IoT Network Security in Smart Homes

Untersuchung der verschieden Schutzmechanismen in Smart Home Netzwerken

Aiman Al-Hazmi & Zohreh Asadi

Übersicht

- Grundlagen von Smart Home Netzwerken
- Verschlüsselung
- Authentifizierung
- Zugriffskontrolle

Übersicht

- Grundlagen von Smart Home Netzwerken
- Verschlüsselung
- Authentifizierung
- Zugriffskontrolle

Grundlagen von Smart Home Netzwerken

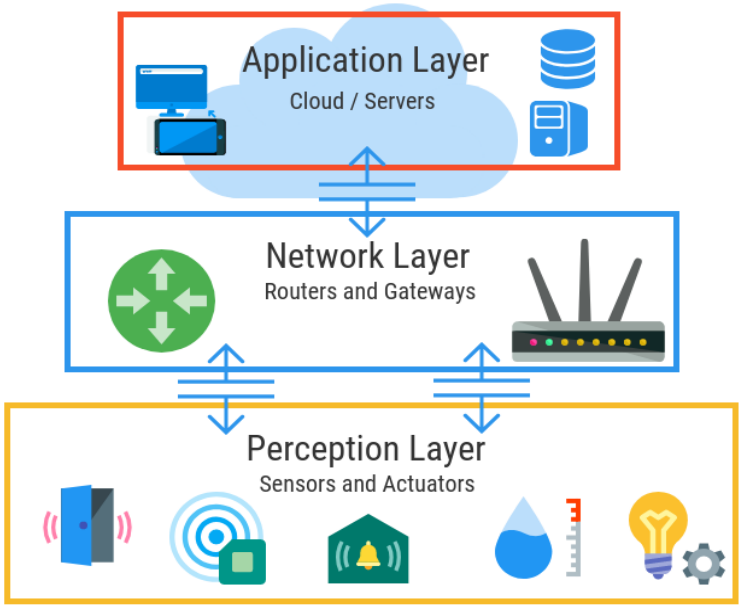
- IoT und Smart Homes Architektur
- Kommunikationsprotokolle
- Bedrohngen und Risiken
- Wichtige Schutzmechanismen

Grundlagen von Smart Home Netzwerken

- IoT und Smart Homes Architektur
- Kommunikationsprotokolle
- Bedrohngen und Risiken
- Wichtige Schutzmechanismen

