

Proposal Tugas Akhir
EC-5010 Keamanan Sistem Informasi

Oleh : Indra Antonius Simalango (13200083)

Judul :

Perancangan Cryptoboard dengan mengimplementasikan OpenSSL 0.9.7 pada Single Board Computer

Abstrak :

Aspek keamanan dalam proses pertukaran data adalah salah satu pendorong munculnya teknologi Kriptografi. Kriptografi berbasis pada algoritma pengkodean data informasi yang mendukung kebutuhan dari dua aspek keamanan informasi, yaitu secrecy (perlindungan terhadap kerahasiaan data informasi) dan authenticity (perlindungan terhadap pemalsuan dan perubahan informasi yang tidak diinginkan).

Pada proses transfer data antar Personal Computer (PC) dalam jaringan, modul Kriptografi akan mengkodekan data informasi sedemikian rupa dengan memanfaatkan resource yang ada. Pemakaian resource secara bersama-sama dengan aplikasi-aplikasi lainnya dalam PC menjadikan proses pengkodean dalam modul Kriptografi dilakukan dalam jangka waktu relatif lama.

Trend teknologi juga mengisyaratkan keamanan mutlak pada source-code modul Kriptografi. Hal ini untuk mencegah terjadinya pembajakan dan penyalahgunaan. Selama modul Kriptografi masih berbentuk perangkat lunak (software), peluang akan terjadi hal ini tetap terbuka.

Ide yang muncul adalah untuk mengintegrasikan modul Kriptografi pada suatu perangkat keras (hardware) tersendiri. Perangkat ini haruslah mempunyai resource sendiri yang dikhususkan untuk mendukung kinerja modul Kriptografi sepenuhnya. Karena akan diimplementasikan pada PC, perangkat ini hendaknya berupa board dengan slot standar pada PC.

Salah satu alternatif yang memungkinkan untuk mewujudkan hal ini adalah dengan menginstal modul Kriptografi pada sebuah Single Board Computer (SBC). Spesifikasi SBC secara teknis memungkinkan implementasi hal ini. Untuk tugas akhir ini, akan dicoba merancang implementasi OpenSSL 0.9.7 sebagai modul Kriptografi pada SBC 456/E.