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

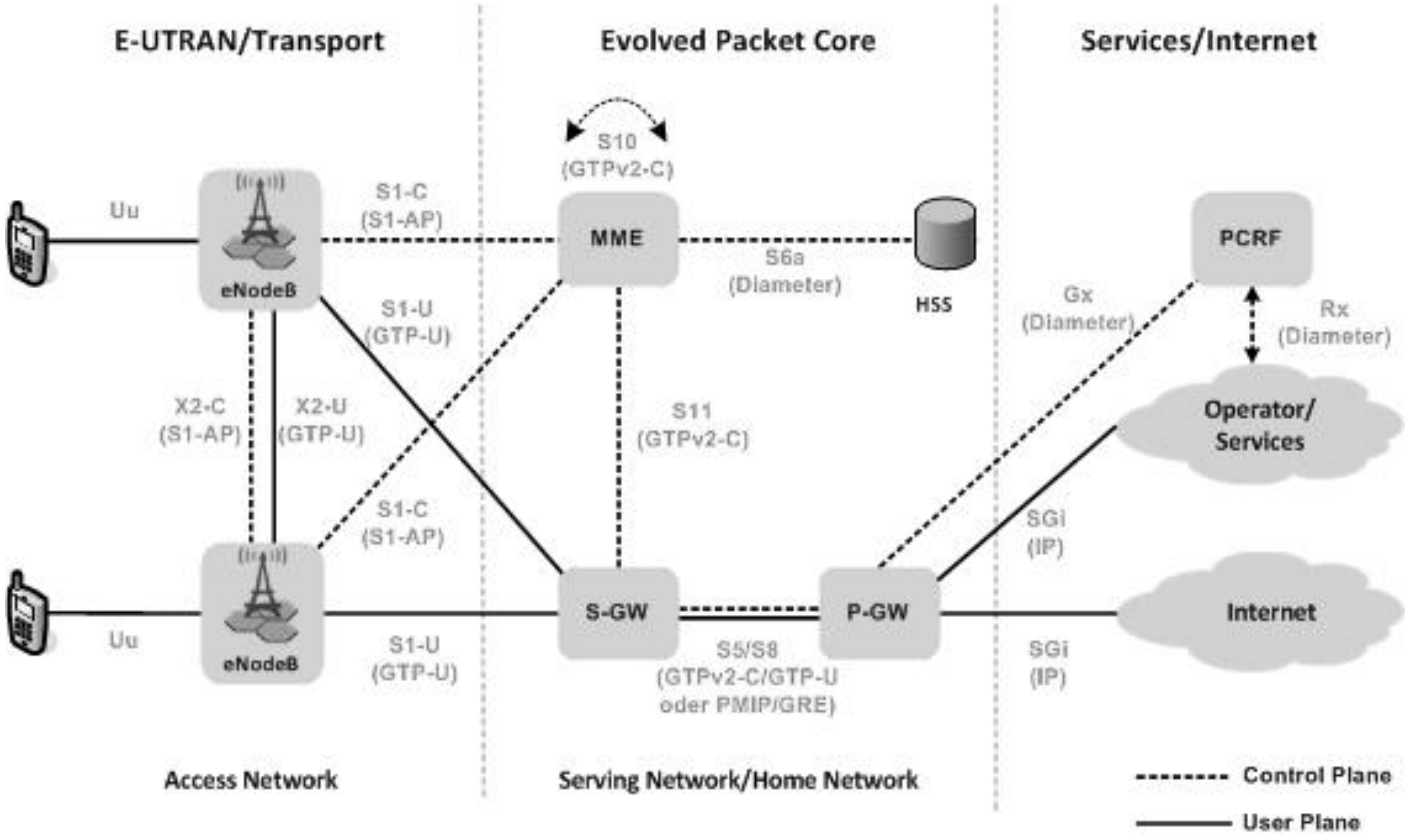
Inhalte

- 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
- Diese wird durch immer neuere Applikationsanforderungen notwendig
- Umgangssprachlich wird sie Long Term Evolution (LTE) genannt
- Die Architektur selbst wird allerdings in den Spezifikationen als Evolved Packet System (EPS) bezeichnet
- Die EPS-Architektur beinhaltet prägnante Änderungen 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 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)



