5G UNDERCOVER:

Geschüttelt, *nicht gerührt*

TEXT Markus Walter

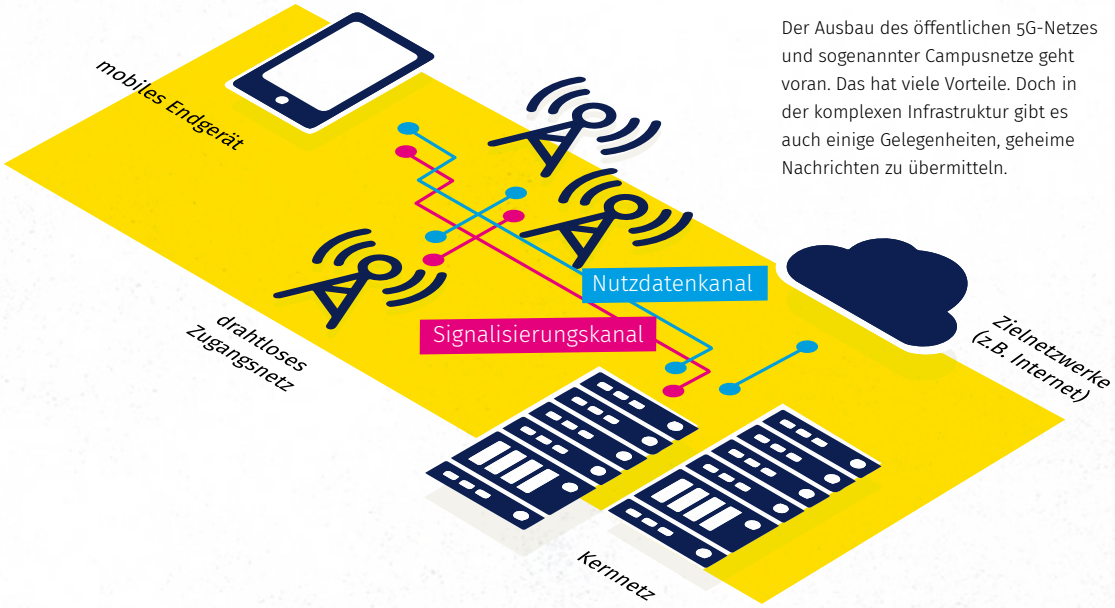
Die Steganografie ist ein Alltagswerkzeug für Agentinnen und Spione, um Informationen versteckt auszutauschen. Doch Papier und Zitronensaft werden dafür schon längst nicht mehr benutzt. Die starke Vernetzung und die zunehmende mobile Kommunikation machen es immer einfacher, große Datenmengen im Verborgenen zu übertragen. Umso wichtiger ist es, moderne Kommunikationstechnologien wie 5G genauer unter die Lupe zu nehmen und zu überprüfen, ob Informationen damit versteckt übertragen werden können.

Es klingt wie eine Szene aus einem James-Bond-Film: Ein Mitarbeiter eines amerikanischen Großkonzerns verschickt eine E-Mail von seinem Unternehmensaccount an seine private Mailadresse. Im Anhang befindet sich eine Bilddatei, die einen Sonnenuntergang zeigt. Auf den ersten Blick wirkt diese Situation ganz alltäglich. Allerdings enthält die Bilddatei nicht nur das Foto des Sonnenuntergangs, sondern weitere verschlüsselte Binärdaten. Schlussendlich stellt sich heraus, dass dieser Mitarbeiter zahlreiche Unternehmensgeheimnisse gestohlen und an eine ausländische Regierung weitergeleitet hat.[1,2] Durch das Einbetten in eine Bilddatei wurde die Übertragung der gestohlenen Daten aus dem Unternehmensnetzwerk verschleiert. Diese Art der verdeckten Übermittlung von Informationen wird als Steganografie oder Information Hiding bezeichnet und schon seit der frühen Antike zur geheimen Kommunikation eingesetzt. In der Netzwerkkommunikation wird von einem sogenannten verdeckten Kanal oder auch Covert Channel gesprochen, wenn die Informationen in den legitimen Nachrichten eines Netzwerkprotokolls versteckt sind.

