Analisis *SIM Card Cloning* Terhadap Algoritma *Random Number Generator*

Nuril Anwar[1], Imam Riadi[2], Ahmad Luthfi[3]
[1,3]Magister Teknik Informatika, Universitas Islam Indonesia
Jl. Kaliurang KM 14.5, Yogyakarta 55584
[2]Teknologi Industri Universitas Ahmad Dahlan
Jl. Jalan Prof. Dr. Soepomo, S.H. Janturan Yogyakarta 55164
E-mail: anwar_nuril@yahoo.co.id, imam.riadi@is.uad.ac.id, ahmad.luthfi@uii.ac.id

Masuk: 9 November 2015; Direvisi: 30 November 2015; Diterima: 2 Desember 2015

Abstract. *Crime in telecommunication sector has increased prevalently, especially with the use of mobile phone which is detrimental both for customers and the providers. In the GSM security system, several weaknesses are found concerning data security outside the network. SIM card clone is part of the security problem in which the data can be transferred to SIM card cloning media. SIM card cloning research can be presented in the form of SRES analysis algorithms A3 and A8 RAND to get Ki Auc for further analysis on SIM card cloning. To test the performance of SIM card cloning, testing parameters such as due under test (DUT) and trial and error are employed. The conclusion of this study is that the SIM card cloning method can occur when Auc Ki is obtained by downloading a crack a8 RAND Random Number Generator analysis algorithms A3 sign SIM card to match the SRES response to the Auc Ki along with supporting data contained in SIM card clones.*
Keywords: *SIM card cloning, Random Number Generator (RAND), Sign Response (SRES).*

Abstrak. *Kejahatan di sektor telekomunikasi kian marak akhir-akhir ini khususnya mobile phone yang merugikan baik bagi customer maupun provider seluler. Pada sistem keamanan GSM, ditemukan beberapa kelemahan di sisi pengamanan data di luar jaringan. SIM card clone adalah bagian dari masalah keamanan pada device SIM card dengan data SIM card yang dapat dipindahkan ke media SIM card cloning. Penelitian SIM Card Cloning ini disajikan berupa analisis algoritma A3 SRES, dan A8 RAND untuk mendapatkan Ki AUc untuk selanjutnya dilakukan analisis SIM Card Cloning. Untuk menguji performa SIM card cloning digunakan parameter pengujian seperti Due Under Test (DUT) dan Trial and Error. Kesimpulan dari penelitian ini didapatkan bahwa metode SIM Card Cloning dapat terjadi bilamana AUc Ki diperoleh dengan melakukan crack A8 Random Number Generator RAND sedang analisis algoritma SIM card dengan mencocokkan A3 Sign Respons SRES terhadap AUc Ki beserta data pendukung yang terdapat pada SIM card hasil kloning.*
Kata kunci: *SIM card cloning, Random Number Generator (RAND), Sign Respons (SRES).*

1. Pendahuluan

SIM card menyimpan informasi yang berkaitan dengan jaringan yang digunakan untuk *authentication* dan identifikasi pengguna. Data yang paling penting adalah nomor identitas kartu (ICCID, *Integrated Circuit Card* ID), nomor pengguna internasional (IMSI, *International Mobile Subscriber Identity*), kunci otentikasi (Ki, *Authentication Key*), kode area (LAI, *Local Area Identity*), dan nomor panggilan darurat operator. *SIM card* juga menyimpan nomor layanan pusat untuk SMS (SMSC, *Short Message Service Center*), nama penyedia layanan (SPN, *Service Provider Name*). Ketika *SIM card* tersebut berorientasi sebagai *smartcard*, maka

membuka kemungkinan keamanan yang beresonansi jauh melampaui dunia yang bersifat *mobile* (Jansen & Ayers, 2006).

