EKSPLOITASI RFID MENGGUNAKAN NFC DENGAN TEKNIK *CLONING* PADA STUDI KASUS KTM

RFID EXPLOITATION USING NFC WITH CLONING TECHNIQUE ON STUDENT CARD

Andes Pratama[1]

[1]Prodi S1 Teknik Informatika, Fakultas Informatika, Universitas Telkom
[1]doremimyfavourite@yahoo.com

Abstrak

Radio-frequency identification (RFID) adalah suatu cara penggunaan gelombang elektromagnet untuk mentransfer data dengan tujuan untuk mengidentifikasi atau melacak suatu objek. RFID terbagi 2 yaitu RFID aktif yang mempunyai sumber daya sendiri serta RFID pasif yang tidak mempunyai sumber energi. Seiring berkembangnya teknologi pada telepon seluler (ponsel) maka RFID dapat dibaca dengan menggunakan Near Field Communication (NFC). Celah keamanan muncul dengan terbacanya RFID pada fitur NFC. Jenis serangan pada RFID menggunakan ponsel ada bermacam macam diantaranya adalah cloning dan modifikasi data pada RFID. Pada tugas akhir ini dilakukan eksploitasi RFID dengan metode cloning dan modifikasi pada RFID. Proses pengujian dilakukan di perpustakaan Universitas Telkom. Hasil akhir yang didapat adalah KTM Universitas Telkom dapat di cloning dan modifikasi.

Kata Kunci : ***cloning*****, kartu tanda mahasiswa (KTM),Modifikasi,** ***near field communication*** **(NFC),** ***radio-frequency identification*** **(RFID)**

Abstract

Radio-frequency identification (RFID) is an electromagnet use to tranfer data that has purpose for identification or searching objects. RFID is divided into two kind, Active RFID which has its own energy source and passive RFID which activates when near energy from other sources. Development of cellphone technology give possibility for RFID to be read by Near Field Communication (NFC). There are several security issues with RFID when it is read by NFC. There is many exploitation of RFID, such as cloning and data modification. The test take place in library. Final results show that University Telkom Student Card (KTM) can be cloned and modified.

Keywords : cloning, university telkom student card (KTM), Modification, Near field communication (NFC), radio-frequency identification (RFID)

1. Pendahuluan

Radio-frequency identification (RFID) adalah penggunaan suatu objek yang diaplikasikan pada barang, hewan atau orang yang bertujuan untuk mengidentifikasi atau melacak menggunakan gelombang radio[1]. Penggunaan RFID semakin sering digunakan dalam kehidupan sehari - hari. Penggunaan yang paling umum diantaranya pada kartu mahasiswa, kartu transportasi, kartu tol atau kartu parkir. Pada beberapa kantor dan perusahaan RFID digunakan sebagai pembuka pintu untuk mengakses suatu ruangan. RFID dibagi 2 jenis yaitu RFID aktif dan pasif. RFID aktif memiliki sumber energi sendiri sedangkan RFID pasif bergantung pada sumber energi pembacanya. Keamanan RFID menjadi alasan utama dibuatnya tugas akhir ini. Dapat dibayangkan apa yang terjadi apabila sesorang dapat melakukan modifikasi pada isi RFID, maka orang tersebut dapat mengendarai alat transportasi secara gratis atau mengakses fasilitas khusus yang hanya dapat diakses orang tertentu[2].

Near Field Communication (NFC) [4] adalah suatu fitur komunikasi nirkabel yang menggunakan induksi magnet sehingga memungkinkan untuk komunikasi jarak dekat. Di Indonesia, penggunaan teknologi NFC belum terlalu banyak, sedangkan di luar negeri NFC merupakan fitur yang biasa digunakan untuk transaksi menggunakan telepon seluler (ponsel) sebagai pengganti kartu serta dapat digunakan untuk bertukar foto, video atau data. Pada beberapa ponsel, NFC dapat digunakan untuk membaca RFID pada kartu mahasiswa, kartu kredit atau kartu akses suatu tempat.

Dengan memanfaatkan fitur NFC pada ponsel, ada beberapa cara penyerangan yang bisa dilakukan peretas diantaranya adalah memodifikasi isi kartu serta melakukan *cloning* pada suatu kartu RFID. Baik melakukan modifikasi atau melakukan *cloning* dapat dilakukan jika sudah mengetahui *key*. Beberapa RFID jenis lama sudah diketahui *key* enkripsinya sehingga cukup mudah untuk melakukan modifikasi pada RFID tersebut.

