e - ISSN 2598-9596

Analisis Keamanan Kunci-Pintu Nirkabel Mobil dengan Software Defined Radio (SDR)

[*Analysis of Wireless Car-Key Security with Software Defined Radio (SDR)*]

Hadipranowo Hartanto[1] dan Ihan Martoyo[1*]
[1]Program Studi Teknik Elektro, Universitas Pelita Harapan, Jl. M.H. Thamrin Blvd. 1100, Tangerang 15811
*Korespondensi penulis: imartoyo@yahoo.com

ABSTRACT

Wireless Communication is not a new phenomenon in the 21st century. Many devices are using wireless technology, including opening a car's door using a remote wireless key. To ensure the security of a wireless system, certain encryption methods and algorithms are used. The rolling code techniques, where the encryption code will be rolled to a different code after usage, are often found in wireless car key systems. This paper describes the analysis of the wireless car-key security by trying to take over control by using Software Defined Radio (SDR). The security is tested using a simple mechanism of save-and-replay, in which the signal from the wireless car-key is received by an SDR and saved into a computer within a large distance from the car. If the car-key signal is not received by the car, the rolling code mechanism might not be triggered. Then the same car-key signal can be replayed to try to open the car door. A few cars which we tested can be opened in such a way. In this paper some security practices will be suggested to avoid the save-replay hacking mechanism with SDR.
***Keywords** : car hacking; software defined radio; wireless control; wireless security.*

ABSTRAK

Komunikasi nirkabel bukanlah suatu fenomena yang baru pada abad ke-21. Banyak alat yang memanfaatkan teknologi nirkabel, termasuk membuka pintu mobil dengan kunci nirkabel. Untuk menjamin keamanan sistem nirkabel biasanya dilakukan dengan algoritma dan metode enkripsi tertentu. Metode keamanan dengan mekanisme *rolling code*, di mana kode enkripsi yang digunakan selalu berganti ke kode yang berbeda setelah dipakai, biasanya ditemukan dalam sistem kunci nirkabel mobil. *Paper* ini menjelaskan analisis tingkat keamanan dari sistem kunci-mobil nirkabel dengan berusaha mengambil alih kendali berbekal *Software Defined Radio* (SDR). Keamanan akan diuji dengan mekanisme yang cukup sederhana, yakni simpan dan kirim, di mana sinyal dari kunci nirkabel akan ditangkap dengan SDR dan disimpan ke dalam komputer dengan jarak yang cukup jauh dari mobil. Jika sinyal kunci tidak ditangkap mobil, maka mekanisme *rolling code* tidak terpicu. Setelah itu sinyal yang sama dapat diputar ulang untuk mencoba membuka kunci mobil. Beberapa mobil yang diuji dapat dibuka dengan cara demikian. Dalam *paper* ini juga akan diusulkan praktik pengamanan untuk menghindari pembukaan kunci dengan mekanisme simpan-kirim dengan SDR.
Kata kunci : keamanan nirkabel; kontrol nirkabel; peretasan mobil; *software defined radio.*

e - ISSN 2598-9596

PENDAHULUAN

Mobil modern biasanya sudah dilengkapi dengan kunci nirkabel. Walaupun memberikan berbagai kemudahan, sistem kunci nirkabel juga memberikan peluang diakses lewat udara oleh siapa saja, sehingga dapat timbul masalah keamanan.

Salah satu cara serangan terhadap sistem kunci nirkabel adalah melalui *relay attack* pada sistem PKES (*Passive Keyless Entry and Start*), yang dilakukan dengan memperpanjang jarak jangkau komunikasi antara kunci-ke-mobil dengan menggunakan relay. PKES yang berfungsi seperti RFID yang dapat membuka kunci mobil dan menyalakan mesin secara otomatis jika berdekatan dengan mobil dapat menyangka bahwa kunci berada dekat mobil dan mulai membuka pintu dan menyalakan mesin, padahal sinyal kunci diteruskan oleh *relay* yang ditambahkan dengan tersembunyi (Francillon, Danev, & Capkun, 2011). Beberapa cara yang dapat digunakan untuk menghindari *relay attack* antara lain adalah dengan melakukan *shielding* pada kunci mobil, atau melakukan modifikasi *software* atau *hardware* sehingga sistem PKES dapat dinonaktifkan sementara jika kunci dibawa menjauh.