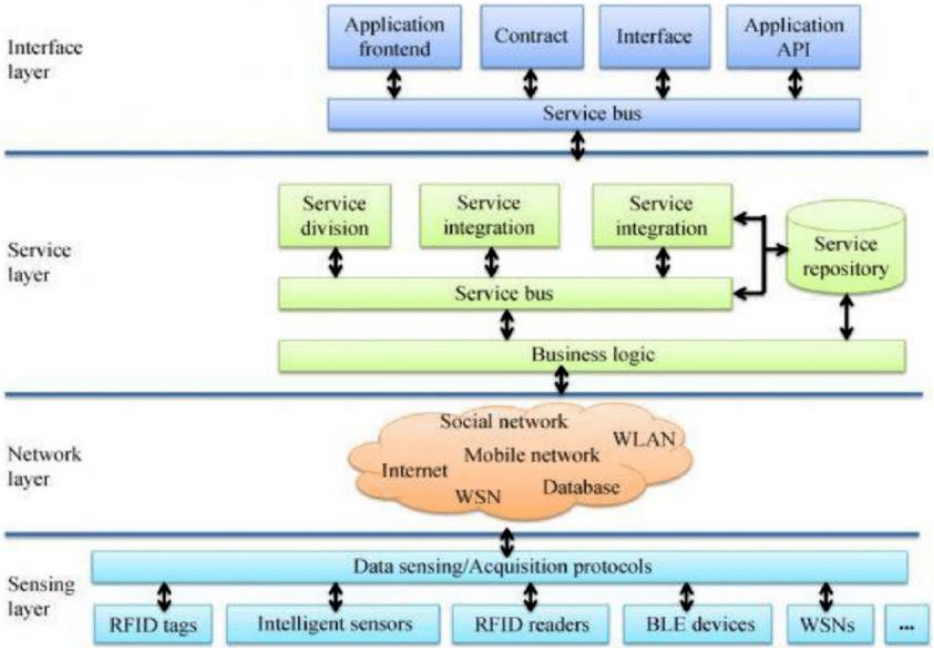
Architektur von Smart Home Netzwerken

- IoT Architektur
  i. Basic Layerd Architecture



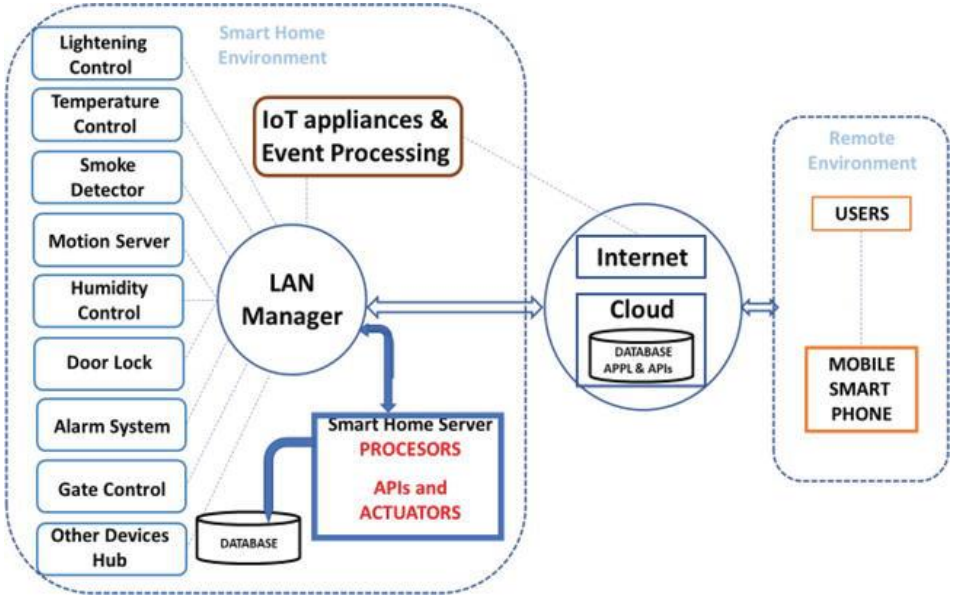
Architektur von Smart Home Netzwerken

- IoT Architektur
  i. Basic Layerd Architecture
  ii. Service Oriented Architecture



Architektur von Smart Home Netzwerken

- ✓ IoT Architektur
- Smart Homes Architektur



Architektur von Smart Home Netzwerken

- ✓ IoT Architektur
- ✓ Smart Homes Architektur

Grundlagen von Smart Home Netzwerken

- ✓ IoT und Smart Homes Architektur
- Kommunikationsprotokolle
- Bedrohngen und Risiken
- Wichtige Schutzmechanismen

Grundlagen von Smart Home Netzwerken

- ✓ IoT und Smart Homes Architektur

- ○ Kommunikationsprotokolle
  - i. Auswahl von Protokollen

    Reichweite, Energieverbrauch, Sicherheit, Kompatibilität..usw.

Grundlagen von Smart Home Netzwerken

- ✓ IoT und Smart Homes Architektur

- ○ Kommunikationsprotokolle
  - i. Auswahl von Protokollen

    Reichweite, Energieverbrauch, Sicherheit, Kompatibilität..usw.

  - ii. Bekannte Protokolle

    Je nach Schicht: Wi-Fi, Bluetooth, Zigbee, Z-Wave, TLS, MQTT, CoAP, usw.

Grundlagen von Smart Home Netzwerken

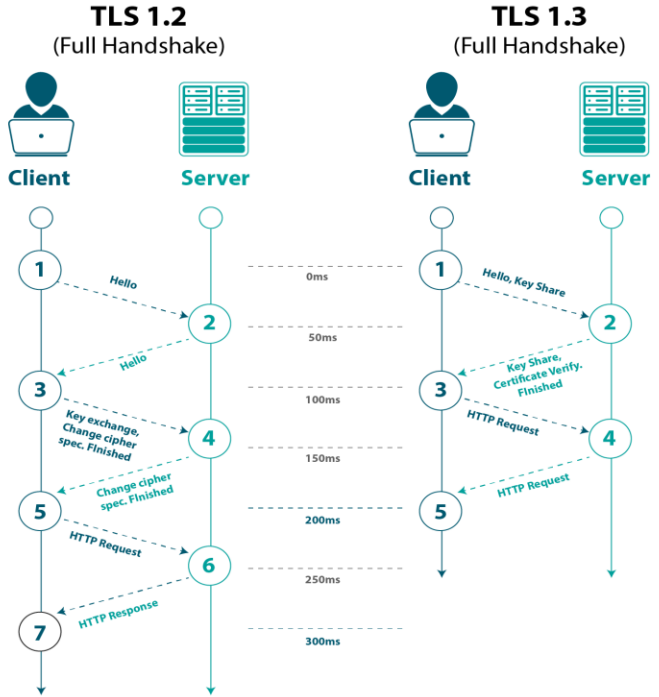
TLS (Transport Layer Security)

I. Sichere und Zuverlässige Kommunikation

II. zwischen der Anwendungsschicht (z. B. HTTP) und der Transportschicht (z. B. TCP)

III. TLS bietet Serverauthentifizierung(Handshake)

IV. Unterstützt eine Vielzahl kryptografischer Algorithmen.



Grundlagen von Smart Home Netzwerken

- ✓ IoT und Smart Homes Architektur

- Kommunikationsprotokolle
  - i. Auswahl von Protokollen
    - Reichweite, Energieverbrauch, Sicherheit, Kompatibilität..usw.
  - ii. Bekannte Protokolle
    - Je nach Schicht: Wi-Fi, Bluetooth, Zigbee, Z-Wave, TLS, MQTT, CoAP, usw.

Grundlagen von Smart Home Netzwerken

Constrained Application Protocol (CoAP)

i. Anwendungsprotokoll auf der Anwendungsschicht

ii. Speziell für eingeschränkte Geräte.

iii. Datenaustausch unter Verwendung des REST-Modells (GET, PUST, DELETE, PUT)

i. Keine Sicherheit für die Übertragung der Daten

ii. Deswegen verwendet DTLS (Datagram Transport Layer Security), welches auf UDP basiert

Grundlagen von Smart Home Netzwerken

- ✓ IoT und Smart Homes Architektur
- ✓ Kommunikationsprotokolle
- ○ Bedrohngen und Risiken
- ○ Wichtige Schutzmechanismen

Bedrohungen und Risiken

- Risikoanalyse ist die große Herausforderung für die Entwicklung von Smart-Home-Systemen.

- Die gefährlichsten Risiken:
    1. Änderungen an den Softwarekomponenten
    2. Unbefugte Änderungen an Systemfunktionen auf mobilen Geräten
    3. Zugriff auf Ressourcen
    4. Manipulationen an physischen Sensoren/internen Gateways

Bedrohungen und Risiken

Intentional-Threads:

- Identitätsbetrug
- DoS
- Datenmanipulation

Konsequenzen:

- Unbefugte Änderungen an Richtlinien
- Identitätsdiebstahl
- Die Ausnutzung von SH-Diensten

Unintentional-Threads:

- Informationen von unbekannte Quellen.
- Zufällige Änderung von Daten/Richtlinien
- Schwache Installation
- Falsche Sicherheitsrichtlinien in Geräten

Konsequenzen:

- Dataverlust
- Verletzung der Sicherheitsrichtlinien
- Systemausfall

Bedrohungen und Risiken

Mulfunction-Threads:

- Häufigsten beispiel in störungsthreads
- Die dritte Party geht (z.B sensor) kaput
- Ausfälle in internet
- Hardware oder softwarefehler

Konzequenzen:

- Fehlfunction
- Functionsverlust

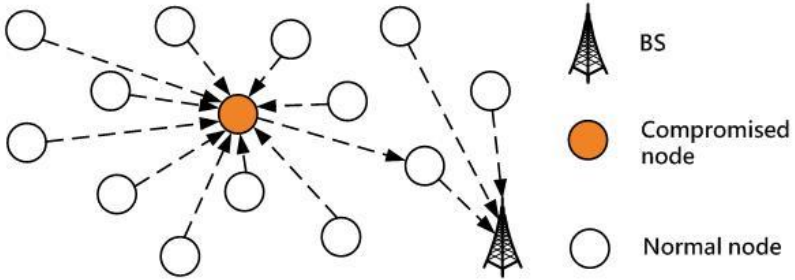
Cyber-attacks

Sinkhole: Umlitung der Daten während der Übertragung

- Reduzirung der Datenverkehr
- Tauschung der Absender
- Generierung der Datenvekehr

Selektiver weiterleitungsangeriff: Einnahme von ein oder mehreren Knoten im Netzwerk durch Hacker

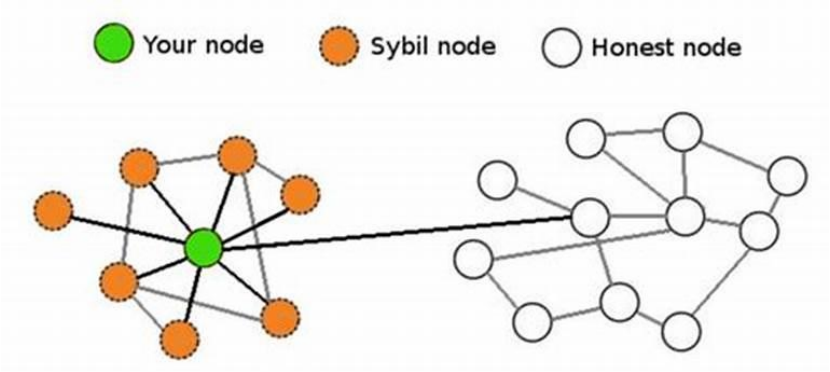
- Paketverlust
- Schwer oder nicht erkennbar
- Übertragung unvollständige Infos (gefährlicher als No-Info)



Cyber-attacks

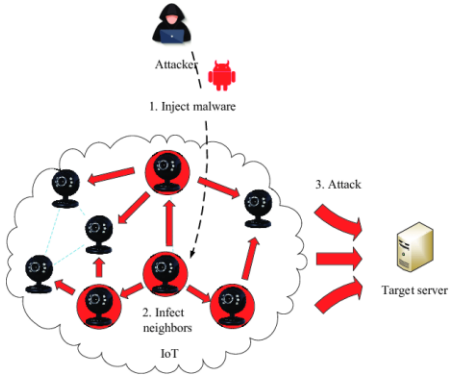
Sybil: Manipulation von Knoten und Erstellung mehrerer Identitäten

- Redudanz/falsche infos
- Erhöhung des Spam-Verkehrs
  - Malware und Phishing



DoS: Mehrere attacks, 1 system

- Überschwemmung des Netzwerks mit nutzlosem Datenverkehr
- Diebstahl vertraulicher Infos
- Herunterfahren des gesamten Netzwerks.



Grundlagen von Smart Home Netzwerken

- ✓ IoT und Smart Homes Architektur
- ✓ Kommunikationsprotokolle
- ✓ Bedrohngen und Risiken
- ○ Wichtige Schutzmechanismen

Schutzmechanismen

- Seven key Konzept

  Integrität, Authentifizierung, Autorisierung, Vertraulichkeit, Accountability, Verfügbarkeit Non-repudiation

- IoT-Sicherheitsarchitekturen
  - IoT Cloud on CoAP
  - SH-BlockCC
  - FIWARE

security architectures	AuthN	AuthZ	Cf'ty	D In'ty	Acb'ty	Av'ty	N-R'ion
IoT Cloud on CoAP	YES		YES	YES			
SH-BlockCC	YES		YES	YES		YES	YES
FIWARE	YES	YES	YES	YES	YES		

