

GSM Security Issues

Iowa State University

Department of Computer Engineering

Wei Zhang

Nov. 15, 2000

References

1. New authentication protocol for GSM networks
Al-Tawil, Khalid (King Fahd Univ of Petroleum and Minerals) Akrami, Ali | Youssef, Habib
Source: Conference on Local Computer Networks Oct 11-14 1998 1998 Sponsored by: IEEE
IEEE p 21-30 0742-1303
2. New authentication protocol for roaming users in GSM networks
Al-Tawil, Khalid (King Fahd Univ of Petroleum and Minerals) Akrami, Ali
Source: IEEE Symposium on Computers and Communications - Proceedings Jul 6-Jul 8 1999
1999 Sponsored by: IEEE Communications Society; IEEE Computer Society IEEE p 93-99
3. Secure communication mechanisms for GSM networks
Lo, Chi-Chun (Natl Chiao-Tung Univ) Chen, Yu-Jen
Source: IEEE Transactions on Consumer Electronics 45 4 1999 IEEE p 1074-1080 0098-3063
4. Secure communication architecture for GSM networks
Lo, Chi-Chun (Natl Chiao-Tung Univ) Chen, Yu-Jen
Source: IEEE Pacific RIM Conference on Communications, Computers, and Signal Processing -
Proceedings Aug 22-Aug 24 1999 1999 IEEE p 221-224
5. A brief overview of GSM
John Scourias
<http://kbs.cs.tu-berlin.de/~jutta/gsm/js-intro.html>, 1994
6. Mobility and security management in the GSM system and some proposed future
improvements
A. Mehrotra, L. S. Golding
Proceedings of the IEEE, vol. 86, Issue 7, July 1998
7. GSM security: a description of the reasons for security and the techniques
Charles Brookson
IEE, 1994
8. GSM protocol architecture: radio subsystem signaling
M. Mouly, M. B. Pautet
Proceedings of the IEEE, vol. 86, Issue 7, July 1998
9. Overview of the GSM system and protocol architecture
Moe Rahnema
IEEE Communication magazine, pp 92-100, April 1993
10. Integration of intelligent network services into future GSM networks
Mikko Laitinen, Jari Rantala
IEEE communication magazine, pp 76- 86, June 1995

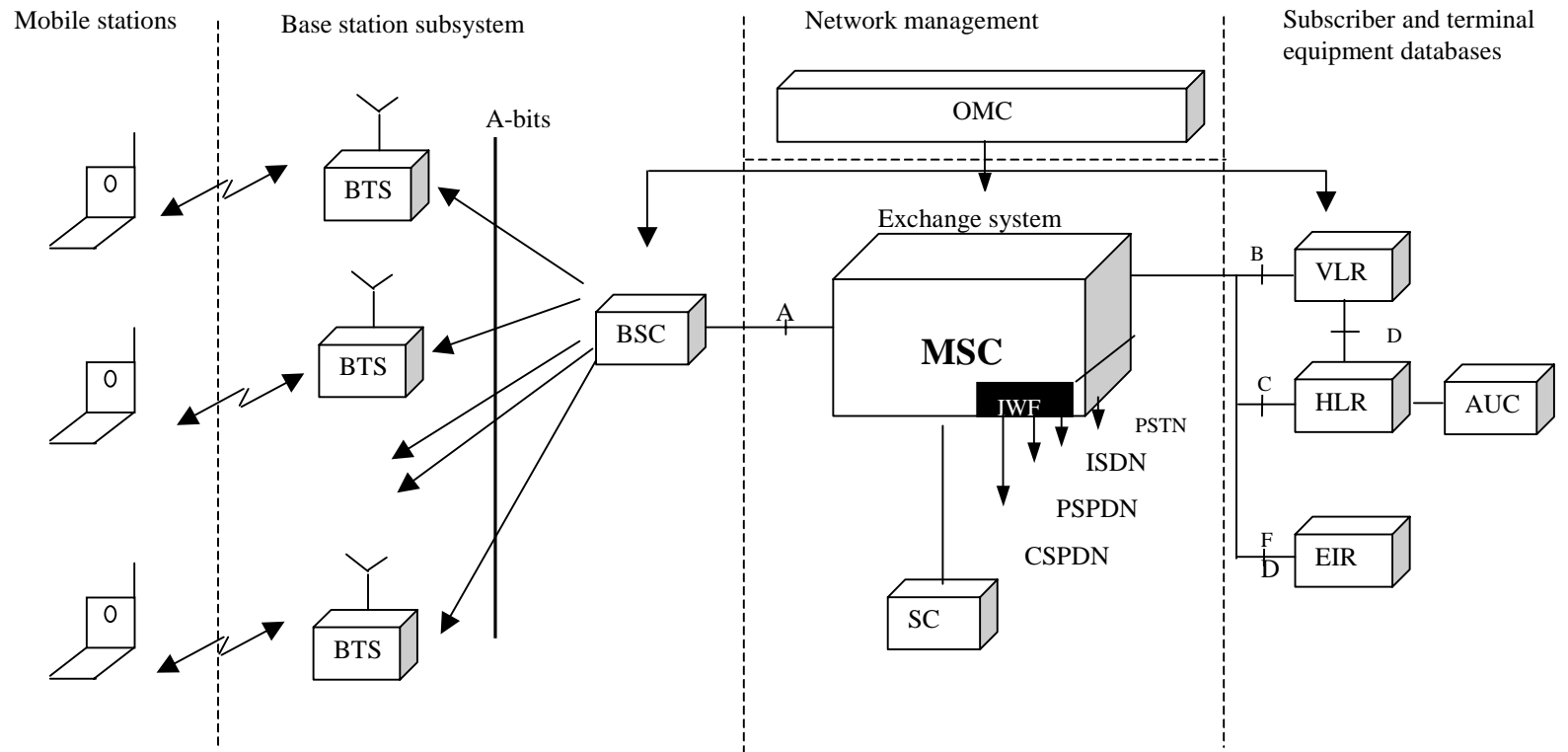
Contents

- Introduction
- GSM Architecture
- Security Issues
 - Security attacks
 - Security services provided by GSM
 - Security architectures and comparison

Introduction

- What is GSM
- Criteria that GSM has to meet
 - good subjective speech quality
 - support for international roaming
- Services provided by GSM
 - bearer service, teleservices, supplementary service