Sistem kunci mobil nirkabel yang hanya digunakan untuk membuka pintu mobil (tidak untuk menyalakan mesin) disebut sistem *Remote Keyless Entry* (RKE). Jenis serangan yang umum disebutkan dapat dilakukan pada RKE adalah varian dari *replay attack*. Sistem RKE biasa dilindungi dengan *rolling-code*, sehingga *code* yang dipakai untuk membuka pintu mobil saat berikutnya selalu tidak sama, akibatnya serangan *replay* sederhana saja tidak cukup, dan diperlukan satu variasi lain, yaitu *jam-listen-replay* (Ibrahim *et al*., 2018). Ketika pintu mobil ingin dibuka dengan kunci secara nirkabel sinyal dari kunci di-*jam*, namun pada saat bersamaan juga direkam. Ketika pemilik mobil terpaksa membuka pintu dengan kunci secara manual, sinyal yang sudah direkam dapat dipakai untuk membuka pintu kemudian, karena sistem *code* belum *rolling*.

Bersamaan dengan perkembangan sistem otomotif, perkembangan teknologi perangkat nirkabel juga sudah menghasilkan *Software Defined Radio* (SDR) dengan harga yang cukup terjangkau (Kumbhar, 2017). SDR adalah perangkat radio yang diimplementasikan dengan *hardware* yang dapat dikontrol dan diprogram secara *software* (Kumbhar, 2017). Salah satu jenis SDR yang cukup mudah didapatkan adalah BladeRF. Satu perangkat BladeRF dapat diprogram secara multifungsi menjadi *spectrum analyzer*, *custom RF modem, GPS receiver, ATSC transmitter*, serta GSM dan LTE *picocell*.

BladeRF diproduksi oleh Nuand LLC memiliki beberapa seri yakni generasi pertama x40 dan x115, serta generasi kedua xA4 dan xA9. Seri yang digunakan pada

e - ISSN 2598-9596

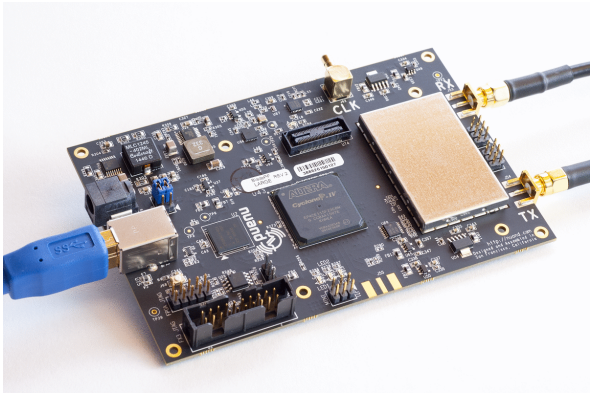
penelitian ini adalah BladeRF x40. Semua seri BladeRF berfungsi secara *full-duplex*, dan untuk seri x40 mempunyai jangkauan frekuensi 300 MHz – 3.8 GHz. Karena kemampuan *full-duplex* yang dapat mengirim dan menerima sinyal secara bersamaan, BladeRF misalnya, dapat difungsikan sebagai mini BTS GSM (Martoyo *et al*., 2018, November).

Dalam analisis awal yang dilaporkan dalam *paper* ini, kami mencoba menggunakan skenario yang lebih sederhana daripada *jam-listen-replay* untuk menyerang RKE, yaitu metode *save-and-replay*, yang terdiri dari dua tahap. Tahap pertama (save) adalah melakukan perekaman sinyal dari kunci pada saat kunci berjauhan dari mobil. Karena berjauhan, mobil tidak menangkap sinyal kunci, sehingga mekanisme *rolling code* yang dipakai kemungkinan tidak terpicu. Tahap kedua adalah percobaan memutar ulang (*replay*) dari sinyal yang sudah direkam untuk membuka pintu mobil.

Bagian berikutnya akan menjelaskan sistem BladeRF x40 yang dipakai untuk melakukan serangan *save-and-replay* pada RKE, *software* yang diperlukan untuk menjalankan BladeRF x40, serta cara kerja sistem RKE. Kemudian dilanjutkan dengan diskusi hasil percobaan, dan ditutup dengan beberapa kesimpulan.

SISTEM SDR BLADERF X40 DAN RKE

Software Defined Radio (SDR) BladeRF x40 yang dipakai di sini mempunyai jangkauan frekuensi 300 MHz – 3.8 GHz, cukup untuk menangkap sinyal dari sistem RKE yang biasanya beroperasi di sekitar 433.92 MHz atau 315 MHz (Smith, 2016; Yang & Huang, 2018). BladeRF x40 berfungsi secara full-duplex dapat digunakan untuk operasi save-and-replay yang melakukan perekaman sinyal dan transmisi sinyal secara terpisah. Spesifikasi lain dari BladeRF x40 seperti memiliki sample rate sebesar 40 Msps 12-bit quadrature sampling, tuned oscillator VCTCXO dari 1 Hz sampai 38.4 MHz, dan pada kondisi peforma RF puncak dapat menangkap 28 MHz dari bandwidth yang dioperasikan tanpa spurs yang signifikan (Martoyo *et al*., 2018, November).



Gambar 1. Modul BladeRF x40 (Martoyo *et al*., 2018)

Gambar 1 menunjukkan modul BladeRF x40 dan rangkaian di dalamnya. Modul BladeRF x40 dioperasikan dengan Laptop. *Operating system* (OS) pendukung

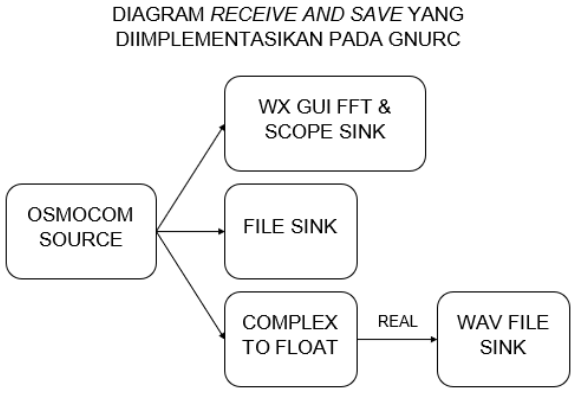
e - ISSN 2598-9596

utamanya adalah Linux dengan aplikasi GNU *Radio Companion* (GNURC). OS yang kami gunakan adalah Linux Ubuntu 18.04. GNURC merupakan *software* yang *open source* berbasis bahasa pemrograman phyton dan dapat digunakan untuk pemrograman sederhana dengan perancangan *block diagram*.

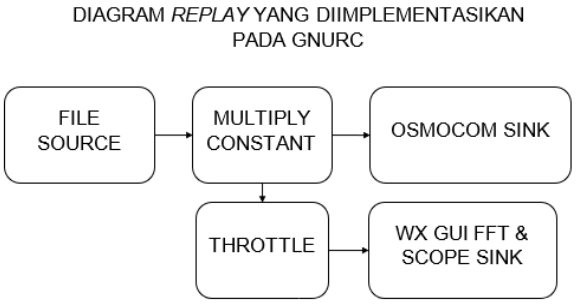
Metode Penelitian

Pemrograman perekaman sinyal dan transmisi sinyal melalui GNURC pada BladeRF x40 dapat dilihat pada Gambar 2 dan Gambar 3 yang merupakan block diagram pada GNURC dengan simplifikasi (bagian variabel tidak ditunjukkan).

Gambar 2 menjelaskan proses penyimpanan sinyal yang dilakukan. Osmocom *Source* merupakan modul *receiver* untuk BladeRF yang ada pada *library* GNURC. Ada 2 jenis modul penyimpanan sinyal yang digunakan, pertama modul *File Sink* yang menyimpan secara utuh sinyal yang diterima dari *source* untuk nanti dikirim ulang pada rangkaian Gambar 3, dan kedua modul Wav *File Sink* yang menyimpan sinyal ke format ekstensi audio (.wav) untuk analisis lebih lanjut dengan aplikasi *audio editing* seperti Audacity. Sebelum memasuki modul Wav *File Sink*, sinyal perlu diproses terlebih dahulu agar hanya bagian riil dari sinyal saja yang diterima dengan modul *Complex to Float*.



