BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin cepat mendasari perkembangan komputasi. Perkembangan komputasi saat ini semakin mendekati komputasi berbasis *mobile*. Sistem operasi yang banyak digunakan pada *platform mobile* adalah Android, yang berdasarkan laporan dari Gartner penjualannya mencapai 78,4% dari total penjualan *smartphone* pada sepanjang tahun 2013. Sedangkan pada pengguna Android sendiri, berdasarkan data di Google Play hingga April 2014, 61,4% menggunakan Android versi 4.1.x hingga 4.3.x (*Jelly Bean*) dan 17,8% menggunakan Android versi 2.3.3-2.3.7 (*Gingerbread*).

Banyaknya pengguna menyebabkan Android menjadi salah satu sistem operasi yang paling ditarget oleh penyerang dan pengembang *malware*. Pada tahun 2013 dideteksi 804 keluarga *malware* baru pada Android, dibandingkan 23 pada *platform* Symbian. Usaha untuk membantu mengatasi efek *malware* telah dilakukan dengan mengimplementasikan perubahan yang berkaitan dengan keamanan pada setiap *platform* Android yang dirilis. Tetapi sifat ekosistem Android yang berbeda-beda pada setiap *vendor* dan bahkan setiap pengguna individu menyulitkan usaha untuk mengimplementasikan standar keamanan yang seragam untuk setiap pengguna.

Salah satu usaha menghindari aplikasi berbahaya adalah sistem *permission* saat instalasi. Sistem *permission* digunakan untuk memberikan pengguna kontrol atas privasi dan mengurangi efek bug dan kelemahan dalam aplikasi. Tetapi aplikasi Android cenderung meminta *permission* lebih banyak dari yang dibutuhkan, mengekspos pengguna dengan peringatan *permission* yang sebetulnya kurang perlu dan meningkatkan dampak dari sebuah *bug* atau kelemahan.

Fitur *inter-application communication (IAC)* pada Android juga telah diobservasi oleh Chin, dkk. (2011) dan Han, dkk. (2013) sebagai celah untuk melakukan serangan pada sistem Android. IAC adalah fitur dimana beberapa aplikasi Android dapat bekerja sama untuk melakukan suatu pekerjaan kompleks, dan merupakan fitur pembeda Android dari kompetitornya. Dengan memanfaatkan fitur ini, beberapa aplikasi *malware* dengan *permission* yang berbeda dapat bekerja sama untuk melakukan serangan.

Banyaknya aplikasi berbasis *mobile* saat ini juga menjadi celah keamanan baru. Kini kegiatan transaksi perbankan, akses e-mail yang mungkin mengandung data-data konfidensial, dan berbagai kegiatan lain dapat dilakukan dari *smartphone*. Dari 128 bank komersial yang beroperasi di Indonesia, hampir setengahnya memanfaatkan fasilitas *mobile banking*. Sebagai salah satu contoh, untuk Bank Mandiri, 40% dari pengguna *mobile banking* memanfaatkan fitur *SMS banking*. Sistem perbankan berbasis SMS ini beresiko tinggi karena mencakup pengiriman informasi tanpa enkripsi, yang mencakup nomor rekening, nomor kartu kredit, jumlah transaksi, dan nomor PIN. Ini meningkatkan resiko pencurian data yang berakibat kerugian finansial. Pada platform Android telah banyak beredar *malware* yang salah satu kinerjanya adalah menyadap pesan SMS, seperti Backdoor:Android/Damon.A dan Trojan:Android/SmSilence.A.

Sejauh ini, sistem operasi Android hingga versi 2.2 Froyo memiliki kelemahan dimana suatu aplikasi dapat mendapat ijin untuk berjalan di belakang latar, sehingga aktivitas aplikasi tersebut tidak di ketahui oleh pengguna. Tidak menutup kemungkinan kelemahan ini dapat dieksploitasi untuk mendapatkan data pribadi pengguna (*phising*), terutama melalui pesan singkat SMS. Data pribadi dapat diperoleh antara lain dengan menggunakan aplikasi yang berjalan di *background* yang merekam kegiatan pengguna dan mengirimkannya kepada penyerang. Untuk memudahkan presentasi, pada tugas akhir ini penyerangan dengan menggunakan penyadapan data pada *smartphone* ini disebut Kleptodata. Pada tugas akhir ini dilakukan analisis proses kleptodata pada Android 2.3 *Gingerbread* melalui desain dan implementasi *malware* yang mengeksploitasi beberapa kelemahan yang ditemukan pada Android.

