Use of IPsec & IKE in Universal Mobile Telecommunication System

Dr. John K. Zao
Sr. Scientist, Information Security
Verizon Communications / BBN Technologies

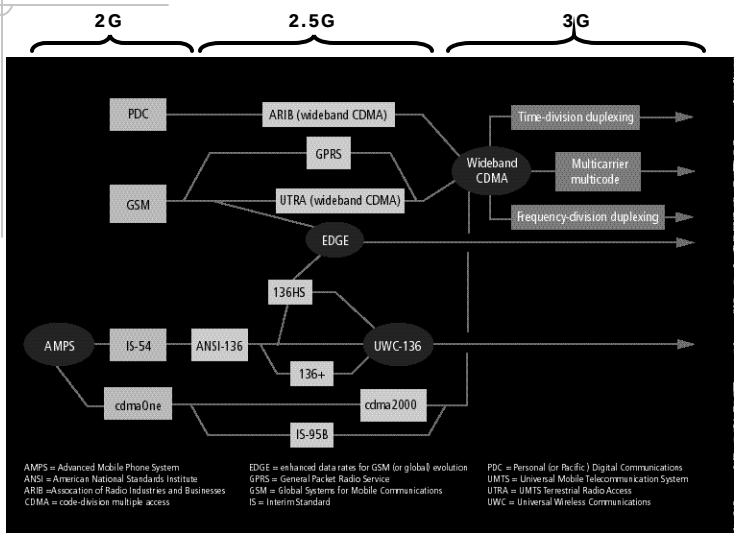
Outline

- Overview: 3G Wireless Data Networks
- Analysis: UMTS Security
- Proposal: Possible Use of IPsec & IKE in UMTS Security

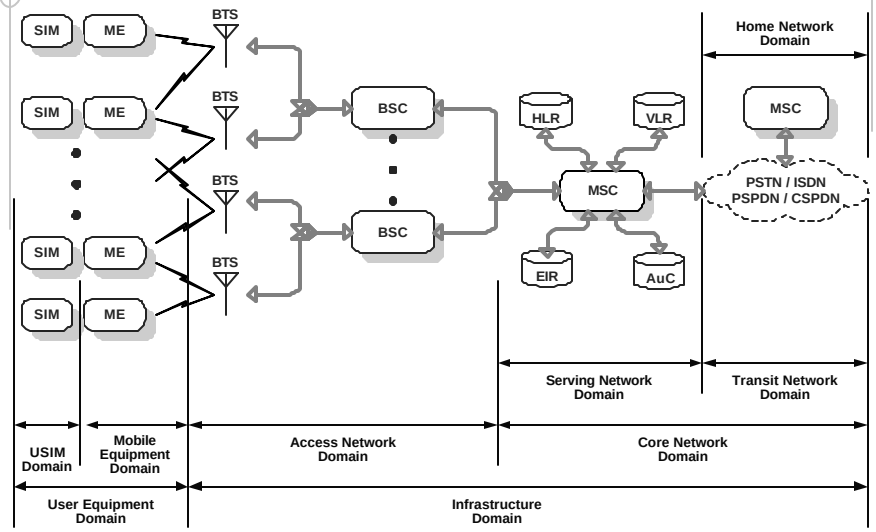
Outline

- Overview: 3G Wireless Data Networks
  - History
  - Architecture
  - Domains
  - Strata
- Analysis: UMTS Security
- Proposal: Possible Use of IPsec & IKE in UMTS Security

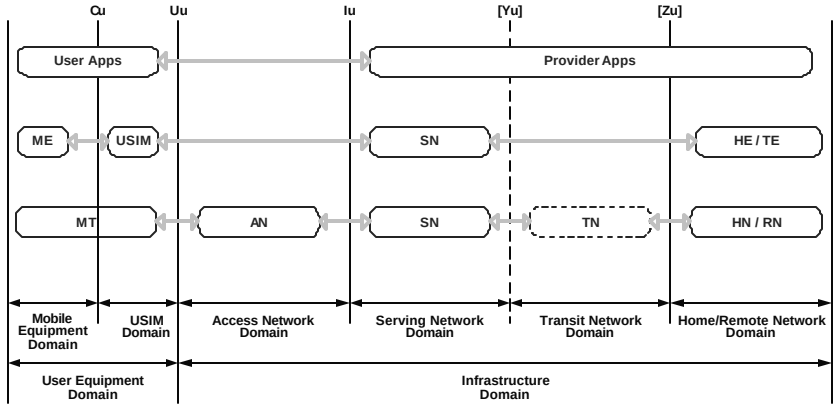
Wireless Data Network Development



GPRS / UMTS System Architecture

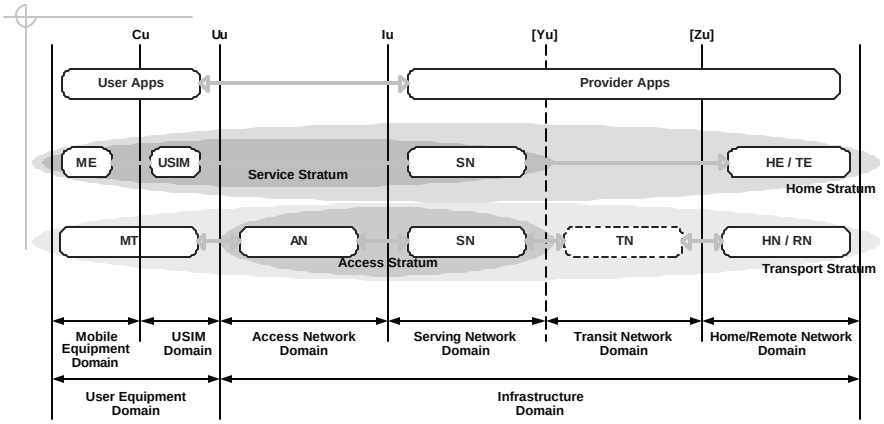


UMTS Domain Hierarchy



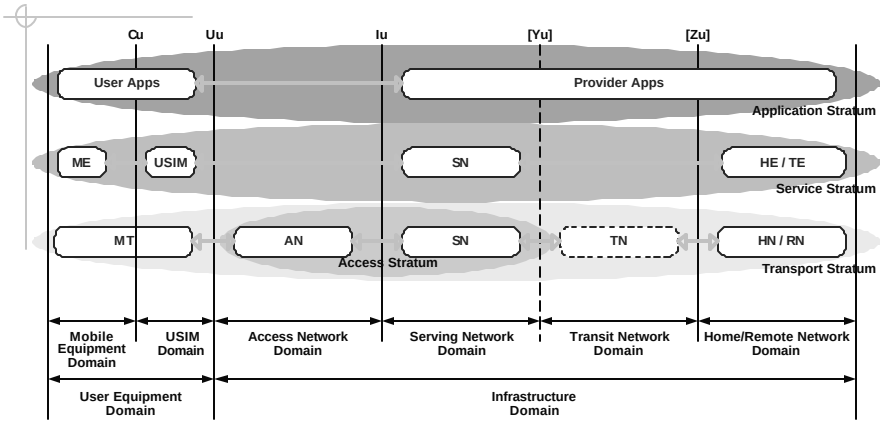
Domain – a high-level group of UMTS entities;
reference points (interfaces) are defined between domains

UMTS MT-HN Strata



Stratum – a group of UMTS protocols that are relevant to one aspect of the services provided by one or more domains

UMTS MT-RN Strata



Stratum – a group of UMTS protocols that are relevant to one aspect of the services provided by one or more domains

Outline

- Overview: 3G Wireless Data Networks
- Analysis: UMTS Security
  - Security Threads
  - Security Architecture
  - Security Features/Services
    - Network Access Security
    - Network Domain Security
    - User Domain Security
    - Application Domain Security
  - Security Mechanisms
    - Mobile User Identity Allocation
    - Entity Authentication & Key Agreement
    - User Traffic Confidentiality
    - Network Domain Security
- Proposal: Possible Use of IPsec & IKE in UMTS Security

3G Security: Threats

Basic Threads	**Confidentiality Violation**	**Integrity Violation**	**Denial of Services**	**Illegitimate Uses**	**Repudiation**
Enabling Threads	Eavesdropping, User Traffic	Alteration, User Traffic	Intervention, Physical	Masquerading, User	Repudiation, Charge
	Eavesdropping, Signal & Control	Alteration, Signal & Control	Intervention, Protocols	Masquerading, Service Net	Repudiation, Traffic Origin
	Masquerading, User	Alteration, ME Download	Masquerading, Net Elements	Masquerading, Home Environment	Repudiation, Traffic Delivery
	Masquerading, Net Elements	Alteration, USIM Download	Privilege Misuse	Privilege Misuse, User	
	Traffic Analysis, Passive	Alteration, System Data	Service Abuse	Privilege Misuse, Service Net	
	Traffic Analysis, Active	Masquerading, Net Elements		Stealing, Terminals	
	Unauthorized Access, System Data	Masquerading, Download Origins			
	Information Leakage User Location				

Source: 3G Security; Security Threats & Requirements [3G TS 21.133]

3G Security : Threats, Radio Interface

Basic Threads	Confidentiality Violation	Integrity Violation	Denial of Services	Illegitimate Uses	Repudiation
Enabling Threads	Eavesdropping, User Traffic	Alteration, User Traffic	Intervention, Physical	Masquerading, User	Repudiation, Charge
	Eavesdropping, Signal & Control	Alteration, Signal & Control	Intervention, Protocols	Masquerading, Service Net	Repudiation, Traffic Origin
	Masquerading, User	Alteration, ME Download	Masquerading, Net Elements	Masquerading, Home Environment	Repudiation, Traffic Delivery
	Masquerading, Net Elements	Alteration, USIM Download	Privilege Misuse	Privilege Misuse, User	
	Traffic Analysis, Passive	Alteration, System Data	Service Abuse	Privilege Misuse, Service Net	
	Traffic Analysis, Active	Masquerading, Net Elements		Stealing, Terminals	
	Unauthorized Access, System Data	Masquerading, Download Origins			
	Information Leakage User Location				

- Radio Eavesdropping & Traffic Analysis
- User & Net Element Masquerading

Relevant Threads | Significant Threads | Major Threads

3G Security : Threats, ME-USIM Interface

Basic Threads	Confidentiality Violation	Integrity Violation	Denial of Services	Illegitimate Uses	Repudiation
Enabling Threads	Eavesdropping, (USIM) User Traffic	Alteration, (USIM) User Traffic	Intervention, Physical	Masquerading, User (Stolen ME & USIM)	Repudiation, Charge
	Eavesdropping, (USIM) Signal & Control	Alteration, (USIM) Signal & Control	Intervention, Protocols	Masquerading, Service Net	Repudiation, Traffic Origin
	Masquerading, User (ME/USIM)	Alteration, ME Download	Masquerading, Net Elements	Masquerading, Home Environment	Repudiation, Traffic Delivery
	Masquerading, Net Elements	Alteration, USIM Download	Privilege Misuse	Privilege Misuse, (Borrowed USIM)	
	Traffic Analysis, Passive	Alteration, System Data (ME)	Service Abuse	Privilege Misuse, Service Net	
	Traffic Analysis, Active	Masquerading, Net Elements		Stealing, Terminals (ME)	
	Unauthorized Access, System Data (USIM)	Masquerading, Download Origins			
	Information Leakage, User Location				

- ME/USIM Masquerading
- ME/USIM Data Alteration & Access
- ME/USIM Download Alteration & Eavesdropping

