Evolutionsfrage

Ist LTE sicherer als seine Vorgänger?

Evren Eren, Kai-Oliver Detken

Die jüngste Mobilfunkgeneration Long Term Evolution (LTE) vervollständigt die Entwicklung hin zu einem angestrebten offenen Netzmodell. Gleichzeitig 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 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 Kernnetz Evolved Packet System.

Prof. Dr.-Ing. Evren Eren unterrichtet an der Fachhochschule Dortmund im Fachbereich Informatik,
Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

Das LTE zugrunde liegende Kernnetz wurde in den 3GPP-Spezifikationen überwiegend mit Evolved Packet System (EPS) bezeichnet. Die EPS-Architektur repräsentiert eine prägnante Änderung sowohl der Funktechnik als auch der Systemarchitektur. Insbesondere das neue Funknetz, das als Evolved Universal Terrestrial Access Network (E-UTRAN) bezeichnet wird, wurde in diesem Kontext erheblich verändert.

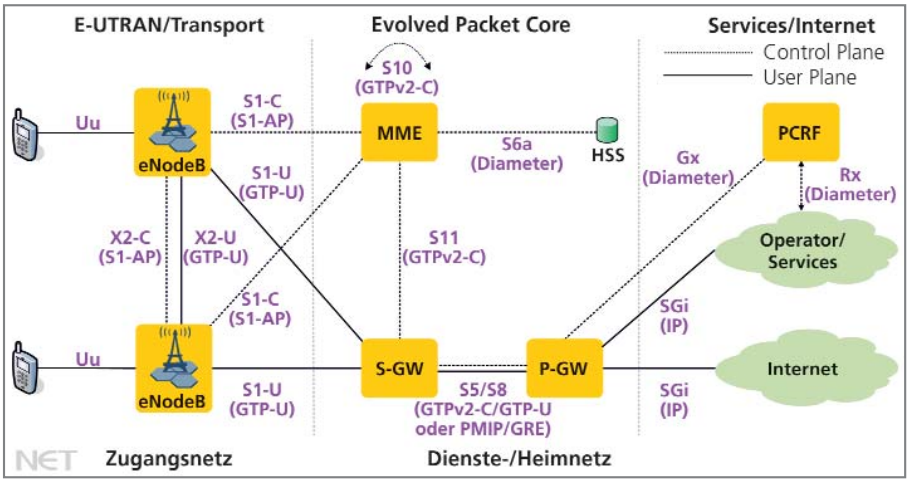

Bild 1: EPS-Architektur

Evolved Packet Core

Das Evolved Packet Core (EPC) führt netzbezogene Funktionen durch, wie z.B. Authentifizierung, Addressmanagement, Internetworking und Interoperator 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 und daher alle auf der IP-Transportschicht basieren. Ferner sind die Interfaces zwischen den einzelnen EPS-Komponenten als Referenzschnittstellen standardisiert. Zur besseren Differenzierung der Protokolle gruppiert man diese entsprechend ihrer Funktionen in User, Control 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 Netzressourcen sowie zur Unterstützung der Funktionen in der User Plane. Die Management Plane ist für den ordnungsgemäßen Betrieb und auch für die Überwachung der Netzelemente verantwortlich.
Das EPC wird durch fünf Komponenten abgebildet:

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

Bild 1 verdeutlicht die EPS-Architektur mit den standardisierten Referenzschnittstellen und den jeweiligen Protokollen. E-UTRAN und EPC zusammen bilden das Evolved Packet System (EPS). Es basiert vollständig auf dem Internetprotokoll (IP) und bildet eine flache Netzstruktur ab.

Die MME terminiert die EPC Control Plane und übernimmt Aufgaben der Signalisierung sowie die Verbindung zu anderen Funknetzen. Zusätzlich dient sie mit Hilfe des HSS der Authentifizierung des User Equipment (UE). Der HSS ist die Datenbank, in der Benutzer- und Abonnementinformationen gespeichert werden wie z.B. die Identifikation oder die Zugangsautorisierung der Teilnehmer. 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 bis 150 Mbit/s im Downlink, 50 Mbit/s im Uplink und die Nutzung von zwei Antennen beinhalten.

