Mobile Computing Architecture– an overview

Lesson 08

Security Issues

Security

- Important for maintaining privacy and for secure mobile e-business transactions
- Wireless security mechanisms for providing security of the data transmitted from one end point to another

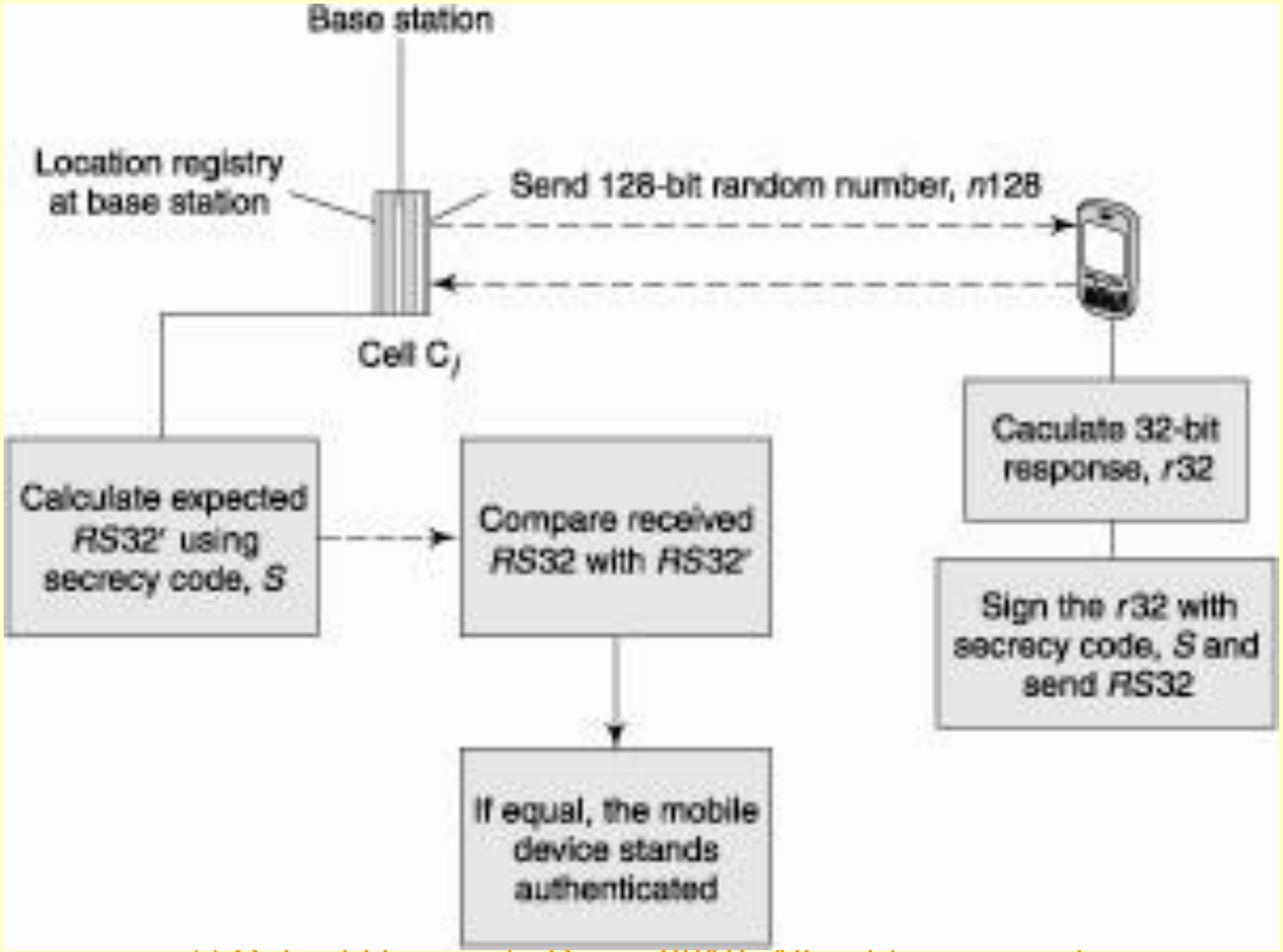
Security

- Provides for wire-equivalent privacy and non-repudiation when some data i sent to an end-point
- No denial of service to authenticated object(s)

Security

- A serving station authenticated before it can provide service to mobile devices

The authentication method of security in case of GSM


Base station
Location registry at base station
Send 128-bit random number, r128
Cell C$_j$
Caculate 32-bit response, r32
Sign the r32 with secrecy code, S and send RS32
Calculate expected RS32' using secrecy code, S
Compare received RS32 with RS32'
If equal, the mobile device stands authenticated

Cryptography

- keep information private and prevent from getting into the hands of unauthorized agents
- Encryption— the transformation of data into coded formats
- Encrypted data decrypted (transformed back to an intelligible form) at its destination

Cryptography Algorithms

- Used for encryption and decryption of transmitted data
- Enable the receiver and the sender to authenticate data
- Discover if data security has been compromised during transmission

Cryptography Algorithms

- Use a secret key, to encrypt data into secret codes for transmission
- RSA (Rivest, Shamir, Adleman) algorithm is a cryptography algorithm used for private key generation.

Cryptography algorithms

- Classified into two categories; symmetric and asymmetric
- Used to create a *hash* of the message or a MAC (message authentication code)

Hash function

- Used to create a small digital fingerprint of the data to be transmitted
- Fingerprint is called the hash value, hash sum, or, simply, hash.
- Hash of the message is a set of bits obtained after applying the hash algorithm (function).
- This set of bits alters in case the data is modifies during transmission

Message authentication codes (MAC)

- Also used to authenticate messages during transmission
- The MAC of a message created using a cryptographic MAC function which is similar to the hash function but has different security requirements

Message authentication codes (MAC)

- The receiver reviews the hash or the MAC of the received message and returns it to the sender
- Exchange enables the sender and the receiver to find out if the message has been tampered with and thus helps verify message integrity and authenticity.

Data encryption standard (DES)

- Uses 56-bits for a key plus 8 bits for parity.
- Block length 64 bit. [Maximum block size = 2^{64} bits

Triple DES

- Triple DES an enhance version of DES
- Multiple encryptions or encryption-decryption-encryption steps in the cryptic message— A different key at each step for cryptic message creation

Advanced encryption standard (AES)

- 9 possible combinations of key lengths and block lengths
- The key-length can be 128, 192, or 256 bits
- The block lengths can also be 128, 192, or 256 bits
- Block length of 128 bits means maximum block length = 2^{128} bits.

RSA– The Asymmetric key based standard

- The RSA (Rivest, Shamir, Alderman) algorithm uses 128, 256, 512, or 1024 bit prime numbers for encryption

DSA (Digital Signature Algorithm)

- Used to sign a record before transmitting
- Provides for a variable key length of maximum 512 or 1024 bits

DSS (Digital Signature Standard)

- Based on the DSA
- Signature enables identification of the sender
- identifies the origin of the message, and
- checks the message integrity

Digital certificate

- An electronic certificate used to establish the credentials of a data set.
- Issued by a certification authority and contains the certificate holder's name, a copy of the certificate holder's public key, a serial number, and expiration dates.

Digital certificate

- Includes the digital signature of the certificate-issuing authority for verification of the authenticity of the certificate
- The certification authority distributes a digital certificate, which binds a public key to a specific sender

Summary

- Cryptographic algorithms
- Hash
- MAC
- DES, Triple DES
- AES
- RSA
- Digital signatures and certificates

End of Lesson 08

Security Issues