IoT Network Security in Smart Homes

Untersuchung der verschieden Schutzmechanismen in Smart Home Netzwerken

Aiman Al-Hazmi & Zohreh Asadi

Rückblick

- Def IoT
- Schwerpunkt
- Alte Quellen (7 Quellen)
- Alte Grundstruktur

Kapitalstrukturänderung

Grundlagen von Smart Home Netzwerken	Verschlüsselung, Authentifizierung und Zugriffskontrolle in Smart Home-Netzwerken	Mutual Authentication und TLS in Smart Home Netzwerken	Best Practices und Implementierungsbeispiele	Zusammenfassung und Ausblick
Architektur von Smart Home-Netzwerken	Verschlüsselungstechnologien	Mutual Authentication und TLS in Smart Home Netzwerken	Best Practices für die IoT-Netzwerksicherheit in Smart Homes	Zusammenfassung der Ergebnisse
Bedrohungen und Risiken für Smart Home-Netzwerke	Authentifizierung	TLS (Transport Layer Security)		Ausblick auf zukünftige Entwicklungen und Forschungsbedarf
Wichtige Schutzmechanismen zur Sicherung von Smart Home-Netzwerken	Zugriffskontrolle und Berechtigungen			
Kommunikationsprotokolle in Smart Home Netzwerken				

Quellen und Kapitalstruktur

IoT-Netzwerksicherheit in Smart Homes	Verschlüsselung in Smart Home-Netzwerken	Authentifizierung und Zugriffskontrolle in Smart Home-Netzwerken	Best Practices und Implementierungsbeispiele
1, 3, 6, 8, 11	1, 2, 5	1, 9	1, 4, 5, 7, 10

Grund für die Auswahl der besten Quellen

- Quelle 1, "Cybersecurity in Smart Homes: Architectures, Solutions and Technologies" bietet einen umfassenden Überblick über IoT-Sicherheit in Smart Homes.
- Das Buch liefert detaillierte Informationen über Architekturen, Lösungen und Technologien zur Sicherung von Smart Home-Netzwerken.
- Quelle 2, "A survey of machine and deep learning methods for privacy protection in the internet of things", gibt einen Überblick über maschinelles Lernen und Deep Learning-Methoden für den Datenschutz im IoT.
- Obwohl der Fokus auf Datenschutz liegt, bietet die Studie Einblicke in verschiedene Schutzmechanismen für Smart Home-Netzwerke.
- Beide Quellen ergänzen sich und bieten einen ganzheitlichen Ansatz zur Untersuchung der Sicherheitsaspekte in Smart Home-Netzwerken.

Quellenzusammenfassung: [1] Chapter 2

- Seven Key Concept
  - Authentication
  - Authorization
  - Confidentiality Data/message
  - Accountability
  - Availability
  - Non-repudiation
- Architektur von Smart Home Netzwerken
- Definition eines Authentifizierungsprotokolls für das Internet der Dinge (IoT)

- Mutual Authentication
  - Mutual Authentication (Gegenseitige Authentifizierung)
  - Mutual Authentication mit einem shared key
  - Mutual Authentication mit Public-Key-Kryptographie
- X.509-Zertifikat

- TLS (Transport Layer Security)

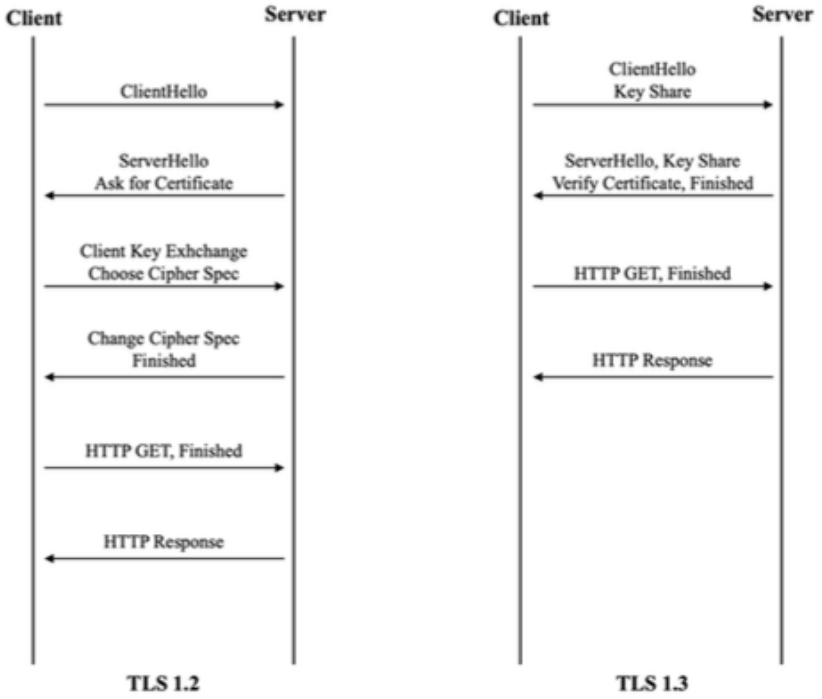

Figure 2.5. *TLS 1.2 and 1.3 comparison*

Quellenzusammenfassung: [1] Chapter 4

- IoT smart home automation is a rapidly growing global trend with numerous concerns and challenges.
- Managing and securing IoT smart home devices requires careful attention to monitoring, energy management, and data protection.
- Network security is a major concern as the deployment of smart home IoT infrastructure continues to increase.
- Lightweight security apps and technologies can effectively address the security challenges in IoT-based smart homes.
- Implementing access monitoring, control systems, and robust communication procedures significantly enhance smart home security.
- Confidentiality and security of IoT-related information processing and threats are continuously analyzed and regulated.
- Standards and initiatives, such as the Open Connectivity Foundation (OCF), Zigbee Alliance, and Bluetooth Special Interest Group (SIG), promote interoperability and enhance security in smart home systems.
- IoT applications encompass various areas, including remote monitoring, energy consumption management, and security systems, requiring the integration of essential components and technologies for functionality and security.

Quellenzusammenfassung: [2]

- The Internet of Things (IoT) connects smart devices, enabling them to exchange information with minimal human intervention.
- The rapid advancement of IoT is expected to result in 27 billion connected devices by 2025.
- The sheer volume of data generated by IoT raises concerns about user privacy.
- Privacy regulations, such as the EU General Data Protection Regulation (GDPR), aim to empower users with control over their personal data.

- This paper presents a comprehensive survey of machine learning (ML) techniques for privacy protection in IoT environments.
- The survey covers the identification and classification of privacy threats, reviews ML-based solutions, and proposes future directions for privacy preservation in IoT systems.
- Previous research has primarily focused on cybersecurity threats in IoT, with limited attention given to privacy-focused surveys and solutions.
- Privacy-preserving ML techniques, such as homomorphic encryption and secure multi-party computation (SMC), are promising approaches for protecting privacy in IoT.

Ergänzende Quellen

1. Internet of things (iot) of smart home: Privacy and security
2. A security authorization scheme for smart home internet of things devices
3. Designing efficient smart home management with iot smart lighting
4. Iot privacy and security challenges for smart home environments

Zwischenstand

- Eine geeignete Umsetzung finden und erläutern, welche Verschlüsselungs- und Autorisierungsalgorithmen verwendet wurden.
- Die relevanten Kapitel mit aussagekräftigen Stichpunkten ausfüllen.
- Eine gründliche Durchsicht der bisherigen Quellen vornehmen, Notizen machen und eine Zusammenfassung erstellen.

Danke für die Aufmerksamkeit!