ABSTRAK

Android merupakan sistem operasi *mobile* dengan peningkatan jumlah pengguna paling pesat. Pesatnya pengembangan jumlah pengguna menyebabkan menyebabkan Android semakin menjadi target untuk serangan keamanan. Serangan keamanan yang dapat dilakukan antara lain pencurian data yang memanfaatkan kelemahan pada Android. Pada tugas akhir ini dilakukan analisis proses pencurian data (kleptodata) pada Android 2.3 *Gingerbread* dan mengimplementasikannya melalui aplikasi *malware* yang mengeksploitasi beberapa kelemahan yang ditemukan pada Android.

Sistem yang dibangun dalam tugas akhir ini memanfaatkan kelemahan pada sistem operasi Android dimana aplikasi yang telah terpasang dapat diizinkan untuk mengunduh dan memasang aplikasi lain yang dapat berjalan di belakang latar. Kelemahan lain yang dimanfaatkan adalah kombinasi sistem *permission* dan fitur *inter-application communication* pada Android. Kelemahan tersebut dimanfaatkan dengan menggunakan sebuah sistem yang terdiri dari dua aplikasi yang berfungsi untuk mencuri data, menyimpannya, serta mengirim data ke *server*. Kedua aplikasi juga mendeteksi keberadaan satu sama lain. Jika salah satu aplikasi diuninstal, aplikasi yang lain pada sistem akan mengunduh dan menginstal kembali aplikasi yang diuninstal, sehingga proses pencurian data tidak terputus.

Hasil penelitian menunjukkan bahwa aplikasi yang digunakan untuk melakukan pencurian data berjalan dengan baik, dengan SMS pada perangkat dapat diambil dan dikirimkan menuju *server*. Proses pendeteksian juga berjalan dengan baik. Hingga waktu pengujian aplikasi pada Mei 2014, aplikasi tidak terdeteksi oleh beberapa *antivirus* yang banyak digunakan pada umumnya. Tetapi sistem penyamaran yang digunakan oleh aplikasi masih kurang sempurna, karena masih belum sesuai dengan *permission* yang digunakan serta fungsi yang diharapkan.

Kata kunci : Android, Keamanan, Kleptodata, *Malware*