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. Ranged Side-channel Attack
5. Conclusion

Outline

1. Background
   - Cryptography
   - GSM and UMTS
2. GSM Weakness in UMTS
3. Application Security Threat
4. Ranged Side-channel Attack
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-text** Unreadable form of the message
- **key** parameter for cryptographic algorithm or cipher
- **cipher** method for transforming plain-text
  - **Encrypt** transform plain-text to cipher-text
  - **Decrypt** transform cipher-text back into plain-text

Shift Cipher

“Hello World!” $\xrightarrow{\text{Shift letters by 1}}$ *“Ifmmp Xpsme!”*

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 and UMTS

- Global System for Mobile Communications (GSM) is a 2G telecommunication standard developed in the early 90s by the European Telecommunications Institute. Has become one of the most widely used standards, reaching an 80% market share at its height.
- Universal Telecommunications Standard (UMTS) is 3G telecommunication standard based on GSM by the Third Generation Partnership Project in the early 2000s.

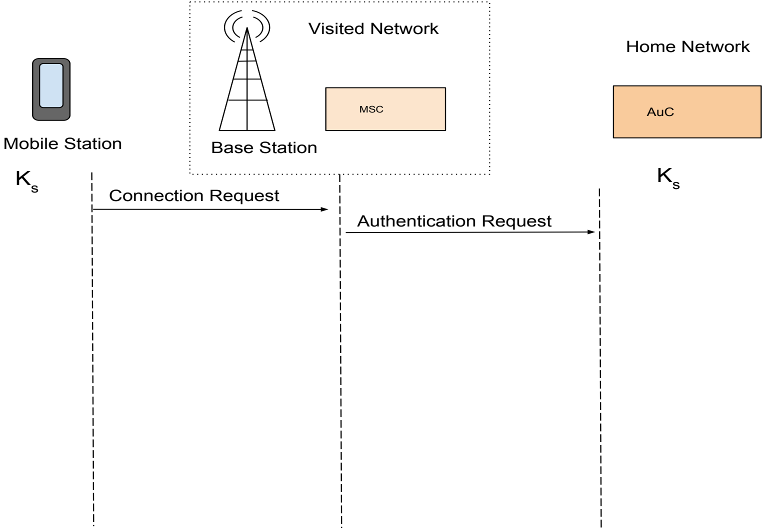
Outline

1. Background
2. GSM Weakness in UMTS
   - Authentication
   - Man-in-the-middle Attack
   - GSM and UMTS Inter-working Networks
   - Solution
3. Application Security Threat
4. Ranged Side-channel Attack
5. Conclusion

