BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan data adalah ilmu pengetahuan dan pembelajaran mengenai metode perlindungan data pada komputer dan sistem komunikasi [1]. Keamanan yang diterapkan mencakup keamanan teknologi, piranti, dan proses transmisi data di dalam sistem jaringan, seperti keamanan pada sistem komunikasi seluler. Keamanan data bertujuan untuk melindungi data dan informasi dari gangguan maupun dari pengakses yang tidak berwenang agar identitas dan privasi tetap terjaga.

Akan tetapi, faktanya masih terdapat sistem keamanan khususnya keamanan jaringan seluler yang masih dapat diakses oleh pihak yang tidak bertanggung jawab. Salah satu potensi terbukanya celah keamanan data pada jaringan seluler khususnya jaringan GSM dan GPRS dapat terjadi pada saat suatu data atau informasi ditransmisikan dari satu perangkat *user* ke perangkat *user* lain melalui sebuah jaringan *wireless*, yaitu transmisi data atau komunikasi antar *user* atau MS (*Mobile Station*) melalui BTS (*Base Transceiver Station*). Transmisi data antar MS pada jaringan GSM dan GPRS menggunakan teknik pensinyalan yang terjadi pada *air interface* dimana MS akan terkoneksi dengan BTS *provider* untuk dapat mengirim data atau berkomunikasi dengan MS lain [2]. Pada *air interface* masih terjadi tindakan kejahatan seperti *sniffing* untuk memperoleh data dan informasi secara ilegal. Proses *sniffing* dapat terjadi dengan cara menyadap data dan informasi pada jaringan GSM dan GPRS saat transmisi data antara MS dan BTS *provider* berlangsung dengan karakteristik tidak mengubah data dan informasi asli. Oleh karena itu, diperlukan sistem keamanan yang dapat mencegah dari serangan *sniffing* tersebut.

Solusi preventif yang dapat dilakukan untuk mengamankan sistem komunikasi seluler jaringan GSM dan GPRS adalah dengan mengevaluasi sistem keamanan yang digunakan saat ini. Evaluasi yang dilakukan yaitu dengan menganalisis sistem keamanan data seluler melalui pengujian penyadapan pada *air*

interface. Penelitian [3] sebelumnya telah dilakukan pengujian penyadapan dengan metode *tapping* pada jaringan GSM. Hasil yang ditunjukkan berupa trafik informasi dasar yang berhasil di-*tapping* pada sinyal GSM. Kemudian, pada penelitian [4] telah dilakukan pengujian penangkapan sinyal dan *decoding* pada *provider* XL Axiata. Hasil yang diperoleh berupa informasi *provider*, GSM *Frame Number*, IMSI (*International Mobile Subscriber Identity*), TMSI (*Temporary IMSI*), dan *burst frame* (data komunikasi) GSM.

Penelitian yang berjudul **"*Analisis Keamanan Data Seluler Terhadap Serangan Sniffing Menggunakan RTL-SDR*"** akan menganalisis tingkat keamanan data seluler melalui pengujian pengiriman data berupa SMS dan email pada jaringan GSM dan GPRS dengan perangkat RTL-SDR sebagai penangkap sinyal pada saat SMS dan email dikirimkan. Operator seluler yang dianalisis dalam penelitian ini adalah *provider* Telkomsel.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang, rumusan masalah pada penelitian ini adalah sebagai berikut.

1. Mengidentifikasi tingkat keamanan data pada jaringan GSM dan GPRS terhadap *sniffing*.
2. Informasi apa saja yang diperoleh dari proses *sniffing* jaringan GSM dan GPRS?
3. Algoritma apa yang digunakan untuk mengamankan data dan seberapa akurat data tersebut dapat diamankan?

1.3 Batasan Masalah

Adapun pembahasan dalam penelitian ini dibatasi pada:

1. Sinyal komunikasi seluler yang dianalisis adalah sinyal komunikasi jaringan GSM dan GPRS pada *band* 900 MHz.
2. Menganalisis sinyal frekuensi *downlink* (dari BTS menuju MS).
3. Media pengiriman data menggunakan SMS dan email.

4. Perangkat penangkap sinyal data pada jaringan GSM dan GPRS menggunakan RTL-SDR.
5. Operator seluler yang dianalisis adalah *provider* Telkomsel.