Gambar 2. *Block diagram* yang diimplementasikan pada GNURC untuk merekam sinyal



Gambar 3. *Block diagram* yang diimplementasikan pada GNURC untuk mengirim ulang sinyal

Gambar 3 menunjukkan proses pemutaran ulang sinyal. Modul *File Source* berfungsi untuk *loading file* sinyal yang telah disimpan di komputer sebelumnya oleh modul *File Sink* pada Gambar 2. Modul *Multiply Constant* digunakan untuk memperbesar amplitudo sinyal, lalu dikirim ke udara melalui Osmocom *Sink* yang merupakan modul *transmitter* untuk BladeRF. Modul *Throttle* berfungsi menyesuaikan *sample rate*. GNURC sendiri memiliki modul GUI FFT untuk *spectrum analyzer* dan GUI *scope* untuk osiloskop, *library* GUI yang digunakan adalah WX GUI.

e - ISSN 2598-9596

Sistem RKE pada setiap mobil bisa berbeda. Sinyal yang dipancarkan pada 433.92 MHz atau 315 MHz dapat menggunakan teknik modulasi yang berbeda. Menurut Yang & Huang (2018), yang umum digunakan adalah modulasi ASK/OOK dan FSK.

Ada beberapa metode *cryptography* yang digunakan pada sistem RKE. Yang sering disebutkan adalah sistem KEELOG dan Hitag2 (Garcia *et al*., 2016). Benadjila *et al*. (2017) menyajikan analisis yang lebih mendalam mengenai mekanisme Hitag2, sedangkan Verstegen, Verdult & Bokslag (2018) menunjukkan cara yang lebih cepat untuk menemukan kunci Hitag2 dengan menebak dan mengabaikan kombinasi yang tak mungkin. Jika metode enkripsi dapat dikalahkan, maka perhitungan kombinasi kunci dapat ditemukan dan kunci mobil dapat dikloning.

Dalam percobaan awal di paper ini, kami tidak akan mencoba mengalahkan metode enkripsi yang dipakai dalam sistem RKE mobil. Dengan serangan *save-and-replay* yang sederhana, kami akan menguji keamanan beberapa jenis kendaraan dengan SDR BladeRF x40 tanpa mencoba mengkloning kunci mobil. Jika terdapat mekanisme *rolling-code* yang diterapkan pada RKE, kami berharap bahwa perekaman sinyal kunci yang dilakukan jauh dari mobil dapat digunakan untuk membuka pintu, karena mekanisme *rolling* belum terpicu.

Sebanyak empat buah mobil dengan merek Mazda2 (2012), Suzuki Sidekick (2002), Toyota Fortuner (2006), dan Ford Viesta (2013) kami sertakan dalam penelitian pendahuluan ini. Secara berurutan, 4 buah mobil yang diuji beroperasi pada frekuensi 315 MHZ, 433.82 MHz, 433.915 MHz, dan 433.937 MHz.

HASIL DAN PEMBAHASAN

Tabel 1 menunjukkan data pengujian dari empat mobil yang disertakan dalam percobaan.

Tabel 1. Tingkat keberhasilan pintu mobil terbuka dengan metode *save and replay*

Merk	Frekuensi (MHz)	Pintu terbuka	*Rolling code*
Mazda2	315	Tidak	Belum diverifikasi
Suzuki Sidekick	433.82	Ya	Tidak ada
Toyota Fortuner	433.915	Ya	Tidak ada
Ford Viesta	433.937	Ya	Tidak ada

Dari Tabel 1 terlihat bahwa tiga dari empat mobil yang diuji dapat dibuka dengan serangan *save-and-replay* dan tidak menggunakan *rolling code*. Ketiadaan mekanisme *rolling code* diketahui karena pintu mobil dapat dibuka berkali-kali dengan satu kode yang sama yang telah disimpan sebelumnya. Dalam penelitiannya, Garcia *et al*. (2016) menemukan bahwa ada mobil Mercedes Benz produk sekitar tahun 2000 yang masih menggunakan *fixed code* seperti ini. Tingkat keamanan RKE yang demikian sangatlah rendah.

e - ISSN 2598-9596

Satu mobil dengan RKE pada 315 MHz tak dapat terbuka. Keberadaan mekanisme *rolling code* belum dapat diverifikasi dan dibutuhkan percobaan yang lebih banyak untuk memastikannya. Selain itu, perlu juga diuji kombinasi setting parameter lain seperti sampling rate, yang dapat saja mempengaruhi mekanisme kunci jika resolusi sampling yang digunakan kurang.