Pada tugas akhir ini akan dilakukan eksploitasi teknik *cloning* dan modifikasi pada kartu mahasiswa Universitas Telkom. Percobaan dilakukan dengan cara membaca isi kartu mahasiswa dengan fitur NFC pada ponsel

kemudian dicek jenis kartu serta enkripsinya. Kemudian isi kartu akan dipindahkan pada kartu RFID lain dan dicek apakah kartu tersebut dapat terbaca. Setelah penelitian selesai maka akan dicari solusi untuk mencegah terjadinya *Cloning* dan Modifikasi pada KTM.

2. Dasar Teori dan Perancangan Sistem

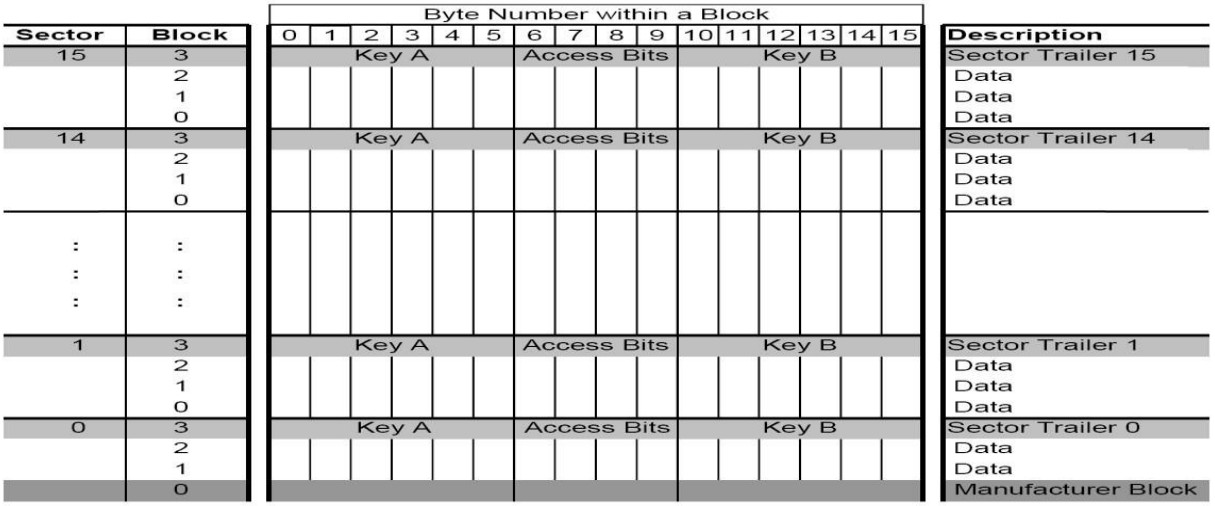
2.1. *Radio Frequency Identification* (RFID)

RFID (*Radio – Frequency Identification*) adalah suatu cara untuk mengidentifikasi benda menggunakan gelombang elektromagnetik[1]. RFID terdiri dari dua komponen utama yaitu label (*tags*) dan pembaca (*reader*). Pembaca menerima gelombang elektromagnetik dari label melalui antena. Pembaca mempunyai memiliki antena yang berfungsi untuk mengirim dan menerima gelombang elektromagnetik. Label terbuat dari *microchip* yang tujuannya untuk menyimpan data dan antena.

Teknologi RFID digunakan untuk berbagai macam aplikasi, mulai dari keamanan sampai pengaturan hak akses, serta transportasi. Teknologi ini cocok digunakan untuk mengumpulkan banyak data pada suatu benda serta untuk pencarian dan proses perhitungan di beberapa aplikasi. Terdapat berbagai jenis RFID yang berjalan menggunakan frekuensi gelombang yang berbeda. Pemilihan frekuensi didasarkan pada kebutuhan dalam pengaplikasian RFID. Secara umum, RFID dapat dikategorikan ke dalam tiga jenis berdasarkan penggunaan frekuensi.

