Improving Mobile Security

Braden Luthi

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

29 April 2014

Outline

Outline

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.

Transitional Periods

- 2011 survey where 2G devices had around 90% population coverage where as 3G only had 45%

Transitional periods

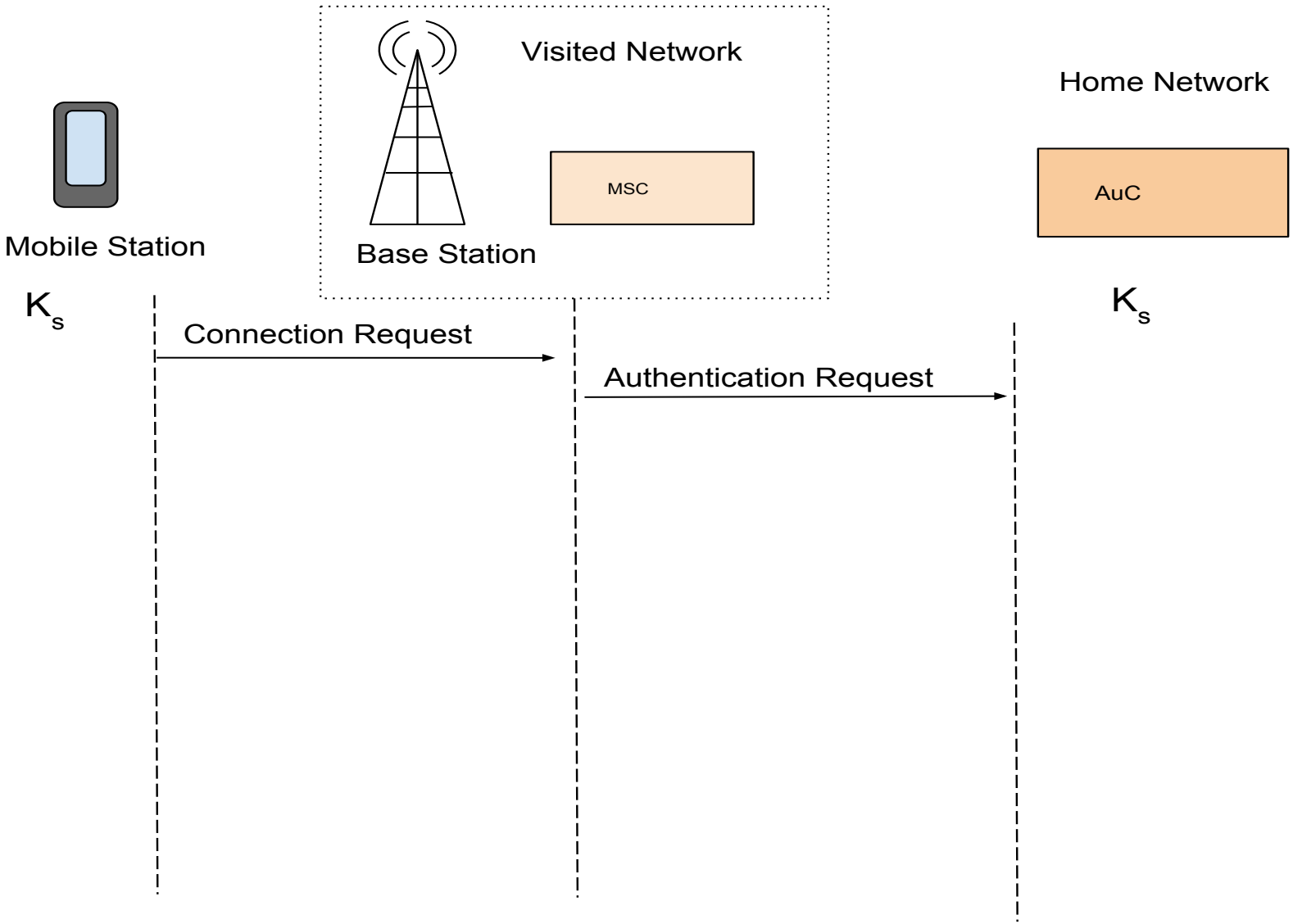
- Periods between old and new technologies
- Old and new technologies will need to work together creating Inter-working networks
- Periods will last as long as the old technology continues to be used

