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 otentikasilayanan internet pada*open source software freeradius*sebagai*simulator* HLR/AuC*server*. 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/AuC*server*, 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 indicatesrequired 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

DAFTAR GAMBAR

DAFTAR SINGKATAN

3GPP	= 3rd 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.