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
5. conclusion

Outline

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

Cryptography

Cryptography or ’secret writing’ is the study and practice of techniques for securing communications between two parties.

- **plain-text** Readable message to be sent during communications.
- **cipher** method for transforming plain-text
- **key** parameter for cryptographic algorithm
- **cipher-text** Unreadable form of the message

Cryptography

- **Symmetric cryptography** Both parties share a secret key for encryption and decryption
- **Asymmetric cryptography** Each individual has a public and a private key. Parties use the public keys for encryption and the private keys for decryption

GSM

Global System for Mobile Communications (GSM) is a 2G telecommunication standard developed in the early 90's by the European Telecommunications Institute. Has become one of the most widely used standards, reaching an 80% market share at its height.

UMTS

Universal Telecommunications Standard (UMTS) is 3G telecommunication standard based on GSM by the Third Generation Partnership Project.

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

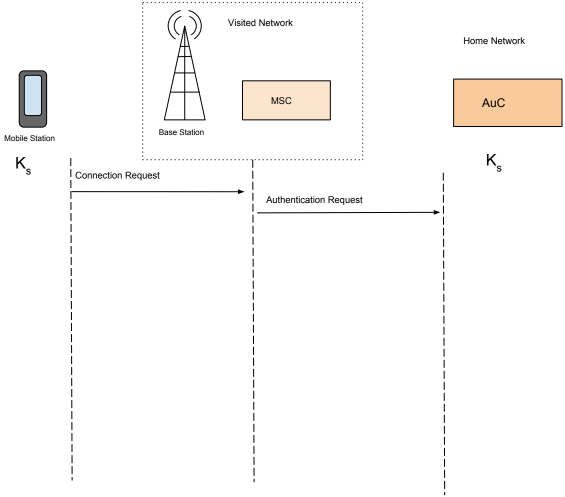
4 EM Leaking Key Information

5 conclusion

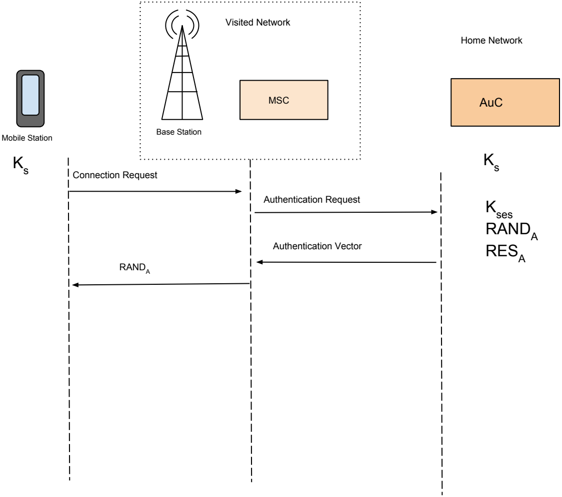
Encryption in GSM and UTMS

- GSM and UMTS both have secret keys that are shared between the mobile and the mobile's home network authentication center.
- GSM and UMTS both utilize the A5 family of encryption algorithms.
    - A5/0
    - A5/1
    - A5/2
    - A5/3

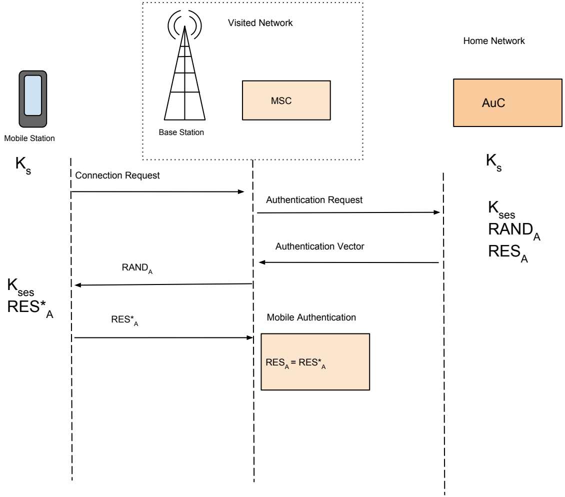
GSM Authentication



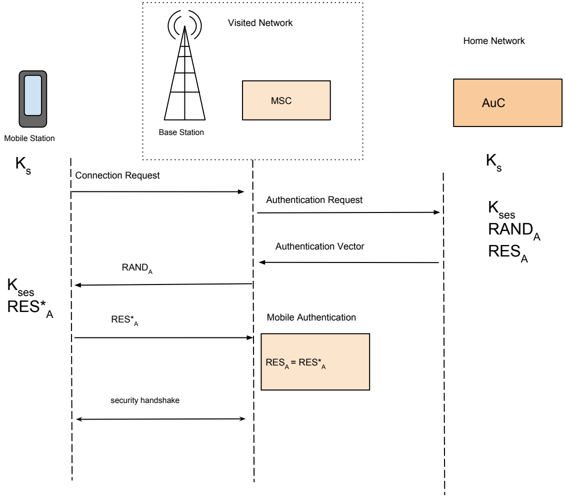
GSM Authentication



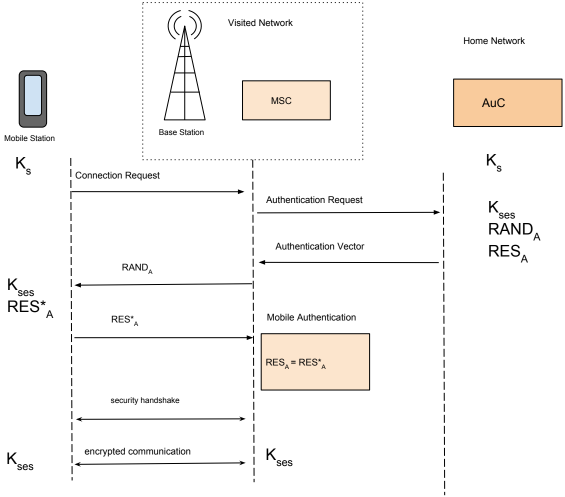
GSM Authentication



GSM Authentication



GSM Authentication



Inter-working Networks

Man-in-the-middle Attack

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
- Applications
- Solution

4 EM Leaking Key Information

5 conclusion

Applications (Apps)

Application Permissions in Android

Application Threat keyboard Key-logger

KBS Checker

Outline

1 Background

2 GSM Weakness in UMTS

3 Application Security Threat

4 EM Leaking Key Information
- Side channel attack
- Side channel through EM

5 conclusion

What is a Side channel attack?

RSA Example

Ranged Side channel

Findings

Solution

Outline

1 Background

2 GSM Weakness in UMTS

3 Application Security Threat

4 EM Leaking Key Information

5 conclusion

Conclusion

Questions

Questions?