Outline

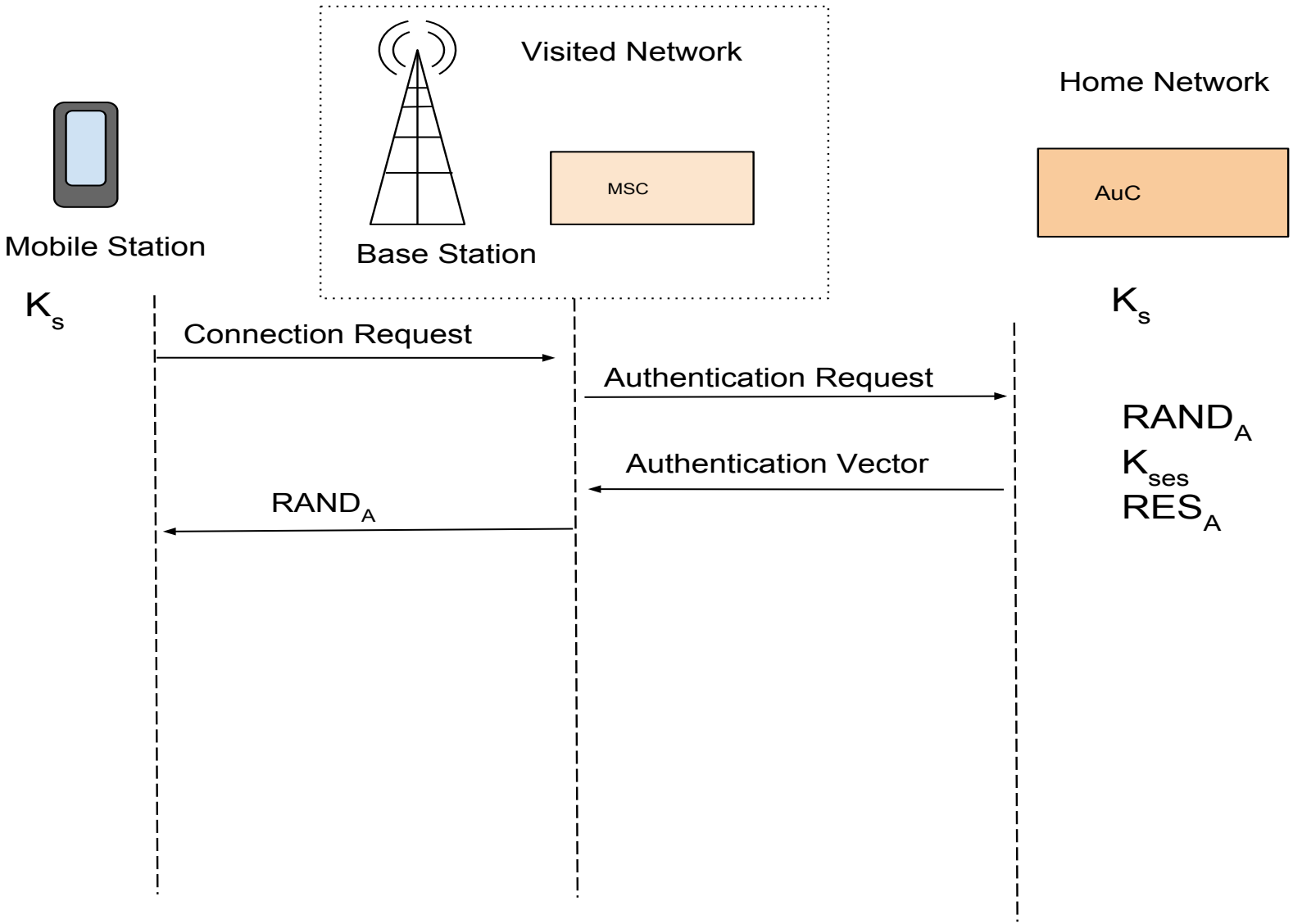
Encryption in GSM and UTMS

- GSM and UMTS both have secret keys that are shared between the mobile and the mobile's home network authentication center.
- Keys in GSM are 64 bits
- Keys in UMTS are 128 bits
- GSM and UMTS both utilize the A5 family of encryption algorithms.
  - A5/0
  - A5/1
  - A5/2
  - A5/3

