

Improving Mobile Security

Braden Luthi

Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA

29 April 2014

Outline

- 1 Background
- 2 GSM Weakness in UMTS
- 3 Application Security Threat
- 4 EM Leaking Key Information

Outline

- 1 Background
 - GSM and UMTS
 - Cryptography
- 2 GSM Weakness in UMTS
- 3 Application Security Threat
- 4 EM Leaking Key Information

GSM

UMTS

Outline

1 Background

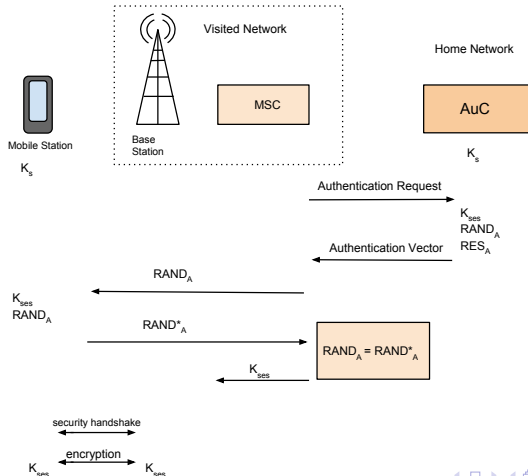
2 GSM Weakness in UMTS

- Authentication
- GSM and UMTS Inter-working Networks
- Man-In-The-Middle Attack
- Solution

3 Application Security Threat

4 EM Leaking Key Information

GSM Authentication



Inter-working Networks

Man-in-the-middle weakness in GSM

Protecting UMTS from GSM Man-in-the-middle attack

Outline

- 1 Background
- 2 GSM Weakness in UMTS
- 3 Application Security Threat**
- 4 EM Leaking Key Information

Outline

- 1 Background
- 2 GSM Weakness in UMTS
- 3 Application Security Threat
- 4 EM Leaking Key Information**