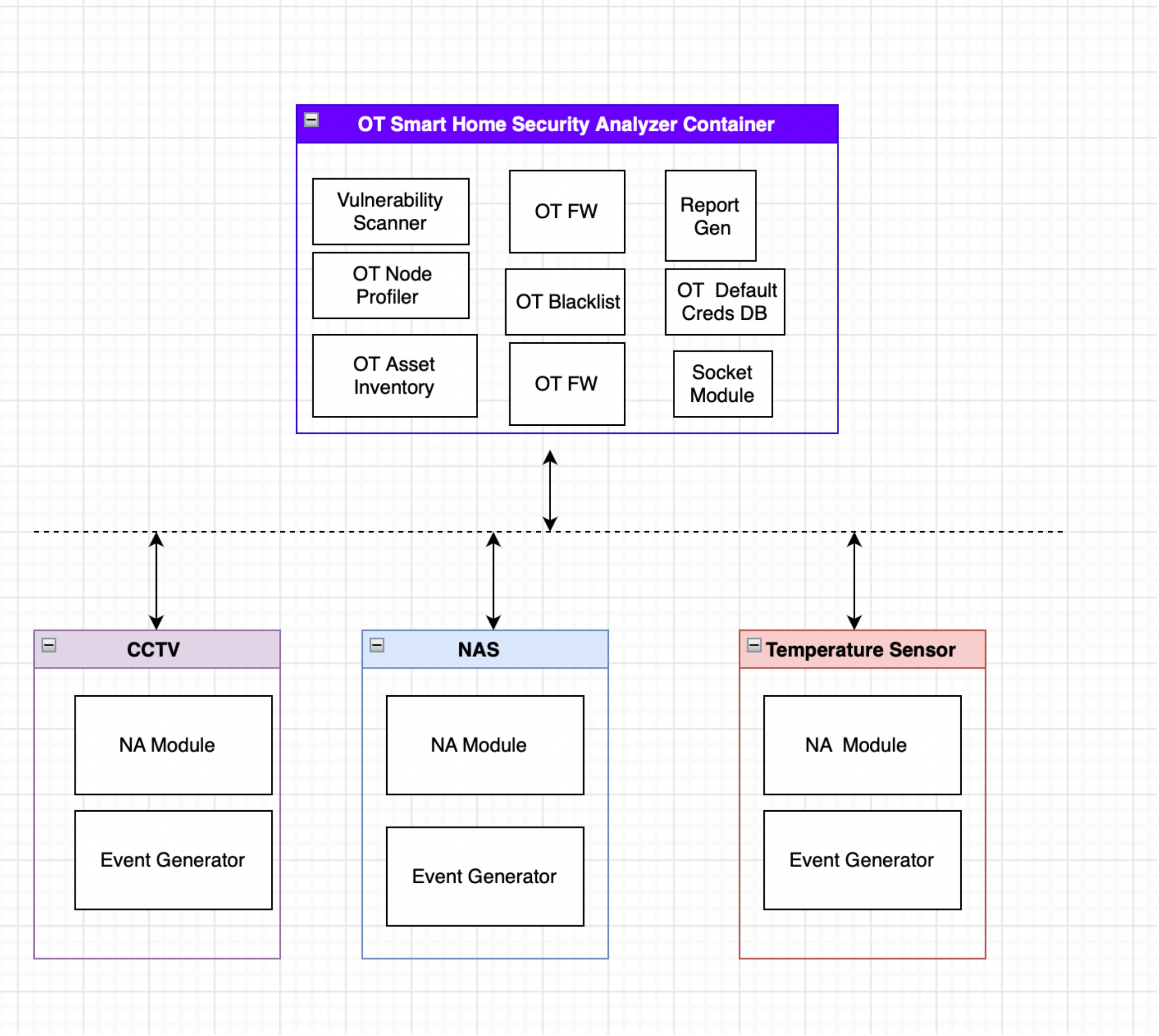
OT Smart Home Security Analyzer (OTSHSA) Design Document

OT Smart Home Security Analyzer (OTSHSA) is an IOT security controller that detects the presence of new IoT nodes in home environment and does Automatic Service Fingerprinting and Security Posture assessment with the help of a scanner module. OT Smart Home Security Analyzer acts as the internet gateway and Proxy Firewall for all connected OT devices. The scanner module periodically scans the existing nodes for any new vulnerabilities. As a remediation measure, devices with known high vulnerabilities are blocked and not allowed to connect to the internet. The rogue device detection capability of the OT Smart Home Security Analyzer prevents the node from connecting to the internet and communicating with other nodes with MAC filtering. Replay attacks and device cloning attack prevention is done with identity verification of OT clients.



The scanning module detects the presence of OT devices with default credentials. In addition to this, the connected OT node sends event notifications as it happens to the OT Smart Home Security Analyzer. Detection of control panel takeover and configuration manipulation, Inadvertent exposure assessment, Control validation of brute force prevention mechanism in nodes, etc., are also part of the solution.

Functional Modules:

The major functional elements planned include the following.

- **Vulnerability Scanner** – This module comprises several community scanning packages for the on-demand and periodic scanning of the security posture of the connected OT clients.
- **OT Node Profiler** – This module is responsible for OT node client profiling and fingerprinting.
- **OT Asset Inventory** – This database stores all the known fingerprinting details of the connected OT clients and is used for comparison at the time of detection of new clients.
- **OT-FW** – This module is responsible for enforcing access control rules for outbound communication based on the security posture of the OT client.
- **OT Blacklist** – This data store maintains a list of blocked OT nodes.
- **OT Default Creds DB** – This data store maintains a list of known default credentials in OT nodes.
- **Report Gen** – This module is responsible for generating OT client assessment reports.

Attack Defense Trees (ADTrees)

The Attack Defense Tree describes threats and vulnerabilities of a system, in perspective of various attacks, and shows possible attack paths that attackers follow to compromise the system(1). The tree represents the attacks against the system. This Threat modeling is used to help in reasoning, identifying, and enumerating possible risks and threats.

