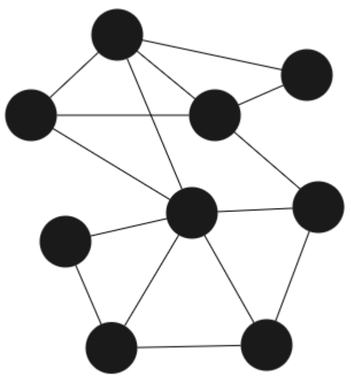
Technische Hochschule Brandenburg
University of Applied Sciences

Die Sicherheit von energiesparenden 2.4GHz-Kommunikationsprotokollen für vermaschte Netzwerke

Friedemann Pruß
Maximilian Schulke



Einführung

Sichere Kommunikation ist eine Grundvoraussetzung im Smart Home. Mesh Netzwerke bieten viele Vorteile, wie eine hohe Ausfallsicherheit und leichte Erweiterbarkeit. Bluetooth Mesh und Thread sind zwei sehr unterschiedliche Low Power Mesh-Protokolle mit hoher Relevanz für die IoT-Industrie (Adomnicai et al., 2018; Patel, 2020; Rzepecki & Ryba, 2019). Im Gegensatz zu Thread baut Bluetooth Mesh auf dem weit verbreiteten Protokolle Bluetooth Low Energy auf. Thread verwendet, ähnlich wie sein Vorgänger Zigbee IP, IEEE 802.15.4 für die drahtlose Datenübertragung (Bluetooth Special Interest Group [SIG], 2020; Thread Group, 2017). Diese Arbeit grenzt sich von vorangegangenen Arbeiten durch den sicherheitsbezogenen Vergleich der beiden Protokolle ab. Wir präsentieren die Ergebnisse unserer Literaturanalyse von Sicherheitsuntersuchungen und Spezifikationen.

Thread Netzwerkerweiterung

On-Mesh Commissioning: Der Commissioner kann dem Joiner festgelegte Credentials bereitstellen um dem Netzwerk beizutreten. Er kann diese Credentials auf die vom Hersteller vergebene EUI64 beschränken. (Thread Group, 2017).

External Commissioning: Der authentifizierte Commissioner stellt die Identität des Joiners sicher. Anschließend weist er den Border-Router an, dem Joiner alle Informationen zum Beitritt des Netzwerks bereitzustellen. (Thread Group, 2017).

Bluetooth Mesh Netzwerkerweiterung

Da Bluetooth Mesh BLE zur Übertragung verwendet, ist analog zu Thread, der gesamte Datenverkehr durch AES-128 verschlüsselt. Der Provisioning Prozess besteht aus 5 Phasen: Beaconing bzw. Advertisement, Invitation zur Aushandlung der Fähigkeiten (kommt von BLE), einem Key-Exchange durch Elliptic-Curve-Diffie-Hellman, der eigentlichen Authentifizierung (die bevorzugt Out-of-Band stattfindet), anschließenden Bereitstellung von Provisioning-Daten.

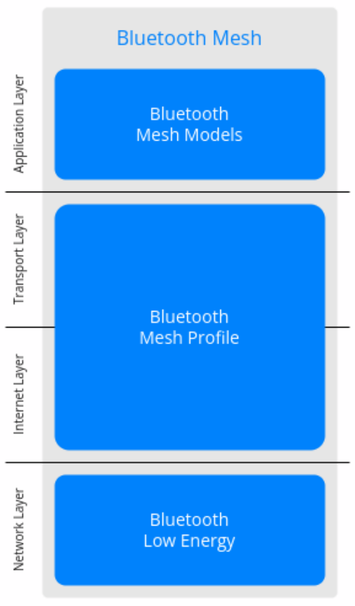


Abbildung nach SIG

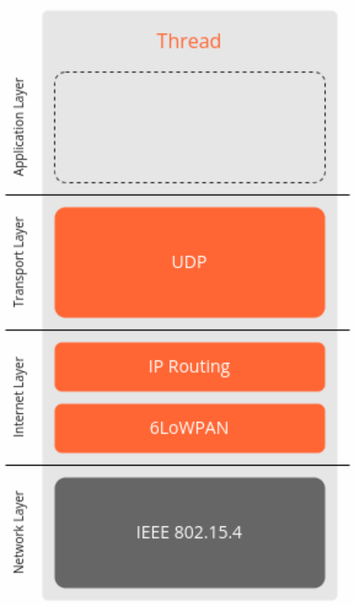


Abbildung nach SIG

Thread Sicherheitsanalyse

Thread ist ein offenes Protokoll, da es im Vergleich zu Bluetooth Mesh, kaum einen Einfluss auf die Anwendungsebene des Netzwerks hat.

Im Jahr 2020 wurde eine Sicherheitsanalyse von Thread anhand der 10 relevantesten Sicherheitsbedenken der OWASP für IoT-Netzwerke durchgeführt (Strayeri, 2020). Diese Analyse zeigt, dass Thread den Fokus primär auf die Verschlüsselung und die Sicherung der Übertragung legt, aber Risiken durch die fehlende Spezifikation der Anwendungsebene entstehen könnten. Hersteller müssen selbst für die Sicherheit auf der Anwendungsebene sorgen. Das macht es möglich, bereits gut erforschte Verschlüsselungsprotokolle, wie z. B. DTLS, zu verwenden und diese im Bedarfsfall auszutauschen. Diese Freiheit birgt aber auch Risiken, da sich der Nutzer auf die Sicherheitsmaßnahmen des Hersteller verlassen muss.