- Low Frequency (125/134 KHz) – Umum digunakan untuk akses pintu masuk
- High – Frequency (13,56 MHz) – Umum digunakan untuk tiket serta sistem pembayaran
- Ultra High – Frequency (860/960 MHz) – Umum digunakan pada pelacakan barang di gudang

Label RFID umum digunakan dalam dunia industry serta ditempel pada mesin ketika proses produksi untuk melacak perkembangan proses *assembly*. Pada hewan, RFID dapat ditempel untuk mengenali hewan tersebut. Pada saat label RFID dapat ditempel di berbagai benda, kemungkinan terbacanya informasi pribadi tanpa izin menjadi masalah privasi yang serius.



Gambar 1 Struktur RFID pada jenis Mifare classic 1K[5]

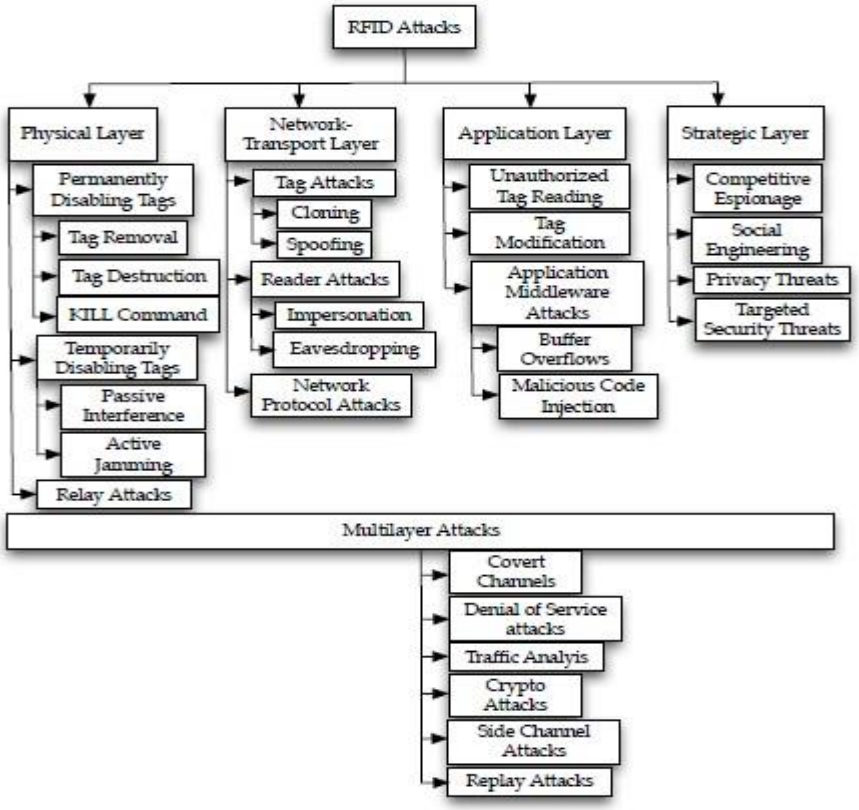
2.2. *Near Field Communication* (NFC)

NFC merupakan suatu bentuk dari komunikasi nirkabel jarak pendek dimana antena yang digunakan memiliki panjang gelombang yang lebih pendek dibandingkan sinyal ponsel[3]. Pada daerah sekitar NFC, antena dapat menghasilkan sinyal elektrik atau sinyal magnetik tetapi tidak dapat menghasilkan sinyal elektromagnetik. Jadi NFC hanya dapat berkomunikasi dengan salah satu dari sinyal elektrik atau magnetik saja. Banyak ponsel yang sekarang menggunakan NFC dengan frekuensi 13.56 MHz dan panjang gelombang 22.11 untuk melakukan transaksi. Karena panjang gelombang yang pendek maka NFC menjadi sulit untuk disadap. NFC banyak digunakan pada ponsel berbasis Android. Fitur ini belum banyak digunakan sampai muncul sistem operasi Android 4.0 *Ice Cream Sandwich.* Perancangan desain *embedded system* NFC dapat menggunakan metode TLM untuk mengurangi waktu desain karena metode TLM lebih baik dibandingkan model RTL Avalon dan RTL Bus[6].

2.3. Jenis serangan pada RFID

Terdapat berbagai jenis serangan pada RFID, disesuaikan dengan maksud yang ingin dicapai serta hambatan yang ada demi mencapai tujuan. Contohnya jika kita ingin mendapatkan akses masuk ke suatu tempat maka dilakukan cloning terhadap RFID yang sudah ada. Jika kita tidak bisa mendapatkan RFID untuk di cloning maka kita

menggunakan *PCD based attack* atau *Sniffer attack*. *Mitrokotsa*[9] mengklasifikasikan serangan pada RFID berdasarkan *layer* mana yang diserang.



