10. März 2017
LLE

Working ZVEI Whitepaper
Security Interessen für die 5G Standardisierung

Warum ist die Beschäftigung mit Security bei 5G jetzt schon wichtig?

Ohne eine Berücksichtigung der Security wird es keinen Einsatz von 5G in der Industrie geben. Denn die Gewährleistung von Integrität, Verlässlichkeit und Robustheit der Industriekommunikation ist eine zwingende Voraussetzung. Gleichzeitig werden aktuell wichtige Architektur- und Designvorgaben für 5G festgelegt. Security lässt sich nicht nachträglich implementieren. Sie muss von Anfang im Design integriert werden, um die oben genannten Ziele und damit die Industrietauglichkeit zu erreichen. Die Unternehmen wünschen individuelle Anpassungsmöglichkeiten des Standards bei ihren Industrieanwendungen - insbesondere für Security-Mechanismen. Nur durch eine frühestmögliche Einbeziehung der Security in die Standardisierung kann diese Flexibilität und der Mehrwert für Anwender realisiert werden.

1) Teilnehmermanagement

Anliegen: Alternativen zum SIM-Karten-Modell ermöglichen, kein Vendor-Lock-in

Hintergrund: Für 5G ist ein flexibles Management der einzelnen Teilnehmer wichtig. Insbesondere soll es Alternativen zu SIM-Karten, zum Beispiel über ein Zertifikat-basiertes Modell, bieten. Dazu gehört die Möglichkeit, unabhängig vom *Mobile Network Operator* (MNO) Geräte hinzuzufügen, zu entfernen und in Gruppen mit unterschiedlichen Zugriffsrechten und Sicherheitsanforderungen einzuteilen. Die Verwaltung einer großen Zahl von Geräten und Gruppen sollte so erfolgen, so dass keine übermäßigen Abhängigkeiten von einem bestimmten Provider entstehen und weiterhin ein gesunder Wettbewerb verschiedener Anbieter möglich ist.

2) Anwenderspezifischer Sicherheitsschichten

Anliegen: Anwenderspezifische Security-Mechanismen sind auch für höhere Schichten flexibel zu zulassen

Hintergrund: Das 5G-Design sollte bereits robuste Security-Funktionalitäten beinhalten. Aufgrund der unterschiedlichen Use Cases und Kundenanforderungen sollte es jedoch jederzeit für die Anwender möglich sein, individuelle Security-Mechanismen sowohl auf Mobilfunkebene, als auch auf höheren Schichten umzusetzen. Insbesondere darf es keine Hindernisse für die Implementierung eigener, anwenderspezifischer Sicherheitsschichten geben, die oberhalb der 5G-Schicht aufsetzen.

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V. • Lyoner Straße 9 • 60528 Frankfurt am Main
Arbeitsbereich Cybersicherheit
Telefon: +49 69 6302-432 • Fax: +49 69 6302-332 • E-Mail: linke@zvei.org • www.zvei.org

Präsident: Michael Ziesemer • Geschäftsführung: Dr. Klaus Mittelbach (Vorsitzender), Frank Bechtloff

3) Offenheit für Ende-zu-Ende-Sicherheit

Anliegen: Anwender benötigen die Freiheit, im Bedarfsfall trotz eines berechtigten Behördeninteresses eine Ende-zu-Ende-Sicherheit realisieren zu können.

Die 5G-Sicherheitskonzepte und -mechanismen müssen nach dem aktuellen Stand der Technik so entworfen und umgesetzt werden, dass sie (nach heutiger Sicht) auf absehbare Zeit sicher sind und wartbar bleiben. Eine absichtliche Schwächung der Sicherheit von 5G - beispielsweise durch den Einbau von „Hintertüren“, Lücken im Standard oder dem Einsatz von schwacher Kryptographie - ist keinesfalls akzeptabel. Die Möglichkeit für echte Ende-zu-Ende-Sicherheit (von Endgerät zu Endgerät, ohne „Aufbrechen“ der Verschlüsselung/Authentifizierung im Netz bzw. Backend) muss gegeben sein.

4) Identifizierung und Authentifizierung

Anliegen: Eine sichere Identifizierung und Authentifizierung der Teilnehmer/Geräte muss gewährleistet sein, um beispielsweise als Grundlage für feingranulare Zugriffskontrolle zu dienen.

5) Langzeittauglichkeit der Security

Anliegen: 5G-Standard muss Stand der Technik in der Security integrieren.

Hintergrund: Die 5G-Sicherheitskonzepte und -mechanismen müssen nach dem aktuellen Stand der Technik so entworfen und umgesetzt werden, dass sie (nach heutiger Sicht) auf absehbare Zeit sicher sind. Darüber hinaus muss die Möglichkeit der Aktualisierung von Sicherheitsmechanismen (insbesondere auch hinsichtlich kryptografischer Algorithmen und Parameter) von vornherein vorgesehen sein, um die Sicherheit von 5G auch in Zukunft gewährleisten zu können.

6) Sichtbarkeit der Security-Mechanismen

Anliegen: Anwender müssen aktive/inaktive Security-Mechanismen jederzeit nachvollziehen können.

Hintergrund: Da 5G-Sicherheit flexibel für verschiedene Anforderungen unterschiedlich konfiguriert werden kann, ist es essentiell, dass der Anwender jederzeit zweifelsfrei feststellen kann, welche Security-Mechanismen gerade aktiv sind.

7) Security bei ad hoc Verbindungen

Anliegen: Security muss auch für ad hoc Device to Device Verbindungen möglich sein

Hintergrund: Die 5G-Sicherheitslösung muss es ermöglichen, dass Teilnehmer auch direkt miteinander kommunizieren (device-to-device), ohne Verbindung zum Backend und ohne sich vorher schon zu kennen (ad-hoc). Insbesondere kommt 5G im Automobilbereich für die Vehicle2X-Kommunikation nur in Frage, wenn Fahrzeuge auch in Gebieten ohne Netzabdeckung sicher miteinander kommunizieren können ohne sich davor bereits begegnet zu sein (beispielsweise im Tunnel oder in entlegenen Gebieten). Da es sich hierbei um safety-kritische Nachrichten handeln kann (z.B. Warnungen vor Notbremsungen, Falschfahrern, Einsatzfahrzeugen, etc.), stehen der Schutz vor Manipulationen (Integrität und Authentizität) sowie die Privatsphäre der Verkehrsteilnehmer (Pseudonymität/Anonymität) im Vordergrund.