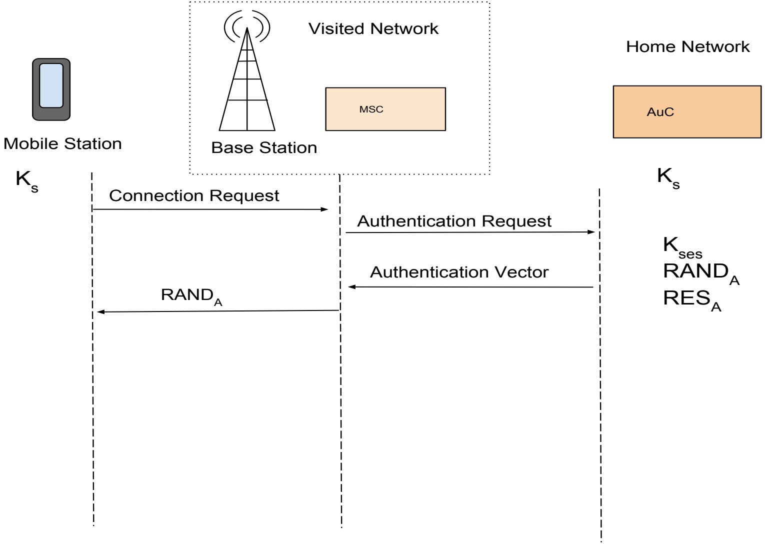
Encryption in GSM and UTMS

- 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

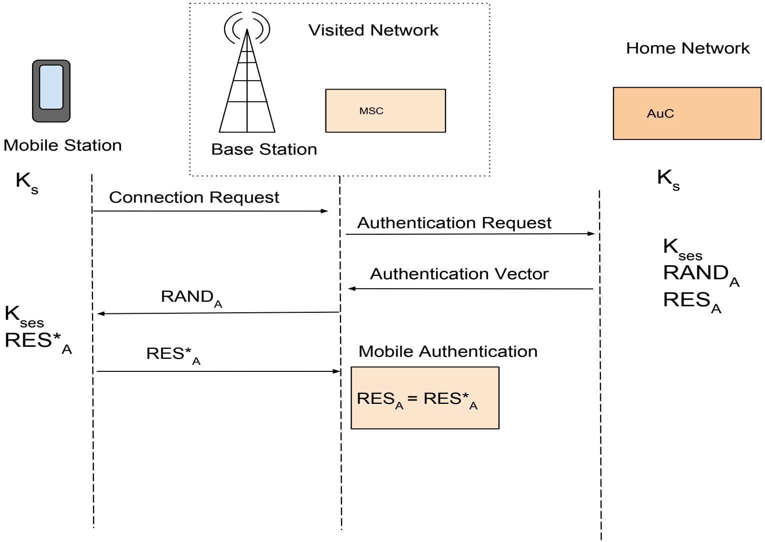
GSM Authentication



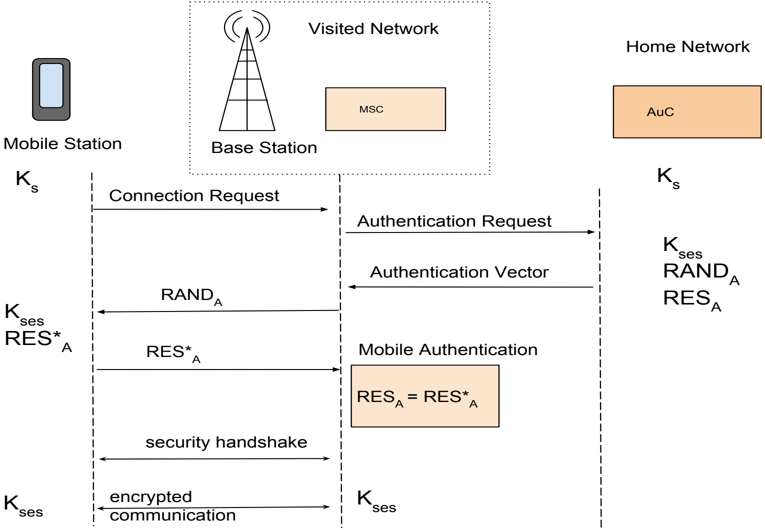
GSM Authentication



GSM Authentication

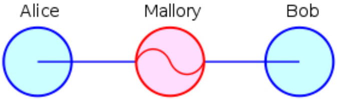


GSM Authentication



Man-in-the-middle Attack

Man-in-the-middle attack is a type of attack in Cryptography where an attacker tricks participants into sending their communications through the attacker.



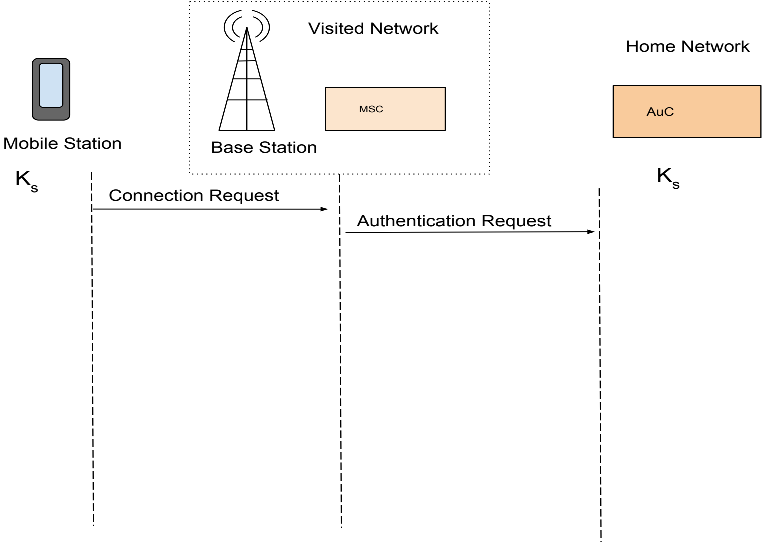
Man-in-the-middle Attack

1. Mallory intercepts Alice's message to Bob asking for his public key.
   Alice: "Hi Bob, it's Alice send me your key" → *Mallory*
2. Mallory relays the message to Bob; Bob cannot tell if the message is really from Alice
   Mallory "Hi Bob, it's Alice send me your key" → *Bob*
3. Bob responds with his key
   Mallory ←[key_{bob}] *Bob*

