RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Mobile Devices Security: Evolving Threat Profile of Mobile Networks

SESSION ID: MBS-T07

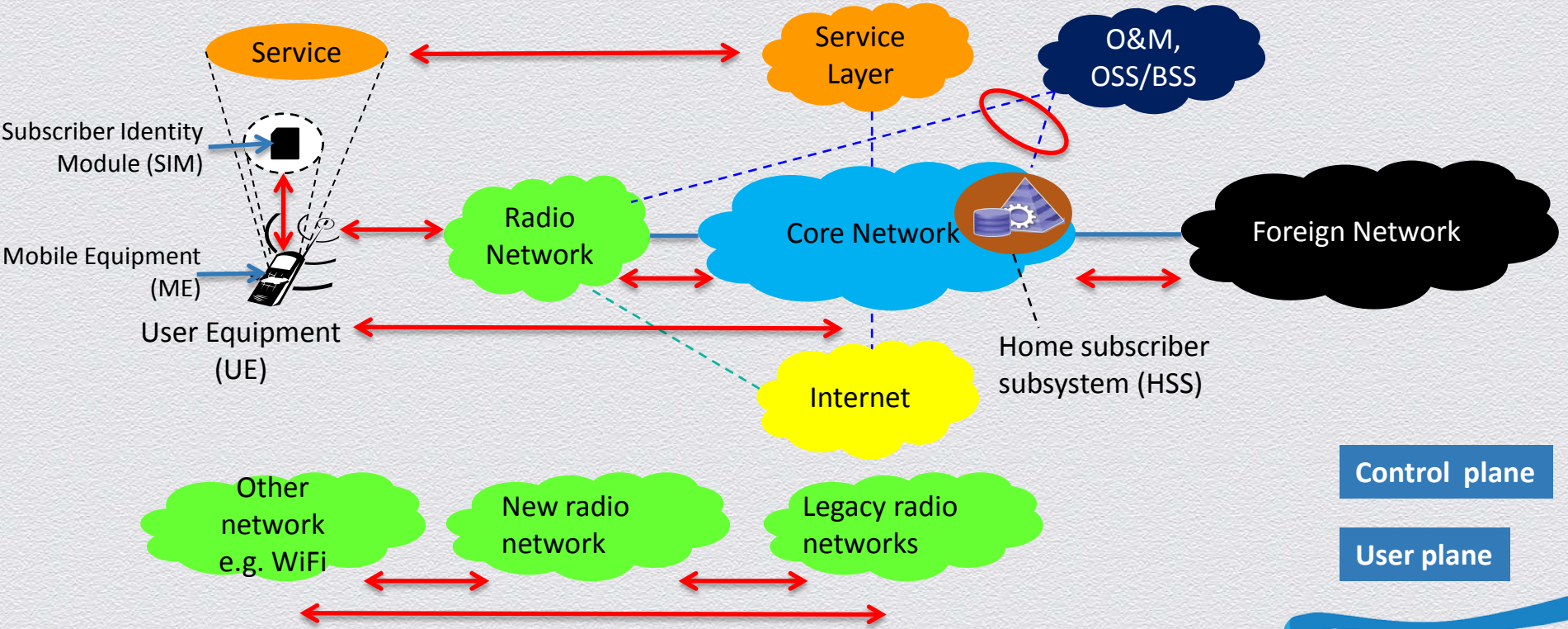
Anand R. Prasad, Dr.,ir., Selim Aissi, PhD

Objectives

- Introduction
- Mobile Network Security
- Cybersecurity Implications
- Mitigations & Future Developments

