ANALISIS PENETRASI TEST PADA TRANSAKSI PEMBAYARAN NEAR FIELD COMMUNICATION MOBILE

ANALYSIS PENETRATION TEST ON PAYMENT TRANSACTION NEAR FIELD COMMUNICATION MOBILE

Agus Handoko[1], Surya Michrandi Nasution, ST.,MT [2], Dr. Marisa Paryasto, ST, MT[3]

[1,3]Prodi S1 Sistem Komputer, Fakultas Teknik Elektro, Universitas Telkom

[1]agus.handoko.smaga@gmail.com, [2]surya.michrandi@gmail.com, [3]marisa.paryasto@gmail.com

Abstrak

Dalam perkembangannya, smartphone dapat melakukan transaksi secara langsung. Fungsi kartu kredit, Anjungan Tunai Mandiri (ATM), dan yang lainnya dapat digantikan dengan menggunakan smartphone yang memiliki modul Near Field Communication (NFC). Terdapat kelemahan dalam transaksi saat menggunakan smartphone, hal tersebut dapat menimbulkan masalah keamanan.

Pada penelitian ini dilakukan penetrasi pada user yang melakukan transaksi melalui NFC reader. Dalam transaksi tersebut dilakukan serangan terhadap pengguna NFC dan diuji berhasil atau tidaknya serangan tersebut. Serangan terdiri atas Man-In-The-Middle-Attack, brute force, replay attack, dan MAC cloning.

Transaksi menggunakan smartphone harus berhati-hati terhadap arus data yang terjadi. Informasi dapat dengan mudah diperoleh tentang pengguna dan digunakan untuk kepentingan pelaku.

Kata Kunci: ***brute force, man-in-the-middle-attack, near field communication (NFC),*** **penetrasi**

Abstract

In its development, the smartphone can conduct transactions directly. Credit card functions, Automated Teller Machine (ATM), and others can be replaced by using a smartphone that has a Near Field Communication (NFC) module. There is a weakness in transactions when using a smartphone, it can cause security issues.

This study conducted penetration on users who make transactions through NFC reader. In the transaction is carried out an attack on the NFC users and tested the success or failure of the attack. The attacks consist of Man-In-The-Middle-Attack, brute force, replay attack, and MAC cloning

Transactions using a smartphone must be careful of the data flow that occurs. Information can be easily obtained about the user and used for the benefit of the attacker.

Keywords: brute force, near field communication (NFC), man-in-the-middle-attack, penetration

1. Pendahuluan

Pada era globalisasi, penggunaan *smartphone* telah menjadi pilihan utama karena sifatnya yang mudah dan praktis. Sehingga setiap orang yang memiliki mobilitas tinggi pasti membutuhkan *smartphone*. Tingginya ketergantungan manusia terhadap *smartphone* menimbulkan masalah baru termasuk dalam hal bertransaksi.

Perkembangan *smartphone* yang dilengkapi modul *Near Field Communication (NFC)* dapat melakukan transaksi secara langsung. Oleh karena itu, pengguna *smartphone* dapat menggantikan fungsi kartu kredit, ATM dan yang lainnya . Dengan adanya hal tersebut, keamanan data pengguna pun menjadi hal penting dalam melakukan transaksi.

Banyaknya jenis serangan yang diterima oleh pengguna dapat membuat konsumen kehilangan data. Pengguna hanya ingin keamanan data mereka terjamin saat bertransaksi. Hal yang sama juga berlaku untuk penyedia jasa layanan transaksi.

Keamanan dalam hal bertransaksi menjadi perhatian banyak pihak. Terdapat potensi masalah keamanan data yang dapat membuat pengguna atau konsumen merasa dirugikan. Oleh karena itu, penggunaan *smartphone* untuk tujuan bertransaksi harus lebih diperhatikan oleh *developer* sehingga dibutuhkan bentuk informasi tentang kelemahan transaksi pembayaran NFC *mobile.*

