

ANALISA TEKNIK OTENTIKASI EAP-SIM PADA 3G WIFI

Disusun Oleh:

Nama : Moris Mario

NRP : 0822106

Jurusan Teknik Elektro, Fakultas Teknik, Universitas Kristen Maranatha,
Jl. Prof.Drg.SuriaSumantri, MPH no. 65, Bandung, Indonesia.

Email :morisdoc@gmail.com

ABSTRAK

Perkembangan pengguna internet yang semakin aktif mengindikasikan diperlukannya *stronger authentications* yang dapat digunakan akses jaringan maupun layanan secara mudah/*seamless* tanpa harus memasukkan *username* dan *password*.

Pada Tugas Akhir ini penulis menganalisa penggunaan kartu SIM GSM sebagai *username* dan *password* dalam otentikasi layanan internet pada *open source software freeradius* sebagai *simulator* HLR/AuCserver. Analisa teknik EAP-SIM yang dilakukan menggunakan software WireShark.

Proses Otentikasi menggunakan kartu SIM dapat dimaksimalkan dengan adanya SRES (A3) yang dapat dibentuk dari nilai *secret key* (Ki) dan RAND. *Username* didapat dari identitas IMSI yang berbeda antar kartu SIM.

Kata Kunci: EAP-SIM, SRES, HLR/AuCserver, WireShark

TECHNICAL ANALYSIS OF EAP-SIM AUTHENTICATION ON 3G WIFI

Composed By:

Nama : Moris Mario

NRP : 0822106

Electrical Engineering Department

Maranatha Christian University

Jl. Prof.Drg.Suria Sumantri, MPH no.65, Bandung, Indonesia

Email :morisdoc@gmail.com

ABSTRACT

The development of internet users which is increasingly active indicates required a stronger authentications that can be used as well as network access services easily / seamlessly without having to enter a username and password.

This project analyzes the function of a GSM SIM card as your username and password in the authentication service on the internet as an open source FreeRADIUS software simulator HLR / AuC server. This analysis technique is performed using Wireshark software.

Authentication process using a SIM card can be maximized with the SRES (A3) that can be formed by the value of the secret key (Ki) and RAND. Username derived from the IMSI which is different in every SIM card.

Keyword : EAP-SIM, SRES, HLR/AuC server, WireShark

DAFTAR ISI

Halaman

LEMBAR PENGESAHAN

PERNYATAAN ORISINALITAS LAPORAN PENELITIAN

PERNYATAAN PUBLIKASI LAPORAN PENELITIAN

KATA PENGHANTAR

ABSTRAK	i
ABSTRACT	ii
DAFTAR ISI.....	iii
DAFTAR GAMBAR	vii
DAFTAR SINGKATAN	ix
DAFTAR ISTILAH	x
BAB 1 PENDAHULUAN	1
1.1. Latar Belakang Masalah.....	1
1.2. Identifikasi Masalah	2
1.3. Tujuan	2
1.4. Rumusan Masalah	2
1.5. Pembatasan Masalah	2
1.6. Sistematika Penulisan	3
BAB 2 LANDASAN TEORI	4
2.1. IEEE 802.1X	4
2.1.1. IEEE 802.1X <i>Authentication Framework</i>	4
2.1.2. <i>EAP Authentication Methods</i>	6
2.2 EAP – SIM	8
2.2.1 <i>GSM Authentication</i>	8
2.2.2 EAP-SIM <i>Authentication</i>	9

2.3 Kartu SIM dan Standarisasi ISO 7816	12
2.3.1 Smart Card	12
2.3.2 ISO 7816 Standart	13
2.4 <i>Authentication Method</i> dan <i>Identity Types</i>	14
2.5. SIM Card.....	17
2.5.1 <i>Servis-Related Information</i>	17
BAB 3 PERANCANGAN DAN REALISASI.....	19
3.1. Protokol EAP-SIM.....	19
3.2. <i>Software WireShark</i>	20
3.3 Metoda Pengambilan Data	21
3.3.1. Terminal	21
3.3.2 SIM.....	21
3.4. EAP-SIM server <i>architecture</i>	22
3.5. Perangkat yang dibutuhkan	23
3.6. <i>Notebook Installation</i> dan Konfigurasi	24
3.6.1. PCSC Chip Drive SIM Card Reader.....	24
3.6.2 WPA Supplicant.....	24
3.6.3. <i>Debug Tool</i>	24
3.6.4. RADIUS <i>Server Installation</i>	24
3.6.5. <i>Generate Simplets.dat</i>	25
3.6.6. Konfigurasi <i>DHCP server</i>	25
3.6.7. Konfigurasi <i>Access Point</i>	25
3.6.8. Konfigurasi Server RADIUS	26
3.6.9. Konfigurasi WPA_Supplicant.....	26
3.6.10. Konfigurasi perangkat Blackberry	27