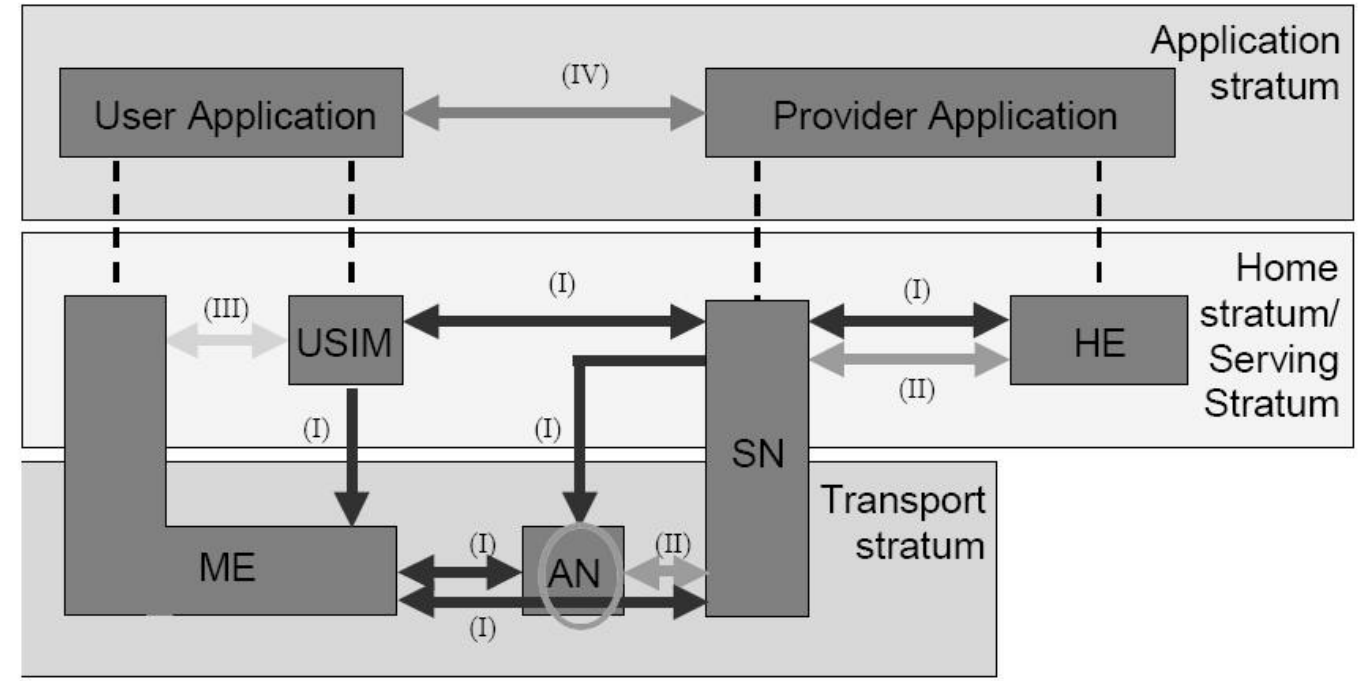
EPS-Architektur (2)

- 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

- Auf die IT-Sicherheit wurde bereits bei der Basisspezifikation höchsten Wert gelegt
- Es wurden daher vier Security Domains definiert:
  - 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

- 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 (Verschlüsselung der Nachrichten)
  - Dynamische Schlüsselgenerierung und -verwaltung
  - 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
- Zusätzlich kommunizieren die E-UTRAN-Komponenten direkt und ohne vorherige Authentifizierung mit dem EPC
- Die Nachrichten in der User Plane und Control Plane zwischen der Base Station (BS) und dem EPC werden durch die Network-Access-Sicherheitsmerkmale ebenfalls 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
  - Daher 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

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

- Die EPS-Architektur hat als Ziel, ein sicheres Zugriffs- und Transport-Rahmenwerk für die Unterstützung der Ende-zu-Ende-Sicherheit von LTE-Datenströmen anzubieten
- Um die Sicherheitsziele zu überprüfen, wurden die folgenden Bereiche bewertet:
  - 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 Schlüsseltrennung
- 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 dem 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 optional auf 256 Bit erweitert werden