Relevant Threads | Significant Threads | Major Threads

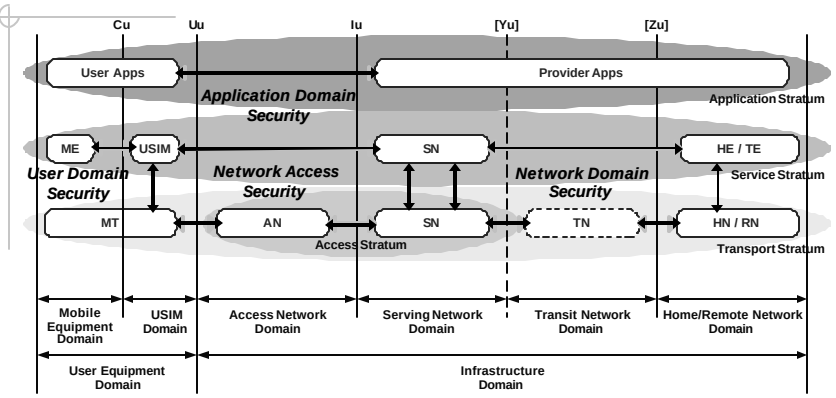
3G Security : Threats, General System

Basic Threads	**Confidentiality Violation**	**Integrity Violation**	**Denial of Services**	**Illegitimate Uses**	**Repudiation**
Enabling Threads	Eavesdropping, User Traffic	Alteration, User Traffic	Intervention, Physical	Masquerading, User	Repudiation, Charge
	Eavesdropping, Signal & Control	Alteration, Signal & Control	Intervention, Protocols	Masquerading, Service Net	Repudiation, Traffic Origin
	Masquerading, User	Alteration, ME Download	Masquerading, Net Elements	Masquerading, Home Environment	Repudiation, Traffic Delivery
	Masquerading, Net Elements	Alteration, USIM Download	Privilege Misuse	Privilege Misuse, User	
	Traffic Analysis, Passive	Alteration, System Data	Service Abuse, Emergency Service	Privilege Misuse, Service Net	
	Traffic Analysis, Active	Masquerading, Net Elements		Stealing, Terminals	
	Unauthorized Access, System Data	Masquerading, Download Origins			
	Information Leakage User Location				

Relevant Threads | Significant Threads | Major Threads

- Privilege Misuse
- Network Element Masquerading
- Wired Link Eavesdropping

UMTS Security Architecture



- *User Domain Security – protection against attacks on ME - USIM/USIM interfaces*
- *Network Access Security – protection against attacks on radio (access) links*
- *Network Domain Security – protection against attacks on wired network infrastructure*
- *Application Domain Security – protection on user & provider application exchanges*
- *Security Management – monitoring & managing user - provider security features*

Network Access Security

User Identity Confidentiality

Services
- Identity Confidentiality
- Location Confidentiality
- Untraceability

Mechanisms
- Temporary Visiting Identity
- Encrypted Permanent Identity
- Encrypted Signal / Control Data

Data Confidentiality

Services
- Cipher Algorithm Agreement
- Cipher Key Agreement
- User Data Confidentiality
- Signal / Control Data Confidentiality

Entity Authentication

Services
- Authentication Mechanism Agreement
- User Authentication
- Network Element Authentication

Mechanisms
- HE-SN Authentication & Key Agreement
- Local Authentication

Data Integrity

Services
- Integrity Algorithm Agreement
- Integrity Key Agreement
- Signal / Control Data Integrity
- Signal / Control Data Origin Authentication

Network Domain Security

Data Confidentiality

Services
- Cipher Algorithm Agreement
- Cipher Key Agreement
- Signal / Control Data Confidentiality

Entity Authentication

Services
- Mechanism Agreement
- Network Element Authentication

Mechanism
- Explicit Symmetric Key Authentication

Data Integrity

Services
- Integrity Algorithm Agreement
- Integrity Key Agreement
- Signal / Control Data Integrity
- Signal / Control Data Origin Authentication

User Domain Security

User - USIM Authentication
Services
- PIN-based Authentication

USIM - ME Authentication
Services
- Shared Secret Authentication

Application Domain Security

User Traffic Confidentiality
Service
- End-to-End Data Confidentiality

Secure USIM Download & Messaging
Services
- Application Identity Authentication
- Application Data Confidentiality
- Application Data Origin Authentication
- Application Data Integrity
- Application Exchange Sequence Integrity
- Application Exchange Replay Protection
- Application Data Non-repudiation

User Profile Confidentiality
[TBD]