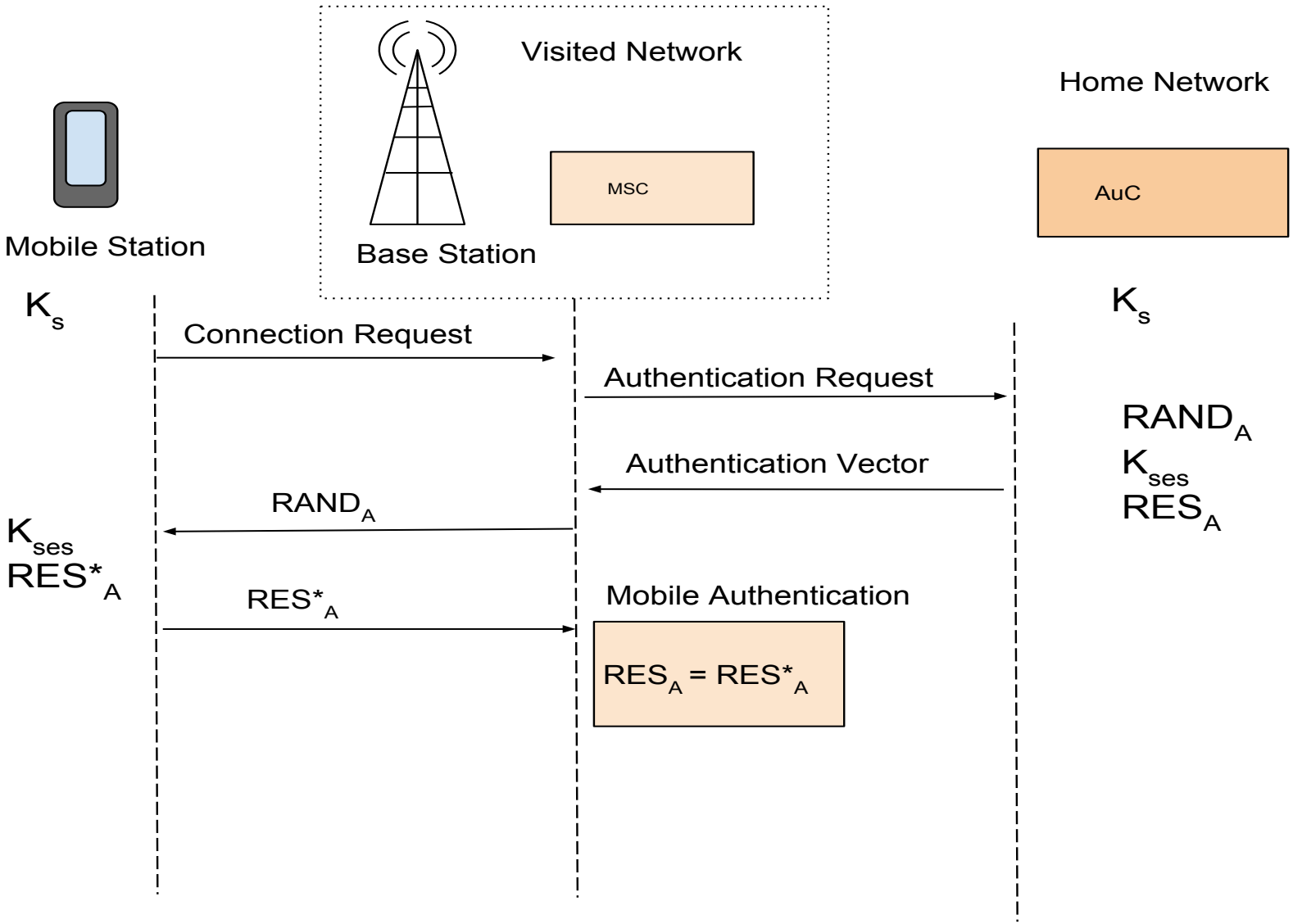
GSM Authentication



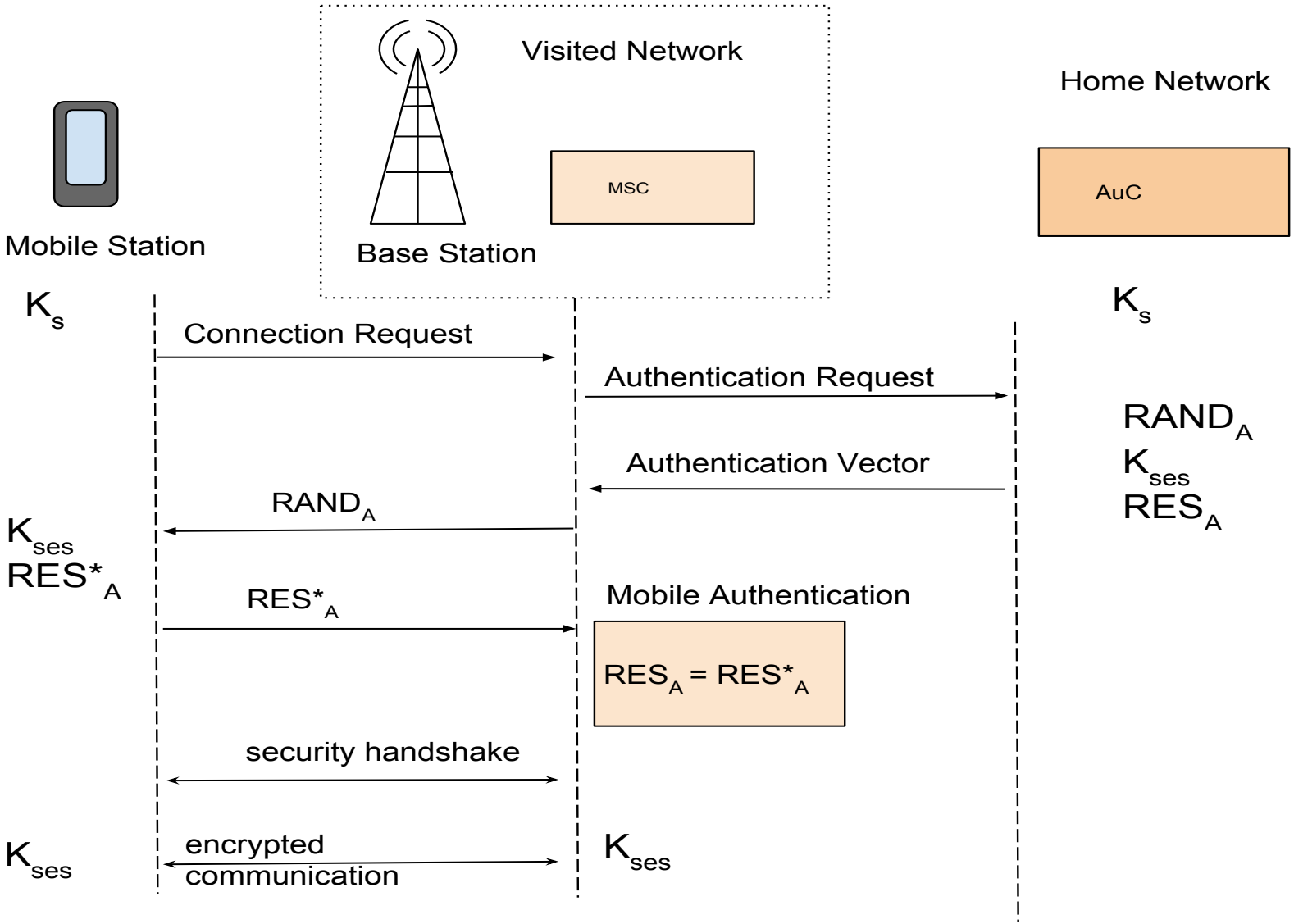
GSM Authentication



GSM Authentication

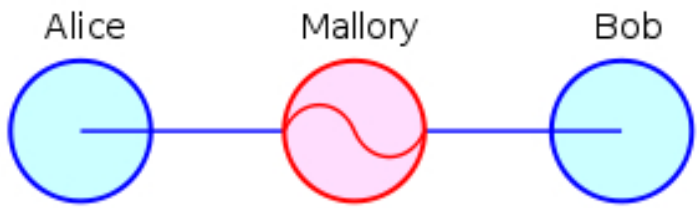


GSM Authentication



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" $\rightarrow$ *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" $\rightarrow$ *Bob*
3. Bob responds with his key
   Mallory $\leftarrow [\text{key}_{bob}]$ *Bob*