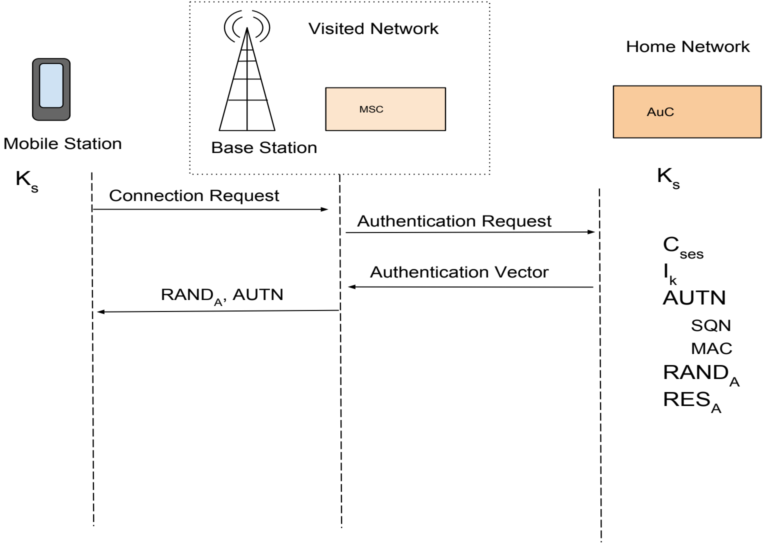
Man-in-the-middle Attack

4. Mallory replaces Bob's key with her own, relays this to Alice, claiming that it is Bobs key
   $Alice \longleftarrow [\text{key}_{Mallory}]\ Mallory$
5. Believing communication is secure Alice sends Bob a message believing only he can read it.
   Alice "send \$2000 to account 2034"$[\text{key}_{Mallory}]$
   $\longrightarrow Mallory$
6. Because the message is encrypted with Mallory's key, Mallory can decrypt it, read and modify this message if she so desires, reencrypt it with Bob's key and Bob forward it to Bob who believes it is a secure message from Alice.
   Mallory "send \$2000 to account 1099"$[\text{key}_{Bob}] \longrightarrow Bob$

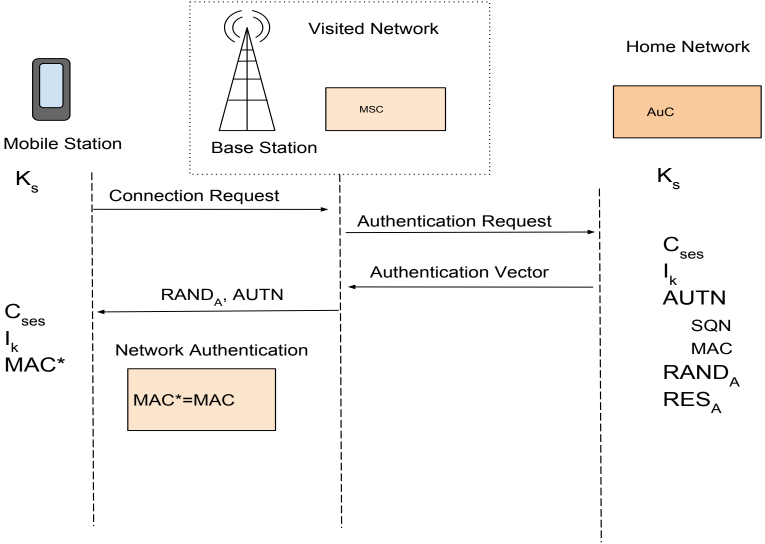
UMTS Authentication



UMTS Authentication



UMTS Authentication



Transitional Networks

bullet points?
There are transitional periods between old and new technologies such as GSM and UMTS are required as old infrastructure and devices are replaced with the new. During these periods both old and new technologies will need to be able to successfully interact with one another.
2011 survey where 2G devices had around 90% population coverage where as 3G only had 45%

Inter-working networks GSM and UMTS Hand Over

In order for GSM and UMTS systems to work all UMTS systems must be capable of performing GSM communication. For encryption this means there needs to be ways of transforming 128 bit UMTS keys into the 64 bit GSM keys
– describe Hand over–

Conversion

$$K_{ses} = c_3(I_K, C_{ses}) = C_{ses1} \oplus C_{ses2} \oplus I_{K1} \oplus I_{K2} \tag{1}$$

$$C_{ses} = c_4(K_{ses}) = K_{ses} \| K_{ses} \tag{2}$$

$$I_K = c_5(K_{ses}) = K_{ses1} \oplus K_{ses2} \| K_{ses} \| K_{ses1} \oplus K_{ses2} \tag{3}$$

GSM Man-in-the-middle weakness in UMTS

1. Meyer et al describe a Man-in-the-middle attack against UMTS using GSM's man-in-the-middle weakness.
2. An attacker sets up a dummy base station tricks a UMTS device into connecting to it
3. Attacker relays messages between mobile device and the legitimate network
4. During Hand Shake procedure the attacker selects A5/0 algorithm

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

Additional authentication step would be performed when a UMTS device would be switching from a UMTS base station to a GSM base station.