IP Security
[TBD]

* Mobile User Identity (MUI) Exchanges

Temporary MUI (TMUI) Allocation

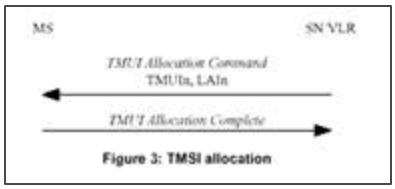


Figure 3: TMSI allocation

- Similar to Mobile IP Registration
- Source: UMTS Security Architecture [3G TS 33.102]

Permanent MUI (IMUI) Identification

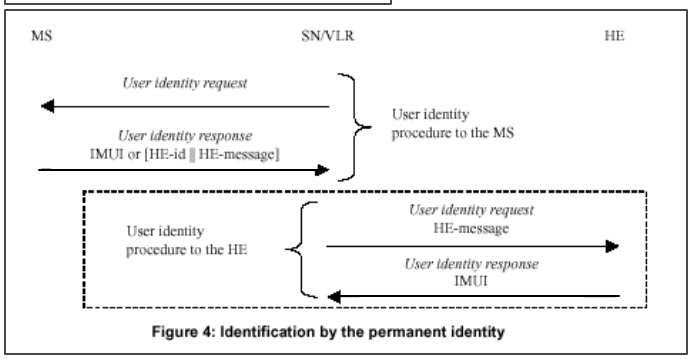


Figure 4: Identification by the permanent identity

Entity Authentication & Key Agreement

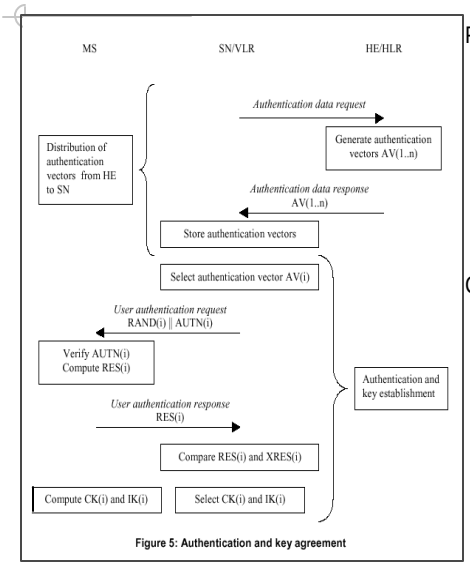


Figure 5: Authentication and key agreement

Parameters

- Authentication Vector
  `AV(i) := RAND(i)||XRES(i)||CK(i)||IK(i)||AUTN(i)`
  `AUTN,CK,IK,XRES` derived from `RAND,SQN,AMF`
- Authentication Data Request
  `Authen_Req := IMUI || HLR_MSG`
- Authentication Data Request
  `Authen_Res := [IMUI] || AV(1..n)`

Comments

- Authentication is conducted between HE/AuC & MS/USIM
- HE is *authentication & key distribution center*
- SN/VLR is *trusted mediator*
- If HE is off-line then MS-SN authenti-cate using shared integrity key & protect their traffic using old **(CK,IK)**

User Traffic Confidentiality

Key Management

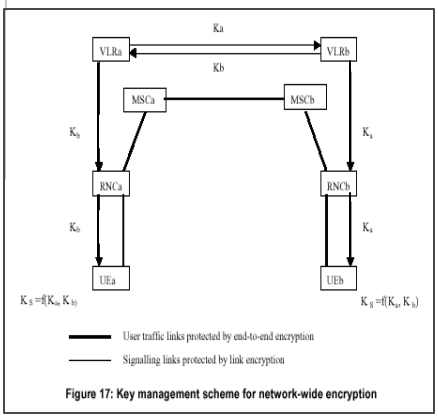


Figure 17: Key management scheme for network-wide encryption

- Cipher Key (Ks)
- Initialization Vector (IV)

Cipher Algorithms

- Synchronous Stream Cipher
  - Data stream XOR with key stream
  - Synchronization controlled by IV

