ABSTRAK

Penggunaan *smartphone* sangat berkembang di masyarakat, terutama *smartphone* dengan Sistem Operasi Android dan IOS. *Smartphone* sering digunakan untuk melakukan pencarian di *internet*, mengambil foto atau merekam video, mendengarkan lagu, melakukan transaksi *banking* dan yang paling diminati adalah aplikasi sosial media. Seiiring dengan meningkatnya penggunaan *smartphone*, menimbulkan suatu kebutuhan baru yaitu sumber daya listrik yang mudah diakses untuk mengisi baterai *smartphone*. *Power bank* adalah salah satu solusi yang memudahkan pengguna dalam pengisian baterai tanpa harus berada lama disatu tempat atau dengan kata lain *power bank* adalah sumber listrik yang dapat dibawa kemana saja.

Pada penelitian ini dirancang sebuah *malware* Android yang dipasang pada *smartphone* yang dapat mengambil data pengguna dan mengirim data tesebut ke *microcontroller*. Data yang diambil antara lain yaitu informasi *smartphone*, sms, contacts, email dan webview. Dengan memanfaatkan fungsi *permissions* yang ada pada Pemrograman Android, *malware* dapat mengakses data sensitif pengguna yang ada pada *smartphone*. Agar melancarkan proses pengambilan data, *malware* disisipkan didalam sebuah Aplikasi normal sehingga tidak menimbulkan kecurigaan pengguna.

Hasil dari penelitian ini adalah *malware* dapat mengambil data pengguna yang ada pada *smartphone* dan mengirimkan ke *microcontroller*. Pengiriman data menggunakan komunikasi serial. Pengolahan *file text* hingga pengiriman ke *microcontroller* masing-masing membutuhkan rata-rata waktu 75023.6 ms per 50 sms, 45013.83 ms per 30 contact , 4502.93 ms per 3 webview dan 30010.66 ms per 20 email. Data yang dikirim mempunyai kemungkinan rusak dikarenakan terjadi *interrupt* dari pengguna sama proses pengirman.

Kata kunci : *android, malware*, *root*, komunikasi serial, keamanan sistem