Matrix of security architectures and security goals (Authentication (AuthN), Authorization (AuthZ), Confidentiality (Cf'ty), Data Integrity (D In'ty), Accountability (Acb'ty), Availability (Av'ty), Non-Repudiation (N-R'ion))

Schutzmechanismen

- Weitere Schutzmechanismen
  - Intrusion detection systems (IDS)
  - Starke Passwörter
  - Aktualisierte Firmware und Sicherheitspatches

Grundlagen von Smart Home Netzwerken

- ✓ Architektur
- ✓ Kommunikationsprotokolle
- ✓ Bedrohngen und Risiken
- ✓ Wichtige Schutzmechanismen

Übersicht

- ✓ Grundlagen von Smart Home Netzwerken
- ➢ Verschlüsselung
- ➢ Authentifizierung
- ➢ Zugriffskontrolle

Verschlüsselungstechnologie

Ziel:

- Vertraulichkeit
- Authentifizierung
- Integrität
- Bestreitbarkeit
- Zugangskontrolle

Klassen

Symmetrik-Verschlüsselung (AES, BLOWFISH):

Public key

- Encryption und Decryption

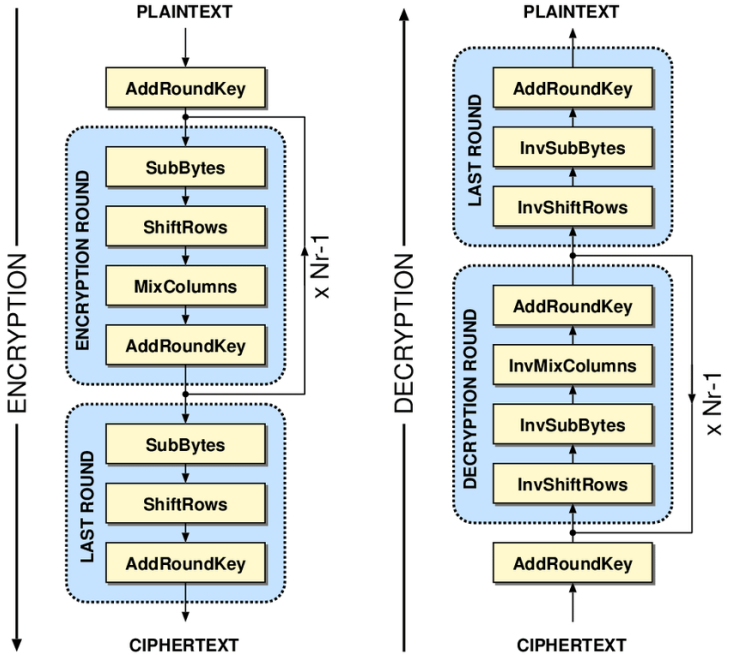
Asymmetrik-Verschlüsselung (RSA):

- Public key
  - Encryption
- Private key
  - Decryption

Verschlüsselungstechnologie

Advanced Encryption Standard (AES)

- Symmetric Verschlüsselung
- Datenblöcken
- Substitutions-Permutations-Netzwerk (SPN)
- Ersetzungs- und Permutationsoperationen
  - Vertraulichkeit
  - Datenintegrität



Verschlüsselungstechnologie

Vorteile

- Schnelle Ver- und Entschlüsselung (HW,SW)
- Flexible Schlüsselgrößen (128, 192, 256 Bit)
- Bessere Sicherheit als DES und Triple-DES
- Kein Wurmlöcher

Nachteile

- Mehr Rechenleistung für große Datenblöcke
- Nicht effizient für große Pakete

Verschlüsselungstechnologie

BLOWFISH

- Symmetric verschlüsselung
- Für Software entwickelt
- Schlüsselgröße: 32-448 Bit
- Schnelle Ver- und Entschlüsselung
- Verwendet Substitutions-Boxen und XOR-Operationen

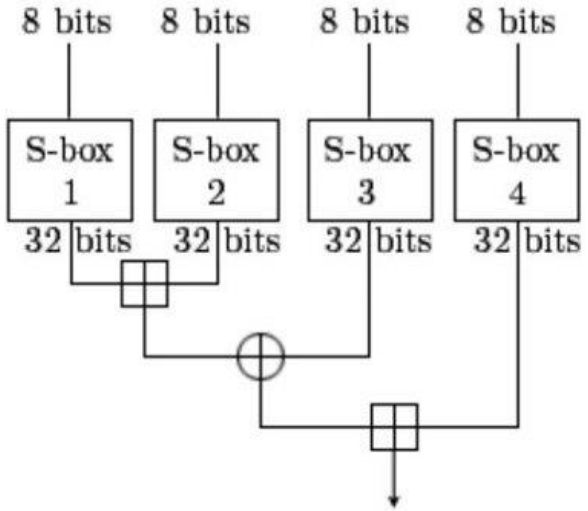


Diagram of Blowfish's F function

Verschlüsselungstechnologie

Vorteile

- Gute Leistung, keine Wurmlöcher
- Effiziente Ver-/Entschlüsselung
- Variable Schlüsselgröße: 32-448 Bit
- Weniger Kryptoanalyseversuche