Ki (*Authentication Key*), GSM *SIM card* menggunakan kriptografi untuk mengurangi penipuan terhadap kerahasiaan pengguna. Sebelum *SIM card* dilepaskan ke pelanggan, *SIM card* diprogram terlebih dahulu untuk keperluan otentikasi. Sedang untuk membacanya diperlukan algoritma komputer khusus yang berjalan secara internal pada *SIM card*. Salinan Ki ini juga disimpan oleh operator jaringan dalam *Authentication Center* (AuC). *SIM card* diproduksi dengan basis algoritma COMP128v1, *SIM card* yang dipakai sekarang sebagian masih dalam pengembangan dari algoritma COMP128v1. Di dalam algoritma COMP128v1 terdapat sistem pengkodean *SIM card* GSM yang terdiri dari algoritma A3 dan A8. Algoritma A3 adalah algoritma otentikasi dalam model keamanan GSM. Fungsi A3 adalah untuk membangkitkan *reponse* yang lebih dikenal dengan SRES sebagai jawaban dari *random challenge* yang dikenal dengan *Random Number Generator* (RAND) dengan kata lain SRES dan RAND adalah algoritma yang terdapat pada jaringan atau *provide on network.* Sedangkan algoritma A8 adalah algoritma yang berfungsi membangkitkan kunci sesi, Kc atau Ki pada *SIM card*, dengan melihat *random challenge*, RAND yang diterima dari MSC dan kunci rahasia Ki, yang terdapat pada kartu SIM (Jansen & Ayers, 2006). COM128v1 mempunyai kelebihan utama yaitu terdapat dua sistem pengkodean atau algoritma A3 dan A8, A3 merujuk pada keamanan *network* sedang A8 mengacu pada keamanan *SIM card* namun di sisi lain terdapat kekurangan yang ditimbulkan oleh algoritma A8 tersebut yang mencakup keamanan enkripsi berupa *Autentication Key* (Ki) yang terdapat pada *SIM card*.

Problem yang muncul dari latar belakang di atas terkait keberadaan algoritma A8 yang melekat pada setiap *SIM card* yang digunakan oleh pengguna jasa telekomunikasi sehingga memungkinkan penggandaan atau *SIM Card Cloning* yang merugikan baik di sisi privasi maupun keamanan pengguna telepon selular. Tujuan dari penelitian *SIM card* kloning ini yaitu memberikan peringatan terhadap keamanan pengguna *SIM card* serta memberikan gambaran kejahatan pengkloningan data *SIM card* beserta penyalahgunaannya.

Authentication SIM card mencakup *Subscriber Based on* IMSI (*Stored on* SIM) dan *Random Number Generator*/RAND (*Provided by Network*), maka akan diteliti lebih lanjut tentang *Authentication SIM card Cloning* dengan mencocokkan respon jaringan pelanggan *login* ke jaringan layanan *mobile*. *Random Number Generator* (RAND) berisi algoritma A3 *(Provide by Network)* sehingga dalam proses *SIM card cloning* RAND berperan serta dalam proses pencocokan algoritma A8 yang terdapat pada *SIM card* terhadap algoritma A3 yang terdapat pada jaringan terkait otentikasi data pengguna.

2. Kajian Pustaka

Studi dan perbandingan keamanan GSM dan sistem keamanan GSM berdasar pada pertukaran data antara HLR (*Home Location Register*) dengan kartu SIM pada MS (*Mobile Station*) RAND, MSC melalui BTS kepada MS. Ki & Kc yang digunakan untuk mengenkripsi pesan antara BTS dengan MS. RAND, SRES otentikasi pada GSM yaitu menggunakan algoritma A3 dengan kunci Ki dengan metode *Challenge and Response*. Otentikasi menggunakan prosedur *Unique Challenge Procedure* (Jansen & Ayers, 2006).

Willassen (2003) secara singkat menjelaskan dasar-dasar dari sistem GSM. *Item* bukti yang bisa diperoleh dari *Mobile Equipment*, SIM dan jaringan inti dieksplorasi untuk mengembangkan prosedur tertentu yang lebih baik. Kesimpulannya bahwa peniruan *SIM card* GSM memang mungkin bagi siapa saja yang bisa. Metode analisis *SIM card cloning* masih kontak fisik dengan ponsel untuk mengakses informasi yang tersimpan.

Pada simulasi oleh Hudoyo (2008) diawali dengan melakukan pembangkitan *ciphering key* sebagai syarat untuk melakukan enkripsi data informasi. Untuk pembangkitan *ciphering key* pada komunikasi GSM, digunakanlah algoritma A8 yang akan melakukan seluruh komputasi data Ki dan RAND yang dibutuhkan. Setelah itu, *ciphering key* yang telah diperoleh akan diproses oleh algoritma A5 dengan tujuan mengacak informasi.

Pada penelitian oleh Hayat (2014) dilakukan *SIM card cloning* serta menganalisis pengkombinasian metode kriptografi ECC *(Elliptic Curve Cryptography)* dengan algoritma A3, A5, dan A8 untuk mendapatkan kualitas keamanan yang lebih baik. Penelitian ini didapatkan bahwa metode ECC hanya dapat dikombinasikan dengan algoritma A3 dan A8 serta metode ECC tersebut ternyata tidak efektif bila dikombinasikan dengan algoritma A5 disebabkan adanya perbedaan sistem dan prosedur antara keduanya.

