

10. WCI-Konferenz in Berlin



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



Prof- Dr.-Ing. Kai-Oliver Detken
DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
URL: <http://www.decoit.de>
E-Mail: detken@decoit.de

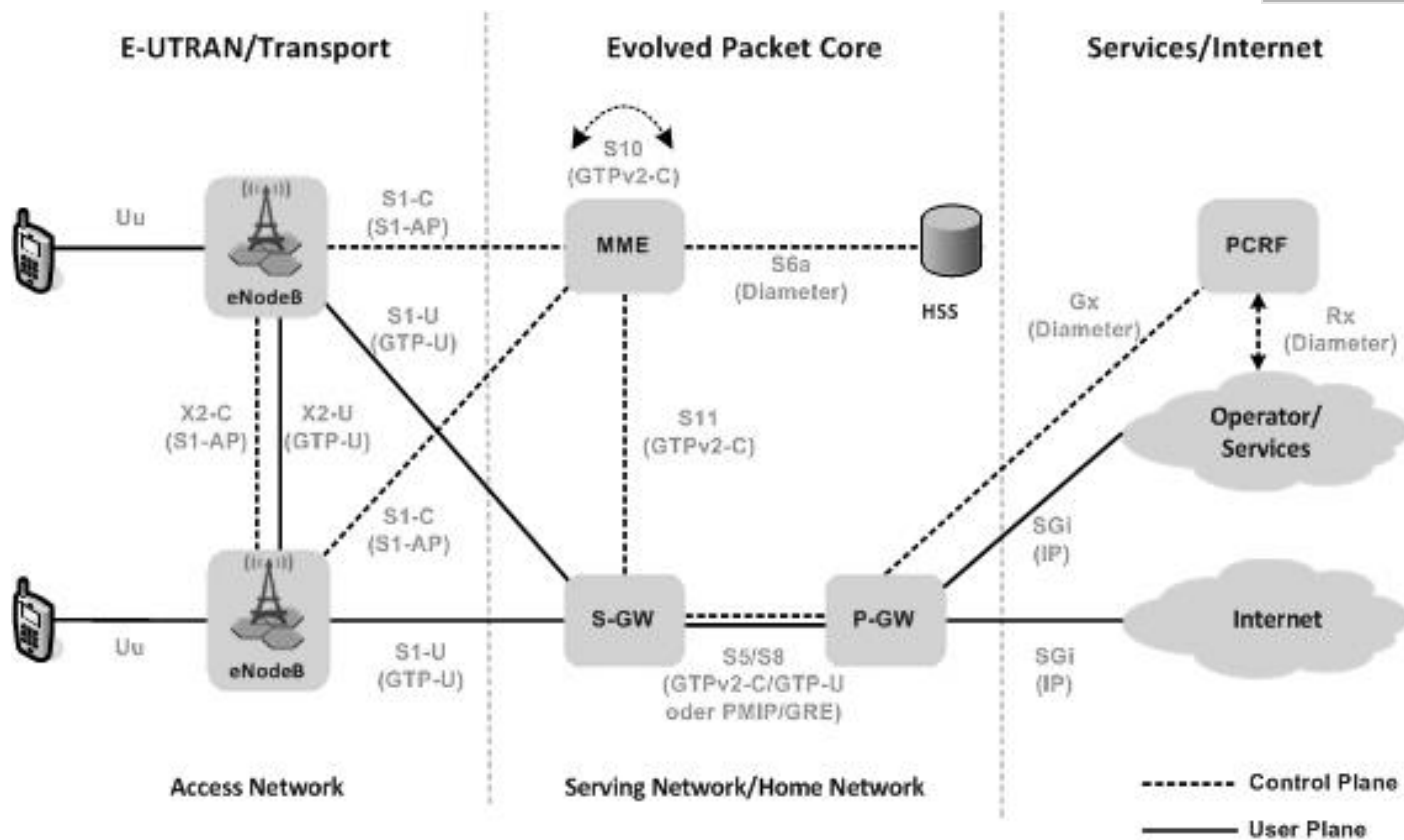
Inhalte

- ◆ Evolved Packet System (EPS)
- ◆ Sicherheitsarchitektur bei LTE
 - Network Access Security
 - Network Domain Security
 - User Domain Security
 - Application Security
- ◆ Bewertung der EPS Sicherheitsarchitektur
 - Sicherheitsparameter
 - Ende-zu-Ende-Sicherheit
 - Schlüsselarchitektur
- ◆ Fazit

