Ende-zu-Ende-Sicherheit bei Long Term Evolution (LTE)

Prof. Dr. -Ing. Evren Eren

Fachhochschule Dortmund
Fachbereich Informatik
Emil-Figge-Str. 42, D-44227 Dortmund
evren.eren@fh-dortmund.de

Prof. Dr. Kai-Oliver Detken

DECOIT GmbH
Fahrenheitstraße 9, D-28359 Bremen
detken@decoit.de

Zusammenfassung

Die aktuellste Mobilfunkgeneration Long Term Evolution (LTE) vervollständigt die Entwicklung zu einem angestrebten offenen Netzwerkmodell. Gleichzeitigt fordert der Markt den ubiquitären Informationszugriff mit unterschiedlichsten Endgeräten, insbesondere Smartphones. Zudem werden immer mehr Dienste sowie Anwendungen entwickelt, um den ständig steigenden Anforderungen des Marktes nach zielgerichteten und kontextbasierten Informationen gerecht zu werden. Diese fortlaufende Entwicklung vergrößert jedoch auch kontinuierlich das Verwundbarkeitsrisiko. Die neue Netzarchitektur von LTE stellt daher auch spezifische Anforderungen an die resultierende Sicherheitsarchitektur und somit an die Ende-zu-Ende-Sicherheit, insbesondere an das Kernnetzwerk Evolved Packet System (EPS). Vor diesem Hintergrund stellt der vorliegende Beitrag die wesentlichen Sicherheitsmerkmale des EPS vor und bewertet die Sicherheit von LTE.

1 Evolved Packet System (EPS)

Die aktuelle Erweiterung der neuen Mobilfunkgeneration wurde 2011 implementiert. Im Rahmen der Entwicklung wurde diese Generation seitens des 3rd Generation Partnership Project (3GPP) sowohl Long Term Evolution (LTE) als auch System Architecture Evolution

(SAE) genannt. Umgangssprachlich hat sich der Begriff LTE durchgesetzt. In den 3GPP-Spezifikationen wird diese Entwicklung aber überwiegend als Evolved Packet System (EPS) bezeichnet. Die EPS-Architektur repräsentiert eine prägnante Änderung sowohl der Radiotechnologie, als auch der Systemarchitektur. Insbesondere das neue Funknetz, welches als Evolved Universal Terrestrial Access Network (E-UTRAN) bezeichnet wird, wurde in diesem Kontext erheblich verändert.

Das Evolved Packet Core (EPC) führt netzwerkbezogene Funktionen durch, wie z.B. Authentication, Address Management, Inter-Network Mobility und Inter-Operator Mobility. Es ermöglicht den Betrieb und die Koordination verschiedener Funknetze, um Mobilität, Handover und Roaming zwischen den Teilnehmern zu ermöglichen.

Die EPS-Architektur verwendet Protokolle, die sowohl von der Internet Engineering Task Force (IETF) als auch von der 3GPP definiert wurden. Daher basieren alle Protokolle auf der IP-Transportschicht. Ferner sind in der Architektur die Schnittstellen zwischen den einzelnen EPS-Komponenten als Referenzschnittstellen standardisiert. Zur besseren Differenzierung der Protokolle gruppiert man diese entsprechend ihrer Funktionen in User Plane, Control Plane und Management Plane. Die Protokolle in der User Plane gewährleisten den Transport der Teilnehmerdaten bzw. -bezogene Informationen wie z.B. Sprache oder Filetransfer. Die Control Plane besteht aus Protokollen zur Steuerung und Kontrolle der Netzwerkressourcen sowie zur Unterstützung der Funktionen in der User Plane. Die Management Plane ist für den ordnungsgemäßen Betrieb und auch für die Überwachung der Netzwerkelemente verantwortlich.

Das EPC wird durch folgende fünf Komponenten abgebildet:

a. Mobility Management Entity (MME)
b. Serving Gateway (S-GW)
c. PDN Gateway (P-GW)
d. Home Subscriber Server (HSS)
e. Policy and Charging Rules Function (PCRF)

E-UTRAN und EPC zusammen bilden das Evloved Packet System (EPS). EPS basiert vollständig auf IP und bildet eine flache Netzwerkstruktur ab. Abb. 1 verdeutlicht die EPS-

Architektur mit den standardisierten Referenzschnittstellen und – unterhalb dieser – das jeweilige Protokoll in Klammern. Der Control-Plane-Verkehr ist gestrichelt dargestellt. Die Management Plane ist hier nicht berücksichtigt, da es sich lediglich um einen IP-Flow von der Management-Station MME zu den entsprechenden Komponenten handelt.