Mit der zunehmenden Digitalisierung werden natürlich auch immer mehr Kommunikationstechnologien entwickelt, die für verdeckte Kanäle missbraucht werden können. Vor allem die modernen, für die Digitalisierung vielversprechenden Telekommunikationstechnologien bieten aufgrund der Vielschichtigkeit an Kommunikationsprotokollen viele Möglichkeiten für das Verstecken von geheimen Informationen. Bei der Mobilfunkkommunikation ist insbesondere 5G eine aufstrebende Technologie, die aufgrund der technischen Eigenschaften nicht nur in den öffentlichen Mobilfunknetzen, sondern in Form von sogenannten Campusnetzen beispielsweise auch im industriellen Umfeld eingesetzt wird. Dort können nun (Echtzeit-)Anwendungen realisiert werden, die von der geringen Latenzzeit und den hohen Bandbreiten profitieren.

Ein Sicherheitslabor für 5G-Netze

Der Ausbau der öffentlichen 5G-Infrastruktur ist international schon weit fortgeschritten und der Anteil des 5G-Datenverkehrs steigt kontinuierlich an. Auch die privaten, lokal betriebenen Campusnetze werden vermehrt aufgebaut. In Deutschland wurden bei der Bundesnetzagentur, die für die Registrierung



Der Ausbau des öffentlichen 5G-Netzes und sogenannter Campusnetze geht voran. Das hat viele Vorteile. Doch in der komplexen Infrastruktur gibt es auch einige Gelegenheiten, geheime Nachrichten zu übermitteln.

und Verteilung der Funklizenzen zuständig ist, bisher über 350 Anträge für eine Campusnetzlizenz bestätigt.[3] Zukünftig sollen auch kritische Infrastrukturen mit 5G vernetzt werden. Ein Beispiel ist die Modernisierung des europäischen Zugleitsystems und dessen Zugfunk, der in der neuen Generation auf 5G basieren wird. Dies verdeutlicht die Relevanz und Kritikalität von 5G-Infrastrukturen für alle Bereiche des alltäglichen Lebens. Um das Sicherheitsniveau und die Resilienz von öffentlichen und privaten 5G-Netzen kontinuierlich zu erhöhen, wurde am Standort des Bundesamts für Sicherheit in der Informationstechnik (BSI) in Freital bei Dresden ein Sicherheitslabor in Form eines 5G-Campusnetzes mit mehreren Funkzellen aufgebaut.[4] Dort werden neue Bedrohungen und Angriffstechniken, zu denen auch Covert Channels gehören, analysiert und bewertet.

Die grundlegende Netzwerkarchitektur von 5G besteht aus einem Zugangs- und Kernnetz. Das Zugangsnetz wird als Radio Access Network (RAN) bezeichnet und setzt sich aus einer Funkschnittstelle für die lokale Signalübertragung und einer Basisstation für die Kommunikationsverwaltung zusammen. Das Kernnetz verbindet alle Zugangsnetze eines Mobilfunkbetreibers und ist das zentrale Gateway für die interne und externe Kommunikation. Die Funkschnittstelle im Zugangsnetz eines 5G-Systems wird als 5G New Radio bezeichnet und enthält mehrere Kommunikationsprotokolle, die die unteren drei Schichten des OSI-Modells, also die physikalische Bitübertragungsschicht, die Sicherungsschicht zur fehlerfreien Übertragung und die Paketvermittlungsschicht, abbilden.

Konkret ist die Kommunikation zwischen einem Endgerät, etwa einem Smartphone, und dem Mobilfunknetz in zwei logische Kanäle aufgeteilt (siehe Grafik oben). Auf dem Signalisierungskanal werden Daten zur Steuerung und Signalisierung des Endgeräts übertragen. Die Daten dieses Kanals werden über das Zugangsnetz an das Kernnetz weitergeleitet und dort verarbeitet. Die Applikationsdaten der Nutzerin oder des Nutzers sind hingegen im Nutzdatenkanal enthalten. Die Nutzdaten gelangen ebenfalls über das Zugangsnetz in das Kernnetz

und werden dort mithilfe eines Gateways an die entsprechenden Zielnetzwerke weitergeleitet. Der gesamte Kommunikationsfluss über die Funkschnittstelle ist bidirektional und kann sowohl vom Endgerät als auch vom Kernnetz ausgehen. Deshalb werden die zwei Richtungen der Datenübertragung als Uplink (vom Endgerät zum Mobilfunknetz) und Downlink (vom Mobilfunknetz zum Endgerät) bezeichnet.