Banyaknya potensi masalah keamanan tentang transaksi menggunakan *smartphone* harusnya lebih diperhatikan oleh pengguna dan dengan alasan tersebut, maka dibutuhkan bentuk informasi tentang kelemahan transaksi pembayaran NFC *mobile.* Dari permasalahan tersebut di angkat lah topik tugas akhir ini yang berjudul "ANALISIS PENETRASI TEST PADA TRANSAKSI PEMBAYARAN NEAR FIELD COMMUNICATION MOBILE" tugas akhir ini ini dibuat untuk melakukan penetrasi test untuk pembayaran *NFC mobile* dan membuat hasil Analisa tentang penetrasi test untuk transaksi pembayaran *NFC mobile.*

2. Dasar Teori

2. 1 *Near Field Communication*

Near-field communication (NFC) merupakan bentuk komunikasi nirkabel jarak-pendek di mana antena yang digunakan lebih pendek daripada gelombang sinyal operator (yang mencegah interferensi gelombang dari antena yang sama). Pada jarak-dekat (tidak ada definisi universal berapa panjang gelombang jarak-pendek namun untuk tujuan praktikal anggap saja panjang gelombangnya seperempat dari gelombang biasa) antena dapat menghasilkan medan elektrik, atau medan magnetik, namun tidak medan elektromagnetik. Komunikasi NFC merupakan medan eletrik yang termodulasi, atau medan magnetik termodulasi, namun tidak berasal dari gelombang elektromagnetik radio. Sebagai contoh, antena putaran kecil (juga dikenal sebagai putaran magnetis) menghasilkan medan magnet, yang dapat diambil oleh antena putar kecil lainnya, jika cukup dekat.

2. 2 *Linux*

Linux adalah nama yang diberikan kepada sistem operasi komputer bertipe Unix. Linux merupakan salah satu contoh hasil pengembangan perangkat lunak bebas dan sumber terbuka utama. Seperti perangkat lunak bebas dan sumber terbuka lainnya pada umumnya, kode sumber Linux dapat dimodifikasi, digunakan dan didistribusikan kembali secara bebas oleh siapa saja. *Tools* yang akan digunakan di Linux ialah Ettercap, Wireshark, Hexinject serta Macchanger.

2. 3 *Mann In The Middle Attack*

Man in the middle attack adalah serangan dimana penyerang diam-diam melakukan relay dan mungkin mengubah komunikasi antara dua pihak yang percaya bahwa mereka saling berkomunikasi satu sama lain.

2.4 ISO 8583

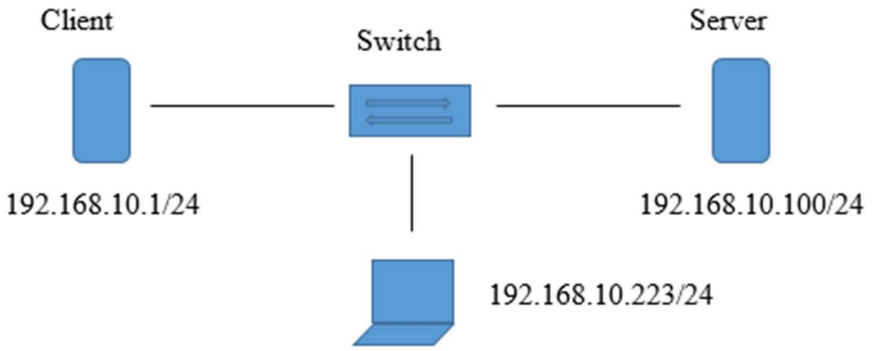
ISO 8583 merupakan standar internasional untuk kartu transaksi keuangan yang berasal dari pesan interchange. Standar Organisasi Internasional untuk Standardisasi untuk sistem yang menukar transaksi elektronik yang dilakukan oleh pemegang kartu dengan menggunakan kartu pembayaran.

2.5 *Java*

Java adalah bahasa pemrograman yang dapat dijalankan di berbagai komputer termasuk telepon genggam. Bahasa ini awalnya dibuat oleh James Gosling saat masih bergabung di Sun Microsystems saat ini merupakan bagian dari Oracle dan dirilis tahun 1995. Bahasa ini banyak mengadopsi sintaksis yang terdapat pada C dan C++ namun dengan sintaksis model objek yang lebih sederhana serta dukungan rutin-rutin aras bawah yang minimal.