3.7. Pengujian Alat.....	27
3.7.1. Test Radius sebagai Simulator HLR/Auc	27
3.7.2. Test PoC Sistem dengan Notebook.....	27
3.7.3. Test PoC Sistem dengan Blackberry.....	28
3.8. Langkah- langkah Pengujian.....	28
3.9. Parameter yang dianalisa	30
3.10. Diagram alir proses otentikasi.....	31
BAB 4 DATA PENGAMATAN DAN ANALISA	32
4.1. Standart Otentikasi EAP-SIM	32
4.2. <i>Sniffing</i> yang dilakukan pada sisi Supplicant.....	34
4.2.1. Paket Pertama	34
4.2.2. Paket Kedua.....	35
4.2.3. Paket Ketiga	35
4.2.4. Paket Keempat.....	36
4.2.5. Paket Kelima	37
4.2.6. Paket Keenam.....	37
4.2.7. Paket Ketujuh	38
4.2.8. Paket Kedelapan	38
4.3. <i>Sniffing</i> yang dilakukan pada sisi Server RADIUS.....	39
4.3.1. Paket Pertama pada sisi Server RADIUS	40
4.3.2. Paket Kedua pada sisi Server RADIUS	40
4.3.3. Paket Ketiga pada sisi Server RADIUS	41
4.3.4. Paket Keempat pada sisi Server RADIUS	41
4.3.5. Paket Kelima pada sisi Server RADIUS	42
4.3.6. Paket Keenam pada sisi Server RADIUS.....	43

BAB 5 KESIMPULAN	45
DAFTAR PUSTAKA.....	46

DAFTAR GAMBAR

Gambar 2.1. The IEEE 802.1x Framework.....	5
Gambar 2.2. Controlled port is switched on after authorized	5
Gambar 2.3. The IEEE 802.1x protocol stack	7
Gambar 2.4. The GSM Security Framework	10
Gambar 2.5. EAP-SIM Full Authentication Message Flow	11
Gambar 2.6. Application Communications Architecture.....	14
Gambar 2.7. Proses Paket EAP-SIM	15
Gambar 3.1. Diagram blok protokol eap-sim.....	19
Gambar 3.2. Struktur Paket <i>Sniffer</i>	21
Gambar 3.3. Gambar Supplicant.....	21
Gambar 3.4. Arsitektur jaringan sebelum jenis 802.1x.....	22
Gambar 3.5. Arsitektur jaringan jenis 802.1x.....	22
Gambar 3.6. Tampilan WireShark ketika menangkap paket data.....	29
Gambar 3.7. Diagram Alir proses Otentikasi.....	31
Gambar 4.1. Standarisasi proses otentikasi EAP-SIM.....	32
Gambar 4.2. <i>Sniffing</i> pada sisi suplicant	34
Gambar 4.3. Paket pertama yang ditangkap pada sisi supplicant	34
Gambar 4.4. Paket kedua yang ditangkap pada sisi supplicant.....	35
Gambar 4.5. Paket ketiga yang ditangkap pada sisi supplicant	35
Gambar 4.6. Paket keempat yang ditangkap pada sisi supplicant.....	36
Gambar 4.7. Paket kelima yang ditangkap pada sisi supplicant	37
Gambar 4.8. Paket keenam yang ditangkap pada sisi supplicant.....	37
Gambar 4.9. Paket ketujuh yang ditangkap pada sisi supplicant	38

Gambar 4.10. Paket kedelapan yang ditangkap pada sisi supplicant.....	38
Gambar 4.11. <i>Sniffing</i> yang dilakukan pada sisi supplicant dan RADIUS 1.....	39
Gambar 4.12. <i>Sniffing</i> yang dilakukan pada sisi supplicant dan RADIUS 2.....	39
Gambar 4.13. Paket pertama yang ditangkap pada sisi Server RADIUS	40
Gambar 4.14. Paket kedua yang ditangkap pada sisi Server RADIUS.....	40
Gambar 4.15. Paket ketiga yang ditangkap pada sisi Server RADIUS	41
Gambar 4.16. Paket keempat yang ditangkap pada sisi Server RADIUS.....	41
Gambar 4.17. Paket kelima yang ditangkap pada sisi Server RADIUS	42
Gambar 4.18. Paket keenam yang ditangkap pada sisi Server RADIUS.....	43
Gambar 4.19. Analisa paket pada sisi Supplicant dan server RADIUS.....	43

DAFTAR SINGKATAN

3GPP	= 3 rd Generation Partnership Project
AAA	= Authentication, Authorization, Accounting
AuC	= Authentication Center
EAP	= Extensible Authentication Protocol
EAP-AKA	= EAP – Authentication & Key Agreement
GSM	= Global System Communication
HLR/VLR	= Home Location Register / Visitor Location Register
ICCID	= Integrated Circuit Card Identification
IMSI	= International Mobile Subscriber Identifier
MSISDN	= Mobile Station International Subscriber Directory Number
PAE	= Port Access Entity
PKI	= Public Key Infrastructure
SIM	= Subscriber Identity Module
TLS	= Transport Layer Protocol
UMTS	= Universal Mobile Telecommunication System
USIM	= Universal Subscriber Identity Module

DAFTAR ISTILAH

Kernel	:adalah suatu perangkat lunak yang menjadi bagian utama dalam sebuah sistem operasi.
Kredential	:adalah proses pembentukan alogaritma A3,A5 dan A8 yang akan dikualifikasi.
Protokol	:adalah aturan yang diberikan pada masing-masing perangkat yang menetapkan kerja dari perangkat tersebut.
Supplicant	:adalah user equipment yang dilengkapi software wp_supplicant sehingga perangkat tersebut dapat mengirim paket data EAP-SIM.