Peretasan Mobil Jarak Jauh

Tugas Akhir Mata Kuliah Keamanan Informasi

II3230

Khoirunnisa Afifah

(13512077)

ABSTRAK

Makalah ini membahas tentang peretasan mobil jarak jauh (*remote car hacking*) mulai dari teori tentang sistem komputer pada mobil, *attack surface,* dan fitur-fitur *automobile modern* yang dapat dimanfaatkan untuk melakukan serangan. Pembahasan lebih lanjut pada makalah ini meliputi eksploitasi nyata yang telah dilakukan oleh beberapa peneliti, attack surface dan fitur yang dapat digunakan untuk peretasan pada mobil-mobil di Indonesia dan penanganan terhadap serangan yang mungkin terjadi.

I. Pendahuluan

Industri *automobile* saling berkompetisi memberikan produk terbaiknya dengan berbagai fitur baru untuk kenyamanan dan keamanan penggunanya. Fitur terbaru yang sekarang ramai dibicarakan adalah berkembangnya penelitian tentang *self-driving car*. Sebelum fitur *self-driving* car tersebut diproduksi secara massal di industri, saat ini sudah banyak fitur pintar yang ada pada mobil, seperti *park assist* dan *collision prevention*. Sebagian besar fitur pintar ini berfungsi untuk mengurangi kerja pengemudi dan untuk meningkatkan keamanan.

Selain fitur-fitur pintar tersebut terdapat beberapa fitur yang bertujuan untuk hiburan. Tidak hanya radio seperti kebanyakan mobil pada saat ini, beberapa mobil baru memiliki pemutar musik yang dapat terhubung dengan perangkat lain melalui *Bluetooth*. Beberapa mobil juga memiliki fitur jaringan selular untuk mendapatkan informasi cuaca, lalu lintas, dan juga sebagai *remote* Wi-Fi hotspot.

Keberadaan fitur-fitur baru tersebut tentu saja memanjakan konsumen. Namun, di sisi lain fitur-fitur tersebut juga membuka celah keamanan baru yang dapat dimanfaatkan oleh pihak tertentu untuk merugikan bahkan membahayakan nyawa konsumen. Meski sampai saat ini belum ditemukan kasus dimana peretasan mobil dilakukan di luar konteks penelitian, namun fakta bahwa peretasan tersebut dapat dilakukan tidak boleh diabaikan. Makalah ini memberikan gambaran mengenai peretasan mobil jarak jauh yang telah dilakukan oleh beberapa peneliti sebelumnya.

II. Sistem Elektronik dan Jaringan pada *Automobile*

Untuk dapat menjalankan fitur-fitur pintar, mobil-mobil keluaran terbaru didukung oleh rangkaian-rangkaian elektronik yang berperan seperti komputer. Sebagaian besar rangkaian itu bertanggung jawab untuk memonitor dan mengontrol keadaan mobil. Rangkaian elektronik pada mobil disebut sebagai *electronic control unit* (ECU). Masing-masing ECU bertugas untuk mengerjakan

tugas tertentu misalnya untuk mengencangkan sabuk pengaman, memonitor setir mobil, atau mengecek apakah ada penumpang di dalam mobil.

Setiap ECU memiliki sensor dan aktuator. Sensor pada ECU digunakan untuk menentukan aksi apa yang akan diambil. Sedangkan aktuator berfungsi untuk melakukan aksi berupa gerakan ataupun untuk menahan objek agar tidak bergerak. Selain sensor dan aktuator, ECU perlu mengirimkan pesan pada ECU lain untuk dapat berkoordinasi. Komunikasi ini dapat dilakukan karena setiap ECU terhubung pada *Controller Area Network* (CAN).

