p-ISSN 2620 – 4843
e-ISSN 2620 – 4924

MODEL PENGUJIAN CELAH KEAMANAN BUG HOST PADA LAYANAN PROMOSI OPERATOR SELULER

Dedy Hariyadi[1)], Imam Ahmad Subhan[2)], Alfirst Radena Julio Vanca3[)]
[1)]Komunitas Forensik Digital Indonesia, milisdad@gmail.com
[2)]Teknik Komputer dan Jaringan, SMK N 1 Sragi Kabupaten Pekalongan, imamamia@gmail.com
[3)]Teknik Komputer dan Jaringan, SMK N 1 Sragi Kabupaten Pekalongan, juliovanca00700@gmail.com

Abstrak

Pertumbuhan penggunaan internet di Indonesia tidak lepas dari peran serta penetrasi pasar oleh Operator Seluler. Dalam hal ini Operator Seluler sering memberikan layanan promosi ke pelanggan. Dibalik layanan promosi terdapat beberapa celah keamanan yang dimanfaatkan oleh pelanggan. Biasanya celah tersebut disebut *bug host*. Penelitian ini mengajukan usulan model pengujian keamanan layanan promosi tersebut.
Kata kunci: *bug host*, cdma, celah keamanan, gsm, operator seluler

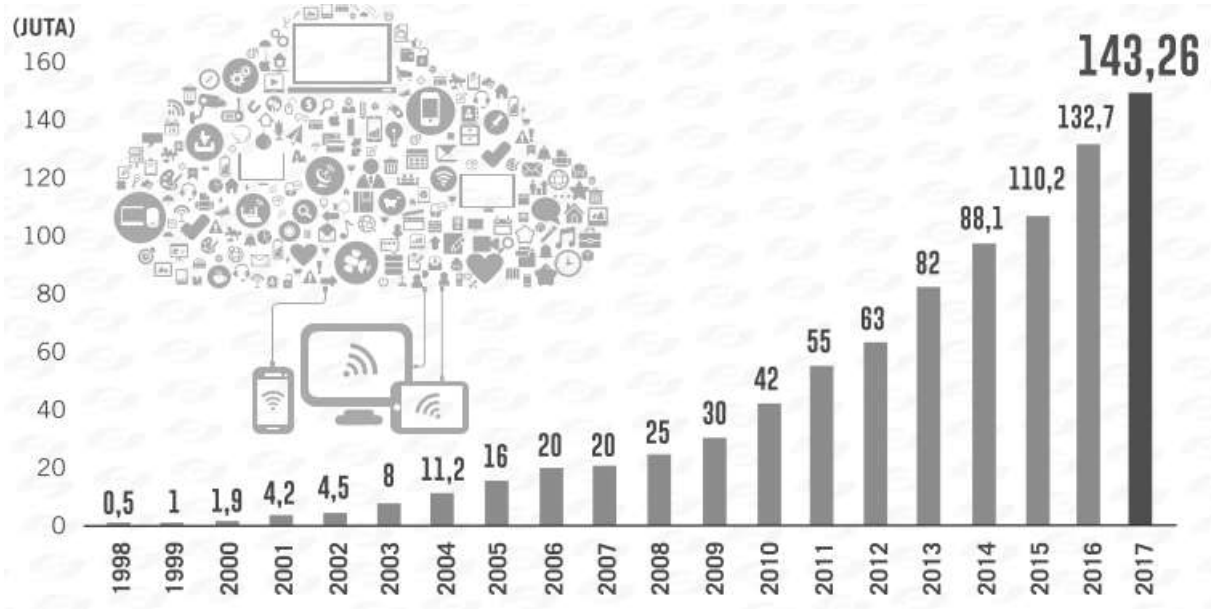
Abstract

The growth of internet usage in Indonesia can not be separated from market penetration role by Cellular Operator. In this case Celullar Operators often provide promotional services to customers. Behind the promotional services there are several security holes that are utilized by customers. Usually the security hole is called a bug host. This research proposes a model of security testing of the promotional services.