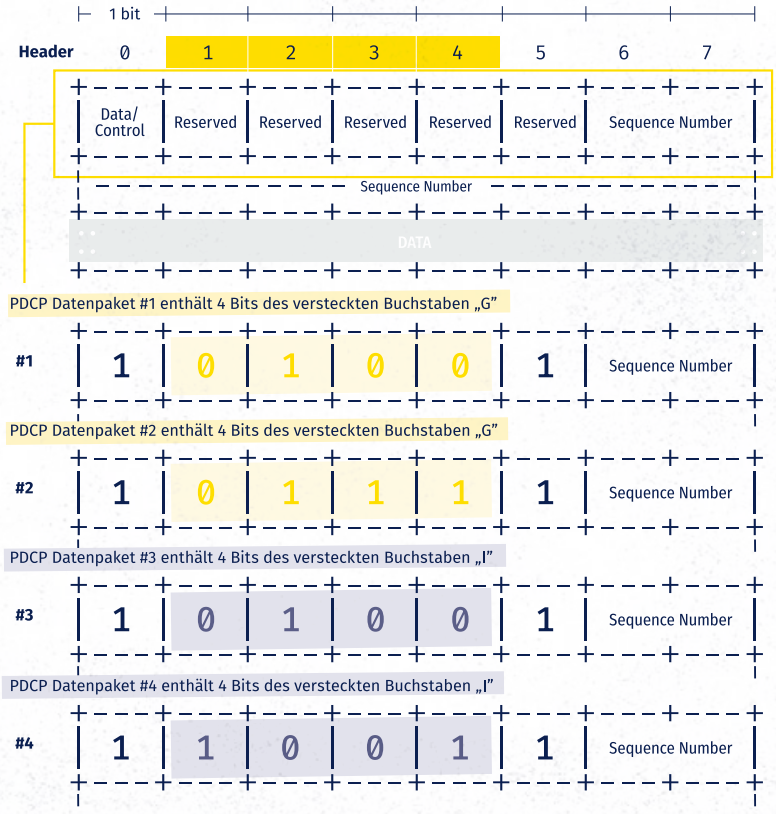
Wenn Zeit zum Geheimcode wird

Die (technische) Funktionsweise der verschiedenen Kommunikationsprotokolle, die auf der Funkschnittstelle eingesetzt werden, wurde von einem internationalen Gremium standardisiert. Nach einer genauen Analyse dieser Protokolle bieten sich vielfältige Möglichkeiten für die geheime Informationsübertragung mithilfe eines verdeckten Kanals.[5] Dabei wird zwischen zwei Arten eines Covert Channel unterschieden. Ein Timing Channel nutzt das Zeitverhalten einer Kommunikation aus, um Daten zu kodieren. Vergleichbar ist das mit dem Morse-Code, der die Buchstaben des Alphabets durch die Kombination von kurzen und langen Lichtsignalen darstellt. In 5G könnte dies beispielsweise durch die absichtliche Verzögerung oder sogar Unterdrückung von bestimmten Protokollnachrichten geschehen. Allerdings ist die Kommunikation über 5G sehr zeitkritisch. Zeitliche Verzögerungen von Netzwerkpaketen führen deshalb mit hoher Wahrscheinlichkeit zu einer (temporären) Störung der Kommunikation und erhöhen das Risiko, dass der verdeckte Kanal entdeckt wird.

Deutlich geeigneter für den Austausch von geheimen Daten auf der 5G-Funkschnittstelle sind hingegen sogenannte Storage Channel. Dabei entsteht der verdeckte Kanal durch das Einbetten der Informationen in die Speicherfelder der legitimen Protokollnachricht, zum Beispiel in den Header. Im Header der Kommunikationsprotokolle sind Informationen enthalten, die für das korrekte Zusammensetzen und Verarbeiten beim Empfangen wichtig sind, also unter anderem Sequenznummern oder optional auch ein Message Authentication Code für den Integritätsschutz. Allerdings sind manchmal auch ungenutzte und reservierte Felder im Header vorhanden, die mit einem Default-Wert (null) belegt sind. Da die reservierten Bits nicht für die legitime Kommunikation genutzt werden, können dort geheime Informationen versteckt werden.

Bit für Bit bestens versteckt

Ein einfaches Beispiel: Über einen verdeckten Kanal in der 5G-Funkschnittstelle soll geheimer Text („GI“) übertragen werden. Ein Textzeichen besteht in der ASCII-Codierung aus einem Byte, also acht Bits. Der Header des Packet Data Convergence Protocol (PDCP) in 5G New Radio enthält allerdings nur fünf reservierte Bits. Also wird ein Buchstabe in zwei Vier-Bit-Pakete geteilt. Eine Hälfte des Zeichens kann im



Die Protokolle der 5G-Funkschnittstelle bieten zahlreiche Möglichkeiten, um Daten zu verstecken. Beispielsweise können Teile eines Buchstabens in den reservierten bzw. ungenutzten Bits des PDCP-Headers eingebettet werden. Mit vier PDCP-Paketen lassen sich so die Buchstaben „G“ und „I“ im Geheimen übertragen.

