1. Pendahuluan

Latar belakang

Electronic Control Unit (ECU) merupakan sebuah komponen komputer yang bertanggung jawab untuk menjalankan suatu fungsi tertentu di dalam *automobile*. Di dalam sebuah automobile terdapat 20-100 ECU dengan berbagai fungsi, contohnya untuk mengencangkan sabuk pengaman, kalibrasi kemudi pada sudut ban, mendeteksi penumpang di dalam mobil, *Keyless Entry and Start* (KES) dan lain-lain [1, 2]. Pada KES terdapat sebuah *key fob* dan *transceiver* (ECU) yang berfungsi untuk membuka dan mengunci pintu pada mobil. Sebagai ganti membuka dan mengunci pintu mobil dengan kunci tradisional, pengguna KES hanya perlu menekan tombol pada *key fob* untuk membuka atau mengunci pintu mobil. Namun KES pada *modern automobiles* sering menjadi target tindak kriminal seperti pencurian, metode yang digunakan salah satunya bernama *Playback Attack*. Penyusup menggunakan sebuah perangkat yang mampu merekam pesan *wireless* yang berisi *identifier*, kemudian pesan tersebut dapat diputar kembali sehingga sistem kunci pada kendaraan tersebut akan mengira bahwa pesan tersebut datang dari *key fob* yang asli [3, 4].

Terdapat beberapa ECU yang dapat berkomunikasi dengan dunia luar sebagai jaringan internal, biasanya komunikasi tersebut betujuan untuk menghubungkan antara pengguna dengan ECU. Akan tetapi hal ini dapat membuka celah baru yang dapat mengakibatkan ECU diserang oleh pihak yang tidak bertanggung jawab. *Denial of Service* (DOS) adalah salah satu contohnya, DOS merupakan metode penyerangan yang bertujuan untuk menyibukkan *server* dengan cara mengirimkan banyak *request* sehingga *server* tidak dapat mengeksekusi perintah [5]. Penyerangan DOS dapat dilakukan pada beberapa ECU contohnya pada KES, dikarenakan pada bagian KES terdapat ECU yang bisa berkomunikasi dengan dunia luar [1, 6, 7]. Penyerangan DOS pada ECU di dalam *Keyless Entry System* akan menyebabkan ECU tidak dapat mengeksekusi perintah baru dan membuat sistem pintu tidak dapat bekerja. Pada umumnya penyerangan DOS dilakukan untuk hal yang merugikan seperti melumpuhkan *server*, membuat jaringan lambat, dan lain-lain [5, 8].

Dalam tugas akhir ini diusulkan sebuah sistem yang mengimplementasi DOS sebagai metode perlindungan *Keyless Entry and Start* (KES) terhadap serangan *Playback Attack* yang mampu meniru *identifier*. Metode ini bekerja dengan cara melakukan penyerangan DOS pada ECU yang bertugas untuk mengoprasikan sistem kunci kendaraan. Ketika ECU tersebut sedang diserang, maka sistem kunci kendaraan tidak akan berfungsi karena serangan DOS telah memakai semua *resource* yang mengakibatkan *request* tidak bisa diproses. Maka *playback attack* tidak akan berhasil karena *identifier* yang asli pun tidak akan bekerja apabila serangan DOS tersebut tidak dihentikan. Untuk prototipe KES akan dibangun menggunakan *smartphone* sebagai *key fob*, raspberry pi dan router sebagai *transceiver* dan IP address pada *smartphone* sebagai *identifier*. Kemudian untuk serang DOS akan menggunakan sebuah *tool* bernama hulk yang dijalankan pada sistem operasi linux.

Tool hulk tersedia di https://github.com/grafov/hulk.

Topik dan Batasannya

Dari latar belakang yang telah dipaparkan, didapatkan beberapa rumusan masalah pada penelitian ini, yaitu pembuatan prototipe KES, melakukan penyerangan DOS menggunakan *tool* yang bernama hulk pada prototipe KES, pemanfaatan serangan DOS untuk pertahanan terhadap jenis serangan *playback attack*.

Adapun batasan masalah dalam pengerjaan Tugas Akhir ini, yaitu ancaman pada KES kendaraan adalah *playback attack*, menggunakan hulk sebagai DOS *tool*, pengujian dilakukan pada satu jaringan yang sama.

Tujuan

Terkait permasalahan yang dipaparkan di atas, dapat ditarik tujuan yang akan dicapai dalam Tugas Akhir ini adalah merancang prototipe KES, merancang dan mengimplementasikan serangan DOS menggunakan *tool* hulk pada prototipe KES, mengimplementasikan dan menganalisa serangan DOS untuk pertahanan terhadap jenis serangan *playback attack*.

Organisasi Tulisan

Pada penulisan Tugas Akhir ini akan dibagi menjadi beberapa bagian yaitu :

1. Pendahuluan : Pada bagian ini menjelaskan latar belakang, Topik dan Batasan, Tujuan dan Organisasi Tulisan untuk Tugas Akhir ini.
2. Studi Tekait : Pada bagian ini berisi teori atau studi atau literatur yang mendukung Tugas Akhir yang sedang dikerjakan.
3. Prototipe KES dan Serangan DOS : Pada bagian ini menjelaskan prototipe dan sistem yang akan dibangun.
4. Evaluasi : Bagian ini berisi dua sub bagian yaitu : Hasil Pengujian dan Analisis Hasil Pengujian
5. Kesimpulan : Bagian kesimpulan memuat kesimpulan dan saran yang diambil dari hasil dan analisis hasil pengujian.