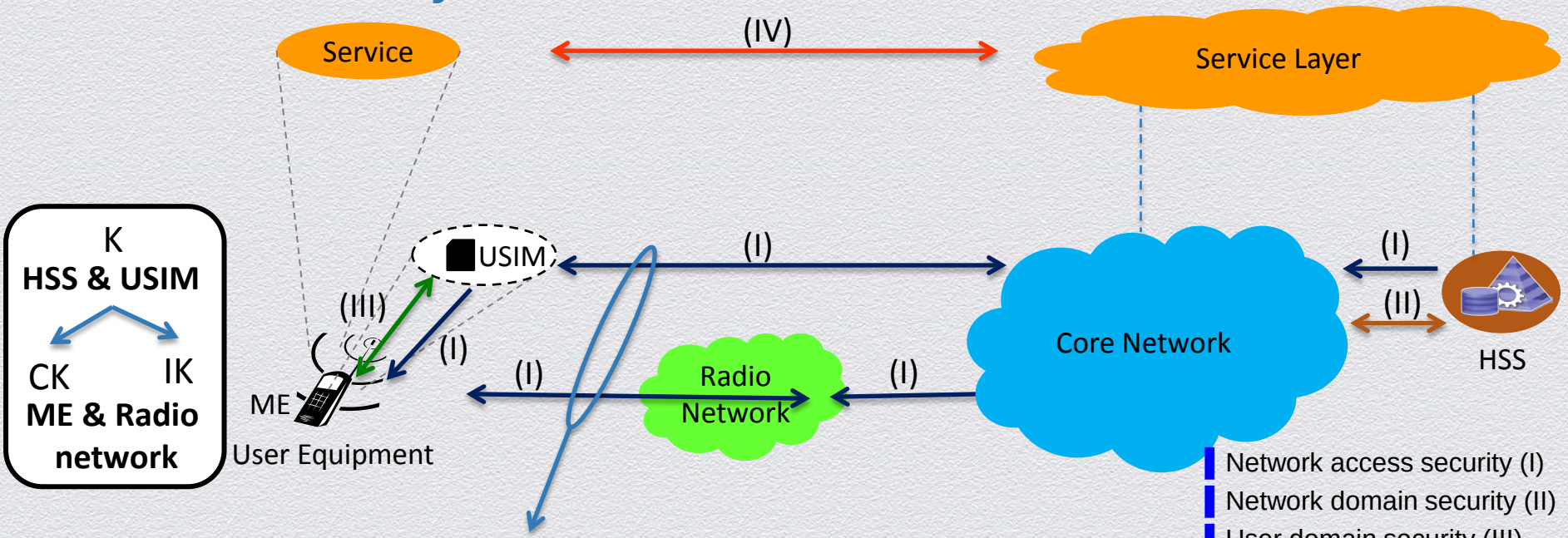
Introduction

Mobile Network Security – Helicopter view



Mobile Network Security

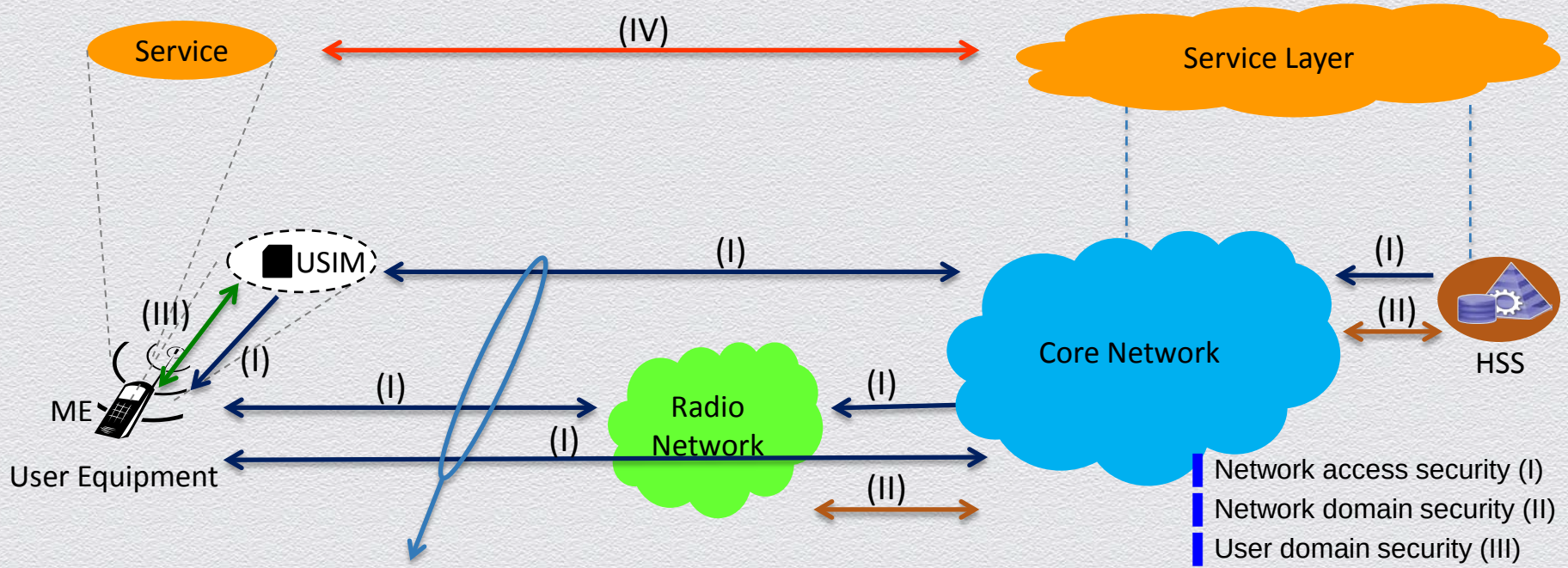
UMTS Security: Architecture



- Mutual authentication, confidentiality (optional) & integrity
- Separate keys for confidentiality & integrity
