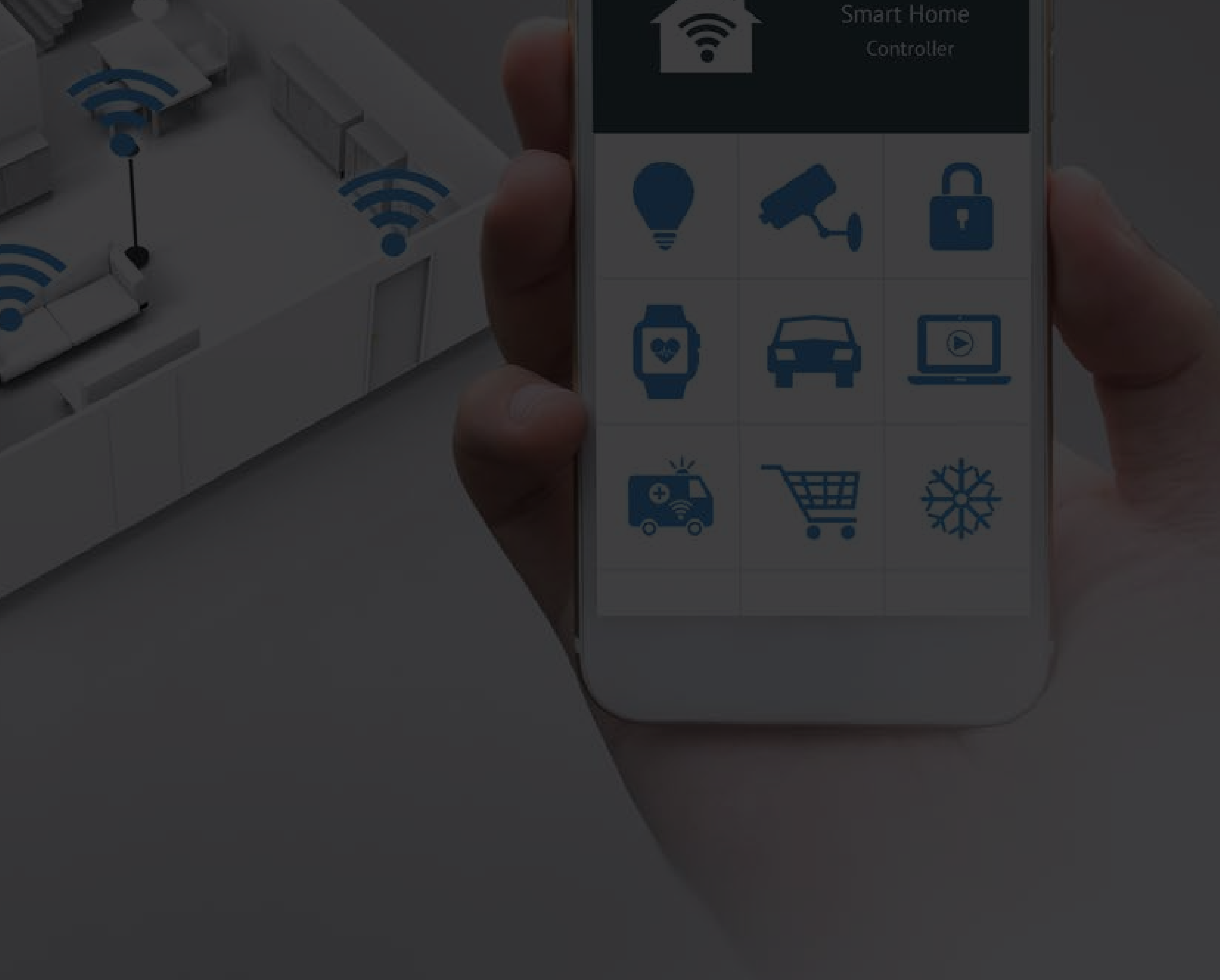
Acronyms

- ACL - Access Control List
- AD – Active Directory
- AES – Advanced Encryption Standard
- BC - Business Continuity
- BLE – Bluetooth Low Energy
- CCTV - Closed-circuit television
- CDMA - Code Division Multiple Access (CDMA)
- CIA – Confidentiality, Integrity and Availability
- CSRF - Cross Site Request Forgery
- C2S - Client to Site
- DDOS - Distributed Denial of Service
- DOS – Denial of Service
- DR - Disaster Recovery
- DTLS – Datagram Transport Layer Security
- EAP – Extensible Authentication Protocol
- ECG - Electrocardiography
- ECU - Electronic Control Unit
- EHR/EMR - Electronic Health Record/Electronic Medical Record
- ETSI - European Telecommunications Standards Institute
- EU DPD - European Union Data Protection Directive
- GPS - Global Positioning System
- GSM - Global System for Mobile Communications
- HIP – Host Identity Protocol
- HIPAA - Health Insurance Portability and Accountability Act
- IAM – Identity and Access Management
- ID - Identity
- IDS/IPS - Intrusion Detection System/Intrusion Prevention System
- IKE – Internet Key Exchange
- IPsec – Internet Protocol Security
- ISAE - International Standard on Assurance Engagements
- IoT - Internet of Things
- IP - Internet Protocol
- ISO 27001 - International Organization for Standardization 27001 (Information Security Management System)
- IT - Information Technology

- MFA – Multi-Factor Authentication
- MITM – Man In The Middle
- MQTT – Message Queue Telemetry Transport
- M2M - Machine to Machine
- NERC CIP - North American Electric Reliability Corporation Critical Infrastructure Protection
- OEM - Original Equipment Manufacturer
- OS – Operating System
- OWASP – Open Web Application Security Project
- PCI DSS - Payment Card Industry Data Security Standard
- PIPEDA - Personal Information Protection and Electronic Documents Act
- RFID - Radio Frequency Identification
- SAFECode – Software Assurance Forum for Excellence in Code
- SANS Institute/CWE - SysAdmin, Audit, Networking, and Security Institute/Common Weakness Enumeration
- SIEM - Security Information and Event Management
- SOC – Service Organization Control
- SSDLC – Secure Software Development Life Cycle
- SSAE - Standards for Attestation Engagements
- SSH – Secure Shell
- SSL – Secure Socket Layer
- S2S - Site to Site
- SQL/SQLi - Structured Query Language/Structured Query Language injection
- TKIP – Temporal Key Integrity Protocol
- TLS – Transport Layer Security
- US FDA - United States Food and Drug Administration
- USB - Universal Serial Bus
- USIM – Universal Subscriber Identity Module
- VM - Virtual Machine
- VPN - Virtual Private Network
- WEP – Wired Equivalent Privacy
- Wi-Fi – Wireless Fidelity
- WPA – Wi-Fi Protected Access
- WPA2 – Wi-Fi Protected Access version2
- XSS - Cross Site Scripting
- 3G - 3rd Generation
- 6LowPAN – IPv6 over Low Power Personal Area Networks

ABOUT L&T TECHNOLOGY SERVICES

L&T Technology Services is a subsidiary of Larsen & Toubro with a focus in the engineering services space, partnering with a large number of Fortune 500 companies globally. We offer design and development solutions through the entire product development chain, across various industries such as Industrial Products, Medical Devices, Transportation, Telecom and Hi-tech and the Process Industry. We also offer solutions in the areas of Mechanical Engineering Services, Embedded Systems & Applications, Engineering Process Services, Product Lifecycle Management, Engineering Analytics, Power Electronics and Machine-to-Machine and the Internet-of-Things (IoT).



L&T Technology Services