

Mendalami Onion Network dengan TOR

M Rizqi R
20051204034
Teknik Informatika 2020 B
Universitas Negeri Surabaya

Alfito Mulyono
20051204038
Teknik Informatika 2020 B
Universitas Negeri Surabaya

March 2, 2022

I Pendahuluan

1.1 Latar Belakang

Bocornya informasi pengguna internet memiliki dampak yang merugikan. Banyak sekali pihak yang ingin mencuri data kita untuk dimanfaatkan dalam kepentingan mereka pribadi. Mereka akan menjual data kita kepada pihak-pihak yang menginginkan data kita.

Kita dapat mengambil contoh dari sebuah perusahaan media sosial ternama seperti Facebook. Pada 19 Desember 2018, Facebook diketahui telah membocorkan 1,5 miliar data pengguna Facebook dan menjualnya kepada pihak ketiga. Mark Zuckerberd, pendiri Facebook dinyatakan bersalah dalam persidangan dan dijatuhi denda sesuai keputusan hakim.

Namun kebocoran data bisa juga terjadi karena kesalahan pengguna. Pengguna kerap mengunjungi situs-situs acak kemudian tanpa sengaja menekan iklan yang muncul dalam situs tersebut. Kemudian pengguna tanpa sadar telah mengunduh perangkat lunak yang berisi virus yang kemudian berjalan di belakang layar. Virus ini dapat berupa berbagai jenis perangkat lunak yang dapat menginfeksi perangkat pengguna.

Ada pula virus yang bahkan bisa digunakan untuk melacak setiap jengkal aktivitas pengguna. Baik itu dari ketikan keyboard, lokasi, bahkan mampu memanipulasi berkas digital yang dimiliki oleh pengguna hingga bisa mencuri berkas tersebut.

Maka dari itu diperlukan cara agar kita terhindar dari kejahatan internet tersebut. Salah satunya ialah memilih alat penjelajah web (*web browser*) yang tepat. Web browser yang tidak melacak kita saat menjelajah internet dan mencegah situs-situs berbahaya melacak dan mencuri data kita.

1.2 Rumusan Masalah

Adapun rumusan masalah pada pemaparan ini adalah:

1. Apa yang dimaksud dengan keamanan internet?
2. Bagaimana mencegah diri dari *cyber crime*?
3. Bagaimana menggunakan TOR sebagai media penjelajah yang aman?

1.3 Tujuan

Berdasarkan latar belakang yang telah dipaparkan. Tujuan makalah ini adalah untuk memberikan wawasan tentang *web browser* yang fokus pada privasi dan keamanan pengguna. Maka dari itu, tujuan spesifik dari makalah berikut adalah sebagai berikut:

1. Membuat pembaca mengerti tentang pentingnya *cyber security*.
2. Membuat pembaca memahami cara mengamankan dirinya dari kebocoran dan pencurian data.
3. Membuat pembaca memahami konsep *Cyber Security*, *VPN*, *proxy*, *TOR Network*.
4. Membuat pembaca memahami cara menggunakan *TOR Network*.

II Pembahasan

2.1 Cyber Security

Adalah istilah yang digunakan untuk metode pengamanan data baik pribadi maupun publik dalam jaringan internet. Metode *cyber security* dirancang untuk melawan ancaman terhadap sistem jaringan dan aplikasi, baik itu serangan yang berasal dari dalam maupun luar sistem.

2.2 VPN

Adalah singkatan dari *Virtual Private Network* merupakan sebuah metode untuk menyembunyikan alamat IP asli dari pelacakan. Dengan VPN, alamat IP akan dipalsukan atau dialihkan dari perangkat asli pengguna ke perangkat yang ada di server penyedia VPN. Contoh kasusnya adalah jika penyedia internet kita mencegah kita untuk mengakses alamat IP tertentu, maka kita bisa memakai VPN untuk melakukan tunneling ke sever luar yang dimana alamat IP tersebut bisa di akses. Dengan ini, alamat IP pengguna yang sesungguhnya dapat di bungkus dan dialihkan ke alamat IP server luar atau pihak ketiga. Namun metode ini tidak sepenuhnya aman. Sudah banyak laporan tentang bocornya data pengguna NordVPN. NordVPN ialah salah satu penyedia layanan VPN yang sudah cukup terkenal. Namun sudah banyak laporan bahwa data pengguna bocor.

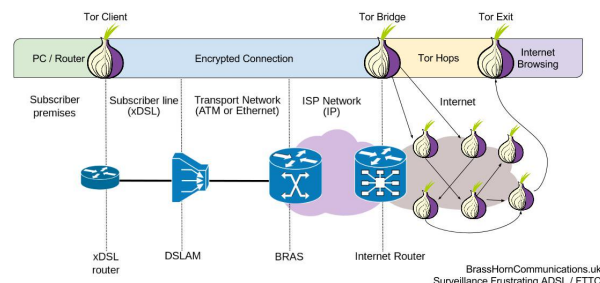
Ini disebabkan adanya tindakan penetrasi pada enkripsi saat pengguna melakukan autentifikasi ketika mencoba terhubung ke layanan penyedia VPN. Kemungkinan yang lain adalah ada yang mengakses server VPN secara langsung dan mencuri data atau kunci autentifikasi pengguna. Juga bisa terjadi ketika pengguna mengakses Wi-Fi publik yang ternyata merupakan Wi-Fi buatan peretas dan peretas tersebut mendapatkan kunci VPN melalui *Man In The Middle Attack*.

2.3 Proxy

Adalah sebuah server pihak ketiga yang menjadi perantara antara pengguna ke server yang dituju sebagai alternatif daripada langsung menghubungi server. Proxy ditujukan bila pihak penyedia internet memblokir alamat IP tertentu. Maka dengan proxy, kita bisa terlebih dahulu terhubung ke server pihak ketiga kemudian mengakses alamat IP tujuan kita melalui server tersebut. Namun metode ini tidak akan menyembunyikan alamat IP kita dan cenderung rawan untuk dipenetrasi dengan *Man In The Middle Attack*. Seseorang bisa sengaja masuk diantara jalur pengguna dan penyedia *proxy* dan melakukan *sniffing* atau melihat data yang lewat melalui jaringan.

2.4 TOR Network

TOR adalah sebuah *Free and Open Source Software* yang merupakan sebuah protokol keamanan diinternet yang bisa digunakan secara gratis. Protokol ini akan menggabungkan teknologi *VPN* dan *Proxy*. Dimana pengguna akan masuk ke dalam jaringan TOR untuk mengakses internet. Alamat IP pengguna akan melompati beberapa server sukarelawan secara acak sebelum terhubung ke internet.



Ini dapat memberikan keamanan lebih kepada pengguna dikarenakan alamat IP pengguna akan dibungkus dengan berlapis-lapis alamat IP yang membuat penyerang kesulitan bahkan tidak mungkin

melacak alamat IP asli pengguna. Ini juga dikarenakan fitur enkripsi akan diterapkan pada setiap pembungkus alamat IP.

2.4.1 Cara Menggunakan TOR

III Penutup