Man-in-the-middle Attack

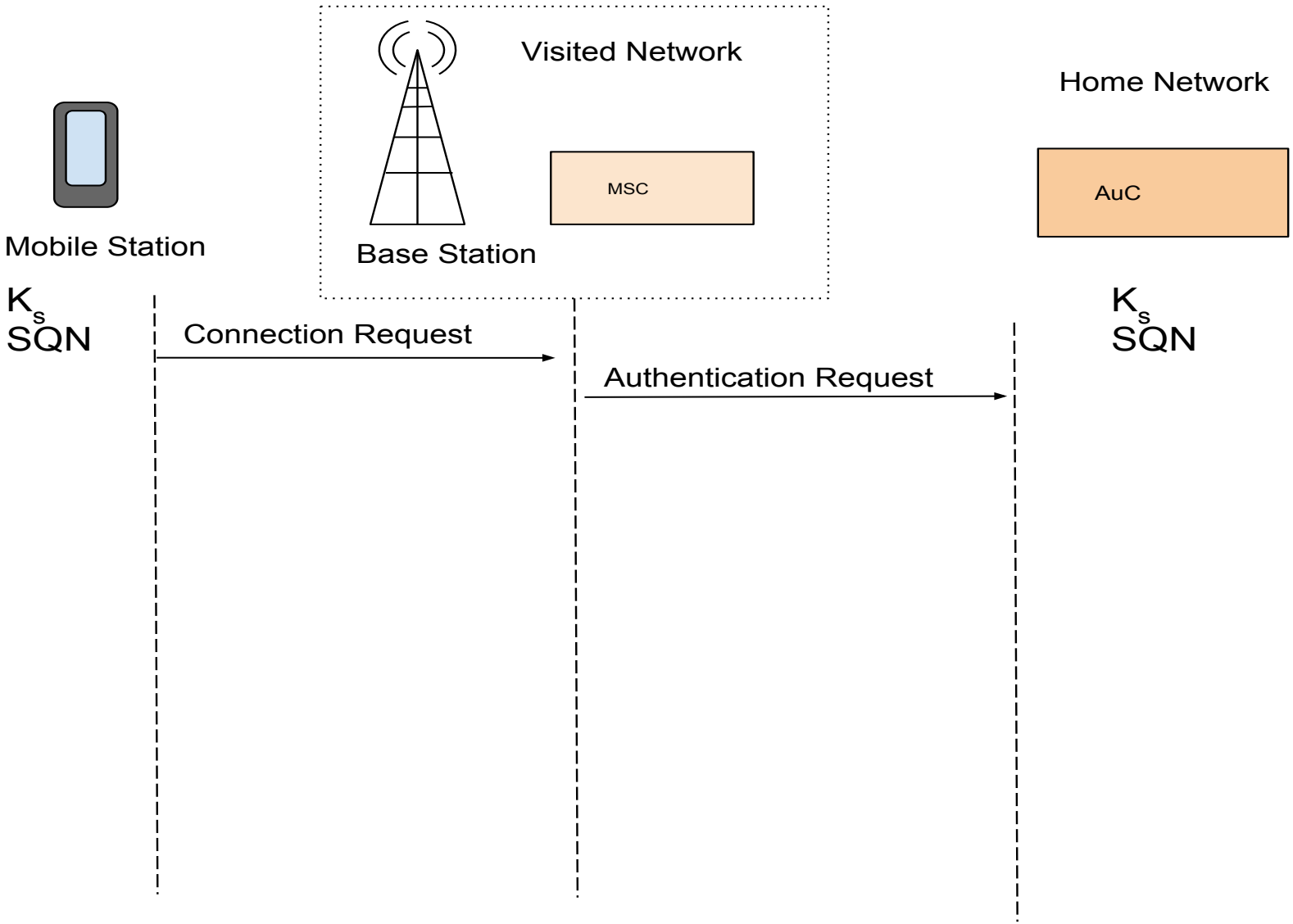
4. Mallory replaces Bob's key with her own, relays this to Alice, claiming that it is Bobs key
   Alice $\leftarrow$[key$_{Mallory}$] *Mallory*
5. Believing communication is secure Alice sends Bob a message believing only he can read it.
   Alice "send $2000 to account 2034"[key$_{Mallory}$]
   $\rightarrow$ *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 $2000 to account 1099"[key$_{Bob}$] $\rightarrow$ *Bob*

GSM Man-in-the-middle attack

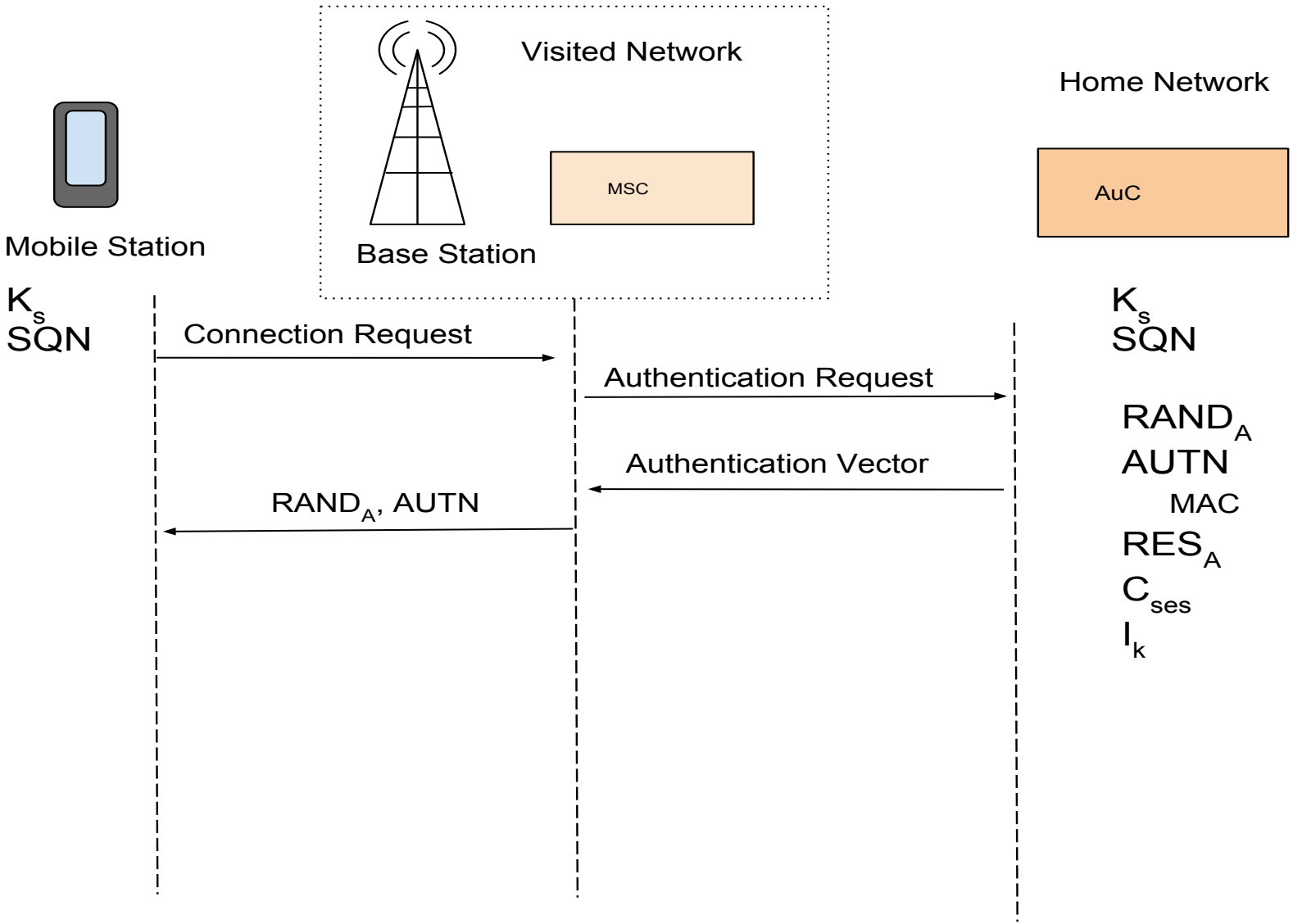
1. An attacker impersonates a GSM base station and tricks a device into connecting to it
2. Attacker relays messages between mobile device and the legitimate network
3. During Hand Shake procedure the attacker can select A5/0 algorithm