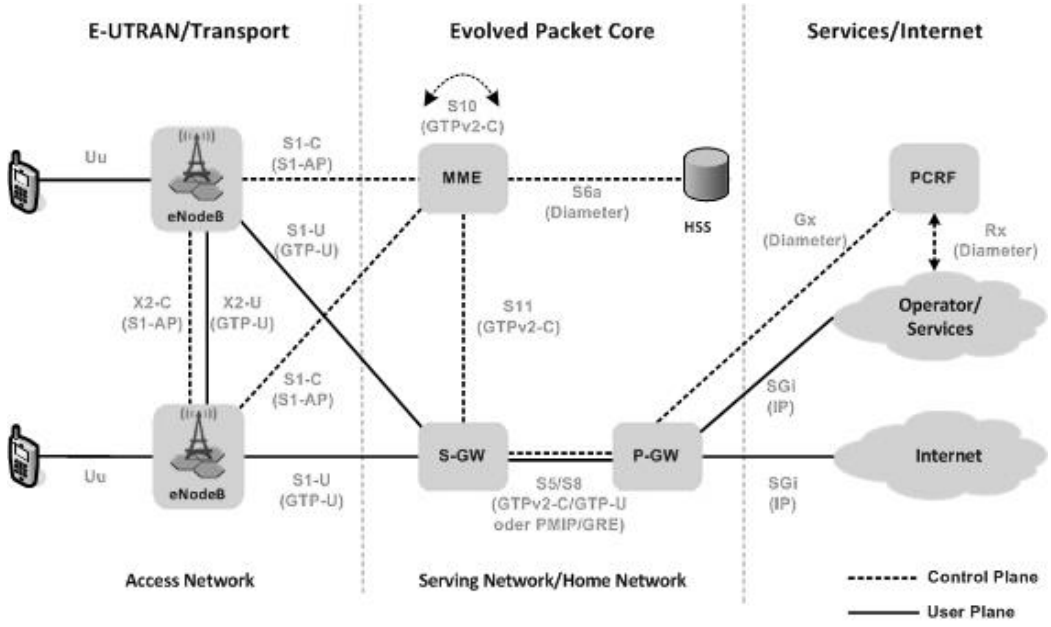

Abb. 1: EPS-Architektur

MME terminiert die EPC Control Plane und übernimmt Aufgaben der Signalisierung sowie die Verbindung zu anderen Funknetzen wie z.B. GSM und UMTS. Zusätzlich dient sie mit Hilfe des HSS der Authentifizierung des UE. Für das UE sind fünf verschiedene Geräteklassen vorgesehen, die zwischen 10 und 300 MBit/s angesiedelt sind. Meistens werden allerdings die Klasse 3 oder 4 verwendet, die 100-150 MBit/s Downlink, 50 MBit/s Uplink und die Nutzung von zwei Antennen beinhalten. P-GW und S-GW transportieren den User-Plane-Datenverkehr im EPC. P-GW stellt dabei das Bindeglied zwischen Internet und LTE-Netz dar. Zusätzlich ist es für die Vergabe von IP-Adressen für das UE zuständig. S-GW nimmt, neben der Weiterleitung von Nutzdaten, auch den Wechsel von GTP (eNodeB) zu IP (P-GW) vor und erstellt neue Tunnel für den Verbindungsaufbau. eNodeB (envolved NodeB) ist das Bindeglied zwischen UE und MME und daher für das Teilnehmer-Management, die Aufteilung der Ressourcen sowie das Interferenz-Management zuständig. PCRF erlaubt eine Implementierung von netzwerkbasierten Policys wie z.B. Bandbreitensteuerung oder QoS-basierte Premiumdiensten.

Der Home Subscriber Server (HSS) ist die Datenbank, in der Benutzer- und Abonnementinformationen gespeichert werden, die man für die Behandlung der Anrufe benötigt. Dazu gehören beispielsweise die Identifikation oder die Zugangsautorisierung der Teilnehmer. Der Server ist mit der MME direkt verbunden.

2 Sicherheitsarchitektur bei LTE

Zur besseren Transparenz und zur Differenzierung der unterschlichen EPS-Sicherheitsmerkmale unterteilt 3GPP TS 33.401 [TS33.401] die EPS-Sicherheitsarchitektur in vier Security Domains, die im Folgenden kurz erläutert werden: Network Access Security, Network Domain Security, User Domain Security und Application Security (siehe Abb. 2).

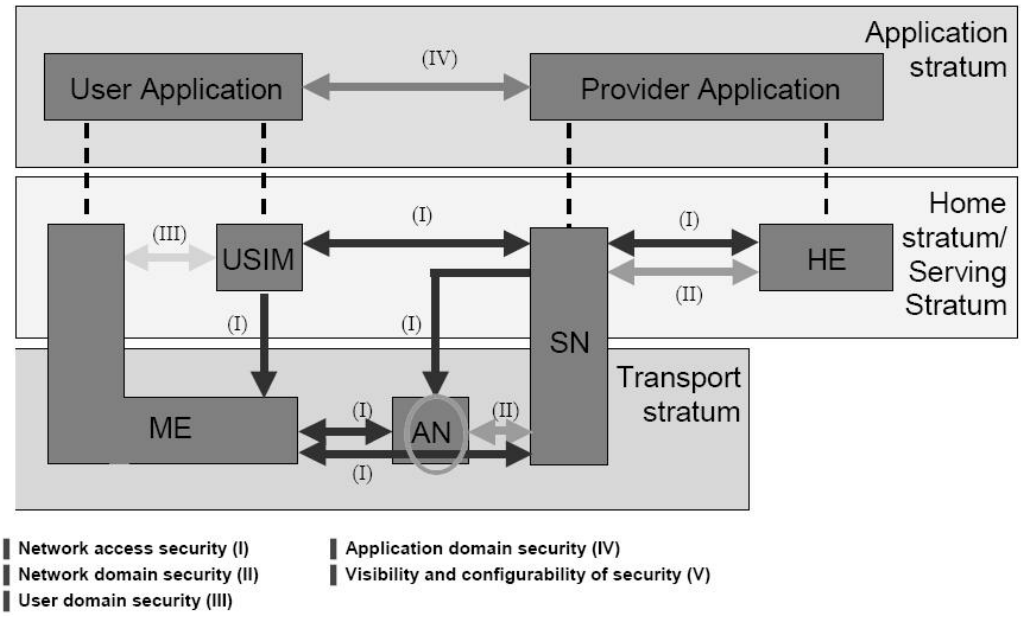

Abb. 2: EPS Security Domains

Jede Domain kann sowohl unterschiedliches Bedrohungspotential als auch sicherheitsrelevante Maßnahmen zur Risikoreduzierung aufweisen.

2.1 Network Access Security

Hier werden alle Funktionen bzw. Sicherheitsmerkmale zusammengefasst, die dem Teilnehmer einen sicheren Zugang zum EPS-Netzwerk gewährleisten. Er schützt die Daten der User Plane über die Luftschnittstelle und den Mobilfunkprovider vor nicht-autorisierter sowie betrügerischer Nutzung des Mobilfunknetzes.

Im Wesentlichen umfasst diese Domain folgende Merkmale:

a. *Beidseitige Authentifizierung zwischen Endgerät und Netzwerk:* Hierdurch kann das EPS-Netzwerk einen kontrollierten Zugriff auf Netzwerkdienste bereitstellen. Endgeräte mit falschen oder betrügerischen Netzwerkelementen haben keinen Zugang. Die Authentifizierung erfolgt zwischen Endgerät und HSS über die MME.
b. *Vertraulichkeits- und Integritätsschutz der Nachrichten der Control Plane und User Plane:* Es erfolgt eine dedizierte Verschlüsselung der Nachrichten in der User Plane und Control Plane. Darüber hinaus ist ein Integritätsschutz der Nachrichten in der Control Plane gegeben, wobei zwischen Signalisierungsdaten in den Funktionsschichten Non Access Stratum (NAS) und Access Stratum (AS) differenziert wird. Beide Signalisierungsschnittstellen terminieren in unterschiedlichen Sicherheitszonen (MME und BS).
c. *Schlüsselgenerierung und Schlüsselverwaltung:* Es werden dynamische Schlüssel generiert und aktualisiert, wobei – abhängig vom Sicherheitsziel und der Terminierung der Schnittstelle – unterschiedliche Schlüssel eingesetzt werden. Dies gewährleistet eine größere Robustheit und Flexibilität, führt jedoch gleichzeitig zu einer komplexeren Schlüsselhierarchie.
d. *Vertraulichkeit der Benutzer- und Geräteidentität:* Die Teilnehmeridentitäten werden ebenfalls dynamisch generiert und einem Endgerät vorübergehend zugewiesen. Die entsprechende Zuweisung erfolgt im Rahmen der Netzwerkregistrierung und ist für den Teilnehmer transparent. Die Verwendung von temporären Identitäten verringert das Risiko, dass personenbezogene Identitäten kompromittiert werden können.

2.2 Network Domain Security

Da sich mobile Netzwerke aus unterschiedlichen Netzkomponenten zusammensetzen unterstützt die EPS-Architektur unterschiedliche Zugangstechnologien. Die resultierenden Komponenten werden in unterschiedlichen Sicherheitszonen implementiert. Jedoch kommunizieren sie untereinander in der Regel über unsichere Transportnetze.

Aufgrund des flachen IP-basierten Netzwerks kommunizieren die E-UTRAN-Komponenten direkt und ohne vorherige Authentifizierung mit dem EPC. Die EPS Network Access Domain implementiert die NAS- und AS-Sicherheitsebene. Letztere terminiert in der Base Station (BS)

und schützt die Nachrichten der User Plane und Control Plane während der Übertragung über die Luftschnittstelle. Die NAS-Sicherheitsebene terminiert in der MME und schützt die Nachrichten zwischen Endgerät und MME in der Control Plane. Die Nachrichten in der User Plane und Control Plane zwischen der BS und dem EPC werden durch die Network-Access-Sicherheitsmerkmale hingegen nicht geschützt. Schlüsselmaterial oder Signalisierungsnachrichten zwischen BS und MME werden über das S1-Application-Protokoll S1-AP (siehe Abb. 1) übertragen. Die Kommunikation zwischen den dezentralen E-UTRAN-Komponenten mit dem zentralen EPC erfolgt über Transportnetze, die jedoch in der Regel auf unsicheren Richtfunkverbindungen oder Mietleitungen basieren.

Aufgrund der flachen IP-basierten Netzwerkarchitektur und der unzureichenden Zugangssteuerung an eNodeB-Punkten (siehe Abb. 1) besteht ein zusätzliches Bedrohungspotential sowohl für den Mobilfunk-Provider, als auch in Sachen Vertraulichkeit und Integrität von Ende-zu-Ende-Verbindungen. Um die Sicherheit des Übertragungsweges zu gewährleisten, müssen daher zusätzliche sicherheitsrelevante Maßnahmen implementiert werden. Vor diesem Hintergrund ist die primäre Aufgabe der Network Domain Security, die Sicherung der Netzwerkschnittstellen zu anderen Bereichen. Gleichzeitig werden Zugangskomponenten authentifiziert, bevor der Zugang auf EPC-Ressourcen erlaubt wird. Mit dieser Maßnahme können dann Netzwerkkomponenten vor netzwerkbasierten Angriffen geschützt werden.

2.3 User Domain Security

Die User Domain Security definiert Funktionen, die den sicheren Zugriff auf Endgeräte sicherstellen. Hier können Leistungsmerkmale wie z.B. PIN-Schutz oder kompliziertere 2-Faktor-Authentifizierung subsummiert werden.

2.4 Application Security

Unter Application Security werden Leistungsmerkmale bezeichnet, die eine Ende-zu-Ende-Sicherheit zwischen Endgerät und Anwendung realisieren. Im Wesentlichen wird dieser Bereich von den Sicherheitsfunktionen der entsprechenden Anwendung geprägt und ist entsprechend Applikationsspezifisch. Dieser Bereich ist mehr oder weniger transparent für das Evolved Packet System (EPS).