Evolved Packet System (EPS)

- ◆ Die nächste Mobilfunkgeneration (4G) steht in den Startlöchern
- ◆ Umgangssprachlich wird sie als Long Term Evolution (LTE) bezeichnet; in den Spezifikationen ist allerdings von Evolved Packet System (EPS) die Rede
- ◆ Die EPS-Architektur repräsentiert eine prägnante Änderung sowohl der Radiotechnologie, als auch der Systemarchitektur
- ◆ Die Architektur verwendet Protokolle, die sowohl von der IETF, als auch von der 3GPP definiert wurden
- ◆ Alle Protokolle basieren daher auf der IP-Transportschicht
- ◆ Zur besseren Differenzierung der Protokolle gruppiert man diese entsprechend ihrer Funktionen in User Plane, Control Plane und Management Plane

EPS-Architektur (1)



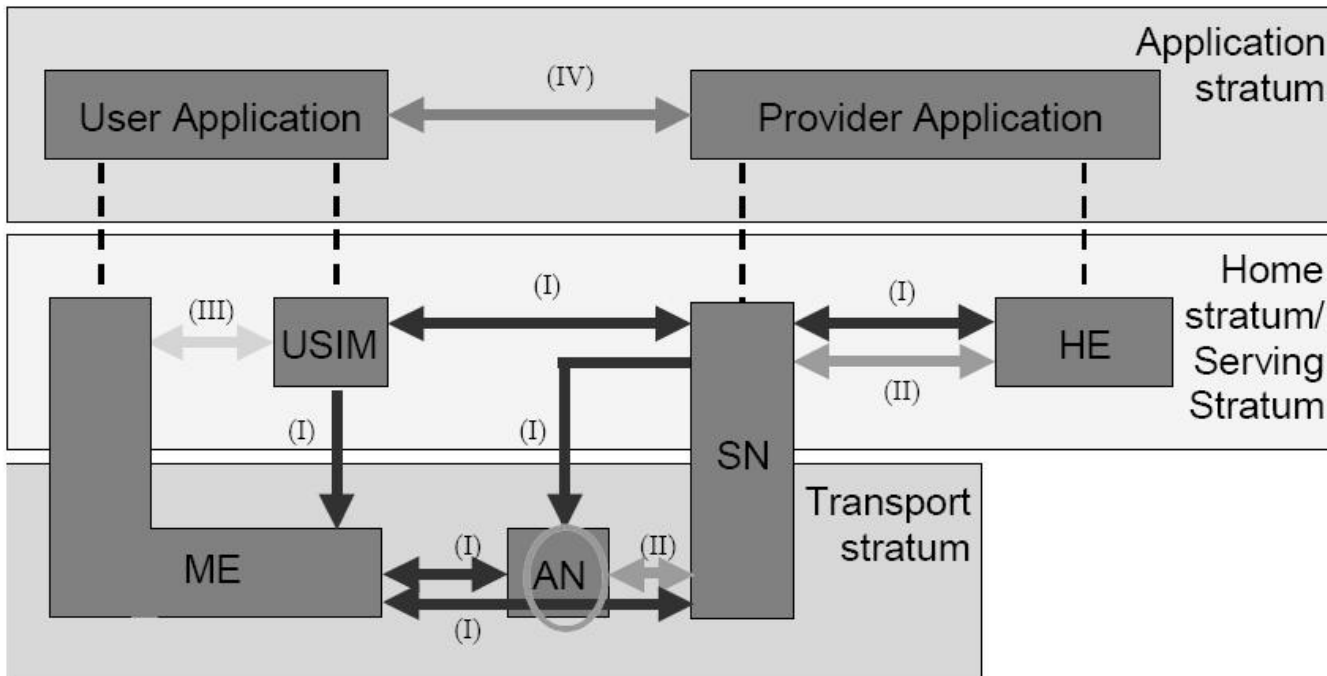
EPS-Architektur (2)