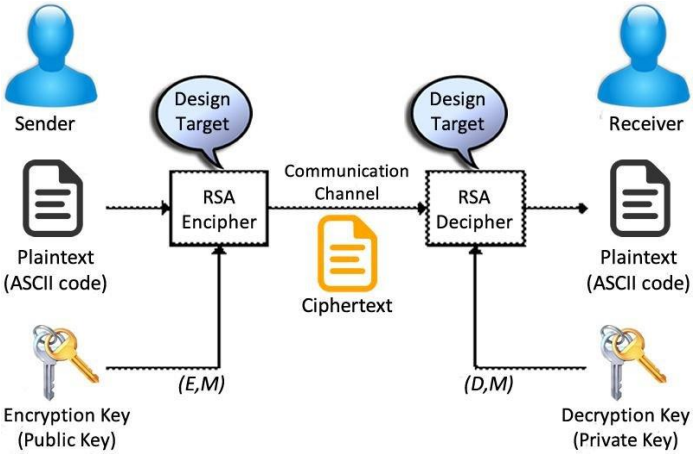
Nachteile

- Rechenintensiver als AES
- Zeit- und Stromverbrauch
- Nicht Hardware-optimiert
- Potenziell weniger analysiert

Verschlüsselungstechnologie

RSA

- Asymmetrischer Algorithmus
- Sicherheit durch Faktorisierungsschwierigkeit
- Encryption (Verschlüsselung): C = M^e mod n
- Decryption (Entschlüsselung): M = C^d mod n
  - C ciphertext, M Plaintext
  - Primzahlen p und q
  - Geheimhaltung von Primzahlen
  - Produkt n = p*q
  - Öffentlicher Exponent e
  - Private Exponent d



Verschlüsselungstechnologie

Vorteile

- Sichere Übertragung
- Digitale Signaturen
- Sicherer Algorithmus

Nachteile

- Rechenintensiver als symmetric-encryption
- Timing-Angriffe
- Spezielle HW- und SW-Implementierungen

Übersicht

- ✓ Grundlagen von Smart Home Netzwerken
- ✓ Verschlüsselung
- ➢ Authentifizierung
- ➢ Zugriffskontrolle
- ➢ Best Practices

Authentifizierung

Authentifizierung

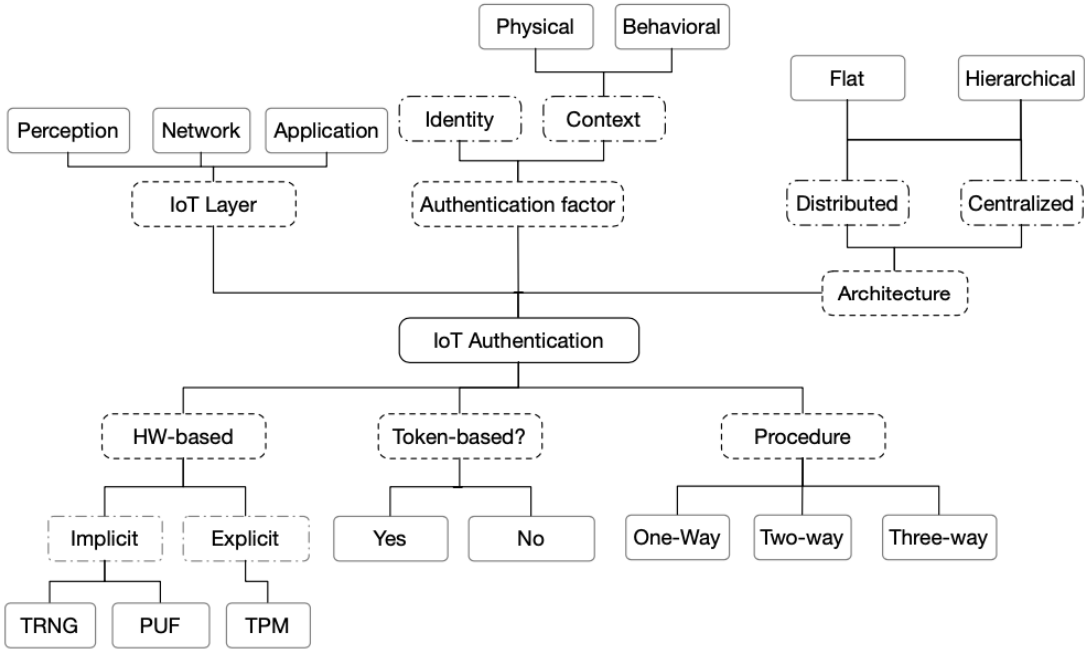
- Taxonomie der IoT-Authentifizierungsschemas
- Mutual TLS(MTLS)
- Lightweight CoAP-based Authentication
- CoAP Payload Based Lightweight Authentication

Authentifizierung

- **Taxonomie der IoT-Authentifizierungsschemas**
- **Mutual TLS(MTLS)**
- **Lightweight CoAP-based Authentication**
- **CoAP Payload Based Lightweight Authentication**

Authentifizierung

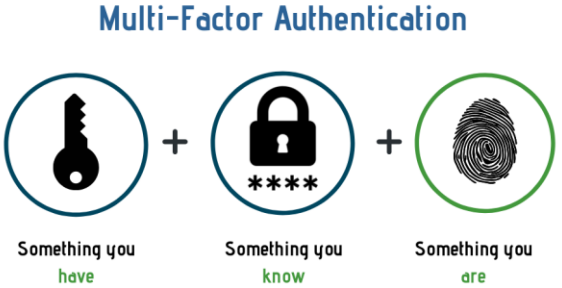
- **Taxonomie der IoT-Authentifizierungsschemas**