With this done the attacker can listen in on or even edit communications between the mobile and legitimate network.

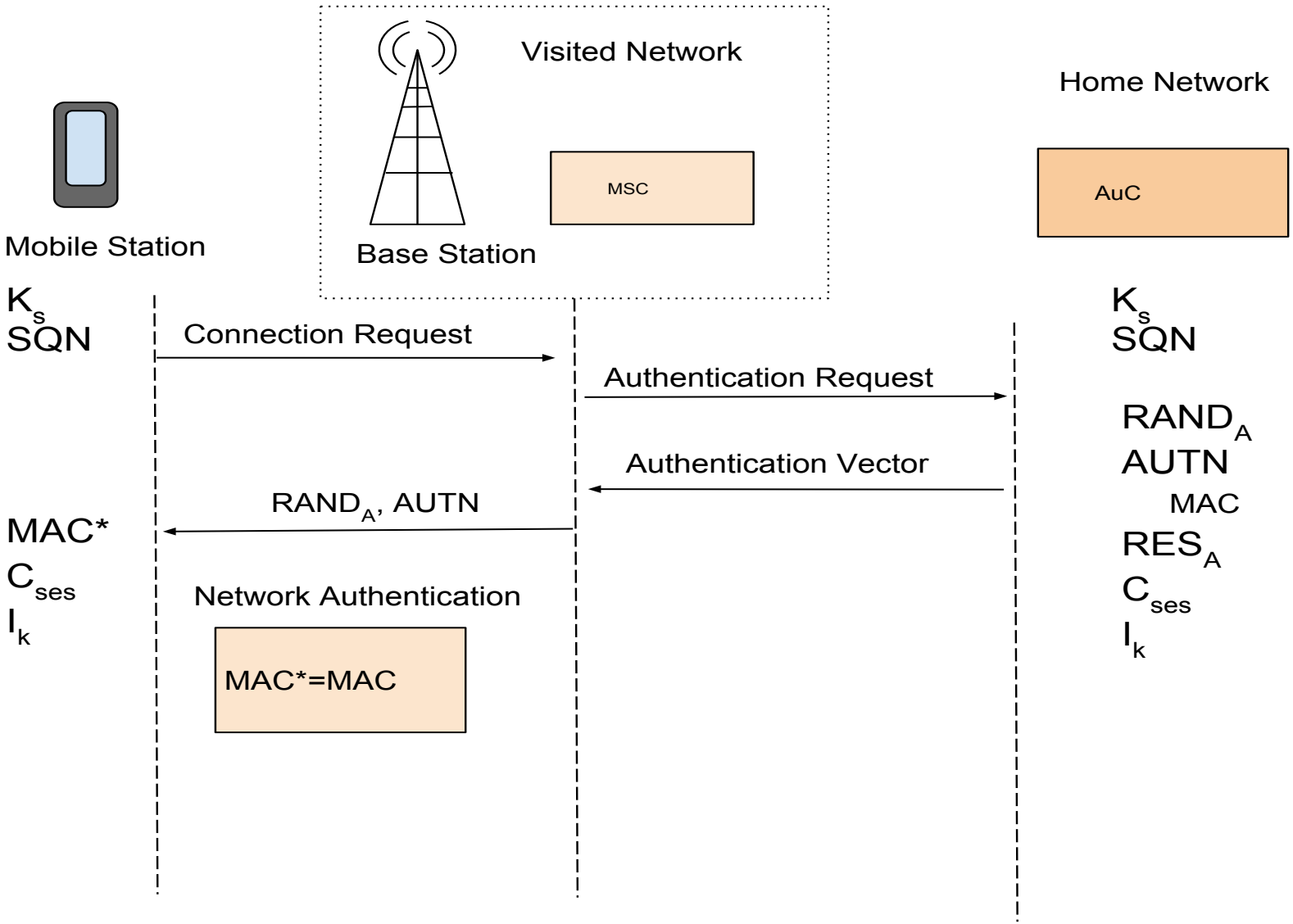
UMTS Authentication



UMTS Authentication



UMTS Authentication



Inter-working networks GSM and UMTS Hand Over

- UMTS systems must be capable of performing GSM
- Handover is when a mobile switches base stations during communication
- For encryption this means there needs to be ways of transforming 128 bit UMTS keys into the 64 bit GSM keys and vise versa

Conversion

GSM: $K_{ses} \longleftrightarrow UMTS$:C_{ses}, I_K
$\oplus$: EXOR
$\|$: Append

UMTS to GSM

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

GSM to UMTS

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

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

GSM Man-in-the-middle weakness in UMTS

Meyer et al describe a Man-in-the-middle attack against UMTS using GSM's Man-in-the-middle weakness.

1. An attacker sets up a dummy base station tricks a UMTS device into connecting to it