Pada sistem keamanan jaringan GSM, ditemukan beberapa kelemahan yang dapat merugikan kepentingan-kepentingan pelanggan dan jaringan. Kelemahan tersebut terutama terjadi pada pengamanan data di luar *link* radio. Penelitian ini mensimulasikan pengkombinasian metode kriptografi ECC *(Elliptic Curve Cryptography)* dengan algoritma A3, A8, dan A5 untuk mendapatkan kualitas keamanan yang lebih baik. Pengkombinasian metode ECC diterapkan dalam layananan sistem keamanan jaringan GSM, terutama pada proses otentikasi dan pengamanan identitas pelanggan. Simulasi untuk menguji performansi metode ECC ini meliputi proses registrasi, *basic call setup*, dan *roaming*. Parameter yang digunakan sebagai perbandingan dalam analisis adalah skema sistem keamanan, waktu proses, *data rate* dan pengujian *avalanche effect*. Dari penelitian ini didapatkan bahwa metode ECC hanya bisa dikombinasikan dengan algoritma A3 dan A8. Pengkombinasian ECC tersebut efektif mengurangi celah ditembusnya kerahasiaan identitas pelanggan dan proses otentikasi tanpa penambahan waktu proses secara signifikan. Begitu pula meski terdapat penambahan jumlah *bit* data yang ditransmisikan, penambahan *data rate* yang terjadi masih dapat ditolerir. Dari penelitian ini juga didapatkan hasil bahwa metode ECC tersebut ternyata tidak efektif bila dikombinasikan dengan algoritma A5. Hal ini disebabkan karena adanya perbedaan sistem dan prosedur antara keduanya (Djauhari, 2008).

GSM *cloning* telah terbukti berhasil di *Code Division Multiple Access* (CDMA) tetapi jarang pada *Global System* untuk komunikasi *Mobile* (GSM), salah satu yang lebih banyak digunakan sistem komunikasi telepon seluler. Namun, kloning ponsel GSM dicapai dengan kloning kartu SIM yang terkandung dalam, belum tentu setiap data internal telepon. Ponsel GSM tidak memiliki ESN atau MIN, hanya nomor IMEI. Kartu GSM SIM akan disalin dengan menghapus *SIM card* dan menempatkan perangkat antara *handset* dan kartu SIM dan memungkinkan untuk beroperasi selama beberapa hari dan penggalian Ki, atau kode rahasia. Kloning telah berhasil menunjukkan di bawah GSM, namun proses ini tidak mudah dan saat ini masih dalam penelitian para peneliti (Anandkumar & Jayakumar, 2012).

Penelitian terkait *SIM card* mempelajari kemungkinan menggunakan kloning *Subscriber Identity Module* (SIM) di *Universal Mobile Telecommunications System*. Hal ini juga mengeksplorasi bagaimana sistem *mobile* dapat menemukan kartu SIM kloning sesegera mungkin dan bagaimana mengurangi kemungkinan menggunakan kloning kartu SIM di jaringan *mobile*. *Mobile station* yang ilegal melekat ke jaringan seluler dapat dideteksi oleh lokasi di *Area Update*, *update* lokasi daerah periodik, dan oleh panggilan keluar yang dikeluarkan dari ponsel asli. Model analitik dikembangkan untuk menyelidiki efek dari *update* daerah lokasi dan panggilan keluar yang dikeluarkan oleh ponsel asli pada penggunaan ponsel ilegal. Manajemen mobilitas, seperti pendaftaran, pembatalan, dan prosedur keluar dan masuk bagi pengguna legal dan ilegal akan diselidiki dan dianalisis. Model analitis untuk mengetahui pengaruh tingkat kedatangan panggilan keluar, dan daerah lokasi waktu tinggal pada pengguna ilegal terdeteksi telah disajikan. Penelitian ini berusaha untuk meningkatkan keamanan komunikasi dengan menghindari penipuan dari ponsel kloning dengan mengusulkan solusi untuk mempercepat deteksi kloning kartu SIM (Al-Fayoumi & Shilbayeh, 2014).