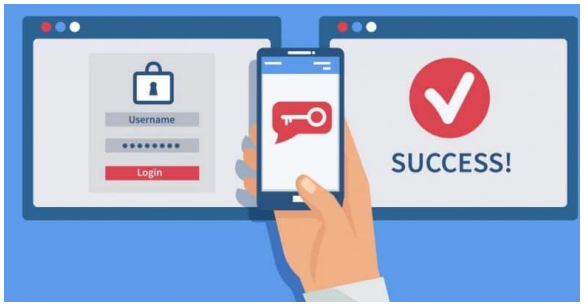


Authentifizierung

- **Taxonomie der IoT-Authentifizierungsschemas**
  - Authentifizierungsverfahren

    Authentifizierungsfaktor



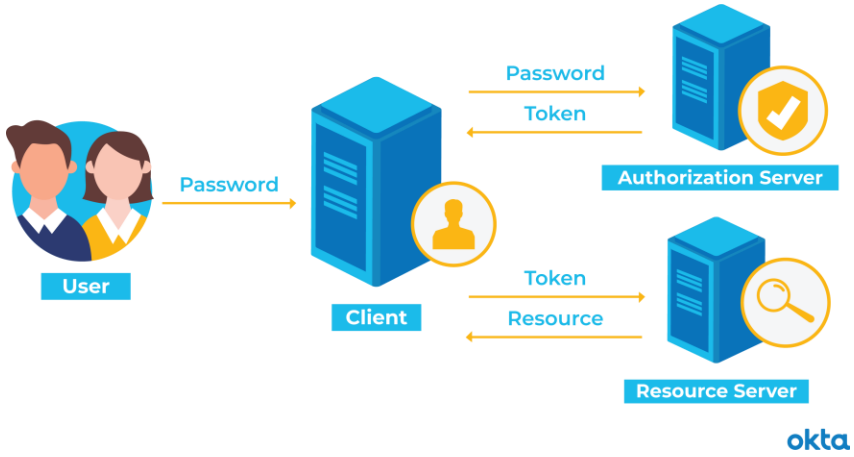


Authentifizierung

- **Taxonomie der IoT-Authentifizierungsschemas**
  - Authentifizierungsverfahren

    Authentifizierungsfaktor

    Token-Based



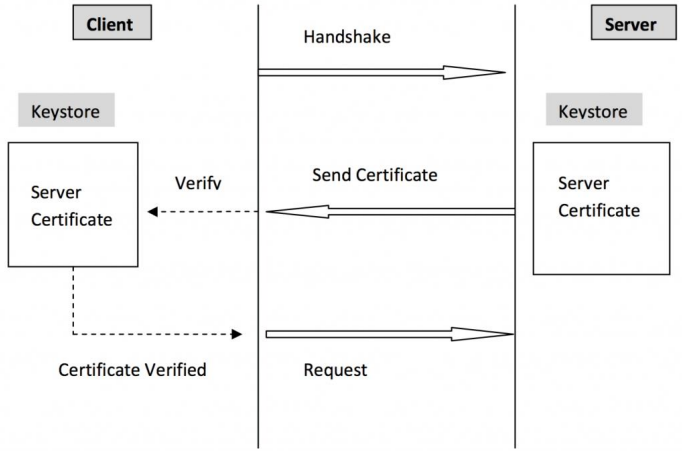
Authentifizierung

- **Taxonomie der IoT-Authentifizierungsschemas**
  - Authentifizierungsverfahren

    Authentifizierungsfaktor

    Token-Based

    One-Way authentication(Handshake)



Einweg (One-Way authentication)

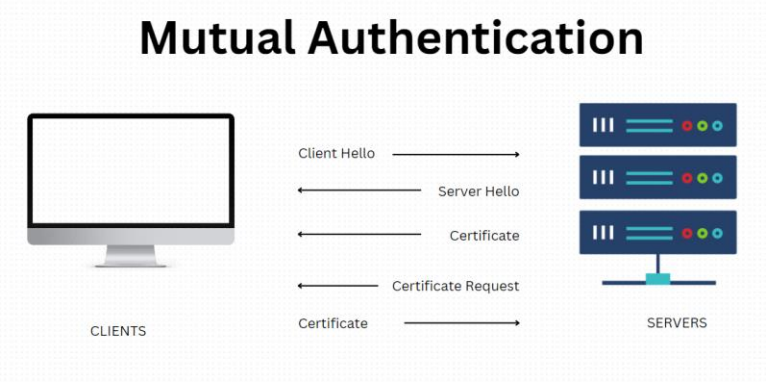
Authentifizierung

- **Taxonomie der IoT-Authentifizierungsschemas**
  - Authentifizierungsverfahren
    - Authentifizierungsfaktor
    - Token-Based
    - One-Way authentication(Handshake)
    - Two-Way authentication (Mutual)