3 Bewertung der EPS Sicherheitsarchitektur

Insgesamt ist festzuhalten, dass die EPS-Architektur ein sicheres Zugriffs- und Transport-Rahmenwerk für die Unterstützung der Ende-zu-Ende-Sicherheit von LTE-Datenströmen abbildet. Im Folgenden werden die Sicherheitsparameter, die Ende-zu-Ende-Sicherheit und die Schlüsselarchitektur abschließend einer Bewertung unterzogen.

3.1 Sicherheitsparameter

Die Prozedur Evolved Packet System Authentication and Key Agreement (EPS-AKA) realisiert eine sichere beidseitige Authentifizierung. Die tiefe Schlüsselhierarchie, verbunden mit der Backward Key Separation, gewährleistet den Schutz des gemeinsamen Masters Key und realisiert die Key Separation. Die dynamische Schlüsselgenerierung in Verbindung mit der Forward Key Separation realisiert zudem eine zielgerichtete und unabhängige Erneuerung der entsprechenden Schlüssel. Datenströme werden zwischen Endgerät und Serving Gateway (S-GW) geschützt übertragen. Darüber hinaus werden die Benutzer- und TE-Identitäten geschützt. Die Länge der symmetrischen Schlüssel beträgt 128 Bit und gewährleistet gegenwärtig einen ausreichenden Vertraulichkeits- sowie Integritätsschutz und bietet bei Bedarf zukünftig die Vergrößerung auf 256 Bit. Ferner wurde die Aushandlung der Integritäts- und Verschlüsselungsalgorithmen dynamisch ausgelegt, so dass in Zukunft weitere Algorithmen relativ einfach integriert werden können. In diesem Zusammenhang wurden auch bereits weitere Algorithmen spezifiziert (EPS Encryption Algorithm 3 (EEA3) bzw. als EPS Integrity Algorithm 3 (EIA3) und sind in der technischen Spezifikation [TS35.221, 2011] beschrieben. Die EPS-Sicherheitsarchitektur ist ferner unabhängig vom verwendeten IP-Protokoll der User Plane.

Die Integration von IPv6 eine große Herausforderung für die Provider dar, insbesondere im sicherheitstechnischen Kontext, auch weil IPv6 parallel zu IPv4 anfangs betrieben werden muss. Aufgrund des Point-to-Point-Linkmodells (beinhaltet pro Station einen IPv6-Präfix) und der Verschlüsselung der Signalisierungsnachrichten zwischen Endgerät und MME, können in der EPS-Architektur viele IPv6-Neighbor-Discovery-bezogene Angriffe entschärft werden. Jedoch ist das Endgerät weiterhin durch netzwerkbasierte Angriffe verwundbar (z.B. Phishing, DoS, Unauthorized Access, Eavesdropping, SPIT).

3.2 Ende-zu-Ende-Sicherheit

Der Vertraulichkeitsschutz der Nachrichten in der User Plane zwischen Endgerät und BS wird in der PDCP-Schicht bereitgestellt. Auf der Transportschicht erfolgt der Schutz der User-Plane-Daten in der IP-Schicht auf Basis von IPsec, was inhärent mittels IPv6 erfolgt.

Eine Ende-zu-Ende-Sicherheit ist bei der EPS-Sicherheitsarchitektur durch die Kombination von Network Domain Security und Network Access Security möglich. Hierdurch ergibt sich ein signifikanter Schutz der Nachrichten in der Control Plane, User Plane und Management Plane. Signalisierungsdaten zwischen Endgerät und MME werden durch das NAS-Protokoll und zwischen Endgerät und BS durch die AS-Sicherheitsebene innerhalb der PDCP-Schicht geschützt. Der Schutz der S1-Application-Protokoll-Signalisierungsdaten erfolgt auf IP-Ebene und wird durch IPsec realisiert. Alle Signalisierungsdaten gemeinsam erfahren einen Integritäts-, einen Vertraulichkeits- und einen Replay-Schutz. Abb. 3 stellt die Sicherheit der EPS Control Plane in Abhängigkeit von der entsprechenden Domain dar, die die Schutzfunktion ausübt.