- ◆ Das EPC wird durch fünf Hauptkomponenten abgebildet:
 - Mobility Management Entity (MME)
 - Serving Gateway (S-GW)
 - PDN Gateway (P-GW)
 - Home Subscriber Server (HSS)
 - Policy and Charging Rules Function (PCRF)
- ◆ Das E-UTRAN-Funknetz und das EPC zusammen bilden das Evolved Packet System (EPS) ab
- ◆ MME terminiert die EPC Control Plane und übernimmt Aufgaben der Signalisierung sowie die Verbindung zu anderen Funknetzen wie z.B. GSM und UMTS
- ◆ Für das UE sind fünf verschiedene Geräteklassen vorgesehen, die zwischen 10 und 300 MBit/s angesiedelt sind

Sicherheitsarchitektur bei LTE

- ◆ Es werden vier Security Domains unterschieden:
 - Network Access Security
 - Network Domain Security
 - User Domain Security
 - Application Security
- ◆ Jede Domain kann sowohl unterschiedliches Bedrohungspotential, als auch sicherheitsrelevante Maßnahmen zur Risikoreduzierung aufweisen

EPS Security Domains



- █ Network access security (I)
- █ Network domain security (II)
- █ User domain security (III)
- █ Application domain security (IV)
- █ Visibility and configurability of security (V)

Network Access Security

- ◆ Es werden im Network Access Security alle Funktionen bzw. Sicherheitsmerkmale zusammengefasst, die dem Teilnehmer einen sicheren Zugang zum EPS-Netzwerk gewährleisten
- ◆ Sie 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:
 - Beidseitige Authentifizierung zwischen Endgerät und Netzwerk
 - Vertraulichkeits- und Integritätsschutz der Nachrichten der Control Plane und User Plane
 - Schlüsselgenerierung und Schlüsselverwaltung
 - Vertraulichkeit der Benutzer- und Geräteidentität

Network Domain Security (1)

- ◆ 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 Nachrichten in der User Plane und Control Plane zwischen der BS und dem EPC werden durch die Network-Access-Sicherheitsmerkmale nicht geschützt

Network Domain Security (2)

- ◆ Aufgrund der flachen IP-basierten Netzwerkarchitektur und der unzureichenden Zugangssteuerung an eNodeB-Punkten besteht ein zusätzliches Bedrohungspotential (für Provider und 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 netzwerkbasierteren Angriffen geschützt werden

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

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)

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
- ◆ Bewertet wurden dabei die folgenden Bereiche:
 - Sicherheitsparameter
 - Ende-zu-Ende-Sicherheit
 - Schlüsselarchitektur

Sicherheitsparameter (1)

- ◆ 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 kann auf 256 Bit erweitert werden