timestamp

Public key

Shared key

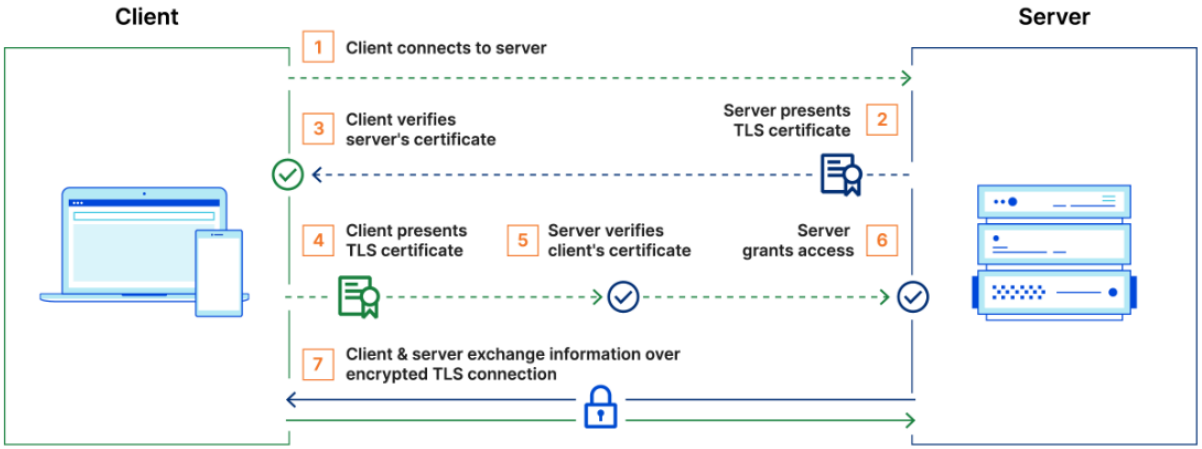


Authentifizierung

- ✓ **Taxonomie der IoT-Authentifizierungsschemas**
- ○ **Mutual TLS(MTLS)**
- ○ **Lightweight CoAP-based Authentication**
- ○ **CoAP Payload Based Lightweight Authentication**

Authentifizierung

- **Mutual TLS(MTLS)**



Authentifizierung

- ✓ Taxonomie der IoT-Authentifizierungsschemas
- ✓ Mutual TLS(MTLS)
- ○ **Lightweight CoAP-based Authentication**
- ○ **CoAP Payload Based Lightweight Authentication**

Authentifizierung

- **Lightweight CoAP-based Authentication**
  - Sichere und zuverlässige Alternative zu DTSL
  - Vier handshake Nachrichten
  - AES zur Verschlüsselung

Authentifizierung

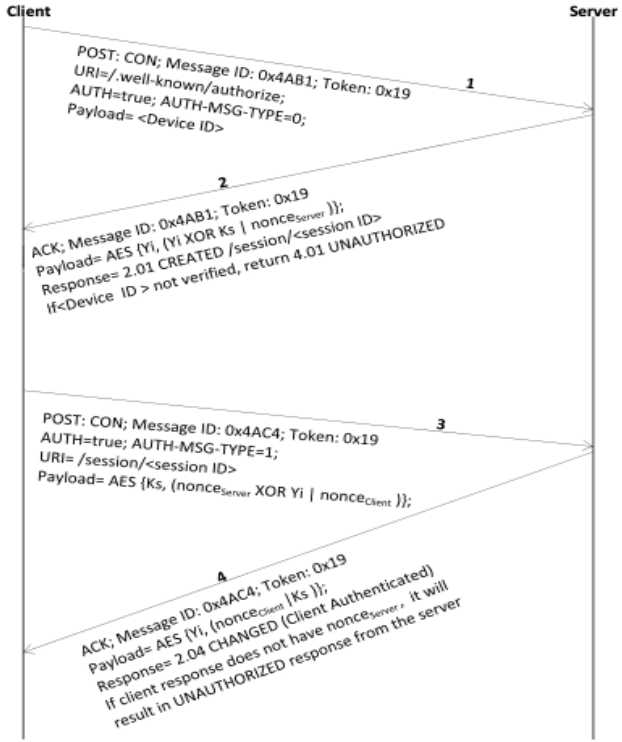
- **Lightweight CoAP-based Authentication**

  - Session initiation:
    M0p = Gerät-ID

  - Server challenge:
    M1p = AES{Yi, ((Yi XOR Ks) | nonceServer)}

  - Client response & challenge:
    E(M1p) &
    M2p = AES{Ks, (nonceServer XOR Yi | nonceClient)}

  - Server response:
    M3p = AES{Yi, (nonceClient | Ks)}



Jetzt erfolgt die Kommunikation unter Verwendung Ks zur Verschlüsselung

Authentifizierung

- ✓ Taxonomie der IoT-Authentifizierungsschemas
- ✓ Mutual TLS(MTLS)
- ✓ Lightweight CoAP-based Authentication
- ○ **CoAP Payload Based Lightweight Authentication**

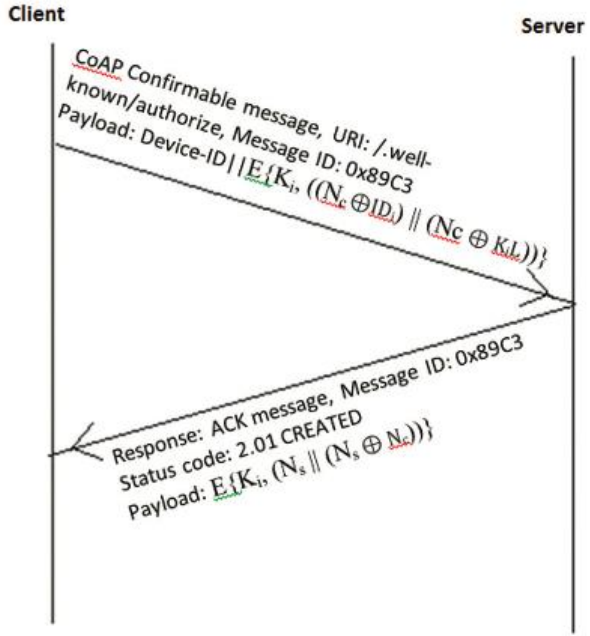
Authentifizierung

- **CoAP Payload Based Lightweight Authentication**

  - Nur zwei Handshke-Nachrichten
  - Gemeinsamer Geheimschlüssel (Ki)