Saat ini, IP *Multimedia Subsystem* (IMS) adalah bidang penelitian yang menjanjikan. Banyak karya yang sedang berlangsung terkait dengan keamanan dan kinerja kerja yang disajikan untuk komunitas riset. Meskipun, aspek keamanan dan privasi data yang sangat penting dalam tujuan global IMS, mereka mengamati sedikit perhatian sejauh ini. Akses aman ke layanan multimedia didasarkan pada SIP dan HTTP mencerna di atas arsitektur IMS. Standar menyebarkan AKA-MD5 untuk otentikasi terminal. Ketiga *Generation Partnership Project* (3GPP) tersedia *Generic Bootstrap Arsitektur* (GBA) untuk mengotentikasi pelanggan sebelum

mengakses layanan multimedia melalui HTTP. Dalam penelitian ini, mengusulkan skema IMS Layanan Otentikasi baru menggunakan *Identity Based Cryptography* (IBC). Skema baru ini akan menyebabkan kinerja yang lebih baik ketika ada permintaan otentikasi simultan menggunakan *Verification Batch* berbasis *Identity*. Selanjutnya menganalisis keamanan protokol baru dan disajikan evaluasi kinerja operasi kriptografinya (Abid, dkk., 2009).

Ponsel komputasi dan *Mobile Commerce* yang paling populer sekarang karena layanan yang ditawarkan selama mobilitas. Ponsel komputasi telah menjadi kenyataan hari ini daripada pasar nirkabel. *Mobile* meningkat dengan pesat. Kualitas dan kecepatan yang tersedia di lingkungan *mobile* harus sesuai dengan jaringan tetap jika konvergensi jaringan komunikasi nirkabel dan *fixed mobile* terjadi dalam arti yang sesungguhnya. Tantangan bagi jaringan selular terletak dalam memberikan jejak yang sangat besar jasa layananan *mobile* dengan kecepatan tinggi dan keamanan. Transaksi *online* menggunakan perangkat *mobile* harus memastikan *security* tinggi untuk kredensial pengguna dan mungkin untuk penyalahgunaan. *M-Commerce* adalah perdagangan elektronik dilakukan dengan menggunakan perangkat *mobile*. Sejak kredensial pengguna harus dirahasiakan, tingkat keamanan yang tinggi harus dipastikan (Prakash & Balachandra, 2015).

Penelitian ini difokuskan pada *analisis SIM card cloning* terhadap algoritma otentikasi *random number generator* (RAND). Pengaruh *SIM card cloning* dan *SIM card* asli dengan mencocokkan algoritma A3 dan A8 untuk mendapatkan *Autentication Key* (Ki) pada *SIM card*. Hasil yang diharapkan berupa analisis terkait *SIM card cloning* serta analisis algoritma *Random Number Generator* (RAND).

3. Metodologi Penelitian

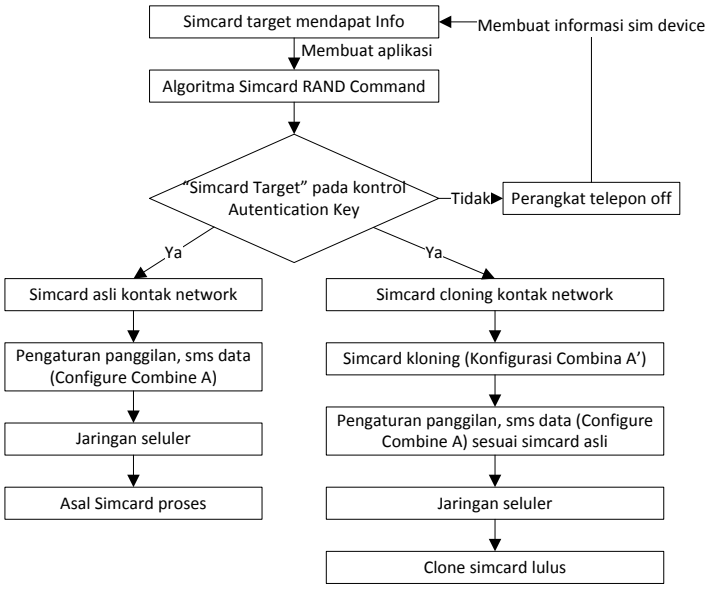
Subjek penelitian ini ditekankan pada analisis *SIM card cloning* untuk selanjutnya dikembangkan ke tahap eksplorasi *SIM card cloning*. Proses analisis dilakukan di Laboratorium IT Centrum Universitas Islam Indonesia yang merupakan bagian dari Pusat Studi Magister Teknik Informatika. Metode penelitian terkait *SIM card cloning* dengan menganalisis berdasarkan teori agar fokus penelitian sesuai dengan fakta di lapangan terkait penanganan barang bukti *SIM card cloning* untuk selanjutnya dilakukan analisis untuk membuktikan bahwa hipotesis yang diangkat sesuai dengan kriteria. Pada tahap akhir akan dikemukakan pengaruh *SIM card cloning* berdasarkan *log SIM card* hasil *cloning* dengan *log SIM card* aslinya. Analisis penelitian meliputi *attack* dan skenario *testing*, pengujian *SIM card cloning*, dan RAND *Autentication*.

