Sicherheitsprobleme bei LTE und 5G

Man-in-the-Midddle-Angriffe auf Mobilfunknetze

31.03.20 | Autor / Redakteur: Bernd Schöne / Andreas Donner

David Rupprecht hat mit einem Wissenschaftler-Team des Horst-Görtz-Instituts der Ruhruniversität Bochum eklatante Fehler in 5G und LTE entdeckt. (Bild: © Bernd Schoene)

Wissenschaftler des Horst-Görtz-Instituts an der Ruhruniversität Bochum haben gravierende Sicherheitslücken in den Mobilfunkstandards LTE (4G) und 5G gefunden. Mit ihrer Anfälligkeit für Man-in-the-Middle-Attacken öffnen auch modernste Mobilfunknetze Hackern Tür und Tor.

Wenn zwei sich über eine Datenleitung unterhalten und ein Dritter schiebt sich dazwischen, nennt man das einen "Man-in-the-Middle" Angriff. Ist der unerwünschte Zuhörer kein Mensch, sondern ein Computer, kann er aber weit mehr als nur zuhören. Neben Cyber-Spionage ist dann bspw. auch Sabotage möglich, wenn Computerbefehle oder Messwerte verfälscht werden.

Forscher des Horst-Görtz-Instituts an der Ruhruniversität in Bochum (RUB) haben einen solchen Angriffsvektor nun bei LTE-Mobilfunksystemen gefunden. Er funktioniert aber auch beim neuen Standard 5G. Damit sind alle Anwendungen des Internets der Dinge potenziell gefährdet.

Die Geräte halten den Angreifer für den gewünschten Kommunikationspartner und vertrauen ihm. Ursache sind mehrere Schwachstellen im Protokoll. Bei der Überprüfung der Integrität sind fatale Fehler möglich, wenn die Netzbetreiber nicht sehr sorgfältig gearbeitet haben.

Auf der Sicherheitstagung "IT-Defense 2020" der Cirosec AG erläuterte David Rupprecht die Erkenntnisse, zu denen er und sein Team in monatelangen Experimenten gelangt sind.

Komplexe Struktur aus Spezifizierung, Implementierung und Auslieferung

So ist es Aufgabe des 3GPP (3rd Generation Partnership Project), einer weltweite Kooperation von Standardisierungsgremien für die Standardisierung von UMTS und LTE. 3GPP erarbeitet in Übereinstimmung mit den staatlichen Regulierungsbehörden die Spezifikationen des Standards. Hier arbeiten Wissenschaftler und Ingenieure zusammen, und stecken den Rahmen ab. Entscheidend ist anschließend aber die konkrete Umsetzung von Herstellern wie Apple, Cisco, Huawei oder Nokia.

Denn die technische Spezifikation lässt den Herrstellern hier gewisse Freiheiten. Auch die Netzwerkbetreiber Vodafone, die Telekom, O2 oder Telefonica besitzen solche Freiheiten. Sie können, müssen aber nicht, alle von der Norm möglichen Features auch an ihre Kunden weiterreichen.

Umgekehrt können Besonderheiten der technischen Umsetzung auf dieser Ebene Folgen haben, die bei der Abfassung des Standards so nicht beabsichtigt waren. "Die Dokumente sind teilweise 1.000 Seiten lang und nicht immer eindeutig", erläutert David Rupprecht von der Ruhruniversität Bochum.

Nutzerdaten, die über LTE-Netze ausgetauscht werden, sind zwar in der Regel verschlüsselt, werden aber nicht auf ihre Integrität überprüft. "Das ist gewollt", so Rupprecht. Eine Integritätsprüfung kostet Zeit und Bandbreite, und die ist für die Netzbetreiber bares Geld wert. Doch diese Sparsamkeit hat Folgen für die Sicherheit. „Ein Angreifer kann den verschlüsselten Datenstrom verändern und dafür sorgen, dass die Nachrichten an einen eigenen Server umgeleitet werden, ohne dass das dem Nutzer auffällt“, erläuterte Rupprecht.

Es gelang seiner Gruppe, sich unbemerkt zwischen Basisstation und Endgerät einzuschleusen. Bei diesem Angriff suggeriert der Angreifer der Basisstation, er sein ein berechtigter Gesprächspartner, während er dem Endgerät suggeriert, er sei die gewünschte Basisstation. Die Existenz solcher Angriffsmöglichkeiten wurde lange geleugnet, allerdings sind sie als so genannte "IMSI-Catcher" bei den Polizeibehörden längst in Gebrauch. Rupprecht und sein Team konnten nun nachweisen, dass dieser Angriff nicht nur bei GSM (2G)und UMTS-Netzen (3G) funktioniert, sondern auch bei LTE (4G).

Einer der Schwachpunkte ist der NULL-Modus des Netzwerks. Er wird verwendet, wenn ein Teilnehmer seine Integrität nicht nachweisen kann, oder nicht in der Lage ist, verschlüsselte Botschaften auszutauschen. Dann wird das Universal Subscriber Identity Module (USIM) nicht verwendet. Die Verbindungen sind dann quasi anonym. So eine Situation kann eintreten, wenn ein Mobiltelefon ohne vorhandene oder gültige SIM-Karte verwendet wird, um einen Notruf abzusetzen. Die Möglichkeit hierzu ist vorgeschrieben. Das technische Feature im Hintergrund ließ sich aber missbrauchen, um anschließend eine normale Verbindung zu beliebigen Kommunikationspartnern aufzubauen. Als Ursache machten die Forscher eine schlechte Umsetzung der vorgesehenen Sicherheitsabfragen aus.

Risikofaktor Roaming-Abkommen

Ein weiterer Risikofaktor sind die weltweiten Roaming-Abkommen. Aus jedem Netz sollte man in jedes Netz telefonieren können. Damit tangiert die Schwachstelle eines falsch konfigurierten Service-Providers alle anderen Netze. Gleichzeitig gibt es etliche Länder, in denen die in der Norm vorgesehene Verschlüsselung ausgeschaltet werden muss, da die Regierungen dies so wünschen, um die Kommunikation leichter abhören zu können.

Da alle Geräte die Möglichkeit besitzen müssen, mit allen anderen zu kommunizieren, genügt es oft, dem Endgerät vorzugaukeln, es befände sich in Kontakt mit einem nur schwach geschützten Netz. In diesem Fall schaltet das Mobiltelefon in den unverschlüsselten Modus.

Die Techniker der Ruhruniversität führten neben theoretischen Arbeiten auch praktische Tests an realen Mobiltelefonen durch, allerdings in einer funktechnisch abgeschotteten Umgebung, um andere Teilnehmer nicht zu stören oder gegen deutsche Gesetze zu verstoßen, denn legal sind IMSI-Catcher oder technisch verwandte Geräte nur in den Händen der Strafverfolgungsbehörden.

Es gelang ihnen, sich erfolgreich zwischen Endgerät und Basisstation einzuklinken, den Funkverkehr mitzuschneiden, und sogar zu verändern. „Ein Angreifer kann den verschlüsselten Datenstrom verändern und dafür sorgen, dass die Nachrichten an einen eigenen Server umgeleitet werden, ohne dass das dem Nutzer auffällt“, erklärt David Rupprecht. Auf dieser Webseite kann der Angreifer dann beliebige Aktionen durchführen, zum Beispiel eingegebene Passwörter abgreifen.

Praktische Versuche

Die verwendeten Angriffswerkzeuge sind frei im Handel erhältlich. Die Forscher verwendeten für ihre Versuche neben einem PC zwei so genannte Software-Defined Radios, die das Senden und Empfangen von LTE-Signalen ermöglichen. Alles zusammen Geräte im Wert von ca. 4.000 Euro. Eines der Geräte gibt sich beim Opferhandy als Mobilfunknetz aus, das andere gibt sich beim echten Mobilfunknetz als Handy aus. So kann das System bestimmte Daten gezielt verändern, während es den Großteil der Daten unverändert weiterleitet. Je nach Equipment kann der Angreifer einige Hundert Meter vom Opferhandy entfernt sein, um den Angriff durchzuführen.

Die Ergebnisse

Zwölf Netzwerke kommerzieller europäischer LTE-Anbieter wurden von der Gruppe überprüft. Vier Netzwerke erwiesen sich als falsch konfiguriert, drei davon waren durch die beschriebenen Methoden angreifbar. Zusätzlich wurden diverse weitere Fälle von unerwünschtem Verhalten festgestellt. Die meisten Lücken wurden inzwischen von den Netzbetreibern geschlossen.

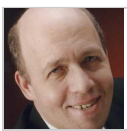
Nicht zu beheben ist die grundsätzlich Möglichkeit, Sicherheitsfeatures abzuschalten. "Dies wird von bestimmten Staaten so gewünscht und ist deshalb im Standard vorgesehen", so David Rupprecht.

Integrierte Schwachstellen

Die meisten Schwachstellen sind inzwischen von den Netzwerkbetreibern behoben worden. Das gilt aber natürlich nicht für jene, die im Standard festgeschrieben sind. "Es wären 4 Bytes mehr pro IP Packet nötig, um den Integritätsschutz zu garantieren", meint David Rupprecht. Vorgesehen ist dieser Schutz selbst bei 5G noch nicht.

Damit könnte auch beim neuen Mobilfunkstandard der Angreifer mit der Identität des Opfers surfen und im Internet Aktionen durchführen. "Müssen wir erst auf 6G warten, bis der Integritäts-Schutz kommt?", fragte Rupprecht am Ende seines Vortrages in Bonn.

Doch schon wenige Tage später hat sich das Blatt offensichtlich gewendet. In den wichtigen Gremien bahnt sich in diesen Tagen aufgrund der Forschungen des Bochumer-Teams ein Umdenken an. Auch die Netzbetreiber sind nun offen für mehr Sicherheitz. "Inzwischen sehen die Provider das ein, und es gibt eine starke Argumentation in der 3GPP, für einen Full-Rate Integritätsschutz", so Rupprecht.



Über den Autor

Bernd Schöne

Publizist