Internet of Things Security

Overview

- Description: The Internet of things (IoT) equips physical objects with computer technology and sensors, and hence enables them to build networks among themselves. Threats can arise by the misuse of integrated sensors (e.g. cameras or microphones), which monitor and gather all types of data on machines and human social life.[1,2]. The malware "Stuxnet" has shown that cyber attacks on such networked devices can have serious physical impact. Hence security issues, such as privacy, authorization, verification, access control, system configuration, information storage, and management, are the main challenges in an IoT environment.
- State of research: IoT security is an active field of research, however IoT security can still be regarded to be in its infancy. Security issues, such as privacy, authorization, verification, access control, system configuration, information storage, and management, are the main challenges in an IoT environment.
- Capabilities: An IoT with high security standards enables secure IT networks between objects such as houshold appliances, wearables, medical devices, but also vehicles, buildings or industrial facilities. This also includes critical infrastructures such as energy supply or transportation.
- Limits: The conventional security architecture is designed based on the perspective of users and not applicable for the communication among machines. Hence different approaches and techniques are used in handling IoT network security issues.

Further Information

- Key player: For example, large IT companies such as Google, Apple, Microsoft or Amazon are active in developing Smart Home devices.
- Readiness: Several commercial IoT devices are already available. However, the security of such devices currently lags behind the present rate of development.
- Users: In can be expected that essentially everybody comes in contact with the IoT and hence depends on its security (e.g. consumers/citizens, industry, military, security, medical, critical infrastructures…)
- Future outlook and foresight: The use of internet of things devices will likely rise dramatically in the future. A well-defined security and privacy policy must be designed and deployed to guarantee confidentiality, access control, and privacy for users and items. Because of considerable research efforts in this area, it can be expected that that these devices will become more secure over time.
- Related Technologies: Industry 4.0, Cyber Physical Systems
- Links: [1] Z. Yan, P. Zhang, A.V. Vasilakos, *A survey on trust management for Internet of Things*, J. Netw. Comput. Appl., 42 (2014), pp. 120–134, doi: 10.1016/j.jnca.2014.01.014, [2] F. A. Alaba, M. Othman, I. A. T. Hashem, F. Alotaibi, *Internet of Things security: A survey*, Journal of Network and Computer Applications, 88, 2017, 10-28, doi: https://doi.org/10.1016/j.jnca.2017.04.002,