

SECURITY, FRAUD AND HACKING IN GSM, UMTS AND LTE NETWORKS

Content

INTRODUCTION TO INFORMATION SECURITY

- Security areas, security technologies
- Public and private cryptography
- Digital certificates

MOBILE NETWORKS SECURITY ASPECTS

- Major mobile networks vulnerabilities
- Security in 1G and 2G networks

SECURITY MODEL OF GSM

- Authentication
- Ciphering
- Equipment verification
- Subscriber identity confidentiality

FLAWS IN GSM SECURITY

- Kerckhoffs's Assumption
- The role of cryptographic key length
- The history of GSM security attacks

HACKING IN GSM - SIM CARD CLONING

- The concept of a card clone and its consequences
- SIM card attacks – challenge attack, side channel attack, over-the-air attack
- SIM card cloning – network countermeasures



POSSIBLE METHODS OF INFORMATION INTERCEPTION

- Cracking the A5 algorithm
- Accessing the signalling network

IMPROVEMENTS IN GSM SECURITY

- Authentication New A3/A8 algorithms
- New A5 algorithm
- End-to-end encryption

SECURITY OF SHORT MESSAGE SERVICE, SMS

- SMS Transmission Characteristics

BRIGHTCOMMS
GO FURTHER

- SMS message classes: ordinary, flash, ping
- Security of ordinary SMS
- SAT messages

SECURITY OF GENERAL PACKET RADIO SERVICE, GPRS

- Security areas of GPRS
- Difference in GSM and GPRS security procedures
- Security issues induced by IP communication

FRAUD IN MOBILE NETWORKS

- The definition of telecom fraud
- Common Mobile Fraud Types
- Influence of roaming on mobile fraud figures
- Premium rate service fraud
- Prepaid service fraud
- Fraud prevention and defense

SECURITY IN UMTS

- Security threats in UMTS
- UMTS security model
- Comparison of GSM and UMTS security
- Lawful interception

SECURITY IN LTE

- LTE security model
- Hierarchy of security keys in LTE

SECURITY OF THE TRANSPORT NETWORK

- The concept of the Security Gateway

Brightcomms

999 Ponce de Leon,
Suite 525, Coral Gables,
Florida, 33134, United States.
Toll Free + 1-800-490-1089.
E-mail: training@brightcomms.com
www.brightcomms.com

- IPSec and its procedures

Target audience

The target audience Core Network and Security Engineers

Pre-requisites

The participants should have prior knowledge of mobile networks

Course length

2 days

BRIGHTCOMMS is an independent company specializing in providing solutions in the engineering of radio frequency (RF) with extensive experience and demonstrated reliability, responsibility and commitment to our clients and their goals, also taking priority attention from the needs they immediately.

You are warmly welcome to contact our representatives at:

Email: training@brightcomms.com or Toll Free + 1-800-490-1089.