2. Attacker relays messages between mobile device and the legitimate network
3. During Hand Shake procedure the attacker selects A5/2 algorithm using a known attack is able to get the session key.

Once the session key is obtained an attacker can use the key transformation functions whenever a handover is preformed.

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

Additional authentication and key generation step would be performed before a handover procedure.
Protects broken session keys from being transformed and carried over after the handover.

Outline

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 data and the system methods 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
Give an application access to application-level features

Dangerous permissions
Give an application access to user information or system features.

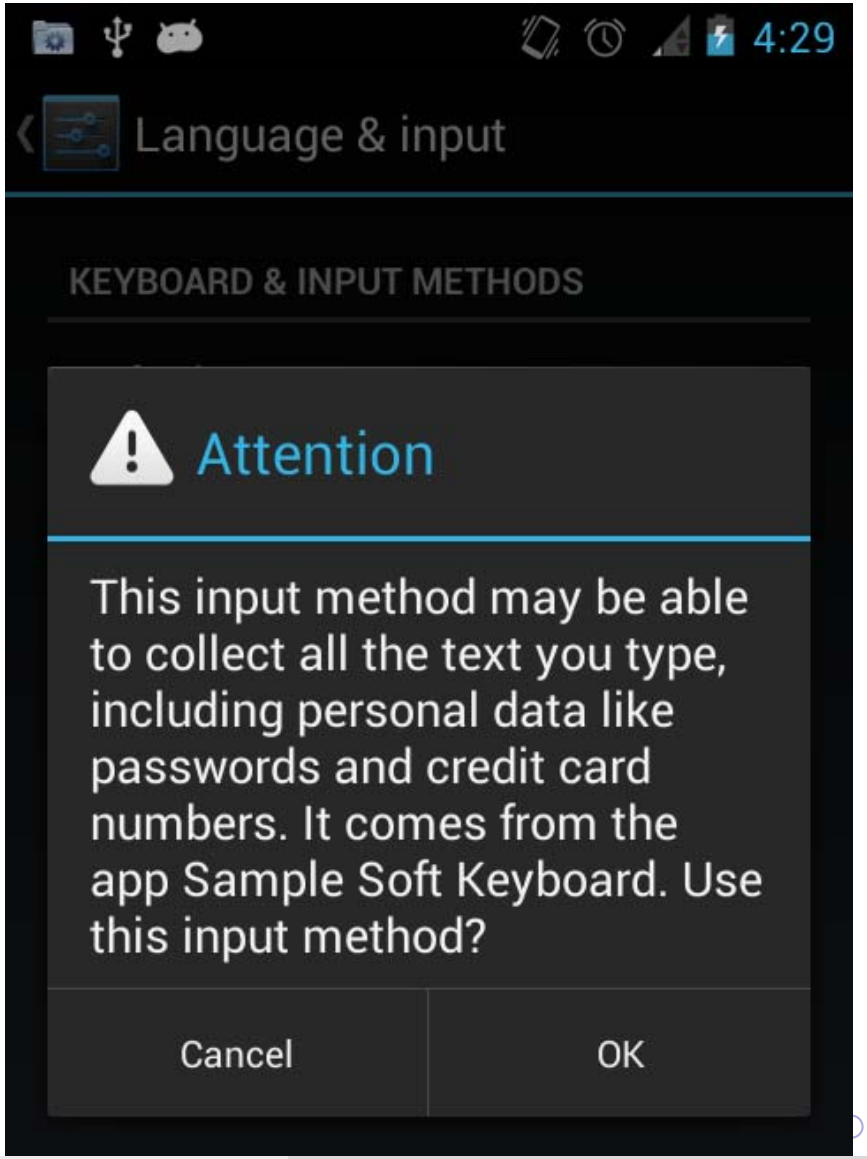
- Permissions are declared in an XML file read during app installation
- Dangerous permissions must be accepted by the user.