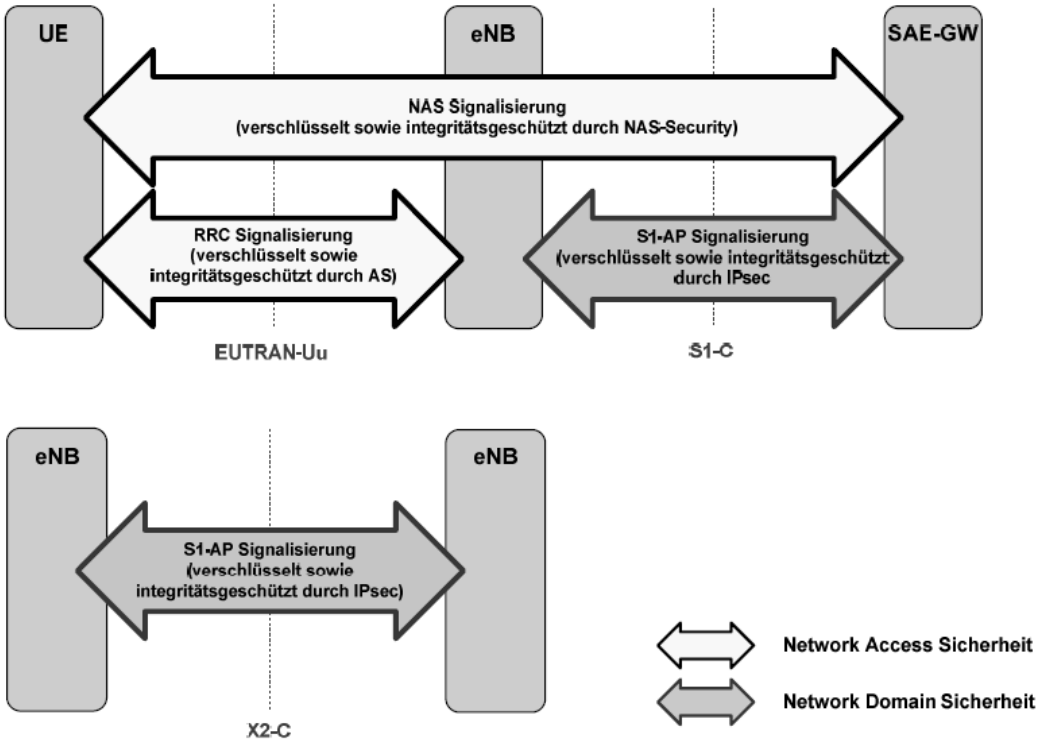

Abb. 3: Sicherheit der EPS Control Plane

Die EPS-Sicherheitsarchitektur bietet folgende Sicherheitsmerkmale, um den Schutz von Ende-zu-Ende-Verkehrsströmen innerhalb der EPS-Domain zu gewährleisten:

a. Beidseitige Authentifizierung zwischen Endgerät und Netzwerk
b. Neue, tiefere Schlüsselhierarchie
c. Integrität der Signalisierungsnachrichten
d. Vertraulichkeit der User- und Signalisierungsdaten
e. Vertraulichkeit der Benutzer- und Endgeräteidentitäten
f. Plattformsicherheit der eNodeB
g. Network Domain Security mit IPsec
h. Schlüsselseparierung

3.3 Schlüsselarchitektur

Die 3GPP hat mit der EPS-Architektur die Sicherheitsarchitektur signifikant verbessert. Dieses resultiert aus einem mehrschichtigen Ansatz, kombiniert mit der neuen und tieferen Schlüsselarchitektur. Abhängig von der Sicherheitsklassifizierung und dem Terminierungspunkt wurden zwei Sicherheitsebenen spezifiziert. Die erste Ebene (AS) terminiert in der BS, da sie dezentral in der Fläche installiert und in der Regel unzureichend geschützt ist. Daher ist von der BS das größte Gefährdungspotential zu erwarten. Die zweite Sicherheitsebene (NAS) terminiert im EPC an der MME. Diese Architekturänderungen spiegeln sich in der EPS-Schlüsselhierarchie wider. Für jede Sicherheitsebene werden temporäre Local Master Keys, d.h. K_{ASME} (Key for Access Security Management Entity) für die NAS und K_{eNB} (Key for Evolved Node B) für die AS-Sicherheitsebene generiert. Diese Master Keys dienen als Basismaterial für die Generierung der entsprechenden Integritäts- sowie Verschlüsselungsschlüssel der jeweiligen Sicherheitsebene. Eine weitere sicherheitstechnische Verbesserung ist die hierarchische Klassifizierung der Schlüssel in Abhängigkeit vom Terminierungspunkt und vom Anwendungskontext.