Gambar 4 menunjukkan sinyal yang ditangkap dari 4 mobil dengan 3 variasi *zoom scale* pada sumbu horizontal (waktu). Pada skala x1 terlihat bahwa sinyal kunci nirkabel terdiri atas beberapa pulsa yang berderet. Sebagian pulsa ini berfungsi sebagai sinyal sinkronisasi dan sebagian pulsa lainnya sebagai sinyal informasi. Bentuk sinyal pada frekuensi 315 MHz sangat berbeda dibandingkan sinyal pada mobil lain, yang terlihat menggunakan modulasi OOK atau FSK/PSK.

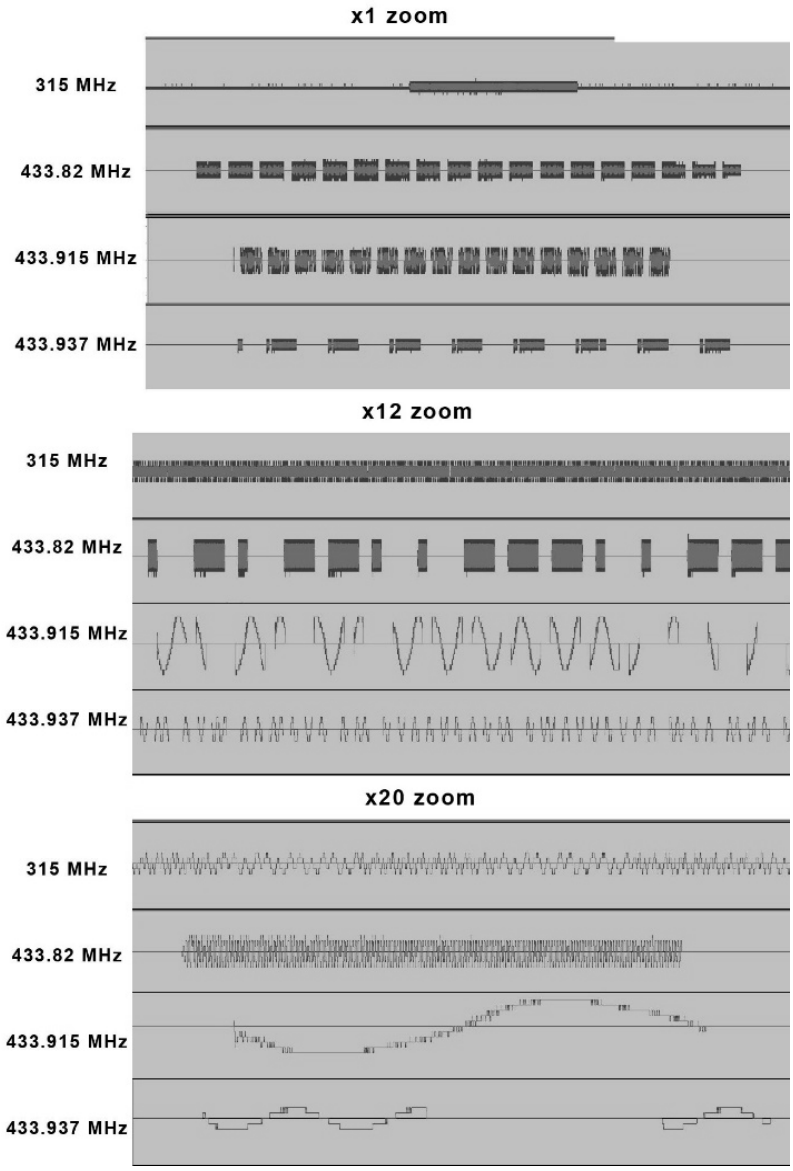
Pada percobaan permulaan ini ditemukan bahwa masih cukup banyak mobil yang hanya menerapkan *fixed code* untuk sistem RKE-nya. Serangan *save-and-replay* dengan mudah membuka pintu RKE yang kebanyakan beroperasi pada frekuensi di sekitar 433 MHz.