Gambar 2 Jenis serangan pada RFID[9]

2.4. RFID *cloning*

Cloning merupakan salah satu teknik yang digunakan untuk memanfaatkan celah pada RFID. Peretas mengkopi seluruh data pada RFID dan mengkopikannya pada kartu yang sejenis[7]. Data yang dikopi peretas adalah label dan isi data yang disimpan pada RFID. Teknik ini dapat dilakukan dengan mudah untuk RFID dengan label yang tidak terenkripsi. Untuk melakukan *clone* pada RFID yang terenkripsi maka peretas memerlukan kunci dari enkripsi tersebut sebelum bisa dikopi. Proses *clone* ini berbahaya karena ketika peretas sudah mendapatkan kopian dari RFID maka mereka dapat menggunakan kopian RFID tersebut seperti benda aslinya. RFID yang biasa dikopi adalah kartu pembayaran, tiket transportasi elektronik serta kartu untuk mengakses suatu tempat.

Contoh id pada RFID

ccaf6d71

Contoh konten pada RFID

ccaf6d717f8804004745741465104507
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFF0078069FFFFFFFFFF

Pada proses *cloning*, yang dilakukan adalah membaca isi kartu dengan menggunakan key a dan key b pada sektor 0 sampai 15. Setelah terbaca semua isinya maka yang dilakukan adalah memindahkan semua isi dari kartu yang hendak dicloning kepada kartu kosong lainnya sehingga kartu baru isinya sama kecuali manufature id. Pada kasus khusus dimana data disimpan langsung pada database dan diakitkan dengan UID maka yang dikopi cukup kode manufakturnya saja. Kartu yang digunakan haruslah memungkinkan untuk menulis ulang sektor 0 blok 0 atau yang biasa disebut *manufacture id*.

2.5 *Tag Modification*

Tag Modification merupakan jenis serangan yang tujuannya adalah melakukan perubahan atau penghapusan pada isi dari RFID[9]. Proses ini dapat dilakukan apabila suatu kartu memungkinkan proses penulisan lebih dari sekali serta *key* a dan *key* b dari sektor yang hendak dimodifikasi telah diketahui. Dengan melakukan modifikasi maka peretas dapat melakukan kontrol terhadap nilai yang terhadap pada RFID

Contoh id pada RFID

ccaf6d71
Contoh konten pada RFID

ccaf6d717f8804004745741465104507
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFF0078069FFFFFFFFFFF

Pada Proses modifikasi yang dilakukan adalah mengubah isi dari RFID menjadi sebagai berikut

ccaf6d717f8804004745741465104507
00000000000000000000000098736412
00000000000000000000000000000000
FFFFFFFFFF0078069FFFFFFFFFFF

2.6. ***Dictionary Based Attack***

Dictionary based attack merupakan jenis serangan yang dilakukan dengan cara membuat daftar kemungkinan dari *Password* yang ada[13]. Pada kasus RFID *dictionary based attack* dilakukan untuk memecahkan *key* A dan *key* B dari suatu RFID. Cara yang dilakukan adalah dengan membuat suatu *file key* yang isinya adalah kombinasi dari *key* pada RFID yang memungkinkan. Jenis serangan ini mirip dengan *Brute Force*, tetapi perbedaannya adalah jenis serangan *Brute Force* melakukan kombinasi dari semua *key* yang ada sedangkan pada *Dictionary attack* penyerang memasukan sendiri kombinasi *key* yang mungkin dalam suatu *file* kemudian melakukan penyerangan. Kelebihan dari metode *Dictionary* adalah kecepatan eksekusi daripada metode *Brute Force*. Kekurangan dari metode *Dictionary* adalah ada kemungkinan *key* tidak didapatkan dikarenakan tidak ada dalam daftar *key* yang sudah didefinisikan oleh penyerang.