Dinu und Kizhvatov (2018) haben herausgefunden, dass durch eine Verkettung von Schwachstellen und einer differenziellen elektromagnetischen Analyse Rückschlüsse auf den Datenverkehr bei Thread zu ziehen ist, und Netzwerkschlüssel abgegriffen werden können. Dies lohnt sich allerdings aufgrund des hohen Aufwands i.d.R. bei Smart-Home-Netzwerken nicht, sondern stellt eher eine Gefahr für kommerzielle Anwendungen dar (Dinu & Kizhvatov, 2018).

Bluetooth Mesh Sicherheitsanalyse

In den letzten Jahren wurden mehrere, teils kritische, Sicherheitslücken in der Bluetooth Spezifikation entdeckt (SIG, 2022). Diese beeinträchtigen zum Großteil die Sicherheit von Direktverbindungen - also Bluetooth BR/EDR und Bluetooth Low Energy (BLE). Zu den schwerwiegendsten Schwachstellen in der Bluetooth Core Spezifikation zählen die sogenannten “Bluetooth Impersonation Attacks”. Diese macht es möglich, dass sich ein Angreifer als bereits authentifiziertes Gerät ausgibt und somit die komplette Authentifizierung bei einem Verbindungsaufbau umgehen kann. Dies ermöglicht Man-In-The-Middle-Attacken (Antonioli et al., 2020), durch die Daten ausgelesen, Daten manipuliert oder gefälschte Nachrichten in Umlauf gebracht werden können.

Bluetooth Mesh verwendet als Übertragungsprotokoll BLE und verwendet, anders als beim BLE-Pairing, elliptische 256-Bit-Kurven und Out-of-Band-Authentifizierung um das Hinzufügen von Netzwerkknoten abzusichern (SIG, 2020). Allerdings wurden diesbezüglich im Jahr 2020 die Sicherheitswarnungen CVE-2020-26556, CVE–2020-26557, CVE-2020-26559, CVE-2020-26560 veröffentlicht (SIG, 2022).

Diskussion

Die aktuell bekannten Sicherheitslücken von Bluetooth Mesh betreffen das Hinzufügen von neuen Netzwerkknoten (SIG, 2022) und vermindern somit die Integrität des Netzwerks. Bislang wurden bei Thread, trotz ausgiebiger Untersuchungen (Elshimi, 2020; Strayeri, 2020), noch keine vergleichbaren Schwachstellen gefunden. Auf der anderen Seite tritt Thread die Verantwortung zu Absicherung der Anwendungsschicht an den Hersteller ab, ist somit zwar flexibler, könnte aber mögliche Sicherheitslücken durch nicht abgesicherte Geräte öffnen. Eine eindeutige Empfehlung für oder gegen eines der beiden Protokolle nur auf Basis der Sicherheit kann nicht klar gegeben werden, da beide Protokolle unterschiedliche Vorteile und Sicherheitsrisiken mit sich bringen. Eine Entscheidung muss vom Implementierung-Kontext abhängig gemacht werden.

Literatur

Adomnicai, A., Fournier, J. J. A. & Masson, L. (2018). Hardware Security Threats Against Bluetooth Mesh Networks. 2018 IEEE Conference on Communications and Network Security (CNS), 1–9. https://doi.org/10.1109/CNS.2018.8433184

Antonioli, D., Tippenhauer, N. & Rasmussen, K. (2020). Key Negotiation Downgrade Attacks on Bluetooth and Bluetooth Low Energy. ACM Trans. Priv. Secur., 23 (3). https://doi.org/10.1145/3394497

Bluetooth Special Interest Group. (2020). Bluetooth Core Specification [Abgerufen am 07.01.22]. https://www.bluetooth.com/de/specifications/specs/core-specification/

Bluetooth Special Interest Group. (2022). Bluetooth Sicherheitshinweise [Abgerufen am 07.01.22]. https://www.bluetooth.com/de/learn-about-bluetooth/key-attributes/bluetooth-security/reporting-security/

Dinu, D. & Kizhvatov, I. (2018). EM Analysis in the IoT Context: Lessons Learned from an Attack on Thread. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018 (1), 73–97. https://doi.org/10.13154/tches.v2018.i1.73-97

Elshimi, A. (2020). Thread protocol simplifies IoT security - Embedded.com [Abgerufen am 07.01.22]. https://www.embedded.com/thread-protocol-simplifies-iot-security/

Patel, P. (2020). Extend the Power of IoT Solutions with BLE Mesh Network [Abgerufen am 08.01.22]. https://www.embeddedcomputing.com/application/networking- 5g/gateways-routers-switches-io-modules/extend-the-power-of-iot-solutions-with-ble-mesh-network

Rzepecki, W. & Ryba, P. (2019). IoTSP: Thread Mesh vs Other Widely used Wireless Protocols – Comparison and use Cases Study. 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), 291–295. https://doi.org/10.1109/FiCloud.2019.00048

Strayeri, K. (2020). Can the “Gorilla” Deliver? Assessing the Security of Google’s New “Thread” Internet of Things (IoT) Protocol - CSIAC [Abgerufen am 07.01.22]. https://csiac.org/articles/security-of-googles-iot-protocol/

Thread Group. (2017). Thread 1.1 Specification [Abgerufen am 07.01.22]. https://www.threadgroup.org/ThreadSpec

Kontakt: Friedemann R. Pruß prussf@th-brandenburg.de & Maximilian Schulke schulke@th-brandenburg.de