Keywords: *bug host, cdma, celullar operators, gsm, security hole*

1. PENDAHULUAN

Pertumbuhan internet di Indonesia mengalami peningkatan dari tahun ke tahun. Pada tahun 2017 tercatat kurang lebih 143.000.000 jiwa dari 262.000.000 jiwa penduduk Indonesia menggunakan internet (Asosiasi Penyelenggara Jasa Internet Indonesia & Teknopreneur Indonesia, 2017). Hal ini diikuti tingginya kepemilikan ponsel cerdas oleh orang dewasa, sekitar 60 % (Hootsuite, 2018). Gambar 1 menunjukan pertumbuhan penggunaan internet di Indonesia dari tahun 1998 sampai dengan 2017.



Gambar 1. Survey Pertumbungan Internet 2017 oleh APJII dan Teknopreneur Indonesia

Berdasarkan survey APJII bersama Teknopreneur Indonesia pada tahun 2017 terkait persepsi masyarakat Indonesia harga langganan internet pada perangkat gemerak (*mobile device*) adalah mahal 23,36%, biasa 56,77% dan murah 19,87%. Pada segmen yang menyatakan langganan internet mahal maka akan mencari sebuah solusi akses internet yang murah. Diantaranya adalah mencari paket promo yang ditawarkan oleh pihak Operator Seluler.

Berdasarkan observasi paket promo yang ditawarkan oleh Operator Seluler adalah layanan internet yang terbagi menjadi 2 paket yaitu paket reguler yang dapat berlaku selama 24 jam dan paket terbatas yang dikemas dengan layanan tambahan. Contoh paket terbatas diantaranya akses internet 10 GB pada pukul 00.00 sampai dengan 07.00, paket 5 GB untuk akses video premium, dan gratis *chatting* selama 1 bulan. Jadi seolah-olah layanan internet yang ditawarkan oleh Operator Seluler sangat besar.

Sebagian paket terbatas tersebut memunculkan celah tersendiri yang dapat dimanfaatkan untuk mengakses internet seolah-olah paket reguler. Dalam penelitian ini celah tersebut dinyatakan sebagai *bug host*. Menurut kamus bahasa Inggris daring[1] *bug* dapat diartikan sebagai suatru galat dari program komputer atau sistem sedangkan *host* yang berasal dari bahasa latin *hostia* yang berarti korban.

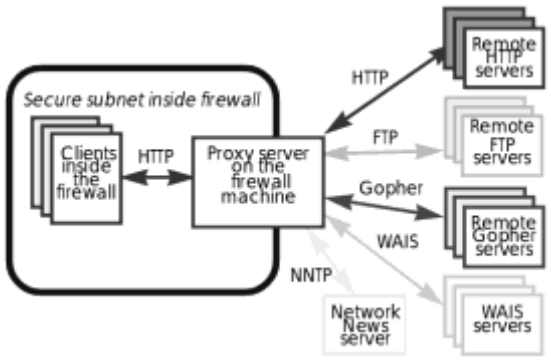
Maka dari itu *bug host* dapat diartikan suatu galat dari sebuah kesalahan sistem koneksi internet dengan sasaran Operator Seluler yang menyediakan layanan akses internet. Bug host dari paket internet terbatas maka dapat dimanfaatkan untuk mengakses internet yang seolah-olah menggunakan paket reguler.

2. *Proxy Server*

Fungsi utama dari *Proxy Server* adalah memberikan akses ke web server dari sebuah

1 https://en.oxforddictionaries.com/

klien yan terlindungi dari *firewall*. Proxy server juga memiliki sebuah kemampuan untuk menyimpan sebuah dokumen yang pernah diakses oleh klien lain. Oleh sebab itu klien dapat dikatakan mendapatkan akses internet dengan "*virtual bandwidth*" dari *Proxy Server* atau *Cache Server* terdekat. Secara umum *Proxy Server* berjalan bersamaan dengan *firewall* seperti yang ditunjukkan pada Gambar 2 (Luotonen & Kevin Altis, 1994).