Untuk mobil yang menerapkan *fixed code*, tidak ada cara lain untuk menghindari serangan *save-and-replay* kecuali mematikan sistem RKE. Menggunakan kunci setang tambahan dapat juga membuat usaha kejahatan lebih sulit. Selain itu, selalu penting untuk tidak meninggalkan barang berharga di dalam mobil.

Jika *rolling code* digunakan, maka serangan *save-and-replay* masih punya kemungkinan membuka sistem RKE, jika proses rekam dilakukan jauh dari mobil. Sehingga penting untuk selalu menjaga akses ke kunci RKE sehingga sinyal kunci tidak direkam oleh pihak lain dengan diam-diam.

Jika serangan ingin dilakukan dari jarak dekat, maka dapat digunakan metode *jam-listen-replay* (Ibrahim *et al*., 2018). Dengan metode ini, ketika sinyal dari kunci terkena *jamming*, maka pintu tak membuka dan pemilik mobil terpaksa membuka pintu secara manual, sementara RKE belum *rolling*. Sinyal kunci yang direkam sambil melakukan jamming kemudian dapat dipakai untuk membuka pintu mobil.

e - ISSN 2598-9596



Gambar 4. Hasil sinyal kunci RKE dari 4 mobil yang memberi perintah buka dengan 3 variasi *zoom*, ditangkap dengan *sample rate* 2 MHz dengan program *audacity*

Walaupun BladeRF x40 memiliki kemampuan *full-duplex* yang dapat mengirim sinyal jam dan menangkap sinyal kunci dengan 1 alat saja, tetapi untuk skenario *jam-listen-replay* umumnya dibutuhkan 2 buah SDR sekaligus, satu dipasang dekat mobil untuk melakukan *jamming*, sedangkan yang lainnya dibawa ke dekat kunci untuk merekam sinyal ketika sinyal ke mobil mengalami *jamming*. Hal ini untuk menghindari *feedback* sinyal dengan frekuensi sama yang terjadi pada *single device*, akibatnya sinyal *jam* akan terlalu besar dan menutup sinyal kunci yang ingin disimpan. Keberhasilan metode ini sangat tergantung jarak kunci ke mobil. Jika kunci terlalu dekat ke mobil, maka frekuensi pancar kunci juga akan ikut terkena *jamming*, sehingga SDR perekam harus berada lebih dekat kepada kunci. Garcia *et al*. (2016) mengusulkan agar memperhatikan kelakuan

e - ISSN 2598-9596

aneh dari kunci mobil jika tiba-tiba tidak bekerja sebagai indikasi ada serangan secara nirkabel.

Sinyal yang berhasil ditangkap BladeRF x40 dan diamati di komputer berpotensi untuk diproses lebih jauh dengan metode decoding tertentu. Jika metode enkripsi RKE dapat dikalahkan, baik dengan kalkulasi *brute-force* (menghitung semua kemungkinan), atau perhitungan yang lebih terarah yang lebih cepat (Verstegen, Verdult & Bokslag, 2018), maka kunci RKE akan dapat dikloning.

Pemanfaatan SDR ditambah dengan klasifikator *Machine Learning* seperti Support Vector Machine (SVM) untuk membedakan antara sinyal kunci asli dan sinyal tiruan diusulkan oleh Quintero *et al.* (2023). Namun penelitian mereka sendiri sebelumnya (Quintero *et al.*, 2021) menunjukkan bahwa banyak mobil di Bogota yang masih rentan terhadap serangan *brute force* atau *replay attack*, terutama jika ada skenario yang membuat pemilik kendaraan meninggalkan kunci mobilnya (misalnya parkir *valet*). Solusi terhadap kelemahan *security* demikian tampaknya tidak dapat diatasi dengan aplikasi *Machine Learning* untuk membandingkan kemiripan sinyal radio, yang dapat berfluktuasi karena interferensi atau jarak. Peningkatan keamanan baru dapat dicapai dengan modifikasi algoritma kunci yang menggunakan angka random yang hanya dihasilkan hanya sekali (*nonce*) untuk menghasilkan sinyal kunci.