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



Outline

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.
- Attacker can analyze these by-products to discover crucial parts of the cryptographic process such as portions of plain-text or key

RSA

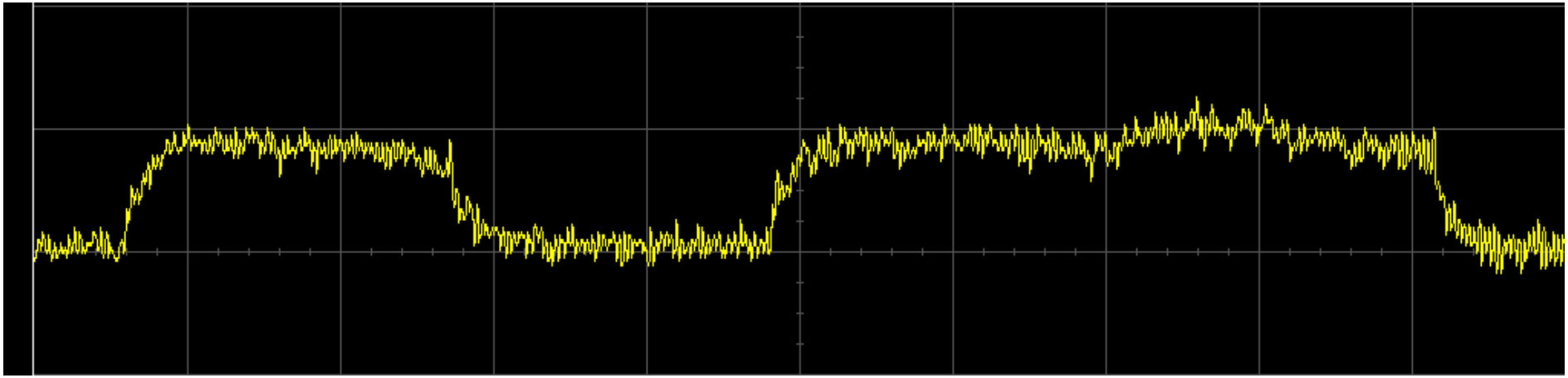
RSA

- 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

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

Power analysis attack on RSA



- Shorter spikes in power consumption are a squaring(S) operation
- Longer spikes in power consumption are a square and multiply(SM) operation
- S: 0 in the key
- SM: 1 in the key

Findings

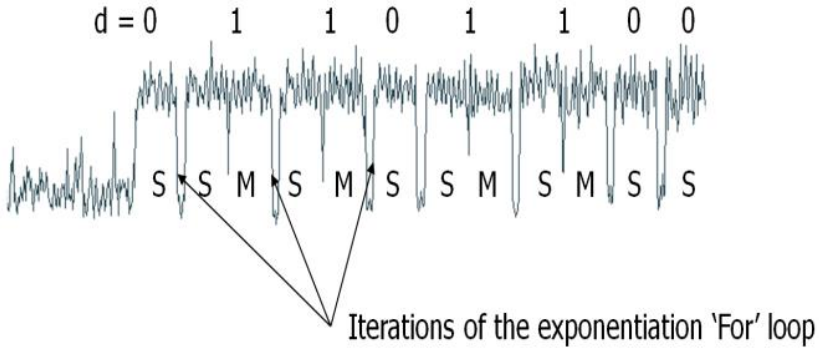
Findings

- tested on multiple os and devices
- tested multiple algorithms

Solution

- add noise to RSA
- Bulk encryption

RSA EM Attack



Outline

Conclusion

Security is often difficult to do as technology continues to rapidly advance old technologies that were once secure become insecure and new technologies continue to add to complexity and need for security.

Questions

Questions?