GSM Architecture



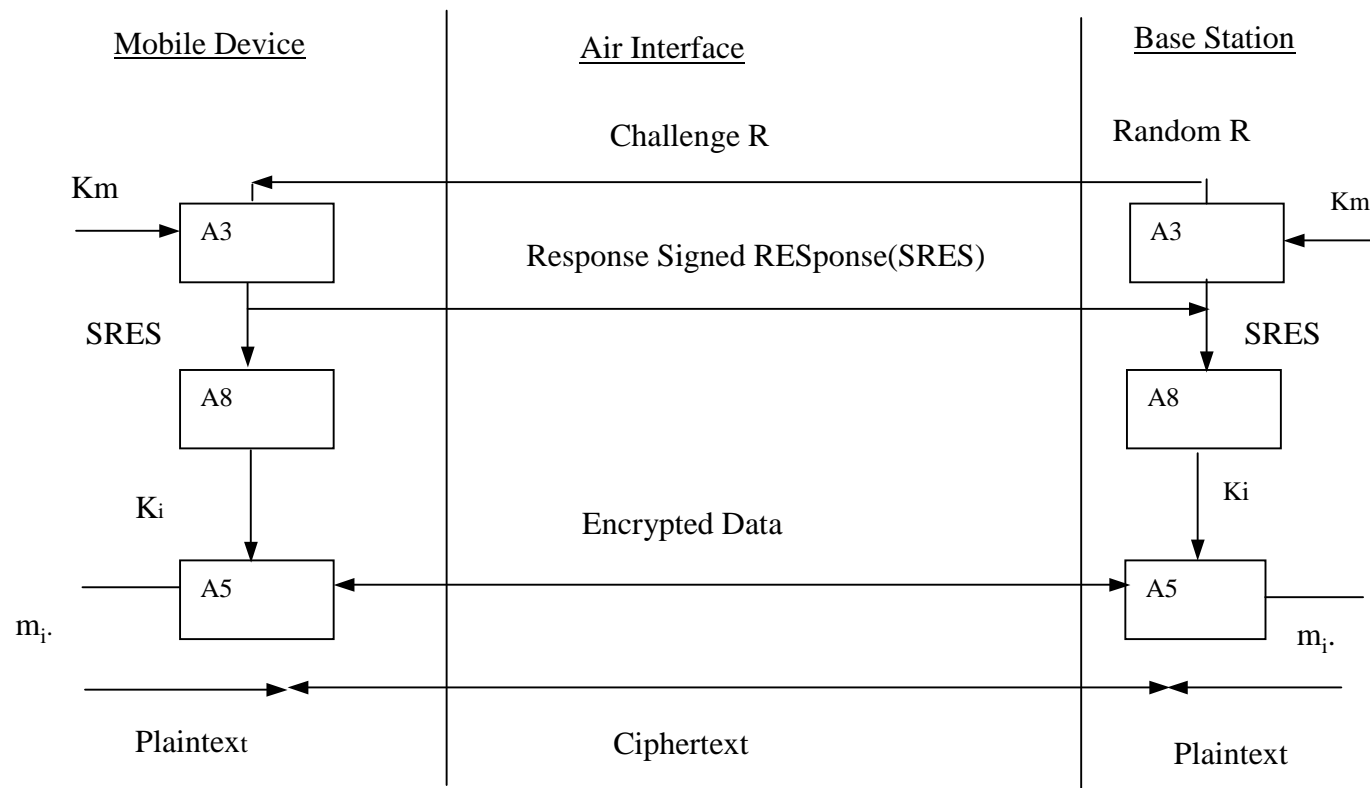
GSM Security

- Security Attacks
 - Replay attack
 - Guessing attack
 - Interleaving attack
 - Man-in-middle attack

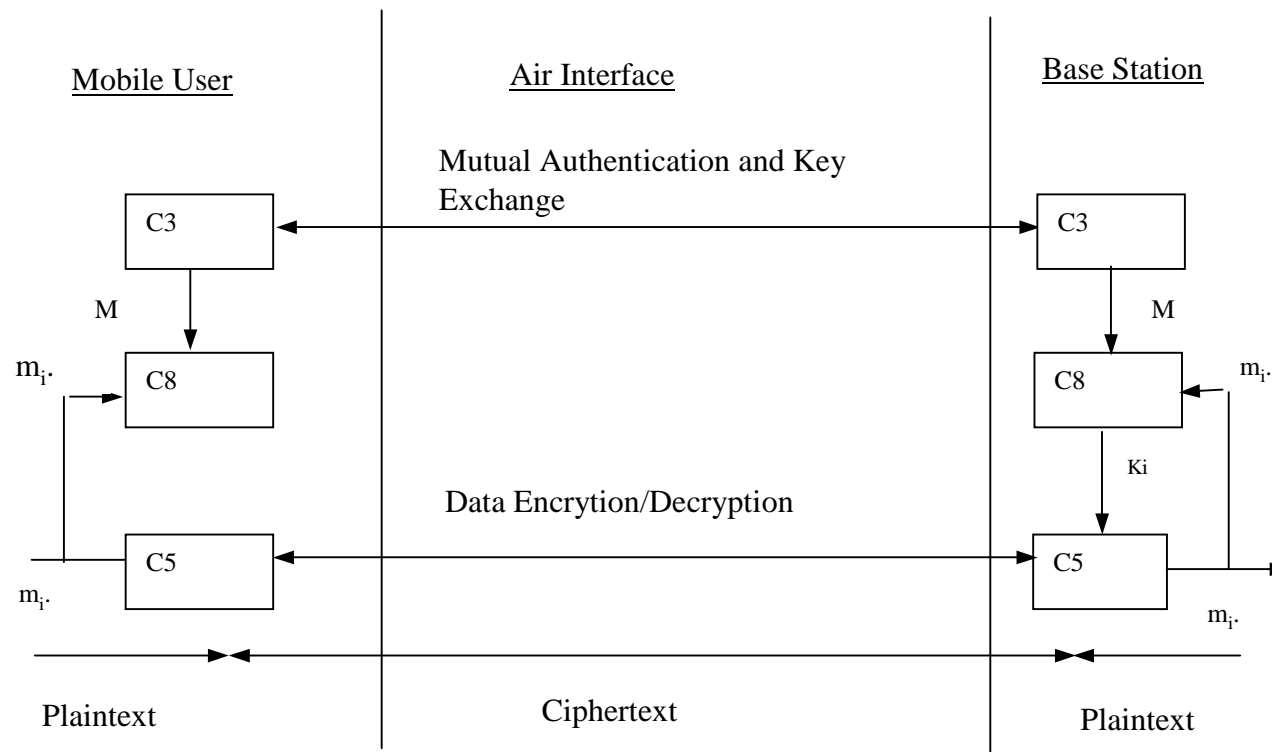
GSM Security(Cont.)