Header eines PDCP-Pakets versteckt werden, die andere Hälfte folgt dann in einem der nächsten PDCP-Pakete des Kommunikationsflusses. Um den Text „GI“ im Geheimen zu übertragen, müssen also die 16 Bits der beiden Buchstaben in vier PDCP-Paketen versteckt werden. Damit die Empfängerin oder der Empfänger den versteckten Text auch finden kann, wird das fünfte reservierte Bit eines PDCP-Paketes als Signalisierung verwendet. Enthält dieses Bit nicht den Standard-Wert, dann ist im Header des empfangenen PDCP-Pakets ein Teil des geheimen Textes enthalten. Wer so alle Buchstabenteile extrahiert und zusammensetzt, kann den geheimen Text lesen.

Das Beispiel verdeutlicht, dass es auch in 5G möglich ist, Informationen über verdeckte Kanäle zu übertragen. Dieses Szenario konnte bereits erfolgreich mit einem Versuchsaufbau im BSI getestet werden. Dabei hat das Team analysiert, welche Gefahren durch einen Covert Channel entstehen können und mit welchen Maßnahmen der verdeckte Kanal enttarnt und eliminiert werden kann. Die Ergebnisse aus solchen Sicherheitsuntersuchungen verwendet das BSI, um Sicherheitsthemen in der Mobilfunkstandardisierung mitzugestalten und Sicherheitstests als Zertifizierungsgrundlage für kritische 5G-Komponenten weiterzuentwickeln. Um die Sicherheit der Netze weiter zu erhöhen, beteiligt sich das BSI außerdem an der Erstellung neuer Sicherheitsanforderungen im Rahmen des Telekommunikationsgesetzes und überprüft als qualifizierte unabhängige Stelle deren Einhaltung in den öffentlichen Mobilfunknetzen. So sollen wichtige Vorkehrungen getroffen werden, damit zukünftig ein Bild von einem Sonnenuntergang auch einfach nur ein Bild von einem Sonnenuntergang bleibt. I

[1] Yong, Nicholas (2023), *Industrial espionage: How China sneaks out America's technology secrets*, https://www.bbc.com/news/world-asia-china-64206950

[2] District Court, N.D. New York (2018), *United States v. Zheng Criminal Complaint – Document #1*, https://www.courtlistener.com/docket/14983061/1/united-states-v-zheng/

[3] Mattauch, Walter und Niebel, Wolfgang (2024), *Monitoring: Campusnetze, 4. Quartal 2023*, https://www.digitale-technologien.de/DT/Redaktion/DE/Kurzmeldungen/Aktuelles/2024/Campusnetze/20240212_weiteres_wachstum_von_campusnetzen.html

[4] Bundesamt für Sicherheit in der Informationstechnik (2023), *5G-Sicherheit: BSI eröffnet 5G/6G Security Lab am Standort Freital*, https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2023/230830_5G6G-Labor.html

[5] Walter, Markus und Keller, Jörg (2024), *5G UnCovert: Hiding Information in 5G New Radio*, https://doi.org/10.18420/sicherheit2024_002

Über den Autor

Markus Walter hat Informatik im Bachelor an der Hochschule Bonn-Rhein-Sieg sowie im Master an der FernUniversität in Hagen studiert und sich auf IT-Sicherheit spezialisiert. Er ist seit 2021 als Sicherheitsexperte beim Bundesamt für Sicherheit in der Informationstechnik (BSI) tätig und beschäftigt sich dort mit der Sicherheit von Mobilfunknetzen und insbesondere mit der drahtlosen Kommunikation in 5G.

Die **SICHERHEIT** ist die regelmäßig stattfindende Fachtagung des Fachbereichs „Sicherheit – Schutz und Zuverlässigkeit“ der GI. Sie bietet einem Publikum aus Forschung, Entwicklung und Anwendung ein Forum, um Herausforderungen, Trends, Techniken und neueste wissenschaftliche und industrielle Ergebnisse zu diskutieren. Die Tagung deckt alle Aspekte der Sicherheit informationstechnischer Systeme ab und versucht, eine Brücke zwischen den Themen IT Security, Safety und Dependability zu bilden. „Dieses Jahr fand die Tagung erstmals in Rheinland-Pfalz statt“, sagt Prof. Dr. Steffen Wendzel, Chair der Veranstaltung. Wissenschaftliche Arbeiten wurden von Universitäten, Hochschulen und Unternehmen aus Deutschland, Österreich und der Schweiz eingereicht.

fb-sicherheit.gi.de