Gambar 2. Gambaran Umum Konfigurasi Proxy Server

Proxy Server yang mampu menampung *cache* dari dokumen yang diakses klien memiliki beberapa 3 model (Huston, 1999) :

A. Explicit Caching

Model implementasi *Proxy Server* ini tidak mengikat kepada klien. Artinya klien dapat menambahkan pilihan *Proxy Server* pada peramban atau pun tidak. Pada setiap peramban saat ini telah diberikan pilihan penggunaan *Proxy Server*.

B. Forced Explicit Caching

Berbeda dengan model *Explicit Caching*, pada model ini pihak klien dipaksa memasukan alamat *Proxy Server* yang telah ditentukan. Dalam hal ini penyedia akses internet menutup semua akses sehingga klien harus memasukan IP atau alamat *Proxy Server* dari penyedia internet.

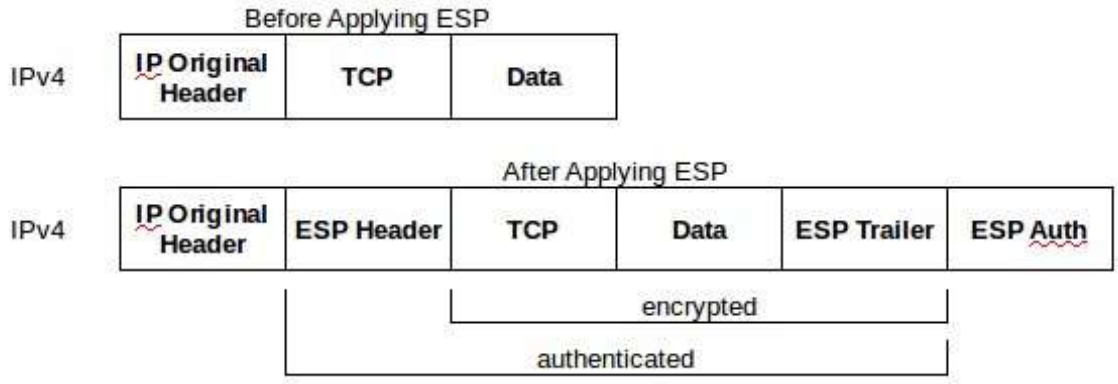
C. Transparent Caching

Klien pada model ini tidak dipaksa memasukan IP atau alamat *Proxy Server* karena penyedia internet melakukan pengalihan jalur paket *http* ke *Proxy Server*. Jadi klien tidak menyadari secara langsung bahwa akses internetnya telah menggunakan *Proxy Server*.

3. *TUNNELING*

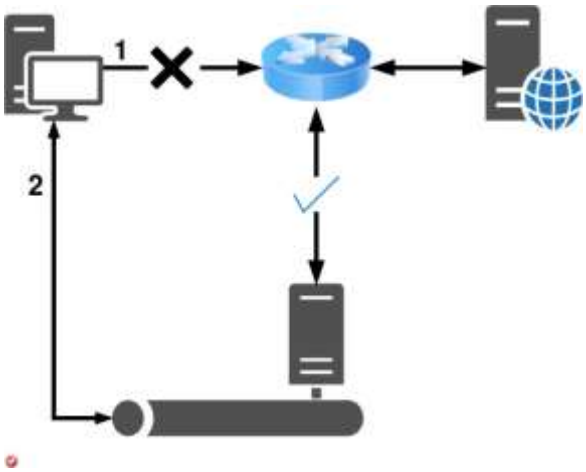
Teknik dasar *tunneling* adalah melakukan pembungkusan *IP Datagrams* ke dalam *Frame Networks* yang selanjutnya dikirimkan ke *host* lainnya. Hal dapat terlihat pada proses *IP Encapsulating Security Payload (ESP)* bahwa TCP dan Data dilakukan enkripsi yang disisipkan pada *IP Header IPv4*. Gambar 3 menunjukan proses sebelum dan sesudah implementasi ESP pada *IP Header* (Kent & Atkinson, 1998).