1.2 Rumusan Masalah

Masalah yang dihadapi dalam pembuatan tugas akhir ini adalah:

1. Penyerangan keamanan terhadap Android dengan metode pencurian data.
2. Celah yang dapat digunakan untuk melakuan serangan pencurian data.
3. Metode yang digunakan dalam proses pencurian data.
4. Mengaplikasikan serangan pencurian data pada sistem operasi Android.

1.3 Batasan Masalah

1. Proses implementasi tidak dibahas dalam penelitian yang dilakukan.

2. Implementasi dan realisasi dilakukan terhadap perangkat telepon cerdas dengan sistem operasi Android dan memiliki fungsi pesan singkat (SMS).
3. Implementasi dan realisasi dilakukan dengan metode pencurian data menggunakan aplikasi *malware*.
4. Penelitian ditekankan pada metode penyerangan pencurian data pada Android, sehingga faktor *hardware* dianggap memiliki fungsi yang sama.

5. Masalah literatur jaringan tidak terlalu diperhatikan dalam penelitian yang dilakukan.

1.4 Tujuan

Tujuan dari tugas akhir ini adalah:

1. Merancang proses pencurian data pada Android dan mengimplementasikannya melalui sebuah aplikasi pada Android yang dapat terinstal dan bekerja tanpa diketahui oleh pengguna, terus merekam dan menyimpan data meski tidak terhubung jaringan, dan mengirimkan data jika sudah terhubung jaringan, dan apabila aplikasi terhapus dapat mendeteksi dan menginstal ulang malware.
2. Mengimplementasikan aplikasi yang dapat mengirimkan data yang dicuri tanpa diketahui oleh pengguna.
3. Menganalisis kelemahan yang dimanfaatkan untuk melakukan pencurian.

1.5 Metodologi Penelitian

Metodologi atau tahap pemecahan yang digunakan adalah:

1. Tahap Studi Literatur

   Pada tahap ini akan dilakukan studi secara mendalam dari literatur yang ada baik dari buku maupun dari jurnal, serta berdiskusi dengan orang yang memiliki kompetensi yang setara.
2. Tahap Perancangan Aplikasi

   Pada tahap ini akan dilakukan perancangan aplikasi, skenario penyerangan yang akan digunakan, serta perencanaan fitur yang akan digunakan.
3. Tahap Pembuatan Aplikasi Pendukung

   Pada tahap ini akan dilakukan pembuatan aplikasi pendukung yang akan digunakan untuk melakukan proses pencurian data.

4. Tahap Pengujian

   Pada tahap ini akan dilakukan pengujian proses pencurian data pada Android dengan bantuan aplikasi pendukung.

5. Tahap Penulisan Laporan Tugas Akhir

1.6 Sistematika Penulisan

Sistematika penulisan proposal Tugas Akhir yang dibuat, dibagi menjadi beberapa bab yang meliputi:

BAB I PENDAHULUAN

Pendahuluan berisi latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metodologi, dan sistematika penulisan dan penelitian.

BAB II DASAR TEORI

Dasar teori berisi berbagai teori yang mendukung penelitian, antara lain mengenai sistem operasi Android, pengamanan pada Android, dan konsep pendukung lainnya.

BAB II MODEL PERANCANGAN SISTEM

Pada bab model dan desain sistem dibahas model penyerangan yang akan dilakukan

BAB IV ANALISIS

Pada bab pembahasan akan dibahas tentang simulasi, pengukuran, dan analisa dari aplikasi yang diimplementasikan.

BAB V KESIMPULAN DAN SARAN

Pada bab kesimpulan akan berisi kesimpulan dari penelitian yang dilakukan dan saran yang didapat setelah melakukan penelitian.