- Same keys for user and control planes

HSS: Home Subscriber Subsystem; ME: Mobile Equipment; USIM: Universal Subscriber Identity Module

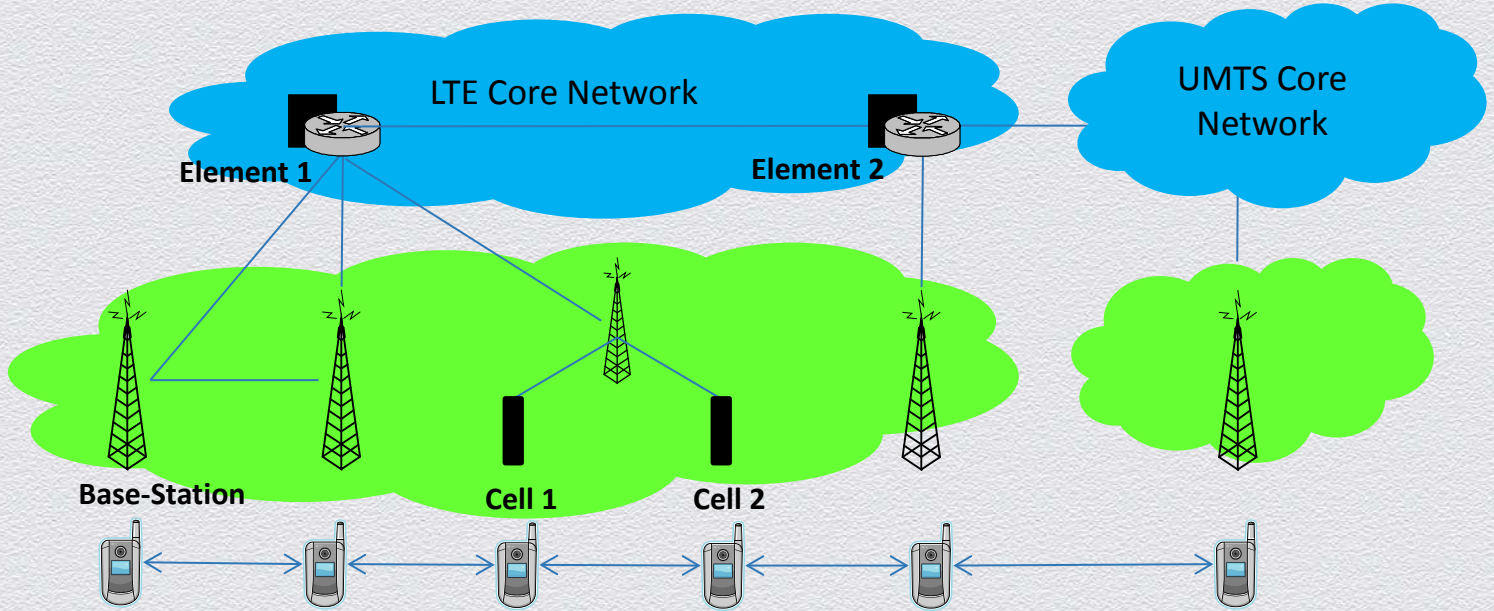
LTE Security: Architecture



- Mutual authentication, confidentiality (optional) & integrity
- Separate keys for each purpose