Implementasi teknik *tunneling* pada jaringan komputer dapat ditunjukan pada Gambar 4. Jalur 1 menunjukan klien yang terhubung ke sebuah router tidak dapat mengakses *web server* yang terletak pada jaringan internet. Sedangkan pada jalur 2 klien melakukan teknik tunneling ke sebuah server yang memiliki akses internet



Gambar 3. Implementasi Sebelum dan Sesudah ESP pada IP Datagrams

sehingga klien dapat mengakses *web server* tersebut. Istilah lain dari *tunneling* adalah forwarding karena pada praktiknya klien melakukan pembelokan koneksi ke *host* lain supaya *router* tidak mendeteksi asal asli klien.



Gambar 4. Tunneling atau Forwarding Koneksi

4. ANALISIS TRAFIK

Dalam klasifikasi serangan keamanan internet diantaranya terdapat teknik analisis trafik. Adapun yang dimaksud analisis trafik adalah pemantauan lalu lintas paket data yang dikirim dari host satu ke host lain dalam sebuah jaringan (Ahmad et al., 2011). Informasi yang didapatkan dalam analisis trafik diantaranya alamat asal, alamat tujuan, *port* asal, dan *port* tujuan.

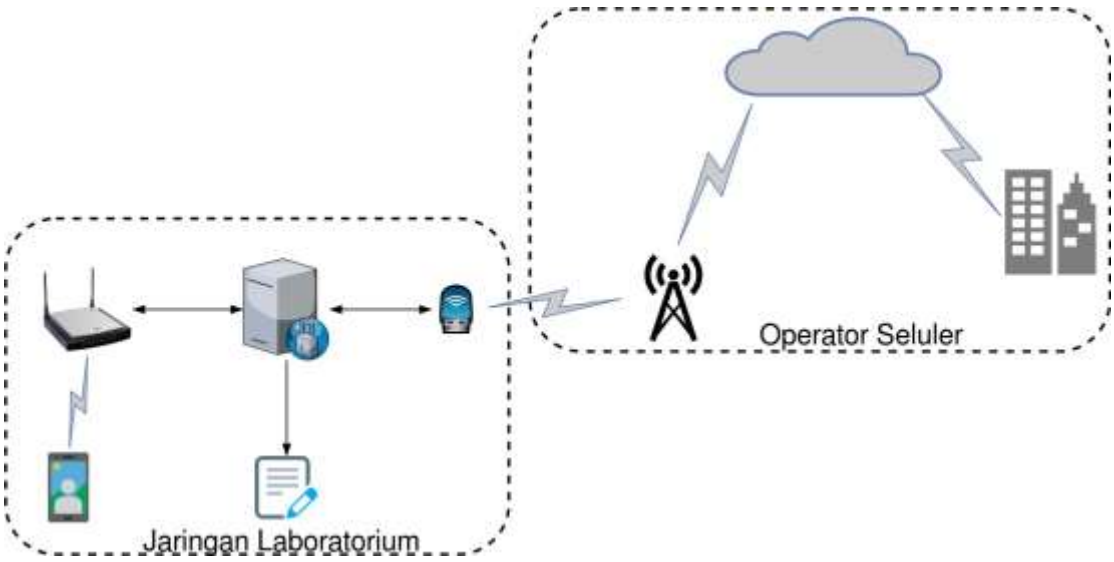
Teknik analisis trafik tidak berarti melakukan intersepsi isi konten pada lalu lintas jaringan walaupun melakukan pencegatan dan pemeriksaan paket data yang lewat. Teknik ini lebih fokus pada komunikasi antar *host*, waktu komunikasi, atau terkadang menunjukan suatu serangan dari *host* (Northcutt, 2007). Sebagai contoh teknik analisis trafik diantaranya membaca *log server* atau mencatat lalu lintas paket kemudian disajikan dalam bentuk *traffic log*.

