

Sachbericht zum Verwendungsnachweis
Teil III
2025

Vorhabenbezeichnung:

Pentest-5GSec

Gefördert durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Zuwendungsempfänger: AWARE7 GmbH	Förderkennzeichen: 01MO23025A
Titel des Teilvorhabens (sofern zutreffend): Mobiles Pentesting für sichere 5G-Netze	
Projektleitung: Herr Jan Hörnemann	
Laufzeit des Vorhabens: von: 01.06.2023 bis: 31.05.2025	
Berichtszeitraum: von: 01.06.2023 bis: 31.05.2025	Datum: 21.08.2025

1. Ursprüngliche Aufgabenstellung und Stand der Technik

Das Projekt Pentest-5GSec hatte das Ziel, ein mobiles Prüflabor und spezialisierte Werkzeuge für Penetrationstests in 5G-Netzen zu entwickeln. Ausgangspunkt war die Erkenntnis, dass gängige Pentesting-Tools (z. B. Nmap, Nessus) nicht auf die besonderen Eigenschaften moderner Mobilfunknetze zugeschnitten sind.

Wissenschaftlich-technisch wurde an aktuelle Arbeiten zur Bedrohungsmodellierung (z. B. MITRE ATT&CK, FiGHT) angeknüpft sowie an dokumentierte Angriffe auf verschiedene Ebenen der 5G-Architektur. Gleichzeitig bestand hoher Bedarf, da 5G-Campusnetze zunehmend in kritischen Infrastrukturen (Industrie, Gesundheit, IoT) eingesetzt werden und neue Sicherheitsanforderungen entstehen.

2. Ablauf des Vorhabens

Das Vorhaben gliederte sich in mehrere Arbeitspakete:

- Projektkoordination: Sicherstellung des Austauschs mit Partnern, Projektträger und Fachcommunity.
- Anforderungserhebung: Analyse der Anforderungen an Laborsysteme und Tools, Integration eines 5G-Campusnetzes der Cocos AG in die Infrastruktur der AWARE7 GmbH.
- Threat Modeling: Untersuchung technischer, organisatorischer und wirtschaftlicher Risiken, z. B. in IoT-Geräten und Smart-Ring-Ökosystemen, sowie Erweiterung bestehender Modelle für 5G.
- Leitfaden für Prüflabore: Entwicklung eines praxisnahen Pentest-Guides (Open Source).
- Implementierung des Demonstrators: Entwicklung des modularen Frameworks MobileSniper und des Basisband-Emulators BaseBridge; Aufbau der Plattform Chipsets.org.
- Evaluation: Technische und wirtschaftliche Bewertung des Laborkonzepts; Tests von MobileSniper hinsichtlich Leistung, Kompatibilität und Praxistauglichkeit.

Parallel wurden die Ergebnisse auf internationalen Konferenzen (NDSS, IEEE S&P, IWCMC, CHI) vorgestellt, in Abschlussarbeiten vertieft und als Open Source für die Fachcommunity veröffentlicht.

3. Wesentliche Ergebnisse und Zusammenarbeit

- Entwicklung und Veröffentlichung von MobileSniper, einem modularen Open-Source-Framework für Pentests in 5G-Netzen.
- Erstellung und Veröffentlichung des 5G-Pentest-Guides zur Unterstützung von Prüflaboren.
- Erweiterung und Anpassung des MITRE ATT&CK Frameworks auf 5G- und IoT-Szenarien.
- Entwicklung des BaseBridge-Emulators sowie der Plattform Chipsets.org.
- Praktische Evaluation von Schwachstellen in IoT- und Medizintechnik-Umgebungen.

Die Zusammenarbeit mit der Ruhr-Universität Bochum ermöglichte die wissenschaftliche Vertiefung und Einbindung in Lehre und Forschung (Bachelor-/Masterarbeiten, Praktika).

4. Fazit

Pentest-5GSec hat wesentliche Beiträge zur Sicherheit von 5G-Netzen geleistet, Lücken in Forschung und Praxis geschlossen und durch offene Ergebnisse (Software, Leitfäden, Plattformen) die Basis für nachhaltige Weiterentwicklung und zukünftige 6G-Sicherheitsforschung geschaffen.

1. Aufgabenstellung

Das Projekt Pentest-5GSec zielte auf die Entwicklung eines mobilen Prüflabors für 5G-Campusnetze sowie die Erstellung spezialisierter Penetrationstest-Werkzeuge. Ausgangspunkt war die Erkenntnis, dass bestehende Tools nicht auf die speziellen Anforderungen von 5G-Netzen ausgerichtet sind. Diese Netze bilden zunehmend die Grundlage für industrielle Anwendungen, kritische Infrastrukturen und das Gesundheitswesen. Das Projekt baute auf dem Stand der Technik in den Bereichen Mobilfunksicherheit, Threat Modeling und Penetration Testing auf.

Der Projektverlauf war durch mehrere Meilensteine geprägt: Kickoff im Jahr 2023, regelmäßige Statusmeetings zur Fortschrittskontrolle, Zwischenevaluierungen der Tools und wissenschaftlichen Ergebnisse sowie die Abschlusspräsentation im Jahr 2025. Die Zusammenarbeit mit Partnern wie der Ruhr-Universität Bochum und der Cocos AG stellte sicher, dass sowohl wissenschaftliche als auch praxisnahe Ergebnisse erzielt wurden.

Projektchronik und Meilensteine

- 2023: Projektstart und Kickoff-Meeting, Definition der Arbeitspakete
- 2023: Aufbau der Laborinfrastruktur, Anforderungserhebung (AP1)
- 2023: Erste Bedrohungsmodellierung und Analyse realer IoT-Geräte (AP2)
- 2023/2024: Entwicklung des Pentest-Leitfadens, Integration bestehender Tools (AP3)
- 2024: Entwicklung und erste Tests von MobileSniper und BaseBridge (AP4)
- 2024/2025: Evaluation der Ergebnisse durch RUB, Dissemination (AP5)
- 2025: Abschlusspräsentation und Veröffentlichung der Ergebnisse

AP0 – Projektkoordination

Zielsetzung: Sicherstellung einer reibungslosen Zusammenarbeit der Konsortialpartner und ordnungsgemäße Kommunikation mit dem Projektträger.

Vorgehen: Regelmäßige Statusmeetings, Koordination über Protokolle, Transparenz über Arbeitsstände und Zeitplanung. Einbindung aller Partner in Entscheidungen, Dokumentation von Kickoff, Zwischenständen und Abschluss.

Soll-Ist-Abgleich: Geplant waren quartalsweise Treffen, tatsächlich wurden monatliche Kurzabstimmungen durchgeführt, was den Austausch verbesserte. Herausforderungen betrafen vor allem die Synchronisation der Arbeitspakete.

Ergebnisse: Stabile Kommunikation, enge Zusammenarbeit, Einhaltung der Zeit- und Ressourcenplanung. Die Dissemination über internationale Konferenzen erhöhte die Sichtbarkeit.

AP1 – Anforderungserhebung

Zielsetzung: Systematische Erhebung der Anforderungen an Labor, Endgeräte und Tools.

Vorgehen: Integration des 5G-Campusnetzes der Cocos AG in die AWARE7-Infrastruktur. Durchführung einer Literaturstudie, Identifikation von Angriffen auf 5G-Architekturschichten, Sammlung praktischer Anforderungen aus der Pentest-Praxis.

Soll-Ist-Abgleich: Ursprünglich war eine reine Literaturlauswertung vorgesehen, tatsächlich wurden zusätzlich eigene Tests im Campusnetz durchgeführt, was die Ergebnisse verbesserte.

Ergebnisse: Katalogisierung von 20 Angriffen auf 7 Schichten, Integration der Anforderungen in die Architektur von MobileSniper.

AP2 – Threat Modeling

Zielsetzung: Systematische Analyse von Bedrohungsszenarien für 5G und IoT.

Vorgehen: Untersuchung des Smart-Ring-Ökosystems (IoT), Analyse von Bedrohungen in 5G-Intensivstationen, Erweiterung des MITRE ATT&CK-Frameworks. Kooperation mit der RUB für wissenschaftliche Auswertung.