3.1. *Attack* dan Skenario *Testing*

Skenario *testing* ditekankan pada proses *cloning* dari *SIM card cloning* itu sendiri meliputi keberhasilan proses *generate authentication key* (Ki) RAND A8 terhadap *SIM card* asli dan selanjutnya diujicobakan *respon*s A3 SRES terhadap jaringan ketika *SIM card cloning* bersinggungan langsung dengan *SIM card* asli, sedangkan skenario serangan *attack* yang ditimbulkan pasca *SIM card* dikloning berupa serangan akses komunikasi atau duplikasi seperti pesan singkat (*sms*), panggilan (*call*) dan akses data dari *SIM card cloning* seolah-olah terdapat nomor yang sama dengan *SIM card* asli selanjutnya diketahui lebih lanjut efek yang ditimbulkan (Willassen, 2003). *Flowchart* attack *SIM card cloning* tampak pada Gambar 1.

3.2. Pengujian *SIM card cloning*

Autentication SIM card cloning dalam skenario pengujian mengacu pada *autentication key* (disebut sebagai Ki *SIM card* GSM), yang terdiri dari IMSI dan nomor ESN, dengan *test trial-and-error*, dengan memberi inputan yang berbeda untuk *SIM card* dan mengamati respon dari kedua *SIM card* keduanya meliputi: (1) Respon terhadap jaringan seluler *pasca SIM card* dikloning. (2) Mengakumulasi otentikasi respon antara RAND dan SRES. (3) Kemungkinan memodifikasi algoritma RAND atau hanya mendistribusikan otentikasi Ki ke media *cloning.* (4) Pengaruh lalu lintas dari ponsel pengguna ke *base station SIM card* yang telah dikloning terhadap *SIM card* asli.



Gambar 1. ***Flowchart Attack SIM Card Cloning***

3.3. *RAND Autentication*

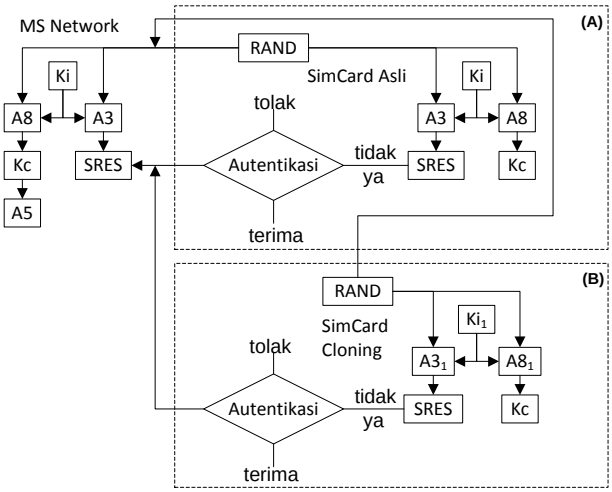
Aspek penting lain dari otentikasi GSM adalah kekuatan algoritma *SIM card* atau sering disebut A3. Pada prinsipnya A3 dimiliki operator selular tertentu, akan tetapi penggunaan algoritma antar operator cenderung sama. Dari pernyataan tersebut selanjutnya kedua algoritma dikomparasi RAND & SRES *Autentication* berdasarkan keamanan GSM. Jika Ki dapat diekstraksi dari *SIM card*, pengguna akan mampu membuat duplikat *SIM card*. Algoritma A3 dan A8 menentukan *input* (RAND dan Ki) dan *output* (SRES dan Kc) dari masing-masing algoritma (Prayudi & Rifandi, 2013).