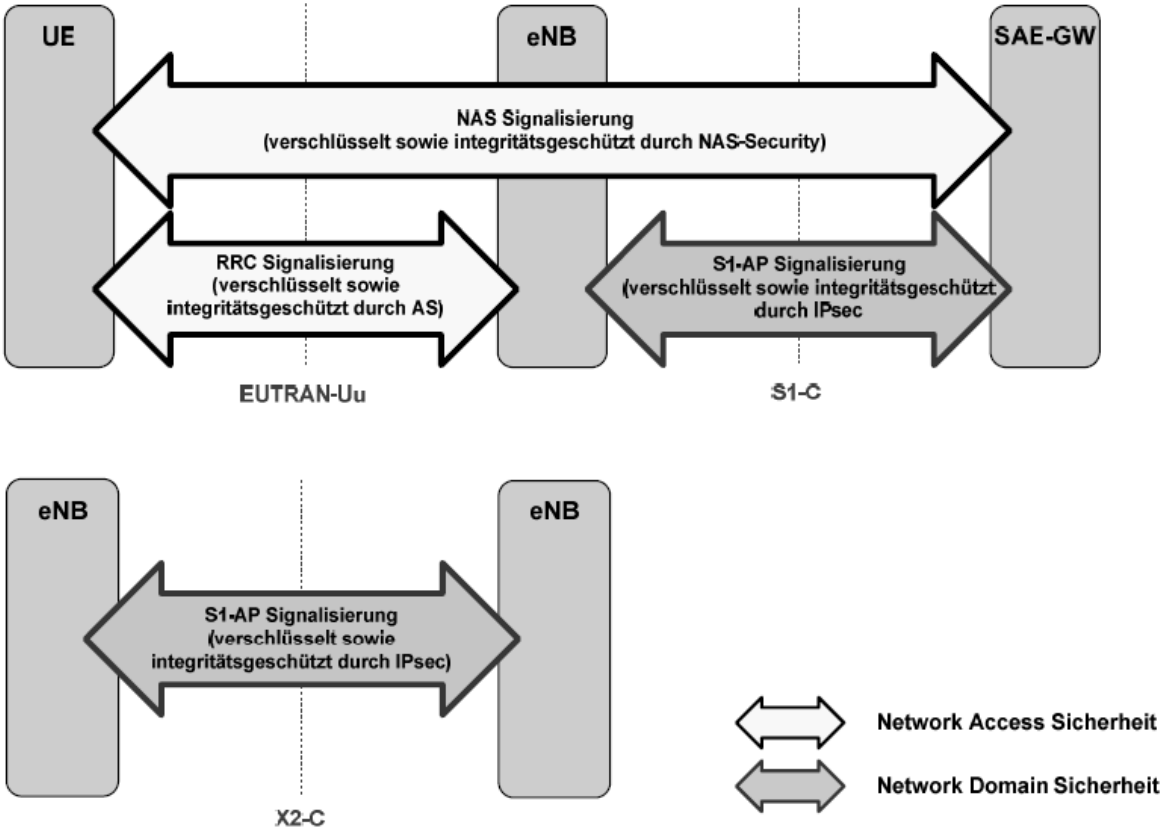
Sicherheitsparameter (2)

- Die EPS-Sicherheitsarchitektur ist ferner unabhängig vom verwendeten IP-Protokoll der User Plane
- Es kann also ebenfalls IPv6 genutzt werden, auch wenn dies immer noch 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 netzwerkbasierte Angriffe verwundbar (z.B. Phishing, DoS, Unauthorized Access, Eavesdropping, SPIT)
- Zudem bietet das IPv6-Protokolle neue Schwachstellen an, die teilweise noch nicht wahrgenommen werden
- Die Sicherheitsalgorithmen können aber beliebig erweitert werden

Ende-zu-Ende-Sicherheit (1)

- 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
- Alle Signalisierungsdaten gemeinsam erfahren einen Integritäts-, einen Vertraulichkeits- und einen Replay-Schutz
- Folgende Sicherheitsmerkmale werden unterstützt:
  - Beidseitige Authentifizierung zwischen Endgerät und Netzwerk
  - Neue, tiefere Schlüsselhierarchie
  - Integrität der Signalisierungsnachrichten
  - Vertraulichkeit der User- und Signalisierungsdaten
  - Vertraulichkeit der Benutzer- und Endgeräteidentitäten
  - Plattformsicherheit der eNodeB
  - Network Domain Security mit IPsec
  - Schlüsselseparierung

Ende-zu-Ende-Sicherheit (2)



Schlüsselarchitektur (1)

- 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 (NAS und AS) 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

Schlüsselarchitektur (2)

- Folgende Sicherheitsmaßnahmen werden berücksichtigt:
  - Schlüsseltrennung zwischen Endgeräten
  - Schlüsseltrennung zwischen den BS
  - Schlüsseltrennung zwischen den NAS- und AS-Sicherheitsebenen
  - Schlüsseltrennung zwischen Control Plane und User Plane
  - Schlüsseltrennung zwischen den Algorithmen (z.B. HMAC-SHA-256)
  - Schlüsseltrennung zwischen Integritäts- und Verschlüsselungsschlüssel
  - Schlüsseltrennung zwischen den unterschiedlichen Zugangstechnologien
  - Schlüsseltrennung zwischen unterschiedlichen Mobilfunkprovidern
- So kann auch der gemeinsame Masterschlüssel, den sich Netzwerk und USIM teilen, geschützt werden
- Die Erweiterung der Schlüsselhierarchie und die Schlüsseltrennung stellt daher eine signifikante Verbesserung der IT-Sicherheit im Vergleich zu UMTS dar

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
- Es ergeben sich höhere Anforderungen an das Schlüsselmanagement
- Die Sicherheitsmaßnahmen gehen zu Lasten der Performance und Skalierbarkeit, weshalb man spezielle Security Gateways einsetzen sollte

Ende

Vielen Dank für ihre Aufmerksamkeit

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