3. Perancangan Sistem

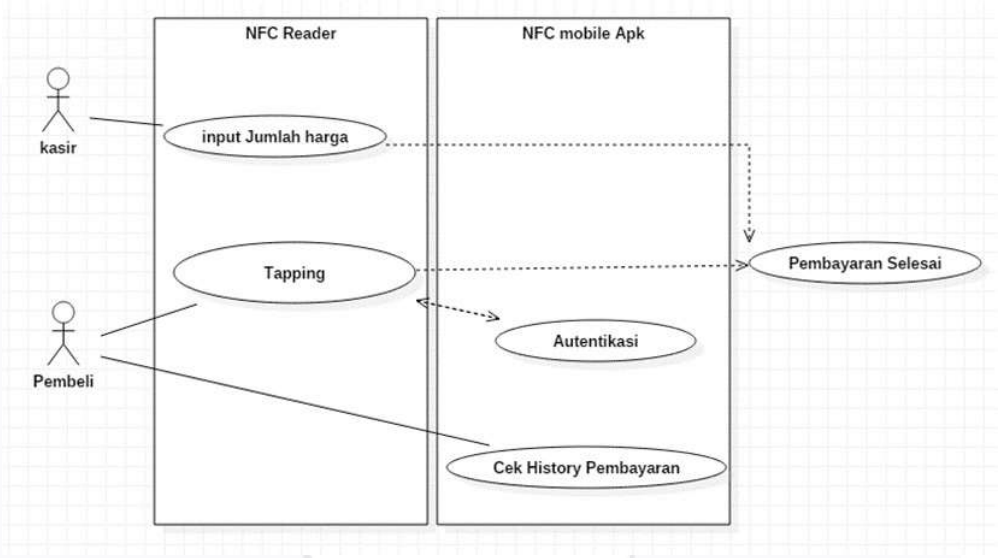
Gambaran umum dari sistem yang dirancang pada penelitian kali ini direpresentasikan oleh gambar berikut



Gambar 3.1 Gambaran Umum Sistem

3. 1 Skema Implementasi

Korban akan melakukan transaksi dengan skenario berikut.



Gambar 3.2 Skema Implementatif

4. Hasil Pengujian Sistem

4. 1 Hasil Pengujian Sistem

Tahap implementasi dilakukan setelah perancangan selesai dilakukan dan selanjutnya diimplementasikan pada bahasa pemrograman yang bertujuan untuk mengkonfirmasi model-model perancangan, sehingga sistem siap untuk dioperasikan. Kemudian Pengujian dilakukan untuk mengevaluasi hasil dari sistem yang dibuat.

4.1.1 Implementasi Perangkat Lunak

Dalam perancangan sistem aplikasi ini membutuhkan spesifikasi untuk membangun program dan melakukan simulasi dan pengujian, dengan kebutuhan sebagai berikut.

1. Sistem Operasi Windows 10

2. Sistem Operasi Kali Linux 2
3. Ettercap
4. Wireshark
5. Hexinject
6. Macchanger
7. NetBeans IDE 8.2
8. XAMPP
9. *MySQL*

4.1.2 Implementasi Perangkat Keras

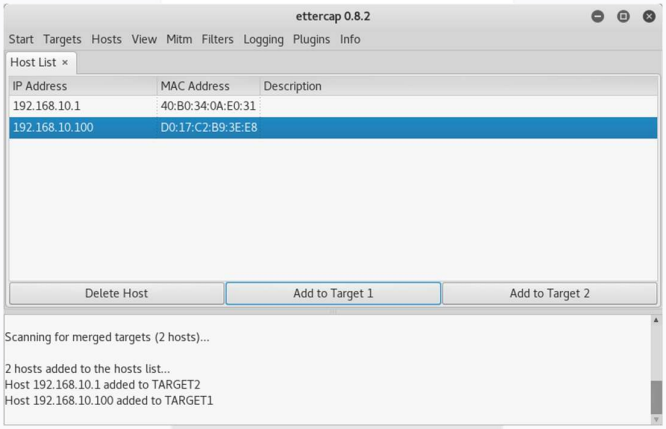
Perangkat keras yang dibutuhkan dalam membangun aplikasi dan simulasi program adalah sebagai berikut :

