IOT: SURVEY OF SECURITY AND PRIVACY

The IoT is intended for ubiquitous connectivity among different entities or "things". It is a state wherein there is no distinguishable difference between the operation of devices surrounding us and our actions and all the devices become a part of our experience.

The IoT's heterogeneous essence, dynamics, intelligence, mobility and undefined perimeters not only makes it a high demand technology domain but also makes it vulnerable and risky under security terms.
Through this research paper, the writers, Diego Mendez, Joannis Papapanagiotou, Baijian Yang, have provided a detailed and exhaustive survey of the "Security Triad" of IoT, i.e. DATA CONFIDENTIALITY, DATA INTEGRITY, AVAILABILITY.

On broad terms, Iot Systems can be divided into three different layers:-

- The Perception Layer
- The Network Layer
- The Application Layer

Perception layer does the work of gathering environmental data, then the Network layer composed of wired and wireless devices transmits the inputs and other important information to carry out upcoming operations. The Application Layer consists of abstracted solutions that interact with the final users in alignment with their final goals.

VULNERABILITIES:

Security issues in IoT systems can be technological, ethical and privacy interfering. In October 2016, the massive DDoS (Distributed Denial of Service) attack on DYN (A leading company name in maintaining the internet's DNS infrastructure) by a botnet army of IoT infected devices has raised alarms on the consequences of insecure IoT systems.

If we try to summarize, IoT systems should incorporate the following set of basic security requirements:

- Secure Authentication
- Secure Bootstrapping and Transmission of Data
- Security of IoT Data
- Secure access to data by authorised persons
- Intrusion Detection Technologies
- Cryptographic Key management
- Physical Security Design

Some security measures are important in some cases while others maybe more important in some other very different systems.
This can be easily analysed through the example that,
"The confidentiality needed for a sensor data may not be as much important as the Integrity and Authenticity of that particular data stream, owing to the fact that the attacker can easily obtain the same environmental values by putting his own rogue sensor near the legitimate one".

Thus it can be safely said that majority of security concerns lie in connection services or data authentication and correctness of the data because, as discussed earlier, if an attacker injects malicious data bytes in the IoT system, then it will surely malfunction and that could create significant Financial Losses, or even Life-threatening situations.

CONCLUSION:

The ongoing IoT state reveals that there is still significant work left in field of 'Security Triad'. It is quite evident that the number of IoT devices as well as new technologies and scientific publications has soared in the last few years, on the other hand, the security solutions and improvements have not kept the pace.

The amount of data generated and handled by IoT devices is increasing exponentially, that leads to higher exposure of sensitive data and more loopholes. Researchers have an opportunity to work upon to fill the loopholes and research on Intrusion Detection Systems (IDS). On the other hand, final users too need to understand and take up some responsibility to follow strict protective measures and scrutiny and by doing so, we can rule out about 25% security concerns that occur due to carelessness or negligence of the end Users.

Together with cutting edge technological advancement, new robust algorithms and personal vigilance, we can create secure IoT systems which would enhance our capabilities as a species.