Die tiefere EPS-Schlüsselhierarchie stellt gewisse Ansprüche an das Schlüsselmanagement. Insbesondere im Rahmen der Handover-Prozeduren müssen kryptographisch unterschiedliche Schlüssel zielgerichtet generiert und übertragen werden. Die größte Bedrohung ist in diesem Zusammenhang die Kompromittierung der Schlüssel. Insbesondere der Schlüsseltransfer K_{eNB} zur BS birgt in diesem Kontext das größte Gefährdungspotenzial. Um dem vorzubeugen verwendet die EPS-Architektur eine erweiterte Schlüsselhierarchie, sodass eine Schlüsseltrennung (Key Separation) auch auf unterschiedlichen Schlüsselhierarchieebenen

gewährleistet wird. Durch die Verwendung einer Hash-Funktion als Schlüsselgenerierungsfunktion (KDF) wird in Verbindung mit unterschiedlichen Eingangsparametern sowohl eine Backward-, als auch (mit bestimmten Einschränkungen) eine Forward-Key-Separation realisiert. Die Backward-Key-Separation in Verbindung mit der tiefen Schlüsselhierarchie schützt das Eingangsschlüsselmaterial, jedoch insbesondere den gemeinsamen Master Schlüssel K, den sich Netzwerk und USIM teilen. Sicherheitstechnisch bedeutet dies eine signifikante Verbesserung im Vergleich zu UMTS.

Im Detail werden folgende sicherheitsrelevanten Maßnahmen im Rahmen der EPS-Schlüsselgenerierung berücksichtigt:

a. Schlüsseltrennung zwischen Endgeräten
b. Schlüsseltrennung zwischen den BS
c. Schlüsseltrennung zwischen den NAS- und AS-Sicherheitsebenen
d. Schlüsseltrennung zwischen Control Plane und User Plane
e. Schlüsseltrennung zwischen den Algorithmen (z.B. HMAC-SHA-256)
f. Schlüsseltrennung zwischen Integritäts- und Verschlüsselungsschlüssel
g. Schlüsseltrennung zwischen den unterschiedlichen Zugangstechnologien
h. Schlüsseltrennung zwischen unterschiedlichen Mobilfunkprovidern

4 Fazit

Die EPS-Entwicklung schreitet immer weiter voran. Bei den aktuellen EPS-Netzwerken handelt es sich um die Release 8. Das Release 10 wird als LTE-Advanced bezeichnet und unterstützt höhere Übertragungsbandbreiten und geringere Latenzzeiten. LTE-Advanced erfüllt die IMT[1]-Advanced-Anforderungen der International Telecommunication Union (ITU). Es ist daher die erste Mobilfunktechnologie, die die Anforderungen der 4. Mobilfunkgeneration komplett erfüllt (u.a. mobile Datenraten von bis zu 100 MBit/s oder 1 GBit/s bei gelegentlichem Ortswechsel). Diese sind bereits im Jahre 2008 beschrieben worden [IMT2008].

[1] International Mobile Telecommunications: definiert die Anforderungen an ein Mobilfunksystem für die ITU-R; IMT Advanced beinhaltet ein Konzept zur Gestaltung des Mobilfunknetzes der vierten Generation (4G)

Aufgrund des kontinuierlichen Wachstums werden Mobilfunkprovider zeitnah gezwungen sein, IPv6 einzufügen. Aus Sicht der Mobilfunkprovider ist die Dual-Stack-Methode die bevorzugte Übergangslösung. Diese Methode sorgt für einen sanften IPv6-Übergang. Im Laufe der Zeit werden immer mehr Services und Dienstleistungen in die IPv6-Domain migriert, so dass die Akzeptanz des IPv6-Protokolls wachsen wird. Nach Beseitigung der ersten Anlaufschwierigkeiten kann IPv6 seine Vorteile, nämlich transparente Ende-zu-Ende Kommunikation, effiziente Übertragung und Autokonfiguration voll ausspielen.