4. Hasil dan Pembahasan

4.1. Analisis *SIM Card Cloning*

Komparasi disini lebih ditekankan peran antar algoritma yaitu algoritma RAND dan SRES, kedua algoritma tersebut saling keterkaitan bilamana A8 RAND pada SIM card bersinggungan dengan A3 AUc *Network* sehingga dapat diperoleh alur proses seperti pada Gambar 2. Dari Gambar 2 dapat diketahui alur proses otentikasi antara *SIM card* asli dan *SIM card cloning*. Pembentukan *SIM card cloning* dengan menempatkan hasil *genarated* dari algoritma A8 dari Ki asli untuk selanjutnya disalin ke perangkat *SIM card cloning writer* dengan spesifikasi tertentu sehingga *SIM card cloning* dapat berperan sama saat melakukan kontak komunikasi dengan jaringan. Dari Gambar 2 dapat dinyatakan bahwa Ki1, A31 dan A81 serupa dengan *variable SIM card* asli, selanjutnya proses kloning diteruskan ke *mobile station network* atau SRES, bilamana *SIM card* ditolak maka proses otentikasi berlaku skema berulang sebelum diteruskan ke *MS network* dan berlaku sebaliknya. *Autentication* bertindak sebagai otentikasi data pelanggan selular, bilamana data yang terdapat pada *device SIM card* (Ki dan *Random Number Generator*) cocok dengan *database central* maka akan diberikan akses komunikasi.

Pada Gambar 2 bagian (A) dan (B) dapat diuraikan alur *SIM card* asli dan *SIM card cloning*. Gambar tersebut merupakan bagian dari Gambar 2 yang dibagi menjadi sub alur masing-masing dengan arah otentikasi dan RAND menuju *MS Network* sedangkan proses otentikasi dapat diterima atau ditolak berdasarkan *authentication key* Ki bilamana ditolak akan berlaku skema pengecekan berulang terhadap Ki dan bilamana diterima maka untuk selanjutnya akan dilanjutkan ke MS *Network*. Berdasarkan hasil pengujian *SIM card cloning* terhadap *SIM card* asli maka dapat diperoleh tabel *test case SIM card cloning* terhadap *SIM card* asli seperti tampak pada Tabel 1.



Gambar 2. RAND dan SRES *Cloning*

Tabel 1. Hasil *Test Case*

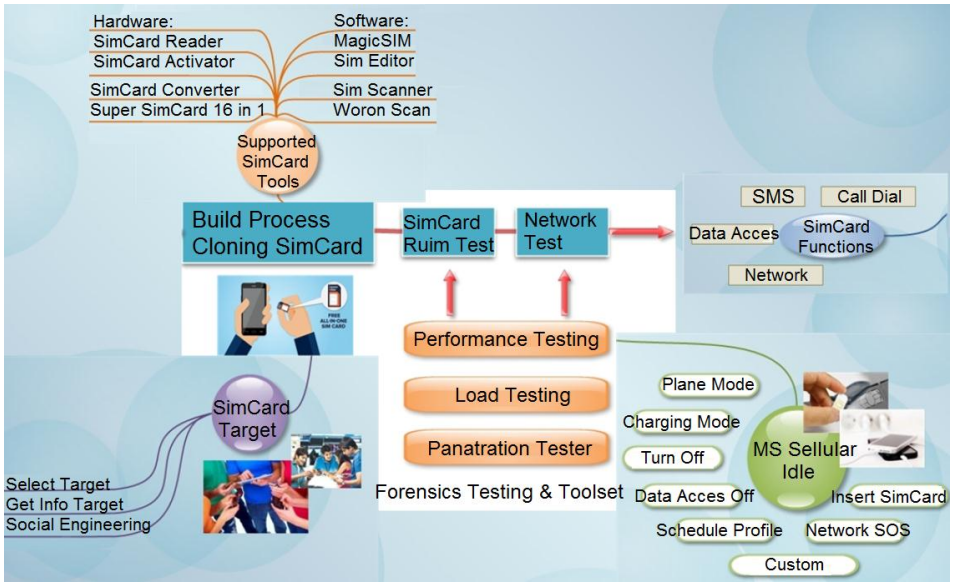
Skenario Pengujian	*Test Case*	Hasil yang diharapkan	Hasil Pengujian	Kesimpulan
SIM card Acquisition and Analysis	*Scan device SIM card cloning* (Ki *generate*)	*Exploration & Repport SIM card Cloning*	Magic SIM 16 in 1 SMSP: 62811000000 ICCID: 8962101xxxxxxx IMSI: 0859010 xxxxxxxx Ki: 9A1154814652D32339360947A69986C4	Diketemukan identitas sim beserta Ki identik
	HLR *Lookup*		$hlrlookup: 08529260xxxx Operator: Telekomunikasi Selular (Telkomsel)-KartuHalo/Simpati/KartuAs HLR: Yogyakarta/Indonesia	Diketemukan *home local register* sesuai dengan SIM card asli
	Acquisition SIM card		MD5 Checksum: BA0A76666C8F1375-E8D87BBAC21EA9F9 SHA1 Checksum: 87D74A0F18C2E943 0AC9473D62A4106547878B1E	Proses akuisisi *file extraksi evidence*
	File Structure Evidence		Slot: 1.9A1154814652D32339360947A6999986C4	Hasil temuan aKey pada *slot sim clone*