1.4 Tujuan Penelitian

Adapun tujuan yang akan dicapai pada penelitian ini adalah:

1. Untuk mengetahui tingkat kesuksesan keamanan data pada jaringan seluler khususnya jaringan GSM dan GPRS.
2. Sebagai bahan analisis terhadap informasi sinyal yang ditangkap dari perangkat RTL-SDR.
3. Untuk mengetahui perbandingan teknik enkripsi berdasarkan media pengiriman data (SMS dan email).

1.5 Manfaat Penelitian

Manfaat yang diperoleh pada penelitian ini adalah:

1. Dapat mengetahui gambaran sistem komunikasi dan sistem keamanan yang diimplementasikan pada komunikasi seluler khususnya GSM dan GPRS.
2. Dapat mengevaluasi sistem keamanan pada teknologi komunikasi seluler berdasarkan hasil pengujian dan analisis data.

1.6 Metodologi Penelitian

Dalam melaksanakan penulisan Tugas Akhir ini, metode yang digunakan sebagai acuan pada penelitian ini adalah sebagai berikut.

1. Metode Studi Pustaka

   Studi pustaka adalah metode dengan cara menelaah referensi dari berbagai sumber yang berkaitan dengan masalah penelitian. Sumber pustaka yang menjadi referensi penelitian dikutip dari beberapa buku, jurnal, dan referensi dari media internet.

2. Metode *Penetration Testing*

   Metode *penetration testing* adalah metode evaluasi keamanan sistem jaringan dimana sistem yang diuji pada penelitian ini adalah sistem

komunikasi seluler pada salah satu operator seluler di Indonesia dengan cara mensimulasikan serangan yaitu serangan *sniffing* terhadap jaringan tersebut dengan tujuan untuk menemukan kelemahan yang ada pada sistem jaringan yang diteliti.

3. Metode Analisis

Metode analisis yang digunakan pada penelitian ini berupa analisis kualitatif berdasarkan proses pengujian dan pengambilan data target yang menjadi tujuan penelitian.

1.7 Sistematika Penulisan

Sistematika penulisan mencakup urutan yang menjadi landasan utama dalam menyelesaikan penelitian dan sebagai sarana untuk mempermudah penyusunan Tugas Akhir. Sistematika penulisan terbagi dalam lima bab dengan rincian sebagai berikut.

BAB I PENDAHULUAN

Pada bab ini menjelaskan mengenai latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metodologi, dan sistematika penulisan pada penelitian yang dibahas.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi referensi tentang informasi teoritis yang berkaitan dengan konsep keamanan data, konsep kanal (*channel*) GSM, sistem *Time Division Multiple Access* (TDMA) dan *Frequency Division Multiple Access* (FDMA) pada jaringan GSM, alokasi frekuensi seluler di Indonesia, sistem GPRS, enkripsi pada GSM, mail server, sistem Postfix, perangkat RTL-SDR, penggunaan *Temporary Mobile Subscriber Identity* (TMSI), serta fungsi sistem operasi dan deskripsi *tools penetration testing*.

BAB III METODOLOGI PENELITIAN

Metodologi penelitian pada bab ini memuat pembahasan mengenai lokasi dan tahapan penelitian, penggunaan perangkat keras dan perangkat lunak, gambaran infrastruktur sistem, diagram alir proses penangkapan sinyal

menggunakan perangkat RTL-SDR, rancangan sistem yang dibangun dalam bentuk *flowchart*, instalasi dan konfigurasi sistem, serta parameter pengambilan data sebagai analisis yang akan ditinjau.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi implementasi pengujian *penetration testing* menggunakan perangkat RTL-SDR terhadap target data berupa SMS dan email yang didukung oleh *tools penetration testing*. Kemudian, terdapat pembahasan hasil identifikasi dan pengujian dengan analisis berdasarkan parameter-parameter yang telah ditentukan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi penjelasan yang terdiri atas kesimpulan yang dirangkum berdasarkan pembahasan pada bab-bab sebelumnya serta saran yang dapat dijadikan sebagai acuan dalam pengembangan dan penyempurnaan pada penelitian berikutnya.