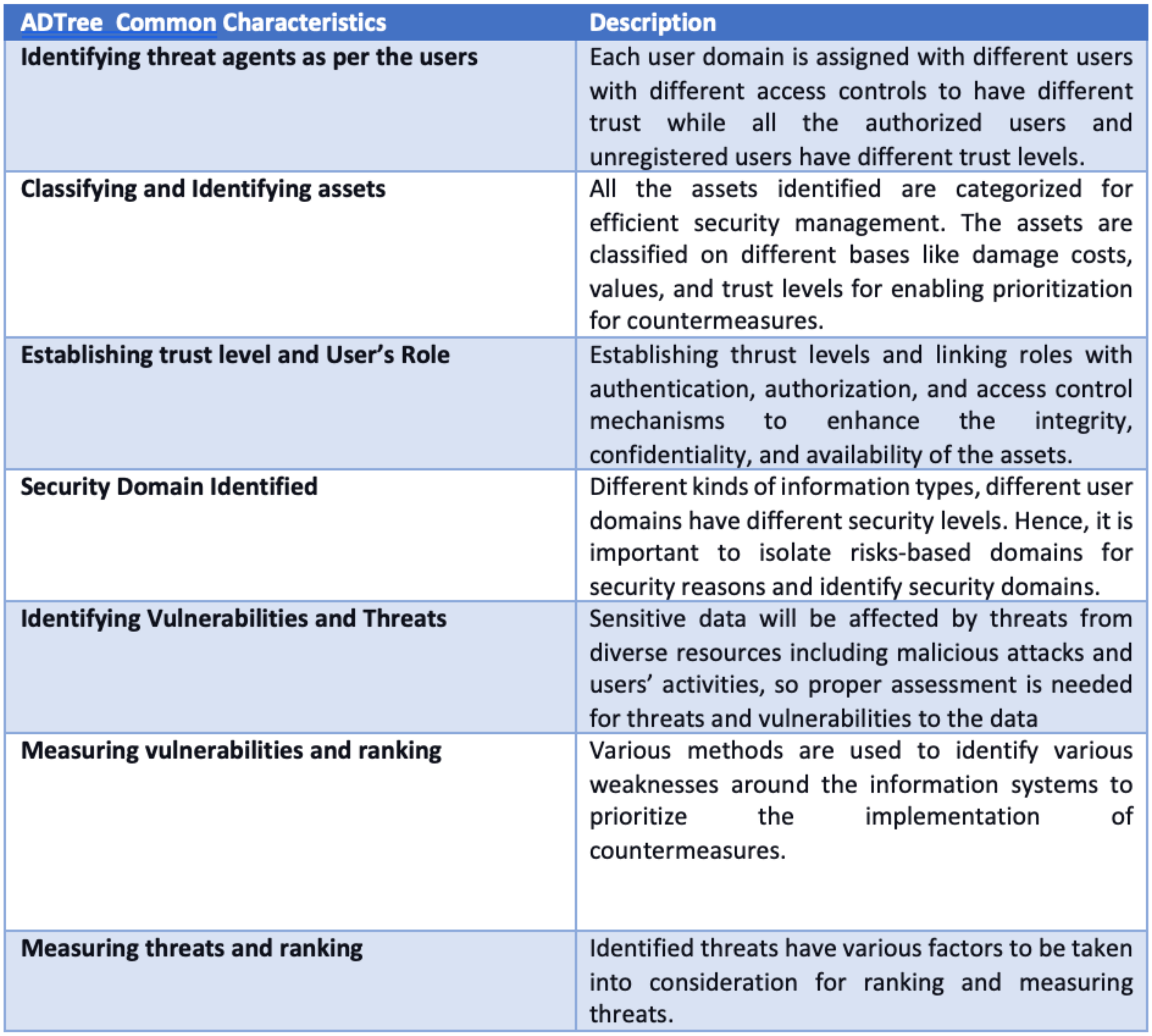
The various type of threat modeling is Attack Tree (AT), Attack Graph (AG), and Attack Surface (AS) (2). The modeling pervasive computing paradigm disclosing Information of Likability, Identifiability, detectability, Non-Repudiation, Unawareness, and Non-Compliance as defined below (3):

- The attacker's primary goal is defined at the root node
- The main goal is divided into sub-goal in terms of leaving nodes(7)
- Stepwise subtasks are continually divided into sub-goals
- Attribute values are assigned with the leave nodes

The Attack graph adapts a graphic view of all attack paths from attack point to attack target (4). The Attack graph assesses network configuration and vulnerability information of the network with the entire dependency interactions of the data (8). The Attack surface captures software features Input post to contribute the vulnerabilities (7).

The Attack Defense Trees use security modeling (6) and analysis with the steps to define the paths, outlining the abilities of threat modeling with the illustration assigning characteristics to the nodes:

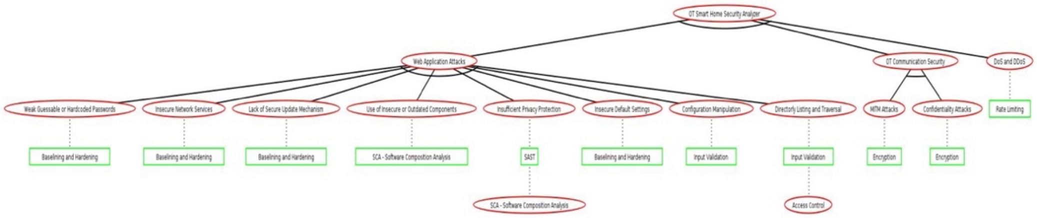
The below table enlists standard features of the address.



