BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

IMSI catcher, atau dikenal juga sebagai "stingray" dalam istilah umum, yaitu perangkat yang digunakan untuk memata-matai atau mengintersep komunikasi nirkabel dalam jaringan seluler, terutama pada jaringan GSM (Global System for Mobile Communications). IMSI catcher bekerja dengan menyamar sebagai stasiun dasar seluler (base station) palsu, yang menarik perangkat seluler di sekitarnya untuk berkomunikasi dengannya. IMSI (International Mobile Subscriber Identity) adalah nomor unik yang diberikan kepada setiap kartu SIM di jaringan GSM, yang digunakan untuk mengidentifikasi pengguna perangkat seluler.

Saat ini, IMSI Catchers digunakan untuk (a) melacak handset; (b) mengirim spam geotarget; (c) mengirim pesan operator yang mengonfigurasi ulang ponsel (misalnya, menginstal perantara permanen dengan mengatur Access Point Number (APN) baru, httpproxy, atau menyerang antarmuka manajemen; (d) langsung menyerang kartu SIM dengan SMS terenkripsi yang difilter oleh sebagian besar operator; dan (e) juga berpotensi untuk mengintersep sistem autentikasi dua faktor (2FA) atau Nomor Otentikasi Transaksi Seluler (mTAN: Mobile Transaction Authentication Number).

IMSI Catcher telah menjadi topik yang menarik dan kompleks. Pell dan Soghoian dalam penelitian lamanya berpendapat bahwa saat ini manusia berada di ambang zaman dimana hampir semua orang bisa mendengarkan pembicaraan telepon, mirip dengan tahun 1980-an ketika scanner analog murah digunakan untuk mendengarkan telepon seluler di AS dan Eropa[1]. Dalam beberapa tahun terakhir, perkembangan teknologi IMSI catcher telah menghadapi tantangan dan perubahan. Beberapa penggunaan IMSI catcher telah dilarang atau diatur ketat oleh undang-undang di beberapa negara, mengingat potensi penyalahgunaan dan pelanggaran privasi yang dapat terjadi. Di Indonesia sendiri, penggunaan IMSI Catcher untuk melakukan penyadapan berdasarkan Mobile Equipment Identity (IMEI) yang telah didaftarkan aturannya belum kuat atau rigid [2]. Penggunaan IMSI Catcher menjadi polemik

karena berdasarkan peraturan praktek penyadapan harus melalui beberapa prosedur di antaranya adalah perizinan dari pengadilan, hingga target penyadapan terbukti melakukan tindak pidana. Apabila prosedur dilakukan, maka penyadapan sah dilakukan dan tidak melanggar privasi data.

IMSI catcher adalah perangkat yang digunakan untuk mengeksploitasi atau menyadap komunikasi seluler dari target yang menjadi sasaran serangan. Perangkat ini akan mencari perangkat seluler yang berada dalam jangkauan atau radius kerjanya. Perangkat seluler yang berkomunikasi dengan jaringan seluler akan mengirimkan sinyal yang dapat dideteksi oleh IMSI catcher. IMSI catcher dapat melakukan pemindaian atau pemeriksaan terhadap perangkat seluler yang terhubung ke jaringan seluler dalam radius kerjanya. IMSI catcher kemudian akan menyamar sebagai menara seluler palsu atau meniru sinyal menara seluler asli. Dengan begitu, perangkat seluler target akan berkomunikasi melalui IMSI catcher, mengira bahwa IMSI catcher adalah menara seluler yang sah. Perangkat ini kemudian akan menangkap sinyal dan data yang dikirimkan oleh perangkat seluler target yang berkomunikasi melalui dirinya termasuk informasi seperti nomor identifikasi unik perangkat seluler (IMSI), nomor telepon, pesan teks, dan data komunikasi lainnya. Setelah data dikumpulkan, IMSI catcher atau operator yang mengendalikan perangkat tersebut dapat menganalisis data yang diperoleh untuk mendapatkan informasi yang diinginkan atau mencari pola komunikasi tertentu. Data yang dikumpulkan oleh IMSI catcher dapat digunakan untuk berbagai tujuan, baik yang sah maupun yang tidak sah. Potensi penyalahgunaan dapat mencakup pencurian identitas, pemantauan ilegal, penargetan individu atau kelompok tertentu, atau pengungkapan informasi pribadi tanpa izin.

Universal Mobile Telecommunication System (UMTS, 3G) dan Long Term Evolution (LTE, 4G) memerlukan otentikasi dua arah mutual, tetapi masih tidak sepenuhnya kebal terhadap IMSI Catcher. Pelacakan dan identifikasi IMSI Catchers didasarkan pada kelemahan bahwa jaringan harus dapat mengidentifikasi pelanggannya sebelum dapat mengotentikasinya. Selain itu, perintah yang tidak diotentikasi dapat digunakan untuk menurunkan ponsel menjadi menggunakan 2G atau 2.5G yang kurang aman, akhirnya memberikan jalan bagi serangan secara penuh. Isu ini semakin menjadi sorotan karena jaringan komersial semakin melampaui jaringan administratif dan pemerintah dalam cakupan dan tingkat data.

Dengan demikian akan membawa lebih banyak data yang semakin sensitif. Faktor lainnya, pada saat ini, banyak sektor ekonomi sangat bergantung pada infrastruktur komunikasi seluler. IMSI catcher dapat ditingkatkan dan dimodifikasi untuk menghindari tindakan pencegahan, sehingga semakin sulit dideteksi dan dilindungi. Seiring berkembangnya teknologi, IMSI catcher mungkin menjadi lebih canggih, yang dapat menyulitkan pendeteksian dan mitigasi penggunaannya. Untuk mengatasi tantangan-tantangan ini, diperlukan pendekatan yang komprehensif yang mempertimbangkan terutama pada aspek teknologi,

1.2 Perumusan Masalah

Dari latar belakang, maka dapat dirumuskan permasalahan dalam penelitian ini yaitu:

a) “Bagaimana mengetahui keberadaan IMSI Catcher sehingga dapat menghindari dari serangan IMSI Catcher”;

b) “Bagaimana mengidentifikasi anomali pada jaringan penyedia layanan komunikasi GSM?”.

1.3 Pendekatan Pemecahan Masalah

Pendekatan pemecahan masalah dalam mendeteksi IMSI catcher, atau sering disebut juga sebagai penangkal IMSI catcher, meliputi hal-hal berikut:

a) Pemantauan jaringan seluler

Menggunakan perangkat pemantauan jaringan seluler yang dapat mendeteksi aktivitas yang mencurigakan atau tidak biasa pada jaringan seluler. Dalam hal ini akan melibatkan pemantauan aktivitas sinyal seluler, deteksi perubahan atau variasi dalam pola jaringan, atau identifikasi perangkat yang tidak dikenal atau tidak sah yang mencoba untuk mengakses jaringan.

b) Analisis trafik

Melakukan analisis trafik data yang melewati jaringan seluler untuk mengidentifikasi pola komunikasi yang tidak biasa atau mencurigakan, seperti perangkat yang terusmenerus berpindah antara menara seluler dengan kekuatan sinyal yang sangat kuat, atau adanya pengiriman data atau pesan yang tidak wajar.

c) Pendeteksian anomali

Menggunakan algoritma atau teknik pendeteksian anomali untuk mengidentifikasi perangkat yang berkomunikasi dengan pola yang tidak biasa

atau mencurigakan. Dalam hal ini akan menggunakan pengenalan pola komunikasi normal yang digunakan oleh perangkat seluler, dan mendeteksi adanya perubahan yang mencurigakan atau tidak wajar dalam pola tersebut. d) Pendeteksian sinyal palsu Menggunakan teknik untuk mendeteksi adanya sinyal palsu atau menara seluler palsu yang digunakan oleh IMSI catcher. Dalam hal ini bisa melibatkan pemantauan dan analisis sinyal radio frekuensi (RF) untuk mengidentifikasi sinyal yang tidak sah atau tidak terdaftar yang berasal dari IMSI catcher.

e) Kolaborasi dengan otoritas

Bekerjasama dengan otoritas yang berwenang, dalam hal ini dengan Balai Monitor Spektrum Frekuensi Radio Kelas II Lampung untuk mengidentifikasi dan menindaklanjuti aktivitas yang mencurigakan atau ilegal yang terkait dengan penggunaan IMSI catcher. Dalam hal ini akan melibatkan pelaporan temuan, pengumpulan bukti, dan mengikuti prosedur hukum yang berlaku untuk menangani masalah IMSI catcher.

1.4 State Of the Arts dan Kebaruan Penelitian

Sebagian besar penelitian sebelumnya berfokus pada pendeteksian stasiun dasar palsu dari sisi konsumen, namun pada usulan penelitian ini mengambil pendekatan dari sudut pandang operator jaringan dan membahas kemampuan deteksi baru dari segi akademik dan praktis. Penelitian sebelumnya [3], [4], [5], [6], [7] difokuskan pada sisi pelanggan (konsumen), penelitian ini mencoba menggeser perspektif dan membahas deteksi serangan tersebut dari sisi operator. Tantangan khusus terletak pada struktur jaringan seluler digital, yang dirancang pada masa koneksi ber-bandwidth rendah, dengan cara lalu lintas sinyal mengambil sejumlah besar infrastruktur jaringan. Oleh karena itu, jaringan ini dirancang dalam mode hierarkis yang terdistribusi secara geografis, dengan sebanyak mungkin lalu lintas sinyal yang ditangani secara lokal atau regional, meskipun tetap memberikan efek terhadap beban backbone. Hal ini menimbulkan tantangan unik dalam mengakuisisi dan mengkorelasikan data yang diperlukan untuk mendeteksi anomali dalam jaringan.

Selain tantangan tersebut diatas, keterbaruan penelitian ini yaitu pada pengembangan teknik baru untuk mendeteksi keberadaan IMSI catcher dan memetakannya dalam cyber threat map yang berbasis web. Inovasi lainnya

yaitu dalam deteksi IMSI catcher digunakan beberapa sumber data dan parameter untuk analisis, termasuk data tingkat jaringan, data sinyal, data lokasi, dan pola perilaku perangkat seluler. Dengan menghubungkan data dari berbagai sumber dan menganalisisnya secara holistik, metode deteksi IMSI catcher dapat menjadi lebih efektif dalam mengidentifikasi pola dan perilaku kompleks yang mengindikasikan aktivitas IMSI catcher.

1.5 Tujuan dan Sasaran Penelitian

Tujuan dari penelitian ini adalah menciptakan sistem pemantauan untuk menemukan pola gejala yang lebih kompleks yang umumnya dihasilkan oleh IMSI Catcher. Selain itu juga untuk mengidentifikasi keberadaan perangkat IMSI catcher yang tidak sah atau tidak diizinkan dalam jaringan seluler. Dengan mendeteksi IMSI catcher, dapat dilakukan tindakan yang diperlukan untuk melindungi keamanan dan privasi pengguna, serta mencegah akses yang tidak sah ke data pribadi atau informasi sensitif. Tujuan lainnya yaitu membantu operator seluler dalam mengambil langkah-langkah untuk melindungi integritas jaringan seluler dan memastikan keberlanjutan layanan yang andal bagi pengguna.

Sedangkan sasaran dari penelitian ini yaitu memastikan keberlanjutan layanan seluler yang andal, melindungi keamanan jaringan dan infrastruktur telekomunikasi, serta mendukung penegakan hukum dan penghindaran kegiatan ilegal.

1.6 Manfaat Penelitian

Adapun manfaat dalam melakukan penelitian ini adalah:

1. Dapat mengetahui keberadaan IMSI Catcher disekitar anda sehingga dapat menghindari dari serangan IMSI Catcher.
2. Dapat mengidentifikasi anomali pada protocol penyedia layanan.

1.7 Ruang Lingkup Penelitian

Dalam penulisan tesis ini, penulis akan membatasi ruang lingkup penelitian dengan menitikberatkan permasalahan yang akan dibahas yaitu:

1. Penelitian dilakukan pada Workshop Yayasan Dina Peduli, LAB IBI Darmajaya.

2. Penelitian menggunakan metode LAC/CID Consistency database synchronous.

1.8 Sususan dan Struktur Proposal Jurnal

Maksud dari susunan dan proposal jurnal ini adalah agar dapat memberikan gambaran secara jelas agar terlihat hubungan antara bab yang satu dengan bab yang lainnya. Susunan dan struktur proposal jurnal dijelaskan dibawah ini sebagai berikut.

BAB I PENDAHULUAN

Bab ini membahas tentang rangkuman dari keseluruhan isi dokumen yang disajikan secara singkat.

BAB II KAJIAN PUSTAKA

Bab ini membahas tentang kajian pustaka, penelitian terdahulu, kerangka berfikir, dan hipotesis penelitian yang akan dilakukan.

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang bagaimana mencegat lalu lintas telepon seluler dan melacak data lokasi pengguna ponsel, mensimulasikan BTS (base transceiver station) "palsu" yang bertindak di antara target ponsel dan BTS (base transceiver station) penyedia layanan, mengidentifikasi informasi yang berada pada BTS (base transceiver station) disekitar, mengidentifikasi informasi anomali pada dengan metode LAC/CID Consistency database synchronous.

LAMPIRAN

- Berisi lampiran pendukung daripada penelitian yang akan dilakukan.