Pesan yang dikirimkan oleh ECU berupa CAN packet. CAN *packet* ini dikirim kepada semua ECU yang ada pada CAN *bus* tanpa autentikasi maupun identitas pengirim. CAN *packet* terdiri dari bagian *identifier* dan *data*. CAN *packet* pada mobil biasanya memiliki *identifier* berukuran 11 bit. *Identifier* ini menyimpan informasi mengenai prioritas *packet* dan tanda agar ECU penerima tahu ia harus memproses *pesan* yang diterima. *Data* berisi pesan yang 8-*byte data* beserta *checksum* dari *data* tersebut. Metode penghitungan *checksum* untuk masing-masing merek mobil bisa berbeda-beda. Apabila ada paket dengan *checksum* yang salah, paket tersebut akan diabaikan oleh ECU.

Pada jaringan *automobile* terdapat dua jenis CAN *packet* yaitu *normal packet* dan *diagnostic packet*. *Normal packet* adalah paket yang dikirim oleh ECU dan dapat dilihat kapanpun oleh ECU lain untuk memproses data yang dikirim tersebut. Pada *normal packet* ini setiap ECU menentukan sendiri mana pesan yang harus mereka proses berdasarkan CAN ID yang ada pada paket. *Diagnostic packet* adalah paket yang dikirim oleh alat diagnostik yang digunakan oleh mekanik untuk berkomunikasi dengan ECU. Paket ini biasanya tidak dikirimkan pada waktu operasi biasa ECU. Pada *diagnostic packet* ini, masing-masing ECU memiliki ID yang sudah ditentukan dan paket akan berisi informasi mengenai ID ini.

Beberapa ECU juga dapat berkomunikasi dengan jaringan di luar jaringan mobil. Komunikasi ini biasanya dilakukan dengan sinyal radio, Bluetooth atau jaringan seluler.

III. Remote Car Hacking

Peretasan mobil jarak jauh (*remote car hacking)* dapat dibagi menjadi beberapa jenis. Jenis pertama adalah peretasan yang memanfaatkan sistem jaringan komunikasi internal pada mobil atau CAN *network*. Peretasan ini bertujuan untuk mengirimkan pesan yang dapat mengubah perilaku ECU yang langsung berhubungan dengan sistem kendali fisik pada mobil, seperti rem dan setir mobil. Jenis peretasan kedua adalah peretasan yang tidak menargetkan sistem kendali fisik mobil. Peretasan jenis ini hanya menyerang ECU yang terhubung pada jaringan luar mobil dan biasanya dilakukan untuk penyadapan. Peretasan jenis ketiga adalah peretasan yang bertujuan mengubah perilaku sistem kendali fisik mobil, namun tidak memanfaatkan sistem jaringan komunikasi internal pada mobil. Peretasan jenis ketiga ini biasanya dilakukan dengan mengubah perilaku sensor, misalnya dengan mengirimkan sinyal radar yang mengganggu sensor pendeteksi tabrakan sehingga menyebabkan mobil melakuakan pengereman.

Menurut [7] terdapat tiga tahap untuk dapat melakukan peretasan ECU mobil dari jarak jauh. Tahap pertama adalah mencari cara untuk mendapatkan akses jaringan internal pada mobil. Cara ini dilakukan dengan meretas ECU yang memiliki jaringan komunikasi keluar seperti Bluetooth atau jaringan seluler. Dengan masuk ke jaringan internal ECU seseorang dapat mengirimkan pesan untuk mengatur perilaku ECU lain. Beberapa peretas mungkin hanya ingin memata-matai pembicaraan di dalam mobil, oleh karenanya ia hanya perlu menyalakan mikrofon. Namun, peretasan lain yang menargetkan sistem kendali fisik pada mobil memerlukan langkah-langkah lain yang lebih sulit dan sangat bergantung pada fitur dari setiap merek mobil.

Tahap kedua yang perlu dilakukan untuk meretas sistem kendali fisik mobil adalah mengirimkan pesan ke jaringan internal mobil untuk berkomunikasi dengan *critical* ECU. ECU yang dimaksud disini adalah ECU yang bertanggung jawab untuk mengatur rem, setir, atau percepatan mobil. Tahap ini cukup rumit untuk dilakukan. Alasan pertama adalah setiap merek mobil akan memiliki mekanisme pengiriman pesan yang berbeda satu dengan yang lainnya. Selain itu,

biasanya ECU yang dijadikan 'pintu masuk' peretasan pada tahap pertama biasanya tidak dapat langsung berkomunikasi dengan ECU yang bertanggung jawab pada sistem kendali fisik mobil. Oleh karenanya, diperlukan sebuah mekanisme *bridging* dari ECU awal ke ECU tujuan.

