JINNAH UNIVERSITY FOR WOMEN

Department of Computer Science & Software Engineering

Information Security

Class Task

1. For this task you must select a recent paper (within the last five years) on the topic of cyber security of an IoT.

Based on the paper you have read, please specify a scenario of attack that you think may be possible to apply to some component of the smart grid/IoT. In your discussion you must specify

1. **Vulnerability**,
2. **Cyber-attack**,
3. **Threat**

**Vulnerabilities in Smart Home Appliances**

* System heterogeneity (Devices of different vendors may increase overall vulnerability of system as their security measure may differ from each other leaving susceptibility)
* Networked system accessibility (data as well as IoT devices themselves are accessible through internet which increases the possibility of attack)

**Scenario**

Web cams are used in IoT devices for surveillance and owners assume that the data gathered by them is accessible by them only. However, a number of sites including Shodan and Censys which legitimately help users in search for nearby sensors that ultimately make them visible to large number of audience as device type, model, firmware and other relevant info get revealed[1].

**Cyber Attack in Smart Home Appliances**

* Denial-of-service is kind of attack that is an attempt to make a machine or network resource unavailable to its intended users.
* Access attacks are the ones in which unauthorized persons gain access to networks or devices to which they have no right to access.

**Scenario**

An intruder may gain access to smart home IoT devices if device address and relevant information is accessible. For example, hackers can [compromise](https://gulfnews.com/technology/smart-light-bulbs-can-hack-your-personal-information-1.1571846229201) infrared-enabled smart bulbs by sending commands via an infrared invisible light emitted from the bulbs to exploit other connected IoT devices existing on the home network.

**Threats in Smart Home Appliances**

* Confidentiality threats are those that result in the unwanted release of sensitive information.
* Authentication threats can lead to either sensing or control information being tampered with.
* Access threats are probably the greatest threats. Unauthorized access to a system controller, particularly at the administrator level, makes the entire system insecure.

**Scenario**

For example, confidentiality breaches in home monitoring systems can lead to the inadvertent release of sensitive medical data. Healthcare data are collected from IoT devices [2]. These devices gather data by remote access mechanisms which have some challenging about privacy and security. Data collected by the sensor is transmitted to the database or cloud over internet. In addition, IoT devices connect internet and communicate with each other from the Internet. Security vulnerabilities on Internet and IoT devices are threatened health data.

**Reference:**

[1] A. Arabo, “Cyber Security Challenges within the Connected Home Ecosystem Futures,” *Procedia Computer Science*, vol. 61, no. February, pp. 227–232, 2015, doi: 10.1016/j.procs.2015.09.201.

[2] C. Eken and H. Eken, “Security Threats and Recommendation in IoT Healthcare,” *Proceedings of The 9th EUROSIM Congress on Modelling and Simulation, EUROSIM 2016, The 57th SIMS Conference on Simulation and Modelling SIMS 2016*, vol. 142, pp. 369–374, 2018, doi: 10.3384/ecp17142369.