SKRIPSI

ANALISIS SERANGAN MALICIOUS PIXELS PADA QR CODE DAN AZTEC CODE

Reynaldo Imanuel

NPM: 2014730060

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS
UNIVERSITAS KATOLIK PARAHYANGAN
2018

UNDERGRADUATE THESIS

MALICIOUS PIXELS ATTACK ON QR CODE AND AZTEC CODE ANALYSIS

Reynaldo Imanuel

NPM: 2014730060

DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND SCIENCES
PARAHYANGAN CATHOLIC UNIVERSITY
2018

LEMBAR PENGESAHAN

ANALISIS SERANGAN MALICIOUS PIXELS PADA QR CODE DAN AZTEC CODE

Reynaldo Imanuel

NPM: 2014730060

Bandung, 06 Desember 2018

Menyetujui,

Pembimbing

Mariskha Tri Adithia, P.D.Eng

Ketua Tim Penguji

Chandra Wijaya, M.T.

Anggota Tim Penguji

Husnul Hakim, M.T.

Mengetahui,

Ketua Program Studi

Mariskha Tri Adithia, P.D.Eng

PERNYATAAN

Dengan ini saya yang bertandatangan di bawah ini menyatakan bahwa skripsi dengan judul:

ANALISIS SERANGAN MALICIOUS PIXELS PADA QR CODE DAN AZTEC CODE

adalah benar-benar karya saya sendiri, dan saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan.

Atas pernyataan ini, saya siap menanggung segala risiko dan sanksi yang dijatuhkan kepada saya, apabila di kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya, atau jika ada tuntutan formal atau non-formal dari pihak lain berkaitan dengan keaslian karya saya ini.

Dinyatakan di Bandung,
Tanggal 06 Desember 2018

Reynaldo Imanuel
NPM: 2014730060

ABSTRAK

Quick Response Code (QR Code) adalah *barcode* 2 dimensi yang digunakan untuk menyimpan data. Kepopuleran penggunaan *QR code* dalam menyimpan data menjadi alasan banyak pihak yang ingin menyerang *barcode* tersebut. Salah satu bentuk serangannya adalah *Malicious Pixels*. *Malicious Pixels* merupakan serangan yang mengubah beberapa piksel pada gambar. Jika diaplikasikan pada *barcode* 2 dimensi, maka modul-modul penyusun tersebut yang akan diubah. Serangan ini mengakibatkan terjadinya perubahan isi pesan pada *barcode*. Penerapan serangan *Malicious Pixels* pada *QR code* memanfaatkan kemampuan *QR code* untuk mengoreksi kesalahan pada *QR code*. Fitur pