Part 1: Assignment Brief (team project) 600 words

Select a case study for the group from those presented in the reading for this unit.

You are required **to design and create a scenario using Python which models the activities associated with the networked devices in a Systems of Systems (SoS)** based on the examples provided.

An SoS, in general terms, are characterised by several features, often represented by the acronym (ABCDE) - that is:

- "**Autonomy** - each system is free and independent with its own purpose of operation;
- **Belonging** - systems function collaboratively to meet a common higher purpose;
- **Connectivity** - synergism is enabled by the highly dynamic distributed network;
- **Diversity** - the constituents are heterogeneous, self-sufficient systems that are open for enhancement by evolution and adaptation;
- **Emerging** - the cumulative actions and interactions between the constituents of an SoS give rise to the behaviours that can be attributed to the SoS as a whole."

(Boardman and Sauser, 2006).

Some examples of an SoS include ***an IoT network (as used in a smart home),*** a connected CPS (i.e., an autonomous or self-driving) car, or a fog computing system (consisting of IoT, edge and cloud devices). Some examples are given in the suggested journal articles.

Deliverable 1: Design Document

Create an Attack-Defence Tree (AD-Tree) that models the security vulnerabilities of a client, a hub or host (i.e the part that gathers data and makes decisions about the operation of the system) **and the overall system, based on the case studies** provided.

The tree should display typical vulnerabilities and you should select a suitable domain to allow quantitative evaluation of security vulnerabilities.

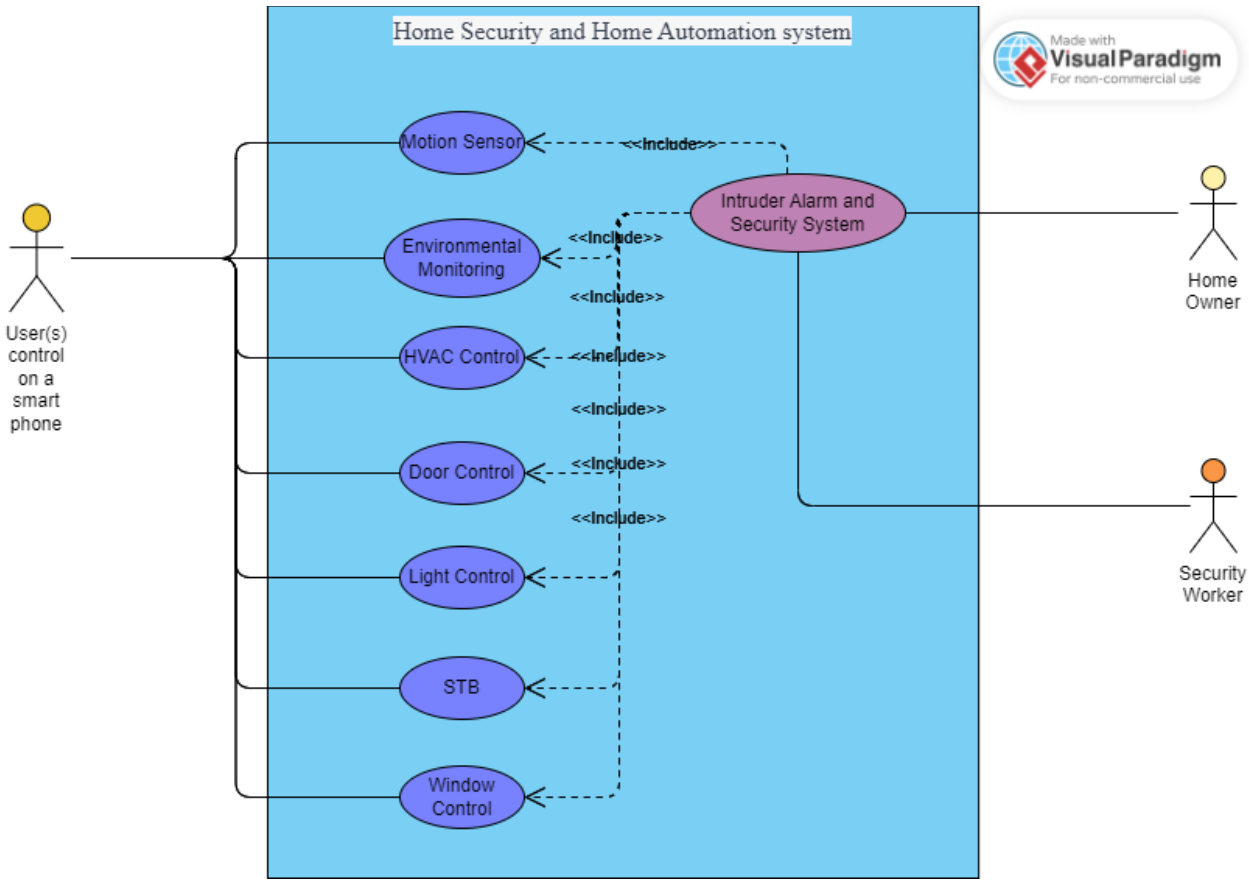
Checklist for Deliverable 1:

