Building a Trusted Smart Home Ecosystem with Zero Trust Principles

Contact

Main Supervisor: Dr Devki Nandan Jha, dev.jha@newcastle.ac.uk (Early Career Researcher)
Dr Varun Ojha, varun.ojha@newcastle.ac.uk

Research project

Smart homes are revolutionizing daily life by offering interconnected devices that enhance convenience, efficiency, and personalization. From energy-saving smart thermostats to voice assistants, they redefine how we interact with technology. However, their dynamic and heterogeneous nature exposes users to evolving cybersecurity threats like unauthorized access and data breaches. Traditional perimeter-based security models struggle to adapt to this dynamic nature of smart homes. This research aims to develop and explore a Zero Trust framework tailored specifically for smart homes, enabling continuous verification and adaptation of access privileges based on real-time user behaviour and device security postures.

The Research Challenges

There exists a complex interplay of various factors that present innumerable challenges in providing a Zero Trust framework for smart home. The main challenges are:

a) Device heterogeneity**:** Smart homes encompass a spectrum of IoT devices, each with distinct security profiles. The diverse range of devices poses challenges in standardizing security protocols and interoperability.

b) *Dynamic environment*: The dynamic nature of smart home environments poses a significant challenge for traditional security models that rely on static configurations and predefined rules. As new devices are added, removed, or updated, the overall security posture of the smart home network constantly changes.

c) *Periodic Authentication Limitations*: Relying solely on periodic authentication methods, such as passwords or biometrics, fails to provide adequate continuous security for smart home environments. Periodic authentication methods only verify user identities at specific points in time, leaving gaps between authentication events where unauthorized access can occur. For instance, a device compromised after authentication may continue to have access until the next authentication cycle. Periodic authentication lacks context awareness, failing to consider factors such as user location or device usage patterns that could indicate anomalies or potential security threats.

d) *Users' privacy*: Smart homes collect a vast amount of data about users' daily lives, including their habits, preferences, and even their physical movements. This data can be used to create detailed profiles of users, which can then be used for targeted advertising, surveillance, or even discrimination. Balancing security with user privacy is a significant challenge, as users often express concerns about data privacy and potential misuse.

The proposed Zero Trust framework provides a comprehensive solution to address the diverse security challenges posed by smart homes. It prioritizes user privacy by minimizing data collection and exposure, implementing granular access control mechanisms, and granting access only to the data and resources necessary for each user or device. To navigate the heterogeneous nature of smart devices, the framework employs device-specific risk assessment and access control policies, continuously evaluating device security postures and dynamically adjusting access privileges based on vulnerability assessments and firmware updates. To handle the dynamic nature of smart homes, the Zero Trust framework employs real-time analytics and anomaly detection techniques to monitor user behaviour, device interactions, and network activity, enabling proactive adaptation of access controls and timely responses to emerging threats. Overcoming the limitations of periodic authentication, the framework incorporates continuous authentication techniques that leverage contextual information, device health checks, and behavioural analysis, ensuring that only authorized entities gain access to sensitive information and resources. To enhance the overall security posture, the framework integrates real-time threat intelligence into its decision-making processes, proactively identifying and responding to emerging threats based on the latest intelligence feeds.

Methodology

The PhD will be divided into 3 work packages (WP):

WP1 - *Continuous Device Monitoring*: This WP will establish a comprehensive device monitoring system to continuously assess device security postures and identify potential threats. Monitoring information will be gathered by intelligent agents at user, kernel, and network levels to capture device behaviour, system logs, and network traffic anomalies [1].

WP2 - *Integration of Trusted Computing Technologies*: This WP will leverage hardware-based security technologies, including TPM and TrustZone, to establish a foundation for device trustworthiness [2]. The main activity involves integrating TPM for secure storage and management of cryptographic keys, ensuring the confidentiality and integrity of critical operations using TrustZone and exploring the hardware-based attestation mechanism.

WP3 - *Proactive Threat Detection and Adaptive Response*: This WP integrates the cutting-edge cryptographic techniques and artificial intelligence (AI) algorithms to develop the Zero Trust framework. It utilises the AI algorithms such as Long Short-Term Memory (LSTM) and Large Language Models (LLMs) to identify anomalous device behaviour, enabling rapid detection and response. It also employs Reinforcement Learning (RL) to dynamically adapt security policies [3].

Project Timeline

Year 1 (Month 1-12): WP1 and associated training to obtain core skills in embedded computing, security technology, data analytics and machine learning.

Year 2 (Month 13-24): Implementation of WP2 and Initial thesis chapters for WP1.

Year 3 (Month 25-36): Design and implementation of the analytical tools for WP2. Initial thesis chapters for WP2.

Year 4 (Month 37-42): Case studies for WP3 and final thesis chapters.

Supervision Environment

Extensive training will be provided on IoT and embedded computing. Training on hardware-based security technology including TPM, SGX and TrustZone and data analytics and AI techniques (e.g. reinforcement learning and large language models) will also be provided.

Applicant skills/background

This applicant should have a solid background in computer science, with strong programming skills in Python. Knowledge of C is highly advantageous, as it can be instrumental in working with embedded systems and low-level security mechanisms often found in smart home devices. A keen interest in smart home technologies and cybersecurity is essential to align with the focus of this research. Additionally, candidates should demonstrate analytical thinking, problem-solving skills, and a willingness to engage with interdisciplinary concepts. Strong written and verbal communication skills are also important for articulating research findings effectively.

References

1. **D. N. Jha**, G. Lenton, et al., "Holistic Runtime Performance and Security-aware Monitoring in Public Cloud Environment." In 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing, pp. 1052-1059. IEEE, 2022.
2. **D.N. Jha**, G. Lenton, et al., "Trusted Platform Module-Based Privacy in the Public Cloud: Challenges and Future Perspective." IT Professional 24, no. 3 (2022): 81-87.
3. B. Qian, J. Su, **D. N. Jha**, et al. "Orchestrating the development lifecycle of machine learning-based IoT applications: A taxonomy and survey." ACM Computing Surveys, 53, no. 4 (2020): 1-47.