USIM: Universal Subscriber Identity Module; ME: Mobile Equipment; HSS: Home Subscriber Subsystem

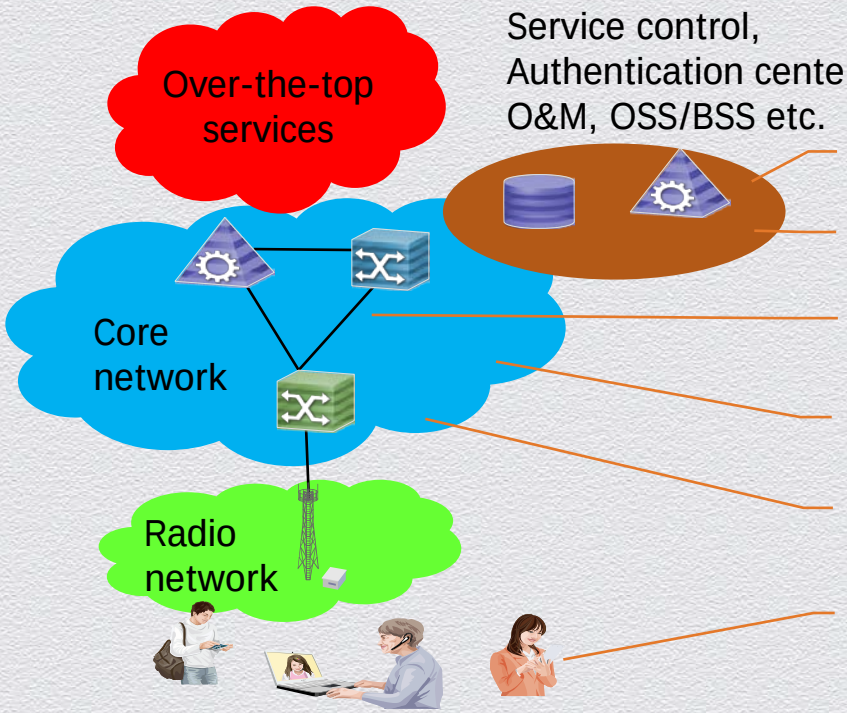
LTE Security: Mobility aspects



- Forward & backward security: Cryptographically separate keys derived at each handover
- Keys mapped between different types of networks

LTE: Long-Term Evolution

Security Considerations



1. Subscriber privacy
2. Fraudulent charging
3. Protocol attack
4. Attack on network elements
5. Finding network topology
6. Overload network (DoS, DDoS): with botnets, malware, home made terminals etc.

BSS: Billing Support System; DoS: Denial of Service; DDoS: Distributed DoS; O&M: Operations and Management; OSS: Operations Support System

Cybersecurity Implications, Mitigations, and Future Developments

Cybersecurity Implications

	GSM	GPRS	UMTS	SAE/LTE
Security Services	• Ciphering • User authentication • Equivalent to wired	Ciphering User authentication	• Ciphering & integrity • Mutual auth.	• Ciphering & integrity • Mutual auth.
Authentication	Authentication: 3 values		UMTS-AKA: 5 values	EPS-AKA: 5 values
Keys	Derivation of a ciphering key after auth.		Derivation of CK & IK	Separate keys for each purpose
Key Length	• Shared key 128 bits for auth. • Derived 64 bits out of which 54 used for ciphering	• Shared key 128 bits for auth. • Derived 64 bits for ciphering	128 bits	128 bits
Key handling	Changed on authentication			Changed on each handover
Algorithm	A5/1 / 2 /3; specification is confidential. A5/3 is based on Kasumi	GPRS Encryption Algorithm (GEA): GEA0/GEA1/GEA2/ GEA3	Kasumi from Rel. 4	SNOW 3G, AES and ZUC
End-Point Security	BTS	SGSN	RNC / SGSN	• eNB for UP & RRC • MME for NAS
Network Security	None	None initially	MAPsec and IPsec	IPsec