4.2. Pembahasan

Berdasarkan hasil penelitian meliputi analisis *SIM card cloning* dan algoritma *SIM card cloning* maka dapat diperoleh intisari dari penelitian terkait *SIM card*. Bahwa motif yang dilakukan pelaku dalam melakukan tindak kejahatan dengan target *SIM card cloning* yaitu penduplikasian data pada *devices SIM card* berupa hasil *generate authentication key* (Ki), proses *generate* serupa dengan melakukan *crack* pada Auc atau *Autentication Key* (Ki) yang terdapat pada *SIM card* asli untuk selanjutnya disalin ke media *SIM card cloner* yang dapat diperoleh atau diperjualbelikan di pasaran secara bebas dan bilamana pelaku dapat melakukan *SIM card cloning* maka dapat dipastikan menambah daftar panjang motif kejahatan khususnya *mobile phone*, sedangkan dari hasil analisis *SIM card cloning* dengan mengekplorasi barang bukti *SIM card cloning* dapat diketemukan struktur *file* dari *SIM card cloning* yang berisikan sebagian data yang identik seperti *authentication key* (Ki) yang diperoleh saat melakukan *generate random number* RAND pada *device SIM card* beserta data-data korban kloning. Proses *crack* Ki hanya dapat dilakukan bilamana pelaku kloning mengetahui *SIM card* fisik beserta keberadaannya dan dibutuhkan kontak fisik terhadap *SIM card* asli, sedangkan RAND merupakan serangkaian proses otentikasi *SIM card cloning* terhadap *SIM card* asli dan peran RAND dalam hal ini akan dikaji lebih lanjut dalam sub penelitian selanjutnya yang lebih difokuskan ke *forensic SIM card cloning* dengan RAND sebagai otentikasi serta investigasi keberadaan *SIM card cloning*.

4.2.1. Fokus Penelitian

Gambar 3 merupakan gabungan antara skema kasus *SIM card cloning* dengan alur proses pengujian. *SIM card cloning* beserta analisisnya merupakan fokus utama dari sub penelitian ini yang merujuk pada skema *SIM card cloning* yang selanjutnya dikomparasikan terhadap skenario *testing SIM card cloning* sesuai dengan metode penelitian. Penelitian terbagi dalam dua sub penelitian diantaranya analisis terkait *SIM card cloning* dan *forensic SIM card cloning* beserta investigasinya. Namun dalam penelitian awal hanya membahas *cloning* secara umum yang dilakukan oleh sebagian besar orang sehingga untuk diperoleh kontribusi yang lebih akan dapat terlihat bilamana penelitian masing-masing sub telah digabungkan.



Gambar 3. Fokus Penelitian *SIM Card Cloning*

4.2.2. *Resume* Penelitian

Berdasarkan hasil dan pembahasan penelitian terkait keberadaan *SIM card* dan telah dilakukan analisis beserta prinsip kerja *cloning* pada *SIM card*, maka dapat diperoleh hasil dan verifikasi seperti pada Tabel 2.

Tabel 2. *Resume* Penelitian *SIM Card Cloning*

Skenario Pengujian	Test Case	Hasil yang diharapkan	Hasil Pengujian	Kesimpulan
SIM card Device Under Test (DUT)	*SIM card Origin* Telkomsel/AS	Identik dengan *SIM card* Asli (RAND, Ki)	Nomor Sim: 085292608008 ICCID: 89621019924260800080F IMSI: 085901012924060880 Ki(A) Origin: 9A1154814652D32339360947A69986C4	Valid
	SIM card Clone MagicSim (16in1)		Ki(A') MagisSim 16 in 1: 9A1154814652D32339360947A69986C4	
SIM card 'Trial and Error'	Satu Lokasi: *Call Voice*, SMS, Data	*Sign Respons* (SRES)	Satu Lokasi BTS: Call Voice, [SRES ON] SMS, [SRES ON] Data [SRES ON]	Valid
	Beda Lokasi: *Call Voice*, SMS, Data		Beda Lokasi BTS: Call Voice, [SRES ON] SMS, [SRES ON] Data [SRES ON]	Valid
SIM card Acquisition and Analysis	*Scan device SIM card cloning* (Ki *generate*)	*Exploration & Repport SIM card Cloning*	Magic SIM 16 in 1 SMSP: 62811000000 ICCID: 8962101xxxxxxxxx IMSI: 0859010 xxxxxxxxxx Ki: 9A1154814652D32339360947A69986C4	Valid