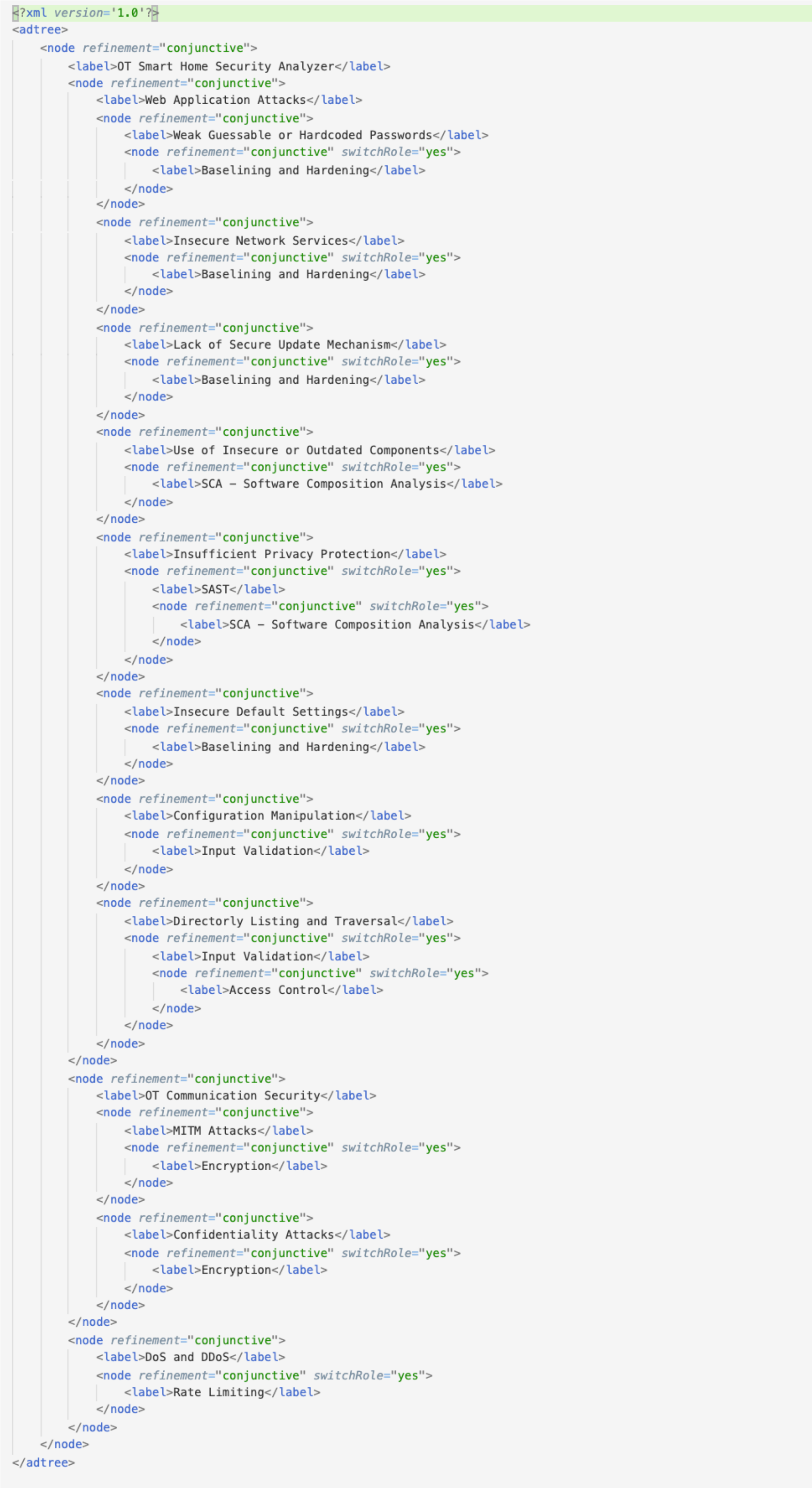
ADTree Common Characteristics	Description
Identifying threat agents as per the users	Each user domain is assigned with different users with different access controls to have different trust while all the authorized users and unregistered users have different trust levels.
Classifying and Identifying assets	All the assets identified are categorized for efficient security management. The assets are classified on different bases like damage costs, values, and trust levels for enabling prioritization for countermeasures.
Establishing trust level and User's Role	Establishing thrust levels and linking roles with authentication, authorization, and access control mechanisms to enhance the integrity, confidentiality, and availability of the assets.
Security Domain Identified	Different kinds of information types, different user domains have different security levels. Hence, it is important to isolate risks-based domains for security reasons and identify security domains.
Identifying Vulnerabilities and Threats	Sensitive data will be affected by threats from diverse resources including malicious attacks and users' activities, so proper assessment is needed for threats and vulnerabilities to the data
Measuring vulnerabilities and ranking	Various methods are used to identify various weaknesses around the information systems to prioritize the implementation of countermeasures.
Measuring threats and ranking	Identified threats have various factors to be taken into consideration for ranking and measuring threats.