P-GW und S-GW transportieren den User-Plane-Datenverkehr im EPC. Ersteres stellt dabei das Bindeglied zwischen Internet und LTE-Netz dar und ist für die Vergabe von IP-Adressen für das UE zuständig. Das 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 ist das Bindeglied zwischen UE und MME und daher für das Teilnehmer- und Interferenzmanagement sowie die Aufteilung der Ressourcen zuständig. PCRF erlaubt eine Implementierung von netzbasierten Policys wie z.B. Bandbreitensteuerung oder QoS-basierte Premiumdienste.

Sicherheitsarchitektur bei LTE

Zur besseren Transparenz und zur Differenzierung der unterschiedlichen EPS-Sicherheitsmerkmale unterteilt das 3GPP die EPS-Sicherheitsarchitektur in vier Security Domains (*Bild 2*):

- Network Access Security;
- Network Domain Security;
- User Domain Security;
- Application Security.

Jede Domain kann sowohl unterschiedliches Bedrohungspotenzial als auch sicherheitsrelevante Maßnahmen zur Risikoreduzierung aufweisen. In der Network Access Security werden alle Funktionen bzw. Sicherheitsmerkmale zusammengefasst, die dem Teilnehmer einen sicheren Zugang zum EPS-Netz gewährleisten. Sie schützt die Daten der User Plane über die Luftschnittstelle und den Mobilfunk-Provider vor nichtautorisierter oder betrügerischer Nutzung des Mobilfunknetzes. Folgende Sicherheitsmerkmale umfasst daher diese Domain:

- beidseitige Authentifizierung zwischen Endgerät und Netz;
- Vertraulichkeits- und Integritätsschutz der Nachrichten der Control/User Plane;
- dynamische Schlüsselgenerierung und -verwaltung;
- Vertraulichkeit der Benutzer- und Geräteidentität.

Da sich mobile Netze aus diversen Netzkomponenten zusammensetzen, unterstützt die EPS-Architektur unterschiedliche Zugangstechniken. Die resultierenden Komponenten werden in verschiedenen Sicherheitszonen implementiert. Jedoch kommunizieren sie untereinander in der Regel über unsichere Transportnetze.

Aufgrund des flachen IP-basierten Net-zes kommunizieren die E-UTRAN-Komponenten direkt und ohne vorherige Authentifizierung mit dem EPC. Die Network Access Security enthält die Sicherheitsebenen Non Access Stratum (NAS) und Access Stratum (AS). Letztere terminiert in der Basisstation (BS) und schützt die Nachrichten der User und Control Plane während der Übertragung über die Luftschnittstelle. Die NAS-Sicherheitsebene terminiert in der MME und schützt die Nachrichten zwischen UE und MME in der Control Plane. Die Nachrichten in der User 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 übertragen.

Zudem besteht ein zusätzliches Bedrohungspotenzial sowohl für den Mobilfunk-Provider als auch in Sachen Vertraulichkeit und Integrität von Ende-zu-Ende-Verbindungen aufgrund der flachen IP-basierten Netzarchitektur und der unzureichenden Zugangssteuerung an eNodeB-Punkten. Um die Sicherheit des Übertragungsweges trotzdem zu gewährleisten, müssen daher zusätzliche sicherheitsrelevante Maßnahmen implementiert werden. Vor diesem Hintergrund ist die primäre Aufgabe der Network Domain Security die Sicherung der Netzschnittstellen zu anderen Bereichen. Gleichzeitig werden Zugangskomponenten authentifiziert, bevor der Zugang auf EPC-Ressourcen erlaubt wird, so dass Netzkomponenten vor netzbasierten Angriffen geschützt sind.