- **Compile a list of potential vulnerabilities from academic resources** (remember to cite all sources). (Knowledge and Understanding – 15, Application of Knowledge and Understanding - 10, Criticality – 5)
- **Create an AD Tree using the Luxembourg (or alternative) software for the client, the controller/ co-ordinator and the overall system to display the vulnerabilities of each and of the whole.** (Knowledge and Understanding – 10, Application of Knowledge and Understanding – 15)
- **Select a suitable domain to assign values to each element of the tree and justify your selection of a domain.** (Criticality – 10)
- Based on your model, **suggest suitable mitigation(s) to ameliorate the vulnerabilities**. (Criticality – 10)
- **All decisions should be supported by related academic literature.**

My Submission

Introduction

The (Kodali, et al., 2016) case study provides an overview of a low-cost system that serves as a smart home security and home automation (as seen on the usecase/figure below).



Below is a table showing the current features of the system that makes it to be vulnerable and the mitigations that can be applied (as referenced from (Touqeer, et al., 2021), (Borgini, 2021), (Apriorit, 2022), (Anand, et al., 2020), (Abdullah, et al., 2019))

Features of the Current System	Risks Accompanied	Potential Vulnerabilities	Possible Mitigations
It relies solely on digits on the phone's keypad to access the security system	• Unauthorized access. • Spoofing • Man-in-the-middle Attacks • Installation of malicious software • Fines and lawsuits that could lead to damaged reputations, bankruptcy and losses	• Lack of Multi-Factor Authentication • Lack of authorization • Unencrypted communication • Not enough security enforcing features • Lack of data privacy and certified compliances like GDPR, ISO 27001, ISO 27017, ISO 27018, etc	• Multi-Factor Authentication • Implement changing of passwords • Implement complex passwords • Limit number of log-in attempts • User Access controls • Authorizations • Session management • Implement data privacy
The system's functionality is dependent on the	• Wi-Fi dependency • Network attack • Denial-of-Service	• System is down and security is compromised	• Set-up other system connectivity e.g.,

Wi-Fi connection only,	(DoS) and Denial-of -Sleep (DoSL) attacks	once Wi-Fi connection is lost or weak • Insecure network • Unencrypted communication	Local Area Connection • Firewalls like Next-generation firewall • Limit device or network bandwidth • Backup connectivity options like 4G or 3G, to ensure that the system remains operational even if the Wi-Fi connection is lost. • Intrusion Detection and Prevention Systems • Implementation of secure socket layer (SSL) Certificates, • Data Encryption

			• Network segmentation
Lack of security tests that make room for the system's improvements	• More prone to breaches	• Lack of security tests and scanning	• Regular security and backup testing, and scanning for threats helps in reinforcing the system
Lack of data storage security	• Injection attacks • Tampering	• Unsecure data storage	• Secure databases • Antivirus • Data encryption
Lack of Security Updates	• More prone to breaches	• Lack of Security Updates and patches	• Regular and automatic System and hardware updates
Unsecured device management	• Unauthorised factory-resetting of devices • Installation of malicious software and updates	• Malicious software updates • Device breaches • Weak firmware or software, servers, backend	• Use of secure updating mechanisms like digital signatures • Practising secure Programming

	• Software and firmware risks and attacks	application	practices • System centralization • Implementing secure device management protocols • Limiting the number of device management access points • Ensure tamper-resistant hardware
Human Error	• Breaches • Social engineering	• Human errors	• Cybersecurity training on users