Tahap terakhir adalah membuat target ECU berperilaku sesuai keinginan peretas. Pada tahap ini diperlukan mekanisme *reverse engineering* untuk mengetahui pesan seperti apa yang dikenali oleh ECU. Kesulitan yang muncul adalah setiap merek mobil akan memiliki struktur pesan yang berbeda-beda. Selain itu, beberapa ECU memiliki sistem keamanan tambahan, misalnya tidak mendengarkan pesan saat mobil sedang berjalan.

Karena setiap merek mobil memerlukan cara yang berbeda dalam mekanisme sistem diperlukan penelitian terlebih dahulu mengenai fitur-fitur yang adala pada mobil yang akan diretas. Fitur-fitur yang harus diperhatikan adalah fitur yang berhubungan dengan komunikasi ke luar jaringan mobil karena dapat menjadi *attack surface* peretasan. Selain *attack surface* yang ada pada setiap merek mobil, perlu diketahui juga arsitektur jaringan dalam mobil dan fitur-fitur yang dikendalikan oleh komputer. Tabel 1 menunjukkan attack surface dari mobil Ford Escape 2010 dan Toyota Prius 2010 yang dianalisa oleh Miller dan Valasek pada [7].

Tabel 1
Attack Surface Pada Modern Automobile

No	**Attack Surface**	**Keterangan**	**Ukuran *vulnerability***
1.	*Passive Anti Theft System*	*Chip* pada *ignition key* yang berfungsi memberikan sinyal RF kepada komputer pada mobil untuk memberitahu bahwa mobil harus berjalan. Apabila sinyal yang didapat tidak valid maka beberapa komponen seperti pompa bensin tidak dapat berjalan.	*Attack surface* kecil untuk *remote code execution*.
2.	*Tire pressure monitoring system* (TPMS)	Sensor tekanan yang ada pada setiap roda dan akan mengirimkan pesan ke ECU menggunakan sinyal radio.	*Attack surface* kecil.
3.	*Remote*	Lubang kunci mobil memiliki radio	Dapat digunakan

No	Attack Surface	Keterangan	Ukuran *vulnerability*
	keyless entry / start	*transmitter* jarak pendek yang mengirimkan pesan terenkripsi ke ECU tertentu untuk menentukan apakah kunci valid kemudian akan mengunci, membuka, atau menjalankan kendaraan.	untuk menyebabkan *Denial of Service*, namun untuk *remote code execution attack surface*-nya kecil.
4.	*Bluetooth*	Sebagian besar kendaraan memiliki fitur Bluetooth untuk melakukan sinkronisasi dengan perangkat lain yang dimiliki pengendara.	*Attack surface* yang cukup besar karena banyak yang menerapkan fitur Bluetooth dan protokolnya cukup umum.
5.	*Radio Data Stream*	Data yang dikirimkan bersama dengan sinyal analog FM yang berisi informasi mengenai nama stasiun radio, judul lagu, dsb. Data ini harus di-*parsing* untuk dapat ditampilkan pada sistem multimedia mobil.	Peluang suksesnya *attack* ini relatif lebih kecil dibandingkan Bluetooth.
6.	*Telematics/ Cellular/Wifi*	Beberapa mobil keluaran terbaru memiliki radio seluler yang digunakan oleh kendaraan untuk terhubung pada jaringan selular. Biasanya digunakan untuk memperoleh informasi cuaca dan kondisi lalu lintas. Pada beberapa kendaraan dapat juga dijadikan remote Wi-Fi hotspot.	*Attack surface* yang paling besar karena jangkauannya yang luas.
7.	*Internet / Apps*	Beberapa mobil baru memiliki fitur untuk dapat menjalankan *browser* dan aplikasi lain yang biasa ada pada desktop komputer.	Banyak *vector* baru yang biasanya hanya ada pada desktop komputer.

Selain *attack surface* perlu diketahui juga fitur-fitur yang dapat dimanfaatkan untuk melakukan serangan. Fitur-fitur yang dimaksud adalah fitur yang melibatkan ECU yang melakukan kendali fisik terhadap kendaraan berdasarkan pesan yang ia terima. Fitur-fitur tersebut antara lain [7].

1. *Park assist*

   Fitur ini bermanfaat untuk membantu pengemudi memarkirkan mobilnya pada tempat yang sempit. Fitur *park assist* bekerja karena ada ECU yang menerima data dari sensor kemudian menghitung berapa besar putaran yang harus

diambil oleh setir mobil untuk dapat parkir. Dengan adanya fitur ini berarti ada pesan yang dikenali oleh ECU untuk mengubah arah setir. Namun, pada umumnya fitur ini hanya bekerja pada saat mobil berjalan pada kecepatan sangat rendah.

2. *Adaptive cruise control*

   Fitur ini berfungsi untuk menjaga kecepatan kendaraan sesuai keinginan dengan memperhatikan keberadaan kendaraan lain. Apabila kendaraan di depan berjalan lebih lambat maka fitur ini akan membuat mobil otomatis berhenti. Begitu juga sebaliknya, saat kendaraan di depannya mulai melaju cepat, fitur ini dapat menambah laju kendaraan. Hal ini mengindikasikan ada komputer yang dapat mengontrol rem dan percepatan mobil berdasarkan pembacaan sensor. Fitur ini biasanya bekerja pada saat mobil ada pada kecepatan tinggi.

3. *Collision prevention*

   Seperti namanya, fitur ini bermanfaat untuk membantu mobil menghindari tabrakan. Pada saat mobil ada dalam kecepatan tinggi dan sensor membaca adanya kemungkinan terjadi tabrakan, akan ada ECU yang mengirim pesan ke sistem rem untuk mengurangi laju kendaraan.

4. *Lane keep assist*

   Fitur ini berfungsi untuk menghalangi mobil berjalan melewati jalurnya secara sengaja. Sebuah kamera akan mendeteksi garis batas jalur kemudian akan ada ECU yang menentukan apakah mobil keluar jalur dan menentukan aksi yang harus dilakukan. Aksi yang akan dilakukan dapat berupa pengereman ataupun mengubah arah setir mobil.

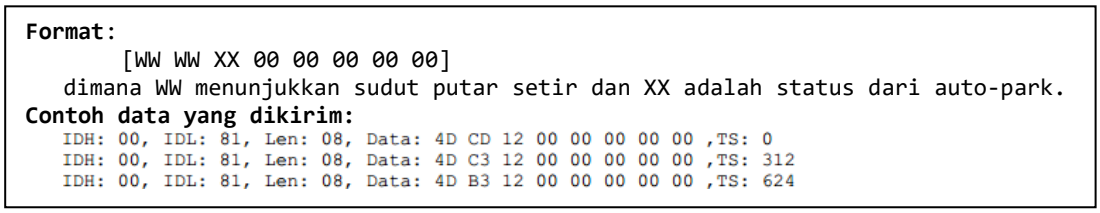
IV. Exploit Yang Pernah Dilakukan

Sampai saat ini peretasan yang membahayakan dan dapat menyerang sistem kendali mobil hanya dilakukan oleh para peneliti [9]. Penelitian yang berkaitan dengan *automotive security* dimulai pada tahun 2010 oleh beberapa peneliti dari

University of Washington dan University of San Diego [5]. Pada penelitian tersebut mereka berhasil mengirimkan CAN *packet* pada dua buah mobil keluaran tahun 2009 (yang tidak disebutkan mereknya) sehingga bisa mengontrol beberapa ECU pada mobil tersebut. Serangan yang mereka lakukan meliputi perubahan tampilan pada *speedometer* dan radio, mengatur rem dan AC, menghentikan mesin, serta mencegah mobil menyala. Meskipun serangan yang dilakukan cukup berbahaya, namun pengiriman pesan tersebut belum dilakukan secara jarak jauh. Oleh karena itu, peretas harus memiliki akses fisik secara langsung pada mobil.