Soll-Ist-Abgleich: Geplant war eine Modellierung basierend auf bekannten Frameworks, tatsächlich erfolgte eine Erweiterung bestehender Frameworks und eigene Bedrohungsanalysen.

Ergebnisse: Veröffentlichung der Ergebnisse in ACSAC 2024, Springer 2023 und als Open-Source-Erweiterung des ATT&CK-Frameworks.

AP3 – Leitfaden für Prüflabore

Zielsetzung: Erstellung eines praxisnahen Open-Source-Leitfadens für 5G-Penetrationstests.

Vorgehen: Sammlung von Best Practices, Integration existierender Tools, Entwicklung neuer Module, Ergänzung durch Abschlussarbeiten (z. B. Virtualisierungssicherheit).

Soll-Ist-Abgleich: Geplant war eine interne Dokumentation, tatsächlich wurde ein öffentlich zugänglicher Leitfaden erstellt.

Ergebnisse: Der Leitfaden dient als Ausbildungsgrundlage und wird in Schulungen eingesetzt.

AP4 – Implementierung des Demonstrators

Zielsetzung: Entwicklung des Demonstrators MobileSniper, um die Anforderungen praktisch umzusetzen.

Vorgehen: Implementierung von MobileSniper, Entwicklung von BaseBridge (Emulator), Aufbau der Plattform Chipsets.org. Durchführung interner Tests, Feedbackschleifen und Open-Source-Veröffentlichung.

Soll-Ist-Abgleich: Ursprünglich war nur MobileSniper geplant, tatsächlich wurden zusätzliche Werkzeuge entwickelt (BaseBridge, Chipsets.org), was den Nutzen steigerte.

Ergebnisse: MobileSniper, BaseBridge und Chipsets.org als zentrale Projektergebnisse.

AP5 – Evaluation

Zielsetzung: Umfassende Evaluation der entwickelten Tools und Konzepte.

Vorgehen: Tests von MobileSniper auf Kompatibilität, Leistung und Genauigkeit. Evaluation durch die RUB auch nach Projektende.

Soll-Ist-Abgleich: Die geplante Evaluation wurde durch externe Faktoren leicht verzögert, jedoch erfolgreich durchgeführt.

Ergebnisse: Bestätigung der Praxistauglichkeit, wissenschaftliche Validierung.

2. Wichtigste Positionen des zahlenmäßigen Nachweises

Die Mittel wurden wie folgt eingesetzt:

- Personalkosten: Entwicklung der Tools, wissenschaftliche Begleitung, Projektkoordination
- Sachmittel: Hardware (5G-Endgeräte, Laborinfrastruktur), Softwarelizenzen, Testausrüstung
- Reisekosten: Teilnahme an Konferenzen, Workshops, Dissemination
- Unteraufträge: Beiträge externer Partner

Jede dieser Positionen war notwendig und zielgerichtet eingesetzt.

3. Notwendigkeit und Angemessenheit

Die Arbeiten waren zwingend erforderlich, da bestehende Pentest-Tools für 5G nicht ausreichen. Nur durch eigene Entwicklungen konnten praxisnahe Lösungen geschaffen werden. Die Mittelverwendung war angemessen und effizient.

4. Voraussichtlicher Nutzen und Verwertbarkeit

Kurzfristige Verwertung (1–2 Jahre):

Unmittelbar nach Projektende werden die entwickelten Werkzeuge und Dokumentationen in die laufenden Tätigkeiten der beteiligten Unternehmen integriert. Das Tool MobileSniper wird direkt in Kundenprojekten eingesetzt, um Penetrationstests in realen 5G-Campusnetzen durchzuführen. Dabei profitieren insbesondere Industrieunternehmen, die eigene Campusnetze betreiben, von praxisnahen Sicherheitsprüfungen, die auf die besonderen Charakteristika von 5G zugeschnitten sind. Zusätzlich wird der erarbeitete Pentest-Leitfaden in Schulungen verwendet, die von den Konsortialpartnern für Unternehmen und Behörden angeboten werden. Damit wird das erworbene Wissen nicht nur in konkrete Dienstleistungen umgesetzt, sondern auch an Fachkräfte weitergegeben. Dieser Transfer stellt sicher, dass die Projektergebnisse bereits in der frühen Phase nach Projektende in der Breite Anwendung finden und eine unmittelbare Wirkung entfalten.