1. Laptop ASUS A46C Series dengan spesifikasi *Intel® Core™* i5-3317U CPU @ 1.70 GHz, RAM 8 GB, VGA 2 GB.
2. Laptop ASUS A46U Serires dengan Spesifikasi *Intel® Core™* i5-6200U CPU @ 2.30 GHz, RAM 4 GB DDR4.
3. TP-LINK 8-Port 10/100Mbps Desktop Switch Model No. TL-SF1008D

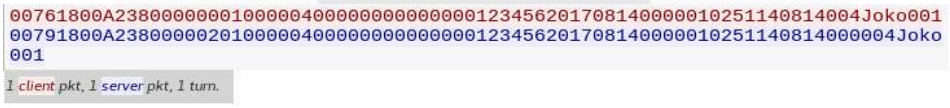
4. 2 Pengujian Sistem

4.2.1 ARP Poisoning

Pada pengujian ini, akan dibuat topologi dimana *server* dan *client* dapat berkomunikasi dan dapat melalui switch yang terhubung. Sehingga penyerang dapat melakukan ARP *Poisoning* terhadap *server* dan *client*. Maka IP *server* akan dijadikan Target 1 dan *client* akan dijadikan Target 2 menggunakan aplikasi Ettercap. Saat *server* dan *client* menjalin komunikasi, maka semua data yang terkirim dari *client-server* dan *server-client* akan terbaca menggunakan aplikasi Wireshark.



Gambar 4.1 Menentukan Target Untuk Serangan MITM Di Ettercap



Gambar 4.2 Data Yang Dikirmkan *Client* Serta *Server* Pada Wireshark

Disini kita dapat melihat *request* dan *respon* ISO8583 di *client-server*. Data tersebut merupakan jenis String yang digunakan secara umum dalam melakukan transaksi melalui ISO 8583. Data tersebut memang pada dasarnya dikirimkan dalam bentuk String. Data yang dikirmkan oleh *client* ke *server* selalu diawali dengan MTI.

Hanya saja dengan format *packager* ISO8583, data yg diterima server maupun *client* terdapat penambahan string untuk dapat membedakan *request* dari *client* dan *respond* dari *server*. Maka kode MTI tersebut diawali dengan string "1800". Disini kita dapat melihat *request* dan *respon* ISO8583 di *client-server*. Data tersebut merupakan jenis String yang digunakan secara umum dalam melakukan transaksi melalui ISO 8583. Data tersebut memang pada dasarnya dikirimkan dalam bentuk String. Data yang dikirmkan oleh *client* ke *server* selalu diawali dengan MTI. Hanya saja dengan format *packager* ISO8583, data yg diterima server maupun *client* terdapat penambahan string untuk dapat membedakan *request* dari *client* dan *respond* dari *server*. Maka kode MTI tersebut diawali dengan string "1800".

```
 Enter The ISO Message :
1800A238000000010000040000000000000012345620170814000001231330081400 4Joko001
MTI='1800'
3='123456'
7='20170814'
11='000001'
12='231330'
13='0814'
48='Joko'
70='001'
BUILD SUCCESSFUL (total time: 3 seconds)
```

Gambar 4.3 *Unpack* ISO8583 *Message* Pada *Request Client*

```
 Enter The ISO Message :
1800A238000002010000040000000000000012345620170814000001231330081400 0004Joko001
MTI='1800'
3='123456'
7='20170814'
11='000001'
12='231330'
13='0814'
39='000'
48='Joko'
70='001'
BUILD SUCCESSFUL (total time: 22 seconds)
```

Gambar 4.4 *Unpack* ISO8583 *Message* Pada *Respond Server*

Perlu di ingat, bahwa ketika melakukan *unpacking* terhadap ISO8583, pastikan format yang digunakan korban dan penyerang sama. Provider pun sebenarnya memiliki *data element* mereka masing-masing agar menjamin kerahasiaan data saat transaksi. Di Indonesia sendiri kebanyakan transaksi menggunakan ISO8583 versi 1987.