We have assessed the overall security posture of the proposed OT Smart Home Security Analyzer (OTSHSA) with separate ADTrees. We have taken steps to improve the solution's comprehensive security architecture with these learnings. Details about the trees along the security observations and remediation steps identified are listed in the below diagrams.

OT Smart Home Security Analyzer (OTSHSA) ADTree


OT Smart Home Security Analyzer
Web Application Attacks
OT Communication Security
DoS and DDoS
Weak Guessable or Hardcoded Passwords
Insecure Network Services
Lack of Secure Update Mechanism
Use of Insecure or Outdated Components
Insufficient Privacy Protection
Insecure Default Settings
Configuration Manipulation
Directorly Listing and Traversal
MITM Attacks
Confidentiality Attacks
Rate Limiting
Baselining and Hardening
Baselining and Hardening
Baselining and Hardening
SCA - Software Composition Analysis
SAST
Baselining and Hardening
Input Validation
Input Validation
Encryption
Encryption
SCA - Software Composition Analysis
Access Control

OT Smart Home Security Analyzer (OTSHSA) ADTree XML



```xml
<?xml version='1.0'?>
<adtree>
    <node refinement="conjunctive">
        <label>OT Smart Home Security Analyzer</label>
        <node refinement="conjunctive">
            <label>Web Application Attacks</label>
            <node refinement="conjunctive">
                <label>Weak Guessable or Hardcoded Passwords</label>
                <node refinement="conjunctive" switchRole="yes">
                    <label>Baselining and Hardening</label>
                </node>
            </node>
            <node refinement="conjunctive">
                <label>Insecure Network Services</label>
                <node refinement="conjunctive" switchRole="yes">
                    <label>Baselining and Hardening</label>
                </node>
            </node>
            <node refinement="conjunctive">
                <label>Lack of Secure Update Mechanism</label>
                <node refinement="conjunctive" switchRole="yes">
                    <label>Baselining and Hardening</label>
                </node>
            </node>
            <node refinement="conjunctive">
                <label>Use of Insecure or Outdated Components</label>
                <node refinement="conjunctive" switchRole="yes">
                    <label>SCA - Software Composition Analysis</label>
                </node>
            </node>
            <node refinement="conjunctive">
                <label>Insufficient Privacy Protection</label>
                <node refinement="conjunctive" switchRole="yes">
                    <label>SAST</label>
                    <node refinement="conjunctive" switchRole="yes">
                        <label>SCA - Software Composition Analysis</label>
                    </node>
                </node>
            </node>
            <node refinement="conjunctive">
                <label>Insecure Default Settings</label>
                <node refinement="conjunctive" switchRole="yes">
                    <label>Baselining and Hardening</label>
                </node>
            </node>
            <node refinement="conjunctive">
                <label>Configuration Manipulation</label>
                <node refinement="conjunctive" switchRole="yes">
                    <label>Input Validation</label>
                </node>
            </node>
            <node refinement="conjunctive">
                <label>Directorly Listing and Traversal</label>
                <node refinement="conjunctive" switchRole="yes">
                    <label>Input Validation</label>
                    <node refinement="conjunctive" switchRole="yes">
                        <label>Access Control</label>
                    </node>
                </node>
            </node>
        </node>
        <node refinement="conjunctive">
            <label>OT Communication Security</label>
            <node refinement="conjunctive">
                <label>MITM Attacks</label>
                <node refinement="conjunctive" switchRole="yes">
                    <label>Encryption</label>
                </node>
            </node>
            <node refinement="conjunctive">
                <label>Confidentiality Attacks</label>
                <node refinement="conjunctive" switchRole="yes">
                    <label>Encryption</label>
                </node>
            </node>
        </node>
        <node refinement="conjunctive">
            <label>DoS and DDoS</label>
            <node refinement="conjunctive" switchRole="yes">
                <label>Rate Limiting</label>
            </node>
        </node>
    </node>
</adtree>
```