2.6. Model sistem penelitian

Model sistem yang digunakan pada percobaan ini adalah model sistem sederhana antara Kartu Tanda Mahasiswa (KTM), Smartphone dan RFID duplikat. Smartphone yang digunakan adalah Google Nexus i9250. Pada smartphone sudah terinstall aplikasi yang bernama NFC Reader untuk membaca info pada KTM serta Mifare Classic Tool yang berfungsi untuk menduplikasi isi dari KTM

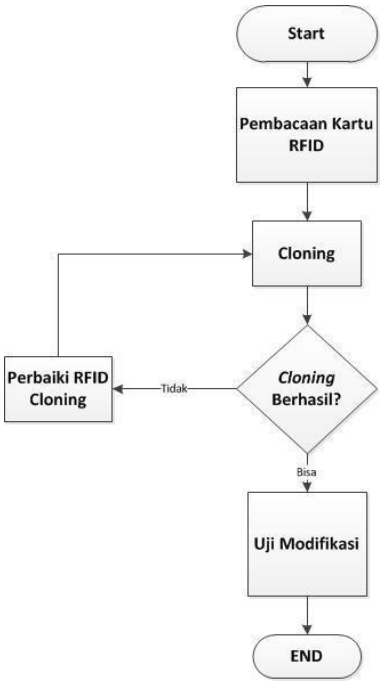
Gambar 3 Model sistem penelitian

Proses pertama adalah membaca isi dari Kartu tanda mahasiswa Universitas Telkom menggunakan fitur NFC pada ponsel. Aplikasi yang digunakan adalah *Mifare Classic Tool.* Setelah diambil datanya kemudian dianalisis isinya untuk menentukan:

- Jenis kartu RFID
- *Key* A dan *Key* B

Setelah selesai dianalisis kemudian isi dari KTM dipindahkan ke kartu RFID lain yang masih kosong isinya menggunakan aplikasi Mifare Classic Tool. Hal yang di cloning adalah Tag id dan Isi dari sektor 0 sampai 15.

2.7. Flowchart pengujian



Gambar 4 Flowchart pengujian

Proses pengujian dilakukan di tempat yang menggunakan RFID. Dalam studi kasus ini tempat yang digunakan untuk uji coba adalah perpustakaan. Di perpustakaan RFID digunakan untuk membuka pintu perpustakaan. Proses diawali dengan membaca issi master key dari kartu perpustakaan yang dipegang oleh admin perpustakaan. Setelah itu dilakukan analisis apakah *key* A dan *key* B pada kartu perpustakaan menggunakan kunci default atau tidak. Setelah diketahui *key* A dan *key* B dari kartu perpustakaan, maka dilakukan penulisan isi dari kartu ke kartu yang sudah dipersiapkan. Setelah itu, kartu diuji coba apakah bisa membuka pintu. Setelah proses membuka pintu berhasil maka dilakukan penggantian isi kartu untuk menguji apakah pintu masih dapat terbuka

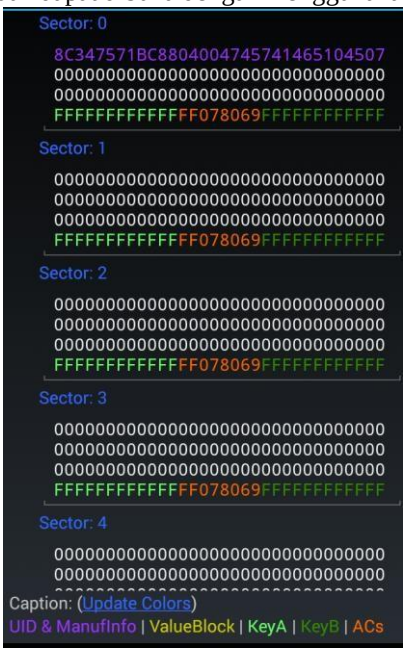
3. Hasil implementasi

Proses ujicoba di perpustakaan terbagi 2 yaitu proses cloning dan proses modifikasi kartu perpustakaan. Sesuai dengan flow chart, maka proses yang pertama kali dilakukan adalah cloning kemudian dilanjutkan dengan proses modifikasi kartu perpustakaan. Proses Ujicoba cloning pada perpustakaan dilakukan sesuai skenario awal dan secara umum prosesnya dilakukan dalam 3 tahap, yaitu

1. Pembacaan isi master key dengan fitur NFC
2. Melakukan penulisan pada *chinese magic card* dengan isi dari Master key
3. Melakukan tes apakah pintu dapat terbuka

