

**Ministère de l'Enseignement Supérieur et de la Recherche
Scientifique**

**Centre de Recherche sur l'Information
Scientifique et Technique**

MEMOIRE

Fin d'Etude

Post Graduation Spécialisé en Sécurité Informatique

Année 2014/2015

Sujet

**CAPTURE ET ANALYSE DU TRAFIC
GSM**

Réalisé par : LACHICHI Yesin

Encadré par : Mme BENMEZIANE Souad

Sommaire

Introduction générale	1
-----------------------------	---

Chapitre 1 : Description du réseau GSM

1 .1 Introduction :.....	2
1 .2 Le réseau GSM :	2
1 .3 Architecture d'un réseau GSM :.....	3
1.3.1 Le sous-système radio (BSS) :.....	4
A. La BTS.....	4
B. La BSC	4
1.3.2 Le sous-système réseau (MSS) :.....	4
A. Le MSC.....	4
B. Le HLR	5
C. Le VLR	6
D. L' AUC	6
1.3.3 Le sous-système exploitation (OSS) :.....	6
A. L'OMC le NMC	6
B. L' EIR.....	6
1.3.4 Les Terminaux :	7
1 .4 L'interface Air :	7
1.4.1 Bandes de fréquences :.....	7
1.4.2 Le Canal Radio :.....	8
1 .5 Conclusion :.....	8

Chapitre 2 : Mécanismes de sécurité des réseaux GSM

2 .1 Introduction :.....	9
2.2 Eléments d'identification :.....	9
2.3 Eléments d'authentification :.....	10

2.3 Le chiffrement des communications:.....	11
---	----

2.4 Conclusion:.....	12
----------------------	----

Chapitre 3 : Vulnérabilités et failles du réseau GSM

3.1 Introduction :.....	13
-------------------------	----

3.2 Les vulnérabilités GSM :.....	13
-----------------------------------	----

3.2.1 Vulnérabilité Man-in-the-Middle :	13
---	----

3.2.2 Vulnérabilité Known-plaintext Attack :.....	19
---	----

3.2.3 Ping SMS :.....	21
-----------------------	----

3.3 Conclusion :.....	22
-----------------------	----

Chapitre 4 : Capture, Analyse et décryptage du trafic GSM

4.1 Introduction :.....	23
-------------------------	----

4.2 Capture du trafic GSM :.....	24
----------------------------------	----

4.3 Analyse du trafic GSM (SMS et appel) :.....	29
---	----

4.3.1 Implémentation téléphone :.....	29
---------------------------------------	----

4.3.2 Capture et analyse SMS :.....	34
-------------------------------------	----

4.3.3 Capture et analyse des appels :.....	40
--	----

4.3.4 Décryptage des communications GSM :.....	48
--	----

4.3.4.1 Principe de fonctionnement de l'algorithme A5/1:	48
--	----

4.3.4.2 Utilisation des tables Raibow	50
---	----

4.3.4.3 Approche Karsten Nohl :	501
---------------------------------------	-----

4.3.4.4 Réalisation de l'attaque de Karsten Nohl :.....	52
---	----

4.4 Conclusion :.....	53
-----------------------	----

Conclusion générale.....	53
--------------------------	----

Bibliographies	54
----------------------	----

Annexe.....	55
-------------	----