5. METODE DAN PEMBAHASAN

5.1. TOPOLOGI JARINGAN

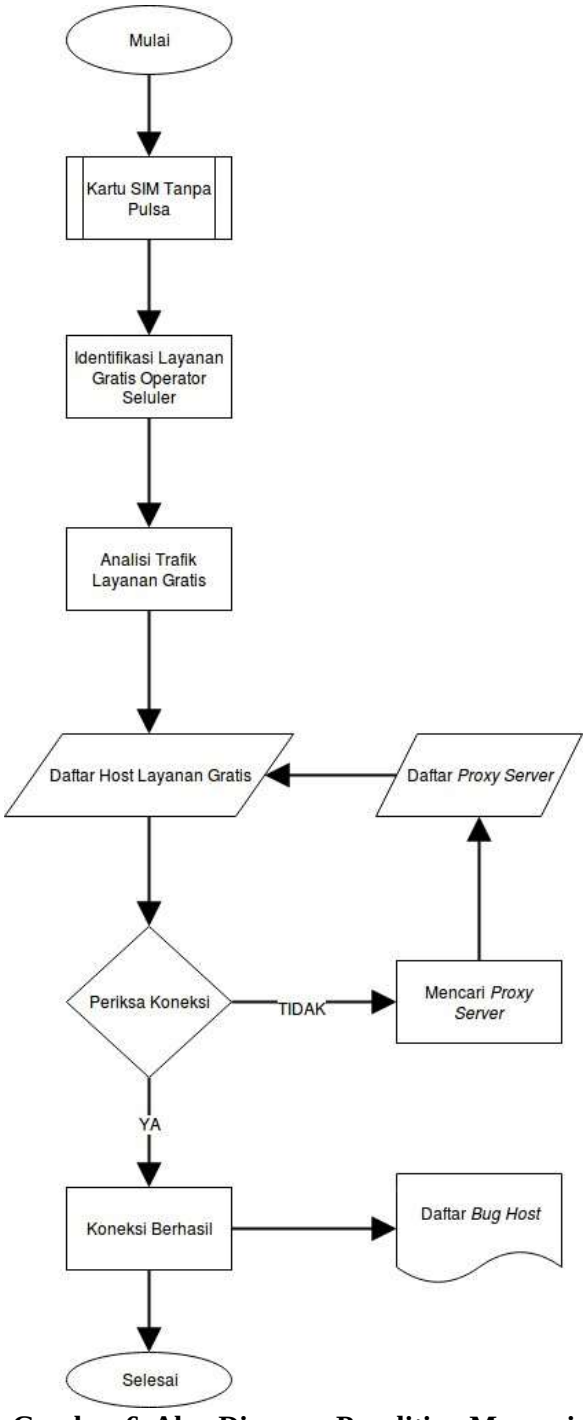
Syarat utama dalam mencari *Bug Host* adalah menggunakan kartu SIM dengan kondisi pulsa kosong pada paket utamanya. Hal ini untuk mengetahui aliran trafik *host* ke *host* walaupun dalam kondisi pulsa kosong. Sebelumnya dilakukan identifikasi layanan atau paket promo yang ditawarkan oleh Operator Seluler.

Oleh sebab itu perlu dibangun infrastruktur untuk melakukan teknik analisis trafik untuk mengetahui informasi *host* yang diakses oleh klien. Koneksi dengan Operator Seluler menggunakan Modem GSM/CDMA yang terhubung ke sebuah komputer sebagai pencatat trafik lalu lintas paket data. Selain sebagai pencatat lalu lintas paket data komputer juga dapat difungsikan sebagai *router* dan *wireless*



Gambar 5. Topologi Jaringan Analisis Trafik

access point. Fungsi *router* dan *wireless access point* juga dapat dipisah, komputer sebagai *router* dan pencatat lalu lintas paket data sedangkan *wireless access point* mendistribusikan koneksi.