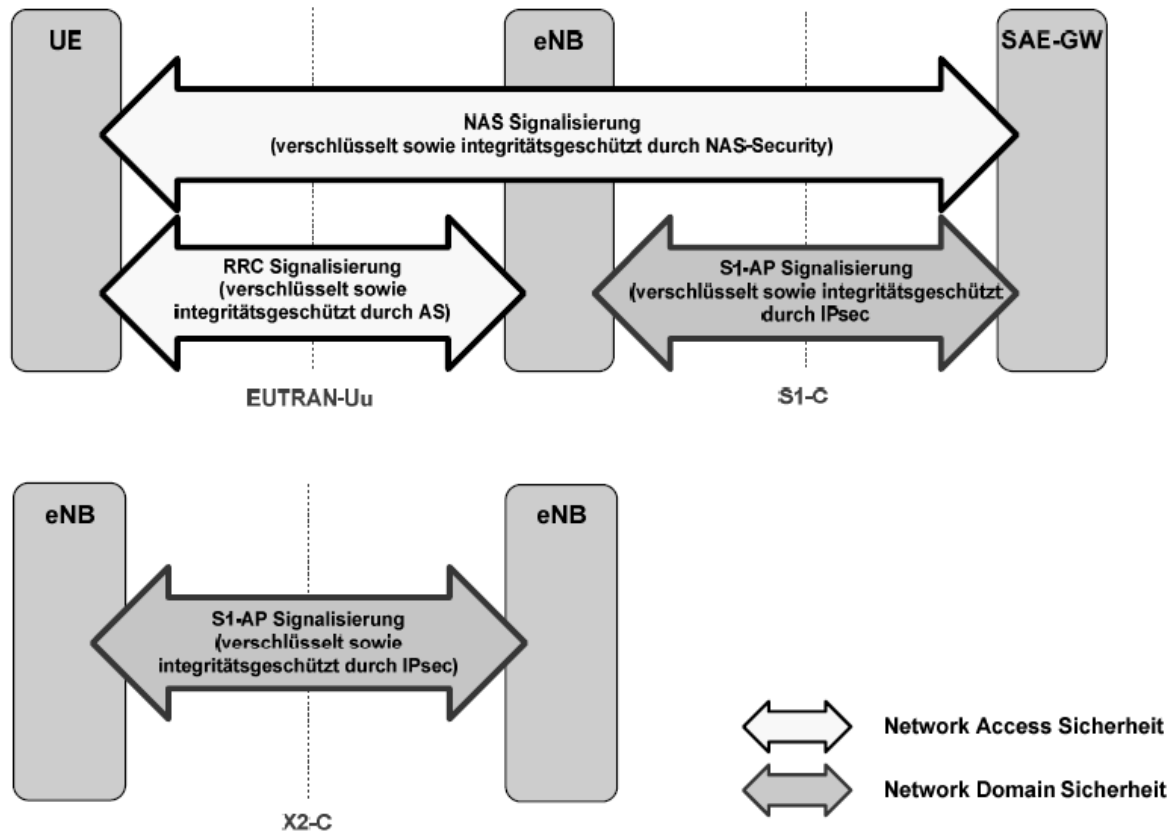
Sicherheitsparameter (2)

- ◆ Die EPS-Sicherheitsarchitektur ist ferner unabhängig vom verwendeten IP-Protokoll der User Plane
- ◆ Es kann also IPv6 genutzt werden, auch wenn dies eine gewisse Herausforderung für die Provider darstellt
- ◆ 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 netzwerkbasierende Angriffe verwundbar (z.B. Phishing, DoS, Unauthorized Access, Eavesdropping, SPIT)

Ende-zu-Ende-Sicherheit (1)

- ◆ 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
- ◆ Alle Signalisierungsdaten gemeinsam erfahren einen Integritäts-, einen Vertraulichkeits- und einen Replay-Schutz

Ende-zu-Ende-Sicherheit (2)



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
- ◆ Für jede Sicherheitsebene werden temporäre Local Master Keys 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

Fazit

- ◆ Aufgrund des kontinuierlichen Wachstums werden Mobilfunkprovider zeitnah gezwungen sein, IPv6 einzufügen
- ◆ Die Sicherheit von Ende-zu-Ende-Datenströmen wird zunehmend durch IPsec realisiert. In diesem Zusammenhang wird der Bedarf an Zertifikat-basierter Authentifizierung steigen
- ◆ LTE-basierte Netze bieten per se mehr Sicherheitsmechanismen an, als dies bei 2G und 3G 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
 - Zudem wird es eine höhere Anzahl kleinerer Funkzellen als in 3G-Netzen geben, die nicht gleichermaßen sicherheitstechnisch überwacht werden können
- ◆ IPsec ist in der Lage, hier entsprechende Abhilfe zu schaffen
- ◆ Dies geht zu Lasten der Performance und Skalierbarkeit, weshalb der Einsatz spezieller Security Gateways notwendig sein wird

Ende

Vielen Dank für ihre
Aufmerksamkeit



DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
Tel.: 0421-596064-0
Fax: 0421-596064-09