Outline

1. Background

2. GSM Weakness in UMTS

3. Application Security Threat
    - Applications
    - Solution

4. Ranged Side-channel Attack

5. Conclusion

Applications (Apps)

- Applications or Apps are software designed to run on mobile devices
- Apple reported 40 billion app downloads in first quarter of 2013
- Apps pose a security threat as they can have access to both user and the system such as to access contacts and send messages.

Application Threat keyboard Key-logger

- Mohsen et al. describes the possibility of an Android keyboard application that acts as a key-logger
- A key-logger is a device or piece of software that records key strokes
- user names, passwords and credit card numbers

Application Permissions in Android

Normal permissions

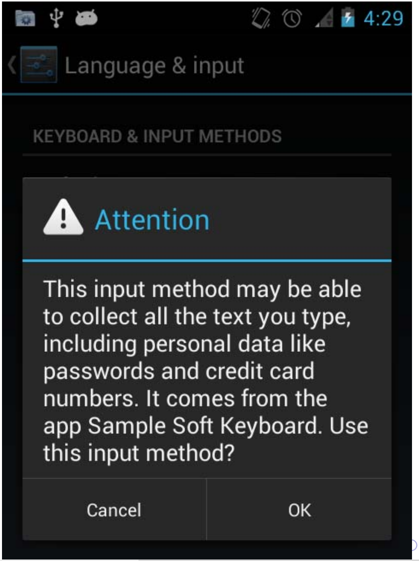
Dangerous permissions
Example would be the ability to access user data, send SMS messages, access camera.

KBS Checker

KBS Checker

- Reads app Permissions
- Looks for dangerous combinations of permissions
- Warns user with the app's name and the threat it could pose

KBS Checker



Attention

This input method may be able to collect all the text you type, including personal data like passwords and credit card numbers. It comes from the app Sample Soft Keyboard. Use this input method?

Outline

1. Background
2. GSM Weakness in UMTS
3. Application Security Threat
4. Ranged Side-channel Attack
   - Side channel attack
   - Side channel through EM
5. Conclusion

Ranged Side channel

Kenworthy et al. described an attack using inexpensive radio equipment to capture and analyze electro magnetic (EM) to perform a ranged side-channel attack.

What is a Side channel attack?

- Cryptographic attack like man-in-the middle
- Uses physical properties of the machine doing the encryption revealing by-products of the encryption process.
- physical properties can include things such as cpu heat, power consumption or even sound.

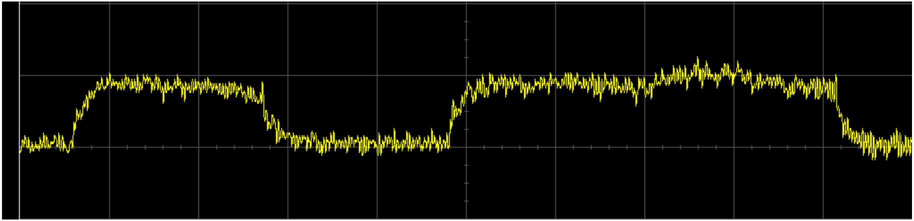
RSA

RSA

- Commonly used asymmetric cipher used for key establishment
- Uses Square and Multiply method for more efficient modular exponentiation of large positive numbers.

Square and Multiply

$$x^n = \begin{cases} x(x^2)^{\frac{n-1}{2}} & : \text{if n is odd} \\ (x^2)^{\frac{n}{2}} & : \text{if n is even} \end{cases}$$



Findings

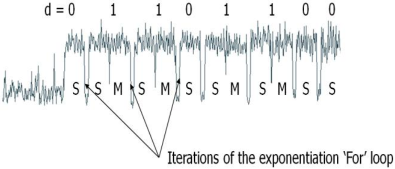
Findings

- tested on multiple os and devices
- tested multiple algorithms

Solution

- add noise to RSA
- Bulk encryption

RSA EM Attack



Outline

1 Background

2 GSM Weakness in UMTS

3 Application Security Threat

4 Ranged Side-channel Attack

5 Conclusion

Conclusion

Questions

Questions?

References