ADTree Analysis Summary: OT Smart Home Security Analyzer

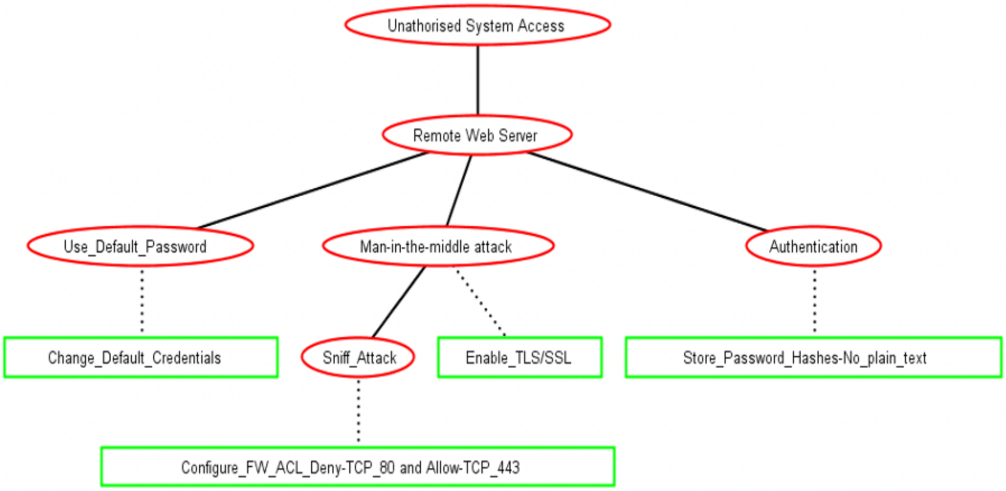
Three major category of security risks that may affect OT Smart Home Security Analyzer are identified as:

- Web Application Attacks
- OT Communication Security Attacks
- DoS and DDoS Attacks

The remediation measures that can be used for addressing this security risks are identified as baslining and hard coding of the application instance, Software composition Analysis, Encryption, Input Validation and Rate limiting. The below table list the specific security risks and the recommended remediation recommendations for it.

Security Risk	**Child Risks**	**Remediation/Counter Measure**
Web Application Attacks	Weak Guessable or Hardcoded Passwords	Baselining and Hardcoding
Web Application Attacks	Insecure Network Services	Baselining and Hardcoding
Web Application Attacks	Lack of Secure Update Mechanisms	Baselining and Hardcoding
Web Application Attacks	Use of Insecure or Outdated Components	SCA - Software Composition Analysis
Web Application Attacks	Insufficient Privacy Protection	SCA - Software Composition Analysis
Web Application Attacks	Insecure Default Settings	Baselining and Hardcoding
Web Application Attacks	Configuration Manipulation	Input Validation
Web Application Attacks	Directory Listing and Manipulation	Input Validation and Access Control
OT Communication Security Attacks	MITM - Man in the Middle Attacks between OT nodes and Controller	Encryption
OT Communication Security Attacks	Confidentiality Attacks	Encryption
DoS and DDoS Attacks	DoS and DDoS Attacks against controller	Rate Limiting