Mittelfristige Verwertung (2–5 Jahre):

Im mittleren Zeithorizont wird der Fokus stärker auf die wissenschaftliche und didaktische Nutzung gelegt. Die im Projekt entwickelten Tools und Konzepte fließen in die universitäre Lehre ein, etwa in Form von Praktika und Abschlussarbeiten. Studierende erhalten dadurch die Möglichkeit, mit praxisnahen Werkzeugen zu arbeiten und sich frühzeitig mit der Sicherheit von 5G- und künftigen 6G-Systemen auseinanderzusetzen. Parallel dazu werden die Open-Source-Repositories, die im Projekt entstanden sind, gepflegt und kontinuierlich erweitert. Damit bleibt der Zugang zu den Ergebnissen dauerhaft gewährleistet, und auch externe Akteure können die Tools in ihren eigenen Forschungsvorhaben nutzen. Zudem wird erwartet, dass sich die entwickelten Konzepte in weitere Forschungsarbeiten einfügen, beispielsweise in Kooperationen mit anderen Hochschulen und Forschungsnetzwerken. Auf diese Weise tragen die Projektergebnisse mittelfristig zur Ausbildung einer neuen Generation von Sicherheitsexperten bei und stärken zugleich die wissenschaftliche Exzellenz auf dem Gebiet der Mobilfunksicherheit.

Langfristige Verwertung (5–10 Jahre):

Im langfristigen Zeithorizont sollen die Projektergebnisse einen nachhaltigen Beitrag zur Entwicklung von Sicherheitskonzepten für die nächste Mobilfunkgeneration (6G) leisten. Die im Projekt gewonnenen Erkenntnisse und entwickelten Werkzeuge bilden eine Grundlage für zukünftige Forschung und Standardisierungsaktivitäten. Es ist zu erwarten, dass MobileSniper, BaseBridge und der Pentest-Leitfaden nicht nur für 5G, sondern auch als Blaupause für

Prüfverfahren in 6G-Netzen dienen können. Darüber hinaus wird die fortlaufende Pflege und Erweiterung der Projektergebnisse die Cybersicherheit in Deutschland langfristig stärken. Insbesondere Betreiber kritischer Infrastrukturen und Unternehmen im industriellen Sektor profitieren von einer erhöhten Sicherheit ihrer Kommunikationssysteme. Durch die Einbindung in internationale Forschungsk Kooperationen und Sicherheitsnetzwerke wird sichergestellt, dass die Projektergebnisse über die Grenzen Deutschlands hinaus Wirkung entfalten und so zu einer globalen Verbesserung der Mobilfunksicherheit beitragen.

5. Fortschritt bei anderen Stellen

Das Projekt schuf Anknüpfungspunkte für weitere Forschungsvorhaben im Bereich 6G, IoT-Sicherheit und kritische Infrastrukturen. Kooperationen mit Hochschulen, Unternehmen und Forschungsnetzwerken wurden intensiviert.

6. Veröffentlichungen

- NDSS 2025: Vulnerability Management in Smartphone-Chipsätzen – Analyse des Umgangs mit Schwachstellen in Mobilfunk-Chipsätzen.
- IEEE S&P 2025: BaseBridge – Beschreibung eines Emulators für Baseband-Firmware.
- IWCMC 2025: MobileSniper – Automatisierte Penetrationstests für 5G-Campusnetze.
- IWCMC 2025: 5G Under Siege – Bedrohungsanalyse in Campusnetzen.
- ACSAC 2024: The Rings of Tracking – Untersuchung von Sicherheitsproblemen im Smart-Ring-Ökosystem.
- ACM CHI 2024: Envisioning Secure and Private 6G-enabled Cognitive Informatics – Vision für zukünftige 6G-Szenarien.
- Springer 2023: Threat Modeling Towards Resilience in Smart ICUs – Bedrohungsmodellierung im Gesundheitswesen.

Alle Publikationen tragen zur wissenschaftlichen Verwertung bei und stellen die Anschlussfähigkeit für Folgeprojekte sicher.