Issues

- Encryption synchronization mechanism
- TFO voice protection adaptation
- Data traffic protection adaptation
- Encryption termination at net gateways
- Encryption management

Network Domain Security

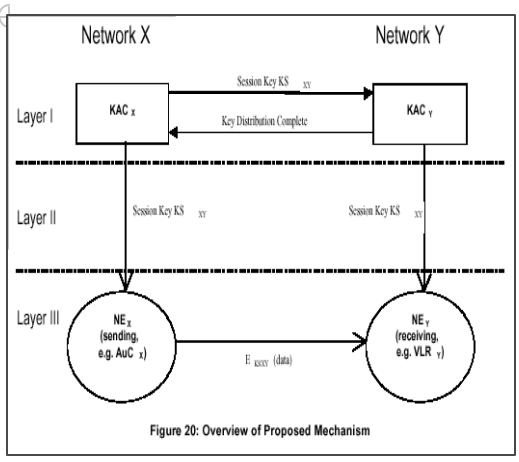


Figure 20: Overview of Proposed Mechanism

Similar to Multi-Realm Kerberos

Layer I

- Symmetric Session Key Negotiation using PK technology

Layer II

- Session Key Distribution within each Operator

Layer III

- Secure communication between Elements of different Operators

Outline

- Overview: 3G Wireless Data Networks
- Analysis: UMTS Security
- Proposal: Possible Use of IPsec & IKE in UMTS Security
  - Motivation
  - Use of IPsec with IKE
  - Use of IPsec with UMTS Key Management
  - Use of IKE with UMTS Cipher Mechanisms
  - Use of IPsec with Stateful Header Compression

Motivation

Why are we thinking of putting IPsec & IKE into 3G?

Because ...

- IP (with XML payloads) is likely to be the networking protocol for future Wireless Internet.
- GSM/GPRS/UMTS Security Architecture is complex & fragmented.
- IPsec & IKE will become widely deployed.
- Use of USIM will make PK technology more accessible.
- ...

What will be the major show stoppers?

- Wireless Voice traffic will NOT be over IP in near future.
- Wireless Signaling & Control traffic is NOT over IP either.

Use of IPsec with IKE in UMTS

- Application Domain Security [Strong Case]
  - User Traffic Confidentiality
- Network Domain Security [Possible but Unlikely Case]
  - Entity Authentication
  - Data Confidentiality
  - Data Integrity
  - *First, UMTS Core Network must speak IP …*

Use of IPsec with UMTS Key Management

- Network Domain Signaling & Control Security [Possible Case]
  - Entity Authentication
  - Data Confidentiality
  - Data Integrity
  - *More likely than IPsec protection for entire UMTS Core Network*
  - *Use UMTS Key Management is reasonable for compatibility*
  - *Still, UMTS Signaling & Control must speak IP …*

Use of IKE with UMTS Cipher Mechanisms

Not so unlikely as we think because ...

- UMTS uses USIM-HE exchanges to establish user security
- USIM & HE/AuC may use IKE technology

◆ Entity Authentication & Cipher/Integrity Key Agreement

- Network Access Security
- Application Domain Security

Use of IPsec with Header Compression

Justification

- Wireless Data Network may have limited bandwidth
- Wireless Access & Network Domains support stateful L2 switching

Approach

- Adopt technologies from IETF Robust Header Compression WG
- Consider possible IPsec header compression ?

Bibliography

3rd Generation Partnership Project, Technical Specification Group (TSG) SA

- 3G TS 21.133 - *3G Security; Security Threats & Requirements*
- 3G TS 21.120 - *3G Security; Security Principles & Objectives*
- 3G TS 33.105 - *3G Security; Cryptographic Algorithm Requirements*
- 3G TS 33.102 - *UMTS; 3G Security; Security Architecture*
- 3G TS 23.101 - *UMTS; General UMTS Architecture*

GSM Documents

- GS 02.60 – *GPRS; Service Description; Stage 1*
- GS 03.60 – *GPRS; Service Description; Stage 2*
- GS 02.09 – *Security Aspects*
- GS 03.20 – *Security Related Network Functions*

Source: http://www.etsi.org/