Closed Circuit Television (CCTV) System Attack-Defence Tree

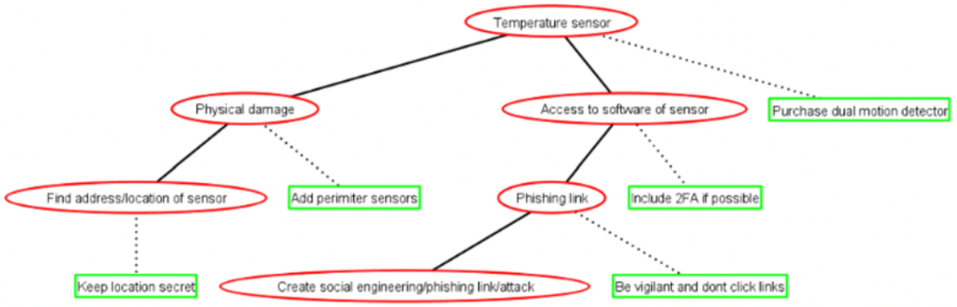

Unathorised System Access
Remote Web Server
Use_Default_Password
Man-in-the-middle attack
Authentication
Change_Default_Credentials
Sniff_Attack
Enable_TLS/SSL
Store_Password_Hashes-No_plain_text
Configure_FW_ACL_Deny-TCP_80 and Allow-TCP_443

Internet Protocol(IP) cameras can host a web application for the management of the devices. The web application hosted on the cameras has a similar attack surface as the one hosted on a web server. The risk ratings on the vulnerabilities associated with the web application hosted are as follows:

Risk Rating.

1. Default Password: High Risk (Ease of exploiting: High, Capability Required: Low.)
2. Man-in-the-Middle Attack: Medium Risk (Ease of exploitation: Medium , Capability Required: Medium)
3. Theft of credentials(authentication): High Risk (Ease of exploitation: High, Capability Required: Medium)

Temperature Sensor Attack-Defense Tree


Temperature sensor
Physical damage
Access to software of sensor
Purchase dual motion detector
Find address/location of sensor
Add perimiter sensors
Phishing link
Include 2FA if possible
Keep location secret
Create social engineering/phishing link/attack
Be vigilant and dont click links

The identified probable security flaws of Temperature Sensor Includes physical damage and access to software of sensor. Addition of perimeter sensors, implementing 2FA solutions and baselining are the identified countermeasures.

References:

1. Hong J B, Nhlabatsi A, Kim D S, Hussein A, Fetais N, Khan K M, (2019) ”Systematic identification of threats in the cloud: A survey,” Computer Networks;150:46-69

2. Shostack A, (2014)” Threat Modeling: Designing for Security: United States:” John Wiley & Sons Ltd;p. 590,

3. Amini A, Jamil N, Ahmad A, Z‘aba M R, (2015)Threat Modeling Approaches for Securing Cloud Computing. Journal of Applied Sciences.;15:953-67,

4. Alhebaishi N, Wang L, Singhal A, (2019)Threat Modeling for Cloud Infrastructures. ICST Transactions on Security and Safety.;5:156246

5. Cheng Y, Du Y, Xu J, Yuan C, Xue Z, (2012) Research on security evaluation of cloud computing based on attack graph. 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems;

6. Yahya F, Walters R J, Wills G B, (2015) Analysing threats in cloud storage. 2015 World Congress on Internet Security (WorldCat); 2015 19-21 Oct.

7. Gholami A., Laure E. Advanced cloud privacy threat modeling. arXiv preprint arXiv:160101500. 2016.

8. Amini A., Jamil N., Ahmad A. R., Z‘aba M. R. Threat Modeling Approaches for Securing Cloud Computing. Journal of Applied Sciences. 2015;15(7):953-67.