4.2.2 DNS Poisoning

Pada serangan ini, terjadi kegagalan. Analisa penulis yaitu DNS *Poisoning* berada di level *http://* yang membutuhkan tampilan atas berpindahnya data. Sedangkan dalam perancangan hanya dibuat dalam bentuk aplikasi saja.. Sedangkan dalam rancangan hanya sampai pada level TCP/IP. Sehingga akan lebih efektif jika dilakukan srangan ARP Poisoning. Jika rancangan serangan dibuatkan pada level *http://*, maka serangan ini pun akan berhasil mengelabui korban dan akan mendapatkan informasi autentikasi korban terhadap *web server*.

4.2.3 Brute Force Web Server

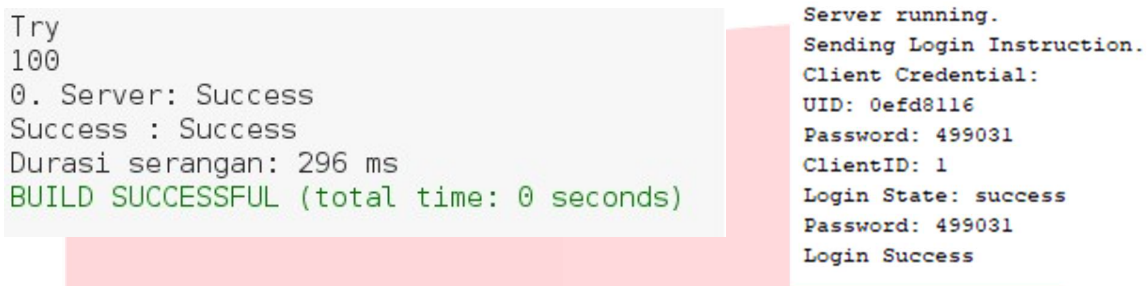
Pada serangan ini dibuat pada dengan bahasa *Java* menyesuaikan dengan keadaaan *web server*. Parameter yang dibutuhkan oleh pelaku untuk korban dalam melakukan serangan ini adalah *wordlist* berisi kombinasi 6 digit yang dapat di isi dari angka 0-9 yang berarti memiliki 10^6 kombinasi. Didalam *wordlist* terdapat kombinasi angka secara acak.

Parameter kedua, pelaku harus mengetahui secara pasti siapa pengguna *smartphone* tersebut atau NFC *tag* pada *smartphone.* Karena jika hanya mengandalkan *password* saja, maka serangan hanya berhasil namun pelaku tidak dapat memperoleh informasi lebih terkait transaksi korban atau informasi akun korban di *web server*

Serangan *bruteforce* pada web server dengan *password wordlist* tercepat ialah 0.296 detik. Untuk *password* terlama didapatkan kendala yaitu aplikasi XAMPP untuk database mengalami *error*. Sehingga serangan ini penulis hentikan pada urutan *wordlist* ke-32462 dalam waktu 5 menit 21 detik. Menurut perhitungan penulis dari urutan yang ada dari 10^6 kombinasi dengan waktu tersebut maka

$$\frac{1000000}{32462} x\ 321\ detik = 9888.485\ detik$$

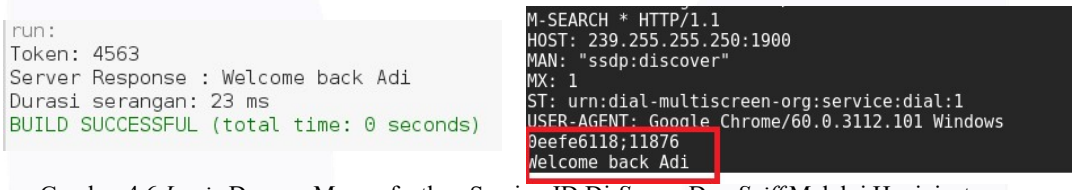
$$\frac{9888.485\ sec}{3600} = 2.747\ jam$$ atau ± 2 jam 26 menit 53 detik.