Gambar 6. Alur Diagram Penelitian Mencari Bug Host

Pengujian akses layanan gratis atau promo hiburan premium dilakukan pada ponsel. Sebagai contoh memantau trafik lalu lintas dari aplikasi Whatsapp maka dari ponsel melakukan komunikasi menggunakan aplikasi tersebut. Gambar 5 menunjukkan topologi jaringan yang digunakan untuk pemantauan lalu lintas paket data.

5.2. PENCARIAN BUG HOST

Dari proses analisis trafik pada layanan gratis atau promo hiburan premium akan didapatkan sebuah daftar host atau alamat layanan tersebut. Seperti tampak pada Gambar 6 bahwa alur diagram mendeskripsikan proses pengujian celah keamanan layanan gratis atau promo dari Operator Seluler. Setelah proses identifikasi layanan gratis atau promo dari Operator Seluler dilakukan proses analisis trafik dari ponsel ke beberapa layanan atau promo yang ditawarkan. Dari hasil analisis trafik diperoleh daftar host atau alamat yang dapat diakses tanpa memerlukan biaya atau mengurangi paket promo hiburan premium.

Daftar *host* atau alamat layanan tersebut tidak semua bisa digunakan untuk mengakses internet secara global, ada beberapa operator telah menutup celah ini. Jika tidak bisa mengakses internet secara global maka diperlukan *proxy server* eksternal untuk mendeteksi layanan gratis atau promo tersebut. Oleh sebab itu perlu melakukan pengujian koneksi menggunakan *proxy server* eksternal.

Dari hasil pengujian *host* atau alamat layanan gratis atau promo Operator Seluler maka akan didapatkan sebuah *host* atau alamat yang dapat digunakan untuk mengakses internet secara gratis atau memaksimalkan layanan promo hiburan premium.

6. SIMPULAN

Layanan gratis atau paket promo hiburan premium masih terdapat beberapa celah sehingga pelanggan dapat mengakses internet secara gratis atau memaksimalkan paket promo hiburan premium untuk akses internet secara global tanpa-batasan yang telah ditentukan. Metode pencarian *Bug Host* ini dapat digunakan sebagai metode

pengujian layanan yang disediakan Operator Seluler untuk mengurangi resiko keamanan lain- nya. Pada metode ini belum dilakukan pengujian yang menggunakan *secure tunneling*. Hal ini da-pat dilakukan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

Ahmad, K., Verma, S., Kumar, N., Shekhar, J., Vivekananda, S., & Pradesh, U. (2011). Classification of Internet Security Attacks, 11–13. Retrieved from http://www.bvi-cam.ac.in/news/INDIACom 2011/321.pdf

Asosiasi Penyelenggara Jasa Internet Indonesia, & Teknopreneur Indonesia. (2017). *Pene- trasi & Perilaku Pengguna Internet In- donesia - Survey 2017*. Jakarta.

Hootsuite. (2018). *Indonesia Digital Landscape - Survey January 2018*.

Huston, G. (1999). Web Caching. *The Internet Protocol Journal*, *2*(3), 2–20. https://doi.org/10.1016/S0001-2092(16)00183-6

Kent, S., & Atkinson, R. (1998). *RFC2406: IP Encapsulating Security Payload*.

Luotonen, A., & Kevin Altis. (1994). *World-Wide Web Proxies*. Retrieved from http://courses.cs.vt.edu/~cs4244/spring. 09/ documents/Proxies.pdf

Northcutt, S. (2007). Traffic Analysis. Retrieved February 28, 2018, from https://www.sans.edu/cyber-research/security-laboratory/article/traffic- analysis