Aufgrund der höheren Bandbreite entwickelt sich LTE zu einer echten Alternative zu Festnetzanschlüssen. Die Sicherheit von Ende-zu-Ende-Datenströmen wird zunehmend durch IPsec realisiert. In diesem Zusammenhang wird der Bedarf an Zertifikat-basierter Authentifizierung steigen.

Abschließend bleibt festzuhalten, dass LTE-basierte Netze per se mehr Sicherheitsmechanismen anbieten, als dies bei den Vorgängern der zweiten und dritten Mobilfunkgeneration der Fall war. Allerdings hat man sich dieses Mal auch komplett auf IP-basierte Netzkommunikation verständigt, so dass es Angreifern leichter fallen wird, mögliche Schwachstellen auszunutzen. Dies liegt zum einen an dem allgemeinen Wissen über IP-Netze, welches im Gegensatz zu TDM- oder ATM-basierten Netzen stärker vertreten ist, und zum anderen an den Sicherheitsproblemen der IPv4- und IPv6-Protokolle. Zudem wird es eine höhere Anzahl kleinerer Funkzellen als in 3G-Netzen geben, die nicht gleichermaßen sicherheitstechnisch überwacht werden können. Bei einer erfolgreichen Zellenattacke kann ein Angreifer dann direkt auf das LTE-Kernnetz zugreifen, weil der Radio Resource Controller durch den eNodeB und die MME verwaltet wird. Auch etabliert das LTE-Netz mehr Signalisierungs- und Trägerverbindungen zwischen verschiedenen Netzelementen als dies in 3G-Netzen der Fall ist. Dadurch kann man bei einem erfolgreichen Angriff viel mehr Netzknoten erreichen und penetrieren. Auch enden die verschlüsselten Teilnehmerdaten im eNodeB, wodurch die Anbindung an übergeordnete Netzknoten zum ersten Mal ein gewisses Sicherheitsrisiko beinhalten kann. IPsec ist in der Lage, hier entsprechende Abhilfe zu schaffen. Jedoch wird auch die Netzlast erhöht und die Skalierbarkeit verschlechtert. Daher werden zukünftig spezielle Security Gateways notwendig sein, um die notwendige Performance, Skalierbarkeit, Verfügbarkeit und Kompatibilität zu den aktuellsten 3GPP-Sicherheitsstandards schaffen zu können. [DONE2011]

Quellen

[DONE2011] Patrick Donegan: *IPsec Deployment Strategies for Securing LTE Networks*. Whitepaper of Heavy Reading on behalf of RadiSys, May 2011

[PRAS2011] Anand R. Prasad: *3GPP SAE/LTE Security*. NIKSUN WWSMC presentation in Princeton, 25.-27. July, NEC, USA 2011

[IMT2008] ITU-Pressemitteilung: *IMT-Advanced standards announced for next-generation mobile technology*. abgerufen am 14. August 2013, URL-Adresse: http://www.itu.int/net/pressoffice/press_releases/2012/02.aspx#.Ugt3dZL0HZY

[ITU-R2008] ITU-R Report M.2134: *Requirements related to technical performance for IMT-Advanced radio interface(s)*. Report ITU-R M.2134, 2008

[SAFA2011] Fataneh Safavieh: *Long Term Evolution and its security infrastructure*. Mobile Security Seminar, University of Bonn, 07. February 2011

[SCHN2012] Peter Schneider: *How to secure an LTE-network: just applying in the 3GPP security standards and that's it?* Telco Security Day at Troppers 2012, Nokia Siemens Networks Research, 2012

[TS33.401] 3rd Generation Partnership Project: *3GPP System Architecture Evolution (SAE)*. Security Architecture (Release 10), 2011

[TS35.221] 3rd Generation Partnership Project: *Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2*. Document 1: UEA2 and UIA2 Specifications (Release 10), 2011