ABSTRAK

Judul : IMPLEMENTASI DAN ANALISIS KERJA PROTOKOL KEAMANAN DNS *OVER* TLS (DOT) DALAM MENGATASI CELAH KEBOCORAN DOMAIN NAME SYSTEM (DNS)
Nama : Karim Amirullah
Program Studi : Teknik Informatika

Domain Name Systen (DNS) merupakan sistem yang memiliki peran cukup penting dalam aktifitas internet. *Domain Name System* (DNS) merupakan sistem yang mengubah *domain* yang memiliki tipe *alphabetical* menjadi IP *address*. Dalam peran tersebut, tidak sedikit masalah keamanan terjadi pada *Domain Name System* (DNS). Salah satu bentuk masalah keamanan adalah kebocoran *Domain Name System* (DNS) atau sering disebut DNS *leak*. Kebocoran tersebut dapat menyebabkan *user privacy* pengguna internet terganggu. Kebocoran tersebut juga menjadi pemantik terjadinya serangan *man-in-the-middle* atau *sniffing*. Melihat kasus tersebut, terdapat peluang untuk turut serta dalam mendukung keamanan pada lalu lintas data. Salah satu bentuk dukungan pencegahan yang dilakukan adalah menciptakan layanan *Core* DNS dengan tujuan menjaga privasi pelanggan. Sejalan dengan upaya mendukung layanan tersebut, diperlukan suatu implementasi konsep yang bertujuan untuk mendukung berjalannya layanan tersebut. Layanan *Core* DNS akan berjalan seiring diterapkannya protokol keamanan DNS *over* TLS. Selama beberapa dekade terakhir, protokol HTTPS telah mendapat perhatian dari seluruh komunitas, pakar, serta developer dari seluruh dunia. HTTPS menjaga integritas dan kerahasiaan lalu lintas data *end user*. Sejak penggunaan SSL hingga TLS, HTTPS terus mengalami pembaruan untuk keamanan yang lebih baik, namun tidak dengan DNS. HTTPS hanya menjamin keamanan setelah sesi *secure* terjadi dan *established*. Secara teknis yaitu kesepakatan (*handshake*) algoritma *cryptography* yang digunakan. Berdasarkan penjelasan diatas, belum menyinggung terkait sesi itu yaitu bagaimana DNS berjalan. DNS dinilai sangat rentan hingga saat ini karen siapapun dapat mengamati lalu lintas DNS seseorang. Beberapa tahun terakhir berita terkait *net neutraility* dan kebebasan berinternet yang menyangkut *user privacy*, DNS mulai mendapat perhatian. Hingga IETF mengeluarkan *draft* yang menanamkan TLS pada DNS sebagaimana HTTPS. Berbekal pengetahuan dan konsep ini, penulis bermaksud mengambil topik DNS *over* TLS sebagai salah satu riset yang akan dilakukan.

Kata Kunci: DNS, HTTPS, TLS, DNS *over* TLS (DoT)