Cybersecurity Implications

- Threat landscape and computational power have evolved much faster, with no significant updates in the overall security architecture
- Local DoS attack against the cell service
- Heterogeneous networks (Metrocells, Femtocells and WiFi)
- Local radio jamming attacks
- Complex DDoS threats targeting essential EPC elements, such as the HSS

Cybersecurity Implications

Attack Mode	Local (Femto/RAN/eNB/WiFi)	EPC (Core)	PDN (Global)
DoS	1. Jamming Attack • DL-LP • UL-LP • Femto-based 2. BS Vulnerabilities	1. Femto-based Attack 2. Core Network Vulnerabilities in GW, MME	1. APT 2. Malware
DDoS	1. LP Jamming Attack 2. BS saturation with SMS 3. Protocol Misbehavior	1. Botnet of MEs 2. Amplification Attacks 3. HSS Saturation 4. EPC Saturation	1. Botnet of MEs 2. Attack against Internet Nodes
Insider	1. Jamming with a BS 2. BS Shutdown	1. Node Damage 2. HSS Saturation 3. EPC Saturation	1. HSS Saturation

Mitigations & Future Developments

	HSS Saturation Attacks	EPC Amplification Attacks	Scalability Attacks	Jamming Attacks
Flexible/Distributed Load Balancing (SDN)	X			
Flexible/Adaptive Management of the EPC (SDN)		X	X	
Advanced Anti-Jamming Techniques (e.g., Multi-Antenna Jamming Mitigation)				X
Distribution/Optimization of EPC Functions	X	X	X	
Optimization of Radio Resource Management		X	X	
Advanced Data Mining Techniques to Detect Attacks	X	X	X	X

Summary

- Introduction
- Mobile Network Security
- Cybersecurity Implications
- Mitigations & Future Developments

Q&A

Anand R. Prasad: anand@bq.jp.nec.com

Selim Aissi: saissi@visa.com

Appendices

References

- Security for Mobile Networks and Platforms, Selim Aissi, Nora Dabbous and Anand R. Prasad, Artech House, July 2006.
- Security in Next Generation Mobile Networks: SAE/LTE and WiMAX, Anand R. Prasad and Seung-Woo Seo, River Publishers, August 2011.
- 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".
- 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".
- 3GPP TS 33.102: "3G security; Security architecture“.

Definitions

	Definitions
APT	Advanced Persistent Threat
BS	Base Station
BTS	Base Transceiver Station
DDoS	Distributed Denial of Service (Attack)
DL	Down Link
DoS	Denial of Service (Attack)
EDGE	Enhanced Data rates for GSM Evolution
EPC	Evolved Packet Core
GERAN	GSM EDGE Radio Access Network
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GW	Gateway
eNB	Evolved NodeB

Definitions

	Definitions
EPS	Evolved Packet System
IMS	IP Multimedia Subsystem
KDF	Key Derivation Function
LP	Low Power
LTE	Long Term Evolution
ME	Mobile Equipment
MME	Mobility Management Entity
NAS	Non-Access Stratum
NCC	Next hop Chaining Counter
NGMN	Next Generation Mobile Networks
NH	Next Hop

Definitions

	Definitions
PCI	Physical Cell Identity
PDG	Packet Data Gateway
PDN	Packet Data Network
PLMN	Public and Mobile Network
PSTN	Public Switched Telephone Network
RAT	Radio Access Technology
RNC	Radio Network Controller
RRC	Radio Resource Control
SAE	System Architecture Evolution (3GPP)
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SMS	Short Message Service

Definitions

	Definitions
UE	User Equipment
UL	Upward Link
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
WiFi	Wireless Fidelity, Wi-Fi is a trademarked term meaning IEEE 802.11x
WLAN	Wireless Local Area Network