

Daftar Isi

ABSTRAK	i
ABSTRACT	ii
LEMBAR PERSEMBAHAN	iii
KATA PENGANTAR	v
DAFTAR ISI	vi
DAFTAR GAMBAR	viii
DAFTAR ISTILAH	x
1. Pendahuluan	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	2
1.3 Tujuan.....	2
1.4 Metodologi penyelesaian masalah.....	2
2. Landasan Teori	5
2.1 Keamanan Jaringan Nirkabel.....	5
2.1.1 Jaringan Nirkabel.....	5
2.1.2 Perkembangan Keamanan Jaringan Nirkabel.....	6
2.2 Protokol IEEE 802.1x.....	8
2.3 Protokol EAP (Extensible Authentication Protocol).....	9
2.3.1 EAP MD5.....	9
2.3.2 EAP TLS.....	9
2.4 Radius (Remote Access Dial-in User Service).....	11
2.5 Timed Automata.....	11
2.6 MITM (Man In The Middle) Attack.....	12
3. Model Autentikasi	13
3.1 Model Autentikasi EAP.....	13
3.1.1 Diagram sequence EAP MD5.....	13
3.1.2 Timed Automata EAP MD5.....	14
3.1.3 Diagram sequence EAP TLS.....	15
3.1.4 Timed Automata EAP TLS.....	17
3.2 Model Serangan Man In The Middle Attack.....	19
3.2.1 Serangan MITM pada EAP.....	19
3.2.2 Diagram sequence serangan MITM pada EAP MD5.....	20
3.2.3 Timed Automata serangan MITM pada EAP MD5.....	20
3.2.4 Diagram Sequence serangan MITM pada EAP TLS.....	21
3.2.5 Timed Automata serangan MITM pada EAP TLS.....	21
4. Pengujian dan Analisis Model	23

4.1 Tujuan dan Parameter Pengujian.....	23
4.2 Strategi Pengujian.....	23
4.3 Verifikasi dan Analisis.....	24
4.3.1 Model Timed Automata EAP MD5.....	25
4.3.1.1 Simulator Timed Automata EAP MD5 dengan serangan MITM.....	25
4.3.1.2 Verifier EAP MD5.....	30
4.3.1.3 Analisis Timed Automata EAP MD5.....	32
4.3.2 Model Timed Automata EAP TLS.....	32
4.3.2.1 Simulator Timed Automata EAP TLS dengan serangan MITM.....	32
4.3.2.2 Verifier EAP TLS.....	38
4.3.2.3 Analisis Timed Automata EAP TLS.....	41
5. Penutup.....	43
5.1 Kesimpulan.....	43
5.2 Saran.....	43
REFERENSI.....	44