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

Mit Application Security werden Leistungsmerkmale bezeichnet, die eine Ende-zu-Ende-Sicherheit zwischen UE und Anwendung realisieren. Im Wesentlichen wird dieser Bereich von den Sicherheitsfunktionen der entsprechenden Anwendung geprägt. Dieser Bereich ist mehr oder weniger transparent für das EPS.

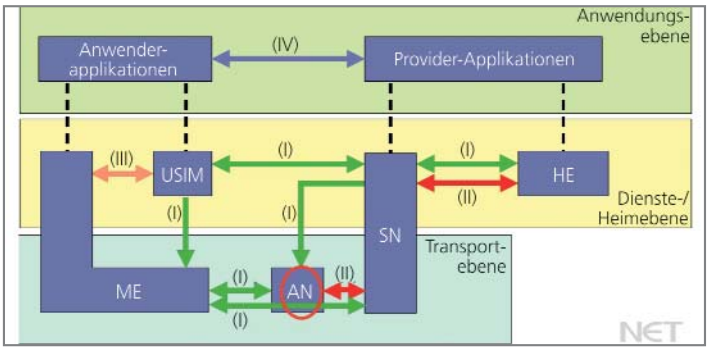

Bild 2: EPS Security-Domains
I – Network Access Security;
II – Network Domain Security;
III – User Domain Security;
IV – Application Domain Security;
V – Visibility and Configurability of Security

Bewertung der Sicherheitsmechanismen

Die EPS-Architektur bildet ein sicheres Zugriffs- und Transportrahmenwerk für die Unterstützung der Ende-zu-Ende-Sicherheit von LTE-Datenströmen ab. So ermöglicht die Prozedur Evolved Packet System Authentication and Key Agreement (EPS-AKA) eine sichere beidseitige Authentifizierung. Die tiefe Schlüsselhierarchie verbunden mit der Backward Key Separation gewährleistet den Schutz des gemeinsamen Master Keys 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 UE und S-Gateway geschützt übertragen. Darüber hinaus werden die Benutzer- und TE-Identitäten gesichert. Die Länge der symmetrischen Schlüssel beträgt 128 bit und gewährleistet gegenwärtig einen ausreichenden Vertraulichkeits- und Integritätsschutz. Bei Bedarf kann eine Vergrößerung auf 256 bit erfolgen. Ferner wurde die Aushandlung der Integritäts- und Verschlüsselungsalgorithmen dynamisch ausgelegt, so dass künftig weitere Algorithmen relativ einfach integriert werden können. Die EPS-Sicherheitsmechanismen sind ferner unabhängig vom verwendeten IP-Protokoll der User Plane.

Der Vertraulichkeitsschutz der Nachrichten in der User Plane zwischen UE und BS wird in der PDCP-Schicht bereitgestellt. Auf der Transportschicht erfolgt der Schutz der User-Plane-Daten in der IP-Schicht auf IPsec-Basis.

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, User und Management Plane. Signalisierungsdaten zwischen UE und MME werden durch das NAS-Protokoll und zwischen UE und BS durch die AS-Sicherheitsebene innerhalb der PDCP-Schicht geschützt. Der Schutz der S1-AP-Signalisierungsdaten erfolgt auf IP-Ebene und wird durch IPsec realisiert. Alle Signalisierungsdaten gemeinsam erfahren einen Integritäts-, einen Vertraulichkeits- und einen Replay-Schutz. *Bild 3* stellt die Sicherheit der EPS Control Plane in Abhängigkeit von der Domain dar, die die Schutzfunktion ausübt.