KESIMPULAN

Sebanyak tiga dari empat mobil yang diuji berhasil dibuka pintunya dengan serangan *save-and-replay*. Mobil-mobil yang pintunya berhasil terbuka ini tidak menggunakan *rolling code*, dan mengindikasikan tingkat keamanan yang rendah. Bagi mobil lama dengan sistem RKE *fixed code* disarankan untuk menggunakan kunci setang dan tidak meninggalkan barang berharga dalam mobil.

Serangan *save-and replay* bagi sistem RKE yang menggunakan *rolling code* dapat dihindari dengan selalu menjaga akses ke kunci RKE agar tidak direkam diam-diam oleh pihak lain. Serangan *jam-listen-replay* membutuhkan dua buah perangkat SDR, dan dapat menghasilkan fenomena bahwa kunci tiba-tiba tidak berfungsi, yang harus dicermati oleh pemilik mobil.

Penelitian awal ini membuka kemungkinan untuk percobaan decoding sinyal RKE lebih jauh dengan BladeRF x40. Mobil-mobil keluaran terbaru mungkin sudah menggunakan sistem *challenge-response* (*nonce*) yang lebih aman.

DAFTAR PUSTAKA

Benadjila, R., Renard, M., Lopes-Esteves, J., & Kasmi, C. (2017). One car, two frames: attacks on hitag-2 remote keyless entry systems revisited. In *11th {USENIX} Workshop on Offensive Technologies ({WOOT} 17)*.

Francillon, A., Danev, B., & Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Eidgenössische Technische Hochschule Zürich, Department of Computer Science.

Garcia, F. D., Oswald, D., Kasper, T., & Pavlidès, P. (2016). Lock it and still lose it—on the (in) security of automotive remote keyless entry systems. In *25th {USENIX} Security Symposium ({USENIX} Security 16)*.

Ibrahim, O. A., Hussain, A. M., Oligeri, G., & Di Pietro, R. (2018). Key is in the Air: Hacking Remote Keyless Entry Systems. In *Security and Safety Interplay of Intelligent Software Systems* (pp. 125-132). Springer, Cham. https://doi.org/10.1007/978-3-030-16874-2_9

Kumbhar, A. (2017). Overview of ISM bands and Software-defined Radio Experimentation. *Wireless Personal Communications*, 97(3), 3743-3756. https://doi.org/10.1007/s11277-017-4696-z

Martoyo, I., Coandi, A., Pratignyo, D., Kanalebe, H. Y., Uranus, H. P., & Pardede, M. (2018, November). Software Defined Radio Applications for Mini GSM BTS and Spectrum Analyzer with BladeRF. In *2018 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)* (pp. 108-111). IEEE. https://doi.org/10.1109/ICRAMET.2018.8683935

Quintero, J. C. M., Cuesta, E. P. E., & Sarmiento, A. T. C. (2021). Vulnerability analysis in RF locking systems of vehicles in Bogotá, Colombia. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *9*(1), 114-129. https://doi.org/10.11591/ijeei.v9i1.2450

Quintero, J. C. M., Cuesta, E. P. E., & Lopez, L. J. R. (2023). A new method for the detection and identification of the replay attack on cars using SDR technology and classification algorithms. *Results in Engineering*, *19*, 101243. https://doi.org/10.1016/j.rineng.2023.101243

Smith, C. (2016). The Car Hacker's Handbook: A Guide for Penetration Tester. No Strach Press, San Francisco. https://doi.org/10.4271/1593277032

Verstegen, A., Verdult, R., & Bokslag, W. (2018). Hitag 2 Hell–Brutally Optimizing Guess-and-Determine Attacks. In *12th {USENIX} Workshop on Offensive Technologies ({WOOT} 18)*.

Yang, Q., & Huang, L. (2018). 433/315 MHz Communication. In *Inside Radio: An Attack and Defense Guide* (pp. 123-171). Springer, Singapore. https://doi.org/10.1007/978-981-10-8447-8_4