HLR *Lookup*	$hlrlookup: 08529260xxxx Operator: Telekomunikasi Selular (Telkomsel)-KartuHalo/Simpati/KartuAs HLR: Yogyakarta/Indonesia	Valid
Acquisition Evidence	MD5 Checksum: BA0A76666C8F1375E8D87BBAC21EA9F9	Valid
File Structure Evidence	SHA1 Checksum: 87D74A0F18C2E9430AC9473D62A4106547878B1E Slot: 1.9A1154814652D32339360947A69986C4	Valid

5. Kesimpulan

Proses dalam pencocokan algoritma atau *Random Number Generator*/RAND terhadap *SIM card cloning* pada penelitian ini ialah dengan melakukan *generate* algoritma RAND A8 atau dapat disebut Ki untuk selanjutnya disalin ke media *SIM card cloning*. Ketika algoritma yang terdapat pada *SIM card* di*generate* maka berkemungkinan besar *SIM card* target dapat dikatakan telah dikloning. Analisis *SIM card cloning* dirasa mampu memberi peringatan terlebih bagi penyedia layanan komunikasi, selain itu juga dapat memberikan pengetahuan kepada pengguna dalam memelihara keamanan perangkat *mobile.* Dari proses ekplorasi *SIM card cloning* dapat disimpulkan bahwa pencocokan atau otentikasi yang berdasarkan algoritma A8 *Random Number Generator* (RAND) sangat membantu dalam pencocokan terkait keberadaan *SIM card cloning* dikarenakan algoritma RAND berperan dalam melakukan *generate authentication* (Ki) sebagai sarana otentikasi terhadap *SIM card* asli. Proses pencocokan dengan algoritma *Random Number Generator* (RAND) pada *SIM card cloning* dapat digunakan sebagai langkah penanggulangan terkait keberadaan *SIM card cloning* untuk selanjutnya dapat diekplorasi keberadaan data-data yang terdapat pada *SIM card* sesuai kebutuhan.

Referensi

Abid, M., Song, S., Moustafa, H., & Afifi, H. 2009. Integrating Identity-Based Cryptography in Ims Service Authentication. *International Journal of Network Security & Its Applications (IJNSA)*, 1(3): 1-13.

Al-Fayoumi, M. A., & Shilbayeh, N. F. 2014. Cloning SIM Cards Usability Reduction in Mobile Networks. *Journal of Network and Systems Management*, *22*(2): 259-279.

Anandkumar, K. M., & Jayakumar, C. 2012. Pro-Active Prevention of Clone Node Attacks in Wireless Sensor Networks. *Journal of Computer Science*, 8(10): 1691-1699.

Djauhari, F. 2008. Simulasi Penerapan Metode Elliptic Curve Cryptography (ECC) Untuk Mengatasi Kelemahan Sistem Keamanan Jaringan GSM. *Jurnal Terra Hertz*, 2(2), ICT Research Center UNAS.

Hayat, C. 2014. *Analisis SIM Card Clone Pada IM3 Smart Serta Penggunaan Ellptic Curve Cryptosystem Untuk Meningkatkan Keamanan Jaringan GSM*. Depok, Indonesia: Jurusan Sistem Informasi, Universitas Gunadarma.

Hudoyo, P.J. 2008. Rancang Bangun Simulasi Enkripsi Pada Komunikasi GSM. *Jurnal Teknik Elektro*. Desember 2008. Fakultas Teknik Universitas Indonesia.

Jansen, W., & Ayers, R. 2006. *Forensic Software Tools for Cell Phone Subscriber Identity Modules*. In Proceedings of the Conference on Digital Forensics, Security and Law (pp. 93-106).

Prakash, K. & Balachandra. 2015. Security Issues and Challenges in Mobile Computing and M-Commerce. *International Journal of Computer Science & Engineering Survey (IJCSES)*, 6(2): 29-45.

Prayudi, Y., & Rifandi, F. 2013. *Ekplorasi Bukti Digital pada SIM card. Pusat Studi Forensika Digital*. Seminar Nasional Sistem Informasi Indonesia, SESINDO FTI - Universitas Islam Indonesia, 2 - 4 Desember 2013.

Willassen, S. 2003. Forensics and the GSM Mobile Telephone System. *International Journal of Digital Evidence*, 2(1): 1-17.