- Security service provided by GSM
 - Anonymity:so that it is not easy to identify the user of the system
 - Authentication:so the operator knows who is using the system for billing purpose
 - User Data and signaling protection: so that user data passing over the radio path is protected

Security Architecture I

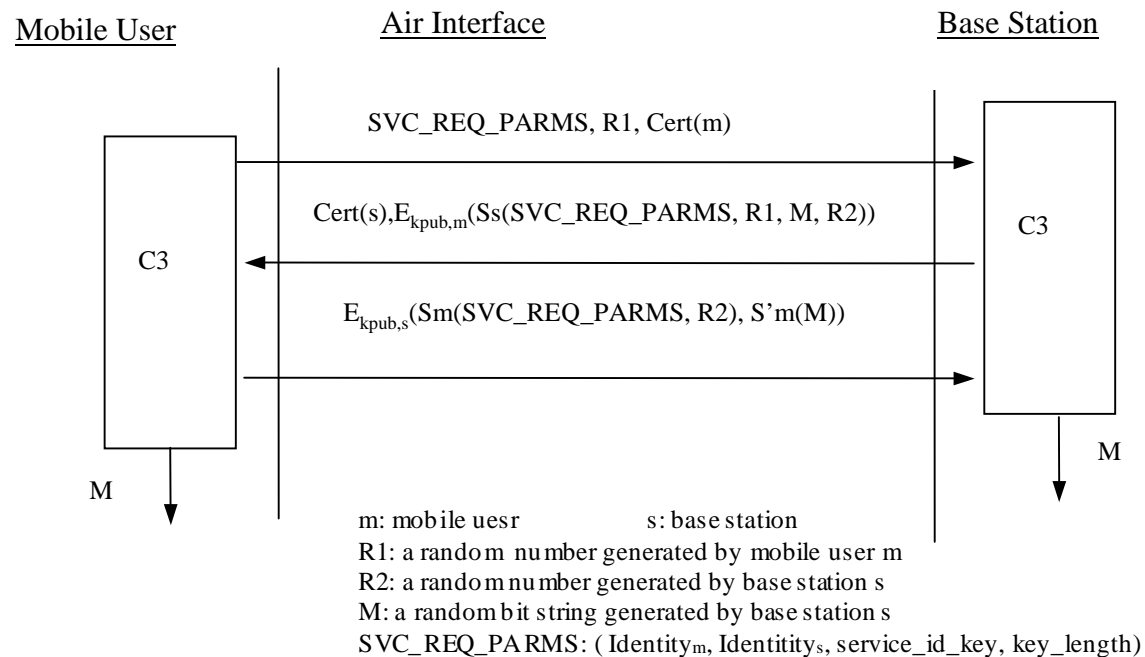


Security Architecture II



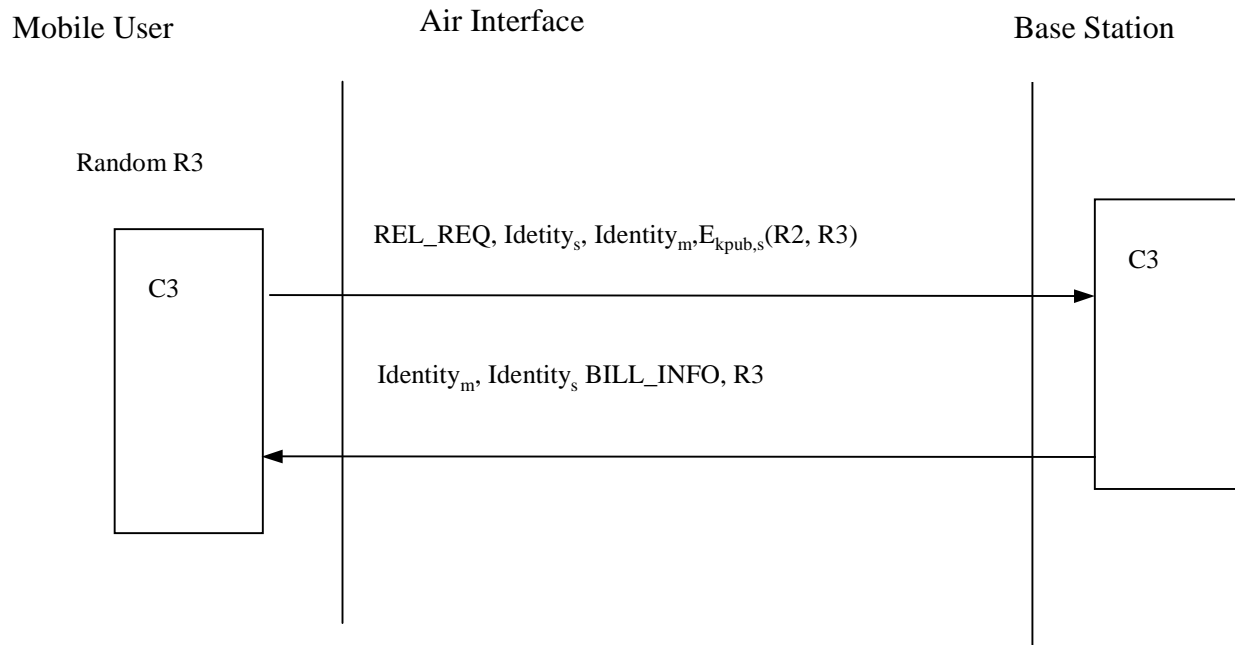
Architecture--Authentication Protocol(C3)

- Connection phase



Architecture--Authentication Protocol(C3)(Cont.)

- Release phase



Architecture--Key Generation(C8)

- C8 algorithm processes input data on a byte-by-byte basis. Some simulation results show that the keystream generated by C8 algorithm maintain a maximal periods, regardless of input patterns. This indicates that C8 algorithm is able to produce key strings with infinite period.

Architecture--Message Encryption/Decryption(C5)

- The C5 algorithm uses stream cipher for encryption/decryption. The simplest stream cipher is using only the XOR operation.

Comparison on two architecture

	Architecture I	Architecture II
Complexity	<ul style="list-style-type: none"> . Authentication is fast . Key exchange is fast . Message encryption is fast 	<ul style="list-style-type: none"> . Authentication is slow . Key exchange depends on the key length . Message encryption is fast
Security	<ul style="list-style-type: none"> . Authentication is not secure enough . Only the mobile user is authenticated 	<ul style="list-style-type: none"> . Authentication is very secure . Both the mobile user and the base station are authenticated(mutual authentication) . Period can be infinite
Flexibility	<ul style="list-style-type: none"> . A3, A8, and A5 are proprietary . The SIM stores user's personal information and the A3 algorithm 	<ul style="list-style-type: none"> . C1, C8, and C5 are publicly available . The SIM only stores user's personal information

Conclusion

- The GSM system is a first approach at a true personal communication system
- GSM provides a basic range of security features to ensure adequate protection for both the operator and customer