Gambar 4.5 Waktu Tercepat Dan Respon Server Terhadap Bruteforce

4.2.4 Replay Attack

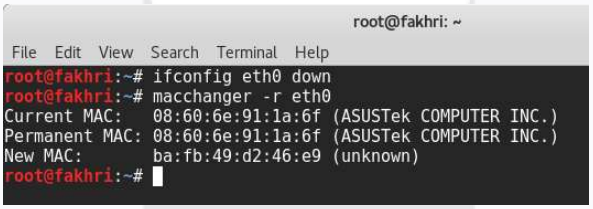
Pada pengujian ini, *replay attack* dimaksudkan pelaku untuk mendapatkan akses yang dimiliki korban terhadap akun *smartphone* yang bersamaan dengan NFC *tag korban.* Dengan melakukan *fake authentication*, memanfaatkan *Session ID korban,* pelaku dapat masuk sebagai *user*. Dengan memanfaatkan fungsi hexinject, pelaku dapat melakukan *sniffing* untuk mengetahui informasi si korban atau pengguna *smartphone*.



Gambar 4.6 *Login* Dengan Memanfaatkan Session ID Di *Server* Dan *Sniff* Melalui Hexinject

4.2.5 MAC Cloning

Pada serangan ini, penyerang dapat menyamarkan jejaknya dalam melakukan serangan dengan cara mengganti MAC *Address* pelaku. Dari sini kita dapat melihat bahwa MAC *Address* pada interface tertentu dapat diubah pada gambar berikut.



Gambar 4.7 Mengubah MAC Address Dengan Macchanger

5. Kesimpulan

Transaksi *mobile* dalam hal ini yang menggunakan NFC harus berhati-hati terhadap arus data saat sedang melakukan transaksi. Pelaku dapat dengan mudah memanipulasi ARP pada modem/*router* yang digunakan pada proses transaksi untuk keuntungan pelaku.

Kurangnya fitur keamanan dari sisi ISO 8583, maka pembacaan paket data ISO 8583 dapat dengan mudah dideteksi di *wireshark*. Namun Karena fleksibilitas dari *data element* membuat ISO 8583 susah di *parsing* sesuai keinginan yaitu mendapatkan informasi yang tepat terkait transkasi yang dilakukan. Karena mengikuti format dari

perusahaan yang membuatnya sehingga *data element* akan di *custom* agar membingungkan para pelaku transaksi *online*.

Daftar Pustaka

[1] Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu dan Monique Jones. 2011. An Overview Of Penetration Testing. *International Journal of Network Security & Its Applications (IJNSA)*. Vol 3 (6)

[2] William G. J. Halfond, Shauvik Roy Choudhary dan Alessandro Orso. 2011. *Improving Penetration Testing Through Static And Dynamic Analysis*.

[3] Kunjan Shah, "*Penetration Testing Android Applications*", Foundstone Professional Services

[4] Ernst Haselteiner, Klemens Breitfuss," *Security In Near Field Communication* (NFC)".

[5] Hassan EL ALLOUSSI, Laila FETJAH dan Abdelhak CHAICHAA. 2014. Securing the Payment Card Data on Cloud environment: Issues & perspectives. *IJCSNS International Journal of Computer Science and Network Security.* Vol 14 (11)

[6] Made Krisnanda. 2011. Penggunaan Teknologi *Near Field Communication* Pada Telepon Seluler Untuk *Micro Payment* dan *Loyalty Management*. *Jurnal Informatika*. Vol 7 (1)

[7] Neeta B. Thorat, C. Sreevardhan. Survey On Security Threats And Solutions For Near Field Communication. *International Journal of Research in Engineering and Technology (IJRET).* Vol 03

[8] J.Coughlan, S. Rehman. An Efficient Mobile Payment System Based On NFC Technology *World Academy of Science. Engineering and Technology International Journal of Computer, Electrical, Automation*

[9] M. Kerschberger, "*Near Field Communication A survey of safety and security measures*", Vienna, 2011.

[10] Nasution, SM, Husni EM dan Wuryandari AI. Prototype of train ticketing application using Near Field Communication (NFC) technology on Android device. *System Engineering and Technology International Conference (ICSET) ,* 11-12 September 2012.