Pada proses pertama yaitu melakukan pembacaan isi pada *master key* dilakukan dengan cara mendekatakan *master key* pada ponsel yang fitur NFC nya sudah aktif. Sama seperti KTM, pada *master key* kartu perpustakaan kunci a dan b pada RFID menggunakan default dari pabrik yaitu FFFFFFFFFF. Selain itu hanya terdapat kode manufaktur saja sedangkan sisa 15 sektor lainnya kosong. *Master key* dari kartu perpustakaan terdiri dari 16 sektor dari 0 sampai 15 dan setiap sektor terdiri dari 4 blok. Ciri ini mengindikasikan bahwa kartu perpustakaan memakai mifare classic 1K. Sektor 0 blok 0 pada kartu perpustakaan berisikan kode manufaktur dari kartu. Sektor 0 blok 1 dan 2 pada kartu perpustakaan kosong, hal ini mennunjukan bahwa tidak ada informasi ataupun nilai yang ditulis pada kartu perpustakaan. *Key A* kartu perpustakaan menggunakan kunci bawaan dari pabrik yaitu FFFFFFFFFF dan *key B* pada kartu perpustakaan juga menggunakan kunci bawaan dari pabrik yaitu FFFFFFFFFF. Pada sektor 1 sampai sektor 15, isi blok 0 sampai 2 dari masing - masing sektor kosong. Hal ini menandakan tidak ada informasi ataupun nilai yang ditulis pada sektor tersebut. *Key A* dan *key B* pada sektor 1 sampai 15 juga menggunakan kunci bawaan dari pabrik yaitu FFFFFFFFFF. Setelah mendapatkan isi tersebut dapat disimpulkan bahwa pembaca RFID pada perpustakaan menggunakan nilai dari kode manufaktur untuk menentukan apakh pintu dapat dibuka atau tidak. Kode manufaktur disimpan dalam database yang kemudian dikaitkan dengan informasi lain. Proses cloning dilakukan dengan mengkopi sektor 0 blok 0 yang berisi kode manufaktur kedalam kartu baru dikarenakan kode manufakturlah

yang dicatat pada database RFID. Proses modifikasi dilakukan dengan mengubah sektor 0 blok 0 secara acak untuk membuktikan apakah pintu perpustakaan dapat dibuka dengan menggunakan kartu acak atau tidak.



Gambar 5 Isi dari Master Key

Pada proses kedua yaitu proses penulisan pada *chinese magic card*, isi dari master key ditulis semuanya kedalam chinese magic card dengan menggunakan opsi tulis pada id manufaktur. Hal ini dilakukan karena data yang terdapat pada master key hanyalah kode manufaktur. Pada saat dilakukan percobaan tidak terdapat kendala pada proses penulisan dan penulisan pun sukses. Pada proses ketiga yaitu tes karu pada pintu masuk dilakukan dengan cara mendekatkan kartu ke alat pembaca dan kemudian sukses atau tidaknya dapat dilihat dari perubahan warna pada alat pembaca. Warna merah jika gagal dan warna hijau jika berhasil. Pada percobaan yang dilakukan alat pembaca berubah warna menjadi hijau dan pintu dapat terbuka sehingga percobaan berhasil

Gambar 6 Tes membuka pintu perpustakaan dengan *cloning*

Proses modifikasi setelah proses cloning selesai dan berhasil maka percobaan selanjutnya adalah percobaan untuk memodifikasi isi dari RFID kemudian dilakukan pengujian apakah dapat membuka pintu atau tidak. Sesuai hasil dari pembacaan kartu, maka bagian yang diubah adalah sektor 0 blok 0 dari RFID. Sektor 0 blok 0 dari RFID diganti menjadi ccaf6d717f8804004745741465104507 sehingga isi sektor 0 berubah menjadi

Sektor 0

ccaf6d717f8804004745741465104507
00000000000000000000000000000000

00000000000000000000000000000000
FFFFFFFFFF0078069FFFFFFFFFF

Setelah dilakukan penulisan isi tersebut pada kartu kosong dan dilakukan ujicoba ternyata pintu perpustakaan tidak mau terbuka dan terdapat tanda merah pada pembaca RFID. Penjelasan dari petugas perpus adalah bahwa pintu akses ke perpustakaan hanya bisa dibuka oleh *master key* atau kartu yang didaftarkan sehingga kartu selain tidak dapat membuka pintu perpustakaan

Gambar 7 Tes membuka pintu dengan modifikasi

4. Kesimpulan

Dari hasil penelitian tentang *cloning* pada Kartu tanda Mahasiswa Universitas Telkom, maka dapat dapat diambil kesimpulan:

1. Kartu Mahasiswa universitas Telkom adalah kartu Mifare classic 1k dilihat dari jumlah sektornya yaitu 16 serta tiap sektor terdiri dari 4 blok. Kartu mahasiswa Universitas Telkom memakai Key A dan Key B yang sama yaitu FFFFFFFFFFFFF. Kartu Tanda Mahasiswa Universitas Telkom dapat di *cloning* dikarenakan memakai *key* standar pabrik yaitu FFFFFFFFFFFFF.
2. Proses Modifikasi Bisa dilakukan pada KTM tetapi tidak memiliki efek terhadap RFID dikarenakan data pada KTM dikaitkan dengan UID pada database Universitas Telkom dan KTM merupakan jenis kartu dimana UID tidak dapat diubah.

5. Saran

Penulis memberikan saran untuk peningkatan keamanan pada RFID Universitas Telkom yang dapat dilakukan dengan cara:

1. Perubahan *key* A dan *key* B pada Kartu Tanda Mahasiswa dari FFFFFFFFFFFF menjadi *key* lain yang telah disepakati oleh admin dari Universitas Telkom dapat mencegah dari eksploitasi dengan teknik *cloning* dan modifikasi.
2. Perubahan *access bits* pada sektor yang berisi informasi dengan mengubah status *write* menjadi *never* dapat mencegah terjadinya modifikasi pada KTM.

Daftar Pustaka

[1]. Paxar, *RFID Basic*, Monarch Products & Services.
[2]. D. Balaban, "Vendor Group Seeks to Crack Mifare Dominance | NFC Times – Near Field Communication and all contactless technology.," 04-Feb-2010. [Online]. Didapat dari: http://nfctimes.com/report/vendor-group-seeks-crack-mifare-dominance. [Diakses: 30-Mar-2015].
[3]. S. A. Weis, "Rfid (radio frequency identification): Principles and applications," *System*, vol. 2, p. 3Principles, 2007.
[4]. "What Is NFC?," *NFC Forum*. [Online]. Didapat dari: http://nfc-forum.org/what-is-nfc/. [Diakses: 21-Jan-2015].
[5]. "The Different Types of RFID Systems," *Impinj*. [Online]. Didapat dari: http://www.impinj.com/resources/about-rfid/the-different-types-of-rfid-systems/. [Diakses: 02-Feb-2015].
[6]. NXP Semiconductors, *MIFARE Classic 1K - Mainstream contactless smart card IC for fast and easy solution development*.196330 *datasheet*, Mei 2011.
[7]. "*Dangerous Things - Custom gadgetry for the discerning hacker*," *Dangerous Things*. [Online]. Didapat dari: https://dangerousthings.com. [Diakses: 08-Maret-2015].

[8]. S. C. Monday, S. 08, 2014, and 11:52 am PT, "iTokens: Why it makes sense for Apple's rumored payment system to use tokenized transactions." [Online]. Didapat dari: http://appleinsider.com/articles/14/09/08/itokens-why-it-makes-sense-for-apples-rumored-payment-system-to-use-tokenized-transactions. [Diakses: 02-Jan-2015].
[9]. "Everything You Need to Know About Near Field Communication | Popular Science." [Online]. Didapat dari: http://www.popsci.com/gadgets/article/2011-02/near-field-communication-helping-your-smartphone-replace-your-wallet-2010/. [Diakses: 08-Jul-2015].
[10]. NXP Semiconductors, *Near Field Communication (NFC) controller*. 120132 *datasheet*, September 2012.
[11]. A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of RFID attacks," *Gen*, vol. 15693, p. 14443, 2010.
[12]. Mou Cheng, Chen, *MIFARE Classic:Completely Broken*, National Taiwan University, 2010.
[13]. J. Wetzels, "Broken keys to the kingdom: Security and privacy aspects of RFID-based car keys," *arXiv preprint arXiv:1405.7424*, 2014.
[14]. "Samsung Galaxy Nexus I9250," *Gsmarena*. [Online]. Didapat dari: http://www.gsmarena.com/samsung_galaxy_nexus_i9250-4219.php. [Diakses: 26-Mar-2015].
[15]. "Samsung Galaxy Nexus Teardown," *Ifixit*. [Online]. Didapat Dari: https://www.ifixit.com/Teardown/Samsung+Galaxy+Nexus+Teardown/7182. [Diakses: 09-Mar-2015].