abstract

Det finns flera protokoll såsom SSL och IPSec som underlättar hanteringen för användaren av de säkerhetskrav som kan uppstå i nätverksmiljöer. De saknar tyvärr mycket av den dynamik som skulle önskas för att kunna erbjuda en lättanvänd konfigurerbar säkerhetslösning som lätt kan anpassas till både användarens krav på säkerhet och prestanda.

För att kunna öka prestandan hos en given krypteringsalgoritm måste antingen algoritmen i sig förbättras, alternativt dess användande. Eftersom det redan pågår kontinuerlig forskning på att förbättra algoritmerna och detta har gjorts under flera år är det användandet av algoritmen som är det intressanta att titta på. Av denna anledningen har vi arbetat fram ett koncept som vi kallar för lättviktskryptering, vilket tillsammans med starka krypteringsalgoritmer leder till konceptet partiell säkerhet. Efter att idén presenterats visas prestandatester mellan konventionella krypteringsmetoder och partiell kryptering. Vidare introduceras begreppet riktad kryptering med idéer till dess användningsområde och fördelar.