1. Request von Client:
M1p = IDi || C1
Wobei C1 = E (Ki, ((Nc XOR IDi) || (Nc XOR KiL))

2. Response von Server:
M2p = E (Ki, (Ns || (Ns XOR Nc))



Authentifizierung

- ✓ Taxonomie der IoT-Authentifizierungsschemas
- ✓ Mutual TLS(MTLS)
- ✓ Lightweight CoAP-based Authentication
- ✓ CoAP Payload Based Lightweight Authentication

Übersicht

- ✓ Grundlagen von Smart Home Netzwerken
- ✓ Verschlüsselung
- ✓ Authentifizierung
- ➢ Zugriffskontrolle

Zugriffskontrolle

- Authentifizierung, Autorisierung und Verantwortlichkeit
- Zugriffskontrollmechanismen:
  - RBAC, ABAC, HyBACAC
- Überprüfung und Verifizierung der Zugriffskontrollrichtlinien
  - Tools: ACLs, Router, Verschlüsselung, Prüfprotokolle, IDS, Antivirensoftware, Firewalls, Smartcards

Zugriffskontrolle

ABAC

- Rollenzentrierung + Autorisierung
- Echtzeit-Umgebungszustände
- Flexibilität, Granularität und Kontextbezogene Steuerung
- Erfordert Eigenschafts- und Richtlinienverwaltung
- Für dynamische Umgebungen geeignet
- Einfacher zu implementieren
- Rollen als Benutzerattribute
- Flexibilität durch Attribute

RBAC

- Verwaltungs- und Sicherheitsvorteile
- Basierend auf vordefinierten Rollen und Berechtigungen
- Vereinfachte Administration
- Einfacher in der Implementierung
- Rollen als Benutzerattribute
- Flexibilität durch Attribute

Zugriffskontrolle

HyBACAC: ABAB + RBAC

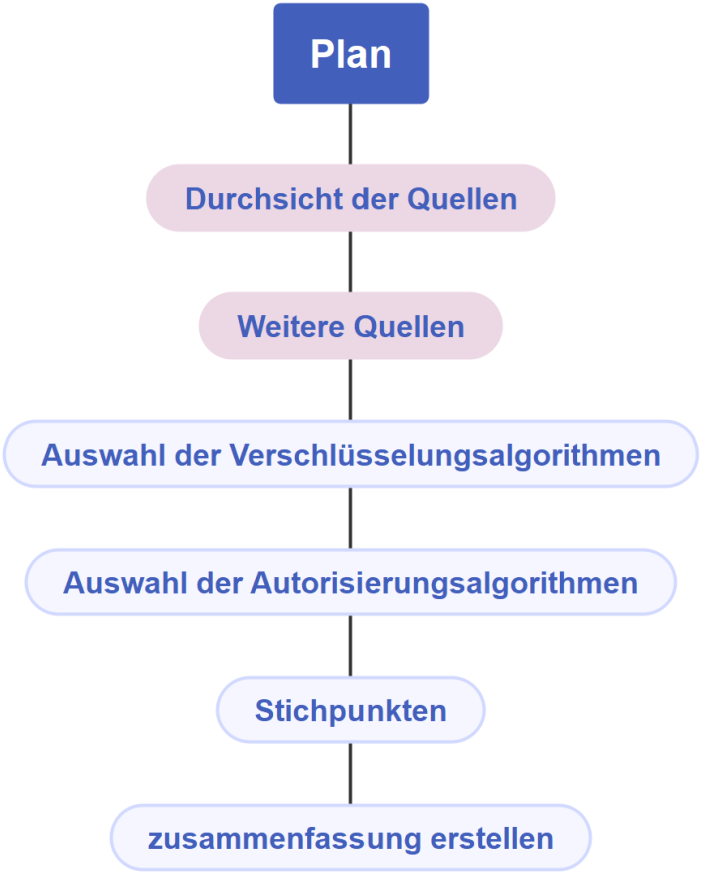
- Verbesserte Skalierbarkeit und Ausdauer
- Dynamische Attribute und Umgebungsrollen für Zugriffsbeschränkungen
- Anpassung an changing Bedingungen in intelligenten IoT-Systemen
- Vereinfacht Administration und Zugriffsverwaltung
- Ermöglichung der Feinkörnige Zugriffskontrolle
- Dynamische Entscheidungsfindung basierend auf Kontextfaktoren
- Kombiniert Rollen- und attributbasierte Zugriffskontrolle
- Komplexität der Implementation
- Kosten
- Abhängigkeit von Workload und Anwendungen

Inhaltsverzeichnis

Plan


Plan
Auswahl der Verschlüsselungsalgorithmen
Auswahl der Autorisierungsalgorithmen
Stichpunkten
Durchsicht der Quellen
zusammenfassung erstellen

Plan


Plan
Durchsicht der Quellen
Weitere Quellen
Auswahl der Verschlüsselungsalgorithmen
Auswahl der Autorisierungsalgorithmen
Stichpunkten
zusammenfassung erstellen

Quellen

Bilder:

- Basic Layerd
- Einseitige Authentifizierung

GitLab

Freie Universität Berlin

Danke für die Aufmerksamkeit!