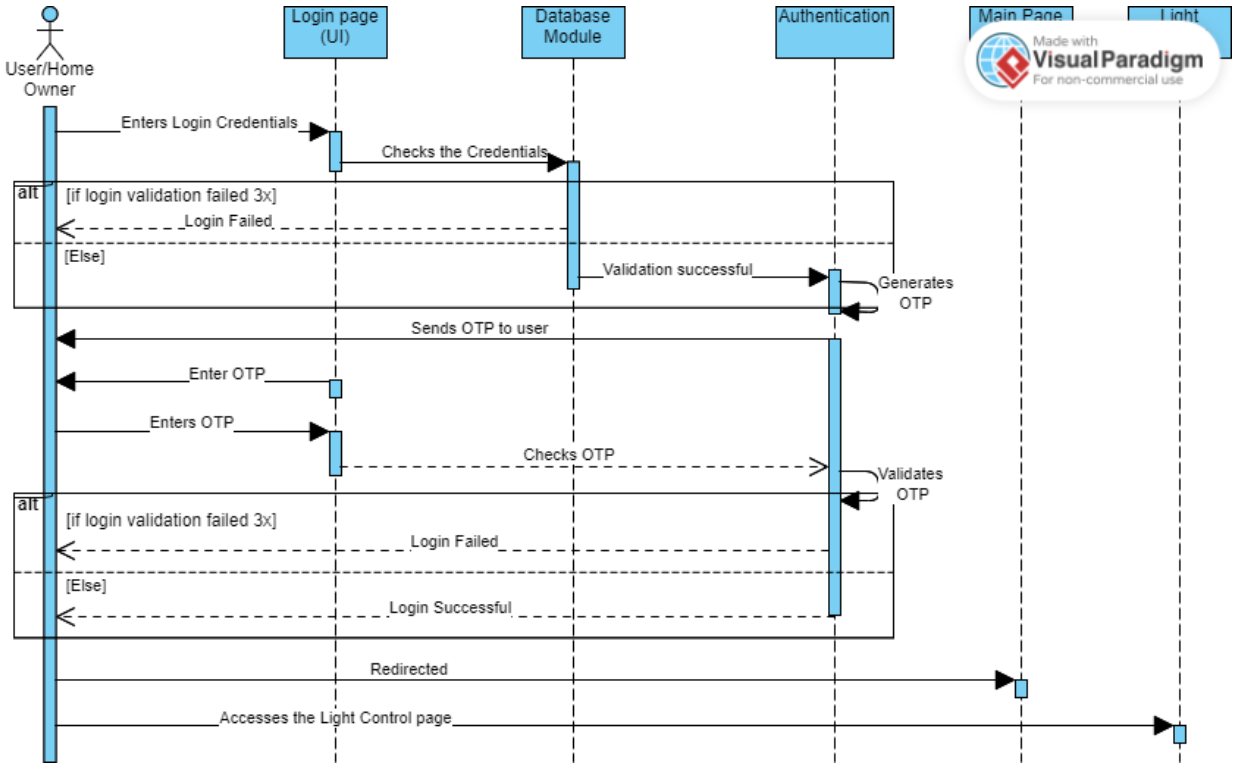
Scrum -Splint 1: with the use of Python language

1. Implement a user interface that will centralize the system
2. Implement Multi-Factor Authorization
3. Implement change of password
4. Validation of complex passwords
5. Access control and Authorization
6. Session Management

7. Prove the chosen *thesis question by perfoming tests*

8. Cookies and certificates csrf token

Activity Diagram of Authentication



References

Abdullah, T., Ali, W., Malebary, S. & Ahmed, A. A., 2019. A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home. *International Journal of Computer Science and Network Security (IJCSNS),* 19(9), pp. 139-146.

Anand, P. et al., 2020. IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges. *IEEE Access,* Volume 8, pp. 168825-168853.

Apriorit, 2022. *Internet of Things (IoT) Security: Challenges and Best Practices.* [Online]
Available at: https://www.apriorit.com/white-papers/513-iot-security
[Accessed 02 February 2023].

Borgini, J., 2021. *Tackle IoT application security threats and vulnerabilities.* [Online]
Available at: https://www.techtarget.com/iotagenda/tip/Tackle-IoT-application-security-threats-and-vulnerabilities
[Accessed 2 February 2023].

Kodali, R. K., Jain, V., Bose, S. & Boppana, L., 2016. *IoT based smart security and home automation system.* Greater Nodia, IEEE.

Touqeer, H. et al., 2021. Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing,* Volume 77, pp. 14053-14089.