Pada tahun 2011, para peneliti tersebut melanjutkan penelitian mereka dan berhasil melakukan peretasan jarak jauh [2]. Pengiriman CAN *packet* dilakukan melalui TPMS, mp3 *parser* pada radio, Bluetooth, dan unit seluler pada mobil. Pada penelitian ini juga dijelaskan mengenai kemungkinan jenis serangan lain yang dapat dilakukan setelah berhasil memasuki jaringan internal mobil. Serangan pertama adalah pencurian mobil secara massal. Serangan ini dapat dilakukan dengan cara melakukan *war dialing* kemudian memerintahkan setiap mobil untuk mengirimkan koordinat GPS dan Vehicle Identification Number (VIN). Serangan kedua adalah mempermudah dalam spionase karena penyerang dapat dengan mudah mengetahui lokasi mobil serta dapat menyalakan mikrofon yang umumnya digunakan untuk panggilan *hands-free*.

Di tahun 2013, Charlie Miller & Chris Valasek melanjutkan penelitian di bidang *automotive security* [6]. Fokus penelitian mereka adalah memberikan petunjuk teknis mengenai cara melakukan serangan. Mereka berhasil memberikan contoh pesan yang dapat digunakan untuk melakukan serangan pada dua jenis mobil Ford Escape 2010 dan Toyota Prius 2010. Selain itu, penelitian ini berhasil menemukan serangan baru yaitu mengubah setir mobil dengan memanfaatkan fitur *park assist* dan *lane keep assist*. Gambar 1 menunjukkan salah satu format CAN *packet* dan pesan yang dikirim untuk melakukan kontrol terhadap setir mobil saat auto parking pada Ford Escape.



Gambar 1 Format pesan untuk mengatur setir pada Ford Escape 2010

Menindaklanjuti penelitiannya, Miller & Valasek pada tahun 2014 melakukan penelitian baru [7]. Penelitian mereka kali ini bertujuan untuk mendapatkan gambaran umum serangan. Untuk itu mereka melakukan survey terhadap 21 jenis merek mobil. Survey dilakukan dengan cara mencari tahu *attack surface* dan fitur-fitur yang dapat dieksploitasi, kemudian mencoba mengirimkan CAN *packet* pada *critical* ECU. Dari hasil survey tersebut mereka juga mendapat kesimpulan bahwa Jeep Cherokee 2014, Cadillac Escalade 2015, dan Infiniti Q50 2014 merupakan mobil-mobil yang cukup mudah diretas karena memiliki *attack surface* yang luas, arsitektur yang sederhana, dan banyak fitur otomatis yang dapat dieksploitasi.

Pada tahun 2015 Miller & Valasek berhasil mendemonstrasikan peretasan jarak jauh terhadap Jeep Cherokee 2014 [8]. Demo dilakukan oleh seseorang yang mengendarai di mobil Jeep Cherokee 2014 di sebuah jalan raya dan kedua peretas berada di tempat lain berjarak 10 mil. Serangan-serangan awal yang dilakukan oleh Miller & Valasek adalah menyalakan AC, radio, dan *wiper* kaca mobil. Aksi selanjutnya yang dilakukan adalah mengatur mobil menjadi mode parkir, sehingga otomatis kecepatan mobil berkurang. Pada video demo terlihat bahwa meskipun pengemudi mencoba menekan pedal gas, kecepatan mobil tetap tidak bertambah. Saat mobil ada dalam kecepatan rendah, Miller & Valasek berhasil menunjukkan bahwa mereka dapat mengatur putaran setir mobil dan menonaktifkan pedal rem.