Die 3GPP hat mit der EPS-Architektur die Sicherheitsarchitektur signifikant verbessert. Dies 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 i.d.R. unzureichend geschützt ist. Auch ist von der BS das größte Gefährdungspotenzial 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. KASME (Key for Access Security Management Entity) für die NAS und KeNB (Key for Evolved Node B) für die AS-Sicherheitsebene generiert. Sie dienen als Basismaterial für die Generierung der ent-

sprechenden Integritäts- sowie Verschlüsselungsschlüssel der jeweiligen Sicherheitsebene. Eine weitere 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 müssen für die Handover-Prozeduren kryptographisch unterschiedliche Schlüssel zielgerichtet generiert und übertragen werden. Die größte Bedrohung ist in diesem Zusammenhang die Kompromittierung der Schlüssel, insbesondere der Schlüsseltransfer KeNB zur BS. Um dem vorzubeugen, verwendet die EPS-Architektur eine erweiterte Schlüsselhierarchie, so dass eine Key Separation auch auf unterschiedlichen Schlüsselhierarchieebenen gewährleistet ist.

Fazit

Mobilfunk-Provider sind gezwungen, zeitnah IPv6 einzuführen, so dass im Lauf der Zeit mehr Services in die IPv6-Domain migrieren werden. Die Vorteile von IPv6 sind eine transparente Ende-zu-Ende-Kommunikation, effiziente Übertragung und Autokonfiguration. Die Sicherheit von Ende-zu-Ende-Datenströmen wird zunehmend durch IPsec realisiert. In diesem Zusammenhang wird auch der Bedarf an zertifikatbasierter Authentifizierung steigen.

LTE-basierte Netze bieten per se mehr Sicherheitsmechanismen als ihre Vorgänger. Allerdings können Angreifer aufgrund der komplett IP-basierten Netzkommunikation leichter mögliche Schwachstellen ausnutzen. Zudem wird es mehr 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. Zusätzlich enden die verschlüsselten Teilnehmerdaten im eNodeB, wodurch die Anbindung an übergeordnete Netzknoten zum ersten Mal ein gewisses Sicherheitsrisiko darstellen kann.
IPsec ist in der Lage, Abhilfe zu schaffen. Jedoch wird auch die Netzlast erhöht, die Skalierbarkeit verschlechtert sich. Daher werden spezielle Security Gateways notwendig sein, um die nötige Performance, Skalierbarkeit, Verfügbarkeit und Kompatibilität zu den aktuellsten 3GPP-Sicherheitsstandards schaffen zu können. *(bk)*

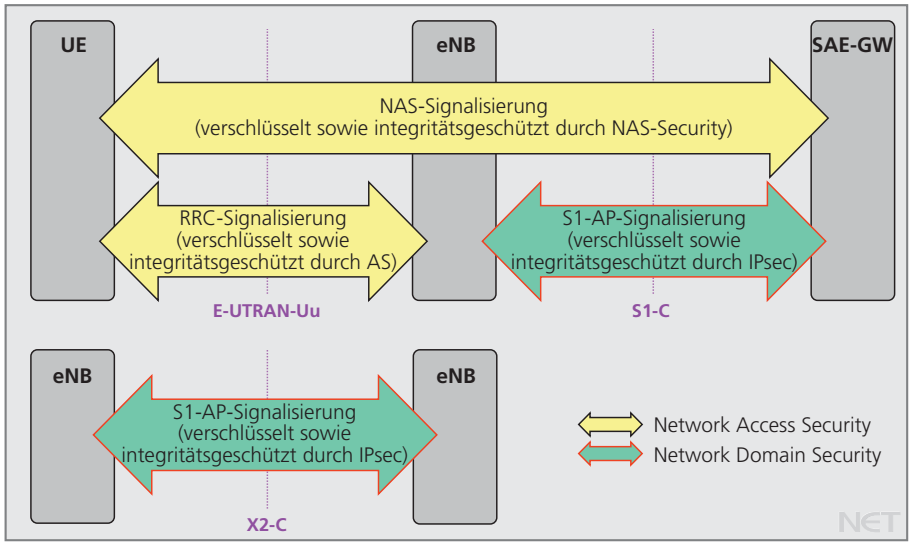

Bild 3: Sicherheit der EPS Control Plane