## Introduction:

Internet of Things (IOT) climate control solutions, from single home to multiple buildings, utilize similar communication and control designs, differing primarily in protection requirements and controlled element numbers. This system (Fig. 1) will provide personalized temperature control within individual areas like an apartment or shop using an internet-based application. Property owners monitor equipment for maintenance and control minimum and maximum temperature limits. Data communication between central application and remote individual devices utilizes the MQTT messaging protocol on a private network. MQTT provides a flexible messaging format, publish/subscribe model, security, and quality of service options (OASIS Open, 2019).

Diagram

Description automatically generated

*Figure 1 IOT Climate Control use cases*

The potential impact to property and persons compared with a small consumer system dictates the design process follow the systems engineering V-model (Fig. 2). The current design phase is focused on cyber security attack surfaces and countermeasures and the complete specification is available for review at <https://t3ssa1121.github.io/climatecontrol/>

Diagram

Description automatically generated

*Figure 2 Systems Engineering V-Model*

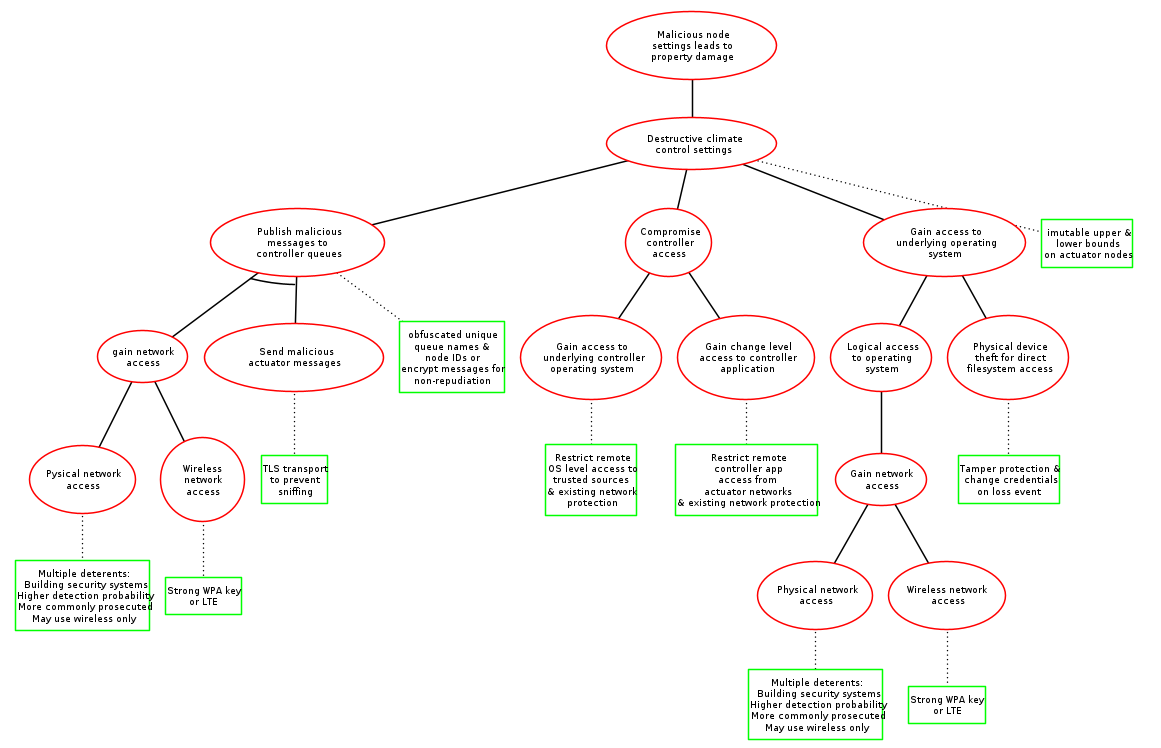
## Threat and Vulnerability Assessment:

Industry guidance like OWASP IOT top 10 (OWASP, 2019) ensures consideration of certain vulnerability classes during assessment (Fig. 6) but potential IOT security impacts must be considered within the implemented solution context (Musman, 2018) like the following example:

* Mirai botnet attacks (Johnson, 2016), often cited but not relevant, the climate controlling devices (MA-node) do not support password authentication and have no internet connectivity
* Weak application passwords are expected (Knieriem et al, 2018) but of limited impact,
  + No application stored information is deemed private (Canadian Privacy Commissioner, 2019).
  + Minimum-maximum temperature safety limits, no shut off capability
* Technical failures detected though fault monitoring
  + Like non-IOT climate control mechanical failure, once detected, individuals will seek repair before property damage occurs

## Attack Surface Analysis:

The MA-node device locations are typically not under direct control of the system owner, therefore the attack-defense tree (Kordy et al, 2014) (Fig. 3) considers physical and logical network-based MQTT attacks from a malicious internal user (Firdous, et al., 2017) (Fig.4). The MQTT broker’s underlying operating system (OS) is also a potential vector for routing malicious traffic to other units (Offensive Security, n.d.) or means to preventing temperature change message delivery by disrupting the MQTT service (National Vulnerability Database, n.d.).



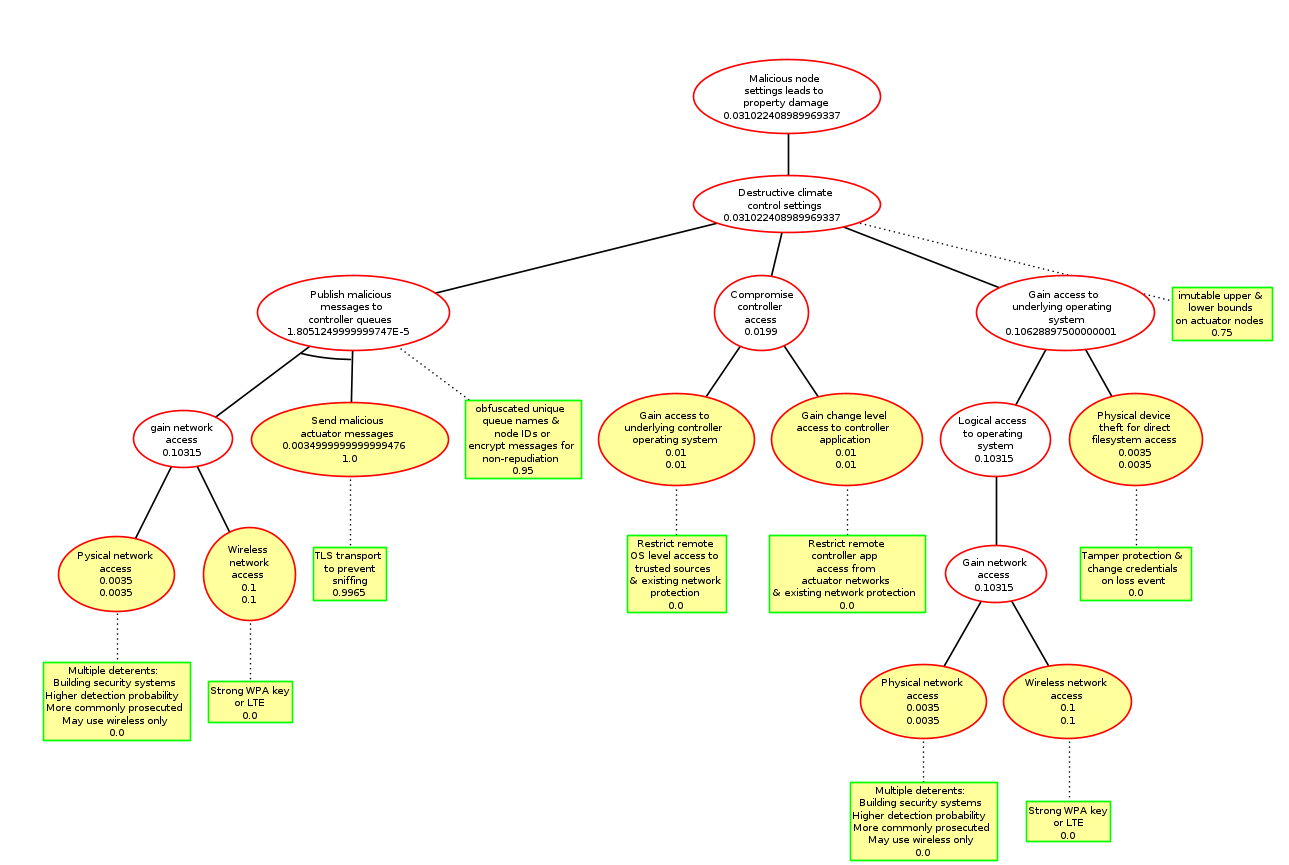
*Figure 3 MA-node Attack-Defense tree*

Diagram

Description automatically generated

Figure 4 Insider MQTT attacks (Firdous, et al., 2017)

Quantitative risk analysis methods can incorporate attack success likelihood into risk scoring (Musman, 2018). Publicly available cyber-crime statistics (Verizon, 2021) can inform attack-defense tree node values when using the probability domain (Bagnato, et al., 2012). Probabilities presented in tree format illustrate how implementing recommended controls reduces the likelihood of cyber-attacks causing property damage to three (Fig. 5) or four percent (Fig. 7).



*Figure 5 Attack-Defense Tree MA-node, probability domain values*

Most OWASP identified vulnerability classes (Fig. 5), (Fig. 7) are addressed through proper system and application hardening.

Diagram

Description automatically generated

*Figure 6 OWASP/Kaspersky IOT top 10 mapping, MA-node*

Widespread system impact only occurs if MQTT nodes or broker process malicious messages, the following measures will protect service integrity (Firdous, et al., 2017):

* Disable anonymous subscribing and publishing
* Encrypt device to controller traffic using TLS
* Encrypt message payloads for non-repudiation
* Limit MQTT broker service exposure to private network only

Internet-based attacks against the controller application have a 16% likelihood of success (Fig. 6), consequently, secure development practices and security validation testing (OWASP, 2021) before deployment are required.

Diagram

Description automatically generated

*Figure 7 Attack-Defense Tree controller application, probability domain values*

Diagram

Description automatically generated

Figure 8 OWASP/Kaspersky IOT top 10 mapping, controller application

The following controls will mitigate administrative account or OS compromises:

* Failsafe temperature boundaries implemented on the MA-Nodes cannot be changed through the application
* OS administration via SSH key authentication is not exposed to the internet or the MA-Node network
* HTTP and MQTT application components implemented as microservices, preventing OS access if exploited
* Cloud hosting physical attack vectors, offers network segmentation options and high reliability

**References:**

Bagnato, A., Kordy, B., Meland, P. H. & Schweitzer, P. (2012) Attribute Decoration of Attack-Defense Trees. *International Journal of Secure Software Engineering* 3(2): 1-35. DOI: <https://doi.org/10.4018/jsse.2012040101>

Canadian Privacy Commissioner. (2019) PIPEDA in brief. Available from: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/> [Accessed 27 November 2021].

Firdous, S., Baig, C., ValliC & Ibrahim, A. (2017) ‘Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol’, EEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Exeter, United Kingdom, 21-23 June 2017. IEEE. 748-755.

Johnson, A. (2016) Mirai: what you need to know about the botnet behind recent major DDoS attacks. Available from: <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=48e65595-ef3d-4653-bc6f-4c04d2667c36&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments> [Accessed 27 November 2021].

Knieriem, B., Zhang, X., Levine, P., Breitinger, E. & Baggili, I. (2018) ‘An Overview of the usage of Default Passwords’, 9th EAI International Conference on Digital Forensics & Cyber Crime. Prague, Czech Republic, 9-11 October 2017. Berlin:Springer. 195-203. Available from: <https://digitalcommons.newhaven.edu/electricalcomputerengineering-facpubs/69/> [Accessed November 24 2021].

Kordy, B., Mauw, S., Radomirovic, S. & Schweitzer, P. (2014) Attack-defense trees. *Journal of Logic and Computation* 24(1):55-87. DOI:<https://doi.org/10.1093/logcom/exs029>

Musman, S. (2018) A game theoretic approach to cyber security risk management. *The journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 15(2):127-146. DOI: 10.1177/1548512917699724

National Vulnerability Database. (n.d.) CVE. Available from: <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=mqtt+mosquitto> [Accessed 27 November 2021].

OASIS Open. (2019) MQTT Version 5.0. Available from: <https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html> [Accessed 27 November 2021].

Offensive Security. (n.d.) Pivoting. Available from: <https://www.offensive-security.com/metasploit-unleashed/pivoting/> [Accessed November 2021].

OWASP. (2019) OWASP Internet of Things Project. Available from: <https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10> [Accessed 27 November 2021].

OWASP. (2021) OWASP Web Security Testing Guide. Available from: <https://owasp.org/www-project-web-security-testing-guide/> [Accessed 27 November 2021].

Verizon. (2021) DBIR 2021 Data Breach Investigations Report. Available from: <https://www.verizon.com/business/resources/reports/dbir> [Accessed 12 June 2021].