Serangan yang dilakukan oleh Miller & Valasek tersebut dapat dilakukan dengan mengeksploitasi UConnect yang ada pada Jeep Cherokee tersebut. UConnect adalah sistem konektivitas untuk kendaraan yang menyediakan fitur hiburan, konektifitas Wi-Fi, navigasi, Bluetooth, komunikasi seluler, *voice command*, dan kontrol [3]. Karena UConnect cukup banyak digunakan oleh merek kendaraan lain,

serangan yang dilakukan oleh Miller & Valasek ini sebenarnya tidak hanya berlaku untuk Jeep Cherokee.

Untuk menjalankan kode melalui UConnect, Miller & Valasek memberikan beberapa cara yang berbeda. Cara pertama adalah dengan melakukan *jailbreaking* terhadap UConnect dengan memasukkan USB berisi file ISO untuk update UConnect. Apabila USB dicabut saat sistem reboot, sistem telah selesai memverifikasi USB dan saat menyala kembali akan meminta pengguna untuk memasukkan USB. USB baru yang dimasukkan ini harus mirip seperti USB awal namun bisa berisi file yang sudah diubah, misalnya mengubah root password dari UConnect atau menambahkan kode lain. Karena sistem sudah menganggap USB tervalidasi, maka update akan langsung dijalankan beserta *malicious code* yang dimasukkan sebelumnya. Kekurangan dari teknik ini adalah diperlukan adanya akses fisik terhadap sistem UConnect pada mobil.

Cara kedua adalah dengan memanfaatkan fitur Wi-Fi hotspot pada UConnect. Pelanggan UConnect dapat menjadikan UConnect sebagai *access point* apabila mereka membayar biaya lebih untuk berlangganan fitur ini. Setelah dilakukan percobaan *port* dan *service scanning* terhadap Wi-Fi yang aktif, diketahui bahwa ada D-Bus Services yang terbuka pada port 6667. Servis ini berfungsi untuk *inter-process communication* dan dapat diakses tanpa memerlukan autentikasi. Salah satu service pada D-Bus Service yang penting adalah NavTrailService yang memiliki fitur untuk menjalankan *shell command* tanpa perlu melakukan *jailbreak* dari sistem UConnect. Meskipun jauh lebih baik daripada teknik pertama, teknik kedua ini masih memiliki kekurangan yaitu tidak banyak orang yang berlangganan untuk Wi-Fi. Selain itu, jangkauan dari sinyal Wi-Fi tidak begitu luas.

Cara ketiga adalah dengan melakukan eksploitasi jaringan seluler. UConnect pada jeep Cherokee memanfaatkan jaringan 3G yang disediakan oleh Sprint. Pada jaringan seluler ini D-Bus yang ada pada port 6667 hanya terbuka untuk koneksi internal Sprint, oleh karena itu eksploitasi harus dilakukan menggunakan device yang juga terhubung pada jaringan Sprint. Hal yang menguntungkan untuk attacker adalah Sprint tower tidak melakukan pemblokiran terhadap komunikasi

antar Sprint *device*. Sehingga *device* apapun yang terhubung pada jaringan Sprint dapat berkomunikasi dengan *device* lainnya yang tersebar di seluruh negara (US). Karena Sprint menyediakan *range* IP 21.0.0.0/8 hingga 25.0.0.0/8 untuk alamat IP kendaraan, untuk mencari mobil yang *vulnerable* dapat dilakukan dengan melakukan *scanning* terhadap port 6667 pada *range* IP tersebut. Setiap *device* yang menjawab pasti salah satu dari UConnect system atau IRC. Setelah terhubung pada D-Bus, eksploitasi yang sama dapat dilakukan seperti pada teknik kedua.

Hal paling rumit dari eksploitasi yang dilakukan oleh Miller & Valasek adalah *reverse engineering* firmware dari chipset Renesas V850/Fx3 yang digunakan oleh UConnect agar dapat memanggil fungsi yang berasosiasi dengan CAN. Setelah dilakukan *reverse engineering* diketahui bahwa komunikasi dapat dilakukan dengan mengirimkan CAN data menggunakan pesan SPI. Setelah mengetahui cara mengirim pesan CAN diperlukan *reverse enginerring* lagi untuk mengetahui pesan CAN yang dianggap valid oleh Jeep Cherokee. Baru pada akhirnya dapat dikirim perintah ke ECU sesuai keinginan.

Secara umum tahapan eksploitasi yang dilakukan oleh Miller & Valasek untuk melakukan *remote car hacking* adalah sebagai berikut:

1. Identifikasi target untuk mendapatkan IP dari target yang diinginkan. Serangan skala besar dapat dilakukan dengan menyebarkan worm.
2. Gunakan perintah execute pada NavTrailService untuk menjalankan SSH.
3. Setelah mendapatkan akses ke D-Bus dapat menjalankan Lua script untuk mengontrol radio, HVAC, dan GPS.
4. Untuk eksploitasi lebih lanjut ubah firmware dari v850.
5. Kirim CAN *messages* untuk melakukan *physical attack*.

V. Analisis Attack Surface Pada Kendaraan Di Indonesia

Penjualan mobil di Indonesia per Mei 2015 sebanyak 79.236 [1]. Dari tahun ke tahun penjualan terbesar rata-rata diduduki oleh brand Toyota, Honda, dan Daihatsu. Fitur-fitur umum pada mobil Toyota, Daihatsu, dan Honda yang dapat

menjadi attack surface dan dimanfaatkan pada peretasan mobil jarak jauh dijelaskan pada Tabel 2.

Tabel 2
Fitur pada mobil Toyota, Daihatsu, dan Honda di Indonesia

No	Fitur	Keterangan	Terdapat pada
1.	Electronic Power Steering (EPS)	Berfungsi untuk membuat setir mobil menjadi seringan mungkin saat kendaraan dalam kecepatan rendah dan menjadi berat saat kendaraan dalam kecepatan tinggi. Membaca putaran setir kemudian ada ECU yang mengirimkan sinyal untuk menggerakkan motor listrik.	Honda Mobilio, Honda Accord, Daihatsu Copen
2.	Anti-lock Breaking System (ABS)	Terdapat ECU yang bertugas untuk membaca kecepatan putaran roda mobil. Apabila ada roda yang berputar jauh lebih lambat dari yang lainnya akan dikirimkan sinyal untuk mengurangi tekanan rem pada ban tersebut, begitu juga sebaliknya saat ada roda dengan kecepatan putar yang terlalu tinggi.	Honda Mobilio, Toyota Avanza, Honda Accord, Daihatsu Copen, Toyota Corolla Altis
3.	Electronic Brakeforce Distribution (EBD)	Biasanya digunakan bersama-sama dengan ABS. Berfungsi untuk otomatis mendistribusikan besar rem untuk masing-masing roda.	Honda Mobilio, Honda Accord, Daihatsu Copen, Toyota Corolla Altis
4.	Brake Assist (BA)	Berfungsi untuk membantu pengemudi menerapkan tekanan pengereman secara penuh saat terjadi kecelakaan. Untuk melakukan hal ini, terdapat sebuah ECU yang mempelajari kebiasaan pengereman sopir. Apabila dideteksi terdapat pengereman yang tiba-tiba, brake assist akan diaktifkan.	Honda Accord, Daihatsu Copen
5.	Collision Mitigation Brake System	Seperti collision prevention	Honda Accord
6.	Adaptive Cruise Control	Sudah dijelaskan pada subbab III	Honda Accord
7.	Lane Assist	Sudah dijelaskan pada subbab III	Honda Accord
8.	Hill Start Assist	Berfungsi untuk membantu supir berpindah dari rem ke gas agar mobil	Honda Accord

No	Fitur	Keterangan	Terdapat pada
		tidak tergelincir saat akan mulai berjalan di tanjakan. Cara kerjanya yaitu dengan tetap menahan rem sesaat setelah supir melepaskan pedal rem. Sistem ini otomatis menyala dengan mendeteksi kemiringan mobil.	
9.	Vehicle Stability Control	Menjaga kestabilan mobil saat bermanuver.	Daihatsu Copen, Toyota Camry, Toyota Alphard, Toyota Vellfire
10.	TRC	Mencegah selip pada roda.	Daihatsu Copen
11.	Brake Override System	Otomatis mengabaikan sinyal pedal gas saat gas dan rem diinjak bersama.	Daihatsu Copen
12.	Buetooth		Daihatsu Terios, Honda Mobilio, Toyota Avanza, Honda Accord
13.	Internet		Toyota Corolla Altis

Sebagian besar fitur yang disebutkan diatas dapat digunakan untuk memanipulasi rem dan setir mobil. Namun, attack surface yang ada pada mobil-mobil tersebut termasuk kecil. Hal ini disebabkan karena sebagian besar hanya menerapkan fitur Bluetooth, hanya ditemukan satu mobil yaitu Toyota Corolla Altis yang menyebutkan fitur konektivitas internet.

VI. Penanganan terhadap Serangan yang Mungkin Terjadi

Terdapat beberapa hal yang dapat dilakukan untuk menghindari *remote car hacking* menurut [7] yaitu:

1. Mengamankan *remote endpoint*. Sebisa mungkin *attack surface* harus dikurangi dan seperti *best practice security* pada umumnya, matikan *service* yang tidak diperlukan.
2. Mempersulit injeksi CAN *message*. Hampir sama seperti nomor pertama, Bluetooth stack mungkin saja tidak perlu kemampuan untuk mengirimkan

CAN *message*. Sistem *sandbox* pada Android dapat diterapkan pada ECU mobil untuk meningkatkan keamanan.

3. Mengenkripsi CAN *message*.
4. Memperbaiki desain arsitektur jaringan mobil dimana ECU dengan *remote functionality* harus diisolasi dari ECU yang mengendalikan *safety unit*.
5. Mendeteksi serangan. Biasanya CAN *injection attack* dilakukan dengan mengirimkan banyak paket sehingga dapat dideteksi dengan mudah.

VII. Kesimpulan

Penelitian-penelitian yang telah disebutkan sebelumnya membuktikan bahwa peretasan jarak jauh terhadap mobil dapat dilakukan. Saat ini di Indonesia belum banyak kendaraan yang memiliki fitur-fitur yang dapat memungkinkan adanya peretasan. Meskipun begitu, kemungkinan adanya peretasan semacam ini tidak boleh diabaikan. Diharapkannya nanti saat fitur-fitur cerdas pada mobil sudah umum digunakan, keamanan dari fitur-fitur ini juga menjadi jauh lebih baik.

DAFTAR PUSTAKA

[1] Akib, S. (2015, June 16). *10 Merek Mobil Terlaris Bulan Mei*. Retrieved from Mobil 123: http://www.mobil123.com/berita/10-merek-mobil-terlaris-bulan-mei/14561

[2] Checkoway, S., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., . . . other. (2011). Comprehensive Experimental Analyses of Automotive Attack Surfaces. *USENIX Security Symposium*. San Francisco.

[3] Fiat Chrysler Automobile. (2016). *UConnect Feature*. Retrieved from UConnect: http://www.driveuconnect.com/features/entertainment/

[4] Honda Indonesia. (2016). Retrieved from Honda Indonesia Website: http://www.honda-indonesia.com/

[5] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., . . . others. (2010). Experimental security analysis of a modern automobile. *Security and Privacy (SP), 2010 IEEE Symposium on* (pp. 447–462). IEEE.

[6] Miller, C., & Valasek, C. (2013). Adventures in automotive networks and control units. *DEF CON*, 260–264.

[7] Miller, C., & Valasek, C. (2014). A survey of remote automotive attack surfaces. *BlackHat USA*.

[8] Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*.

[9] Pogue, D. (2016, February 22). *Why Car Hacking Is Nearly Impossible*. Retrieved from Scientific American: http://www.scientificamerican.com/article/why-car-hacking-is-nearly-impossible/

[10] PT Astra Daihatsu. (2016). Retrieved from Daihatsu: http://daihatsu.co.id/

[11] Toyota Astra Motor. (2013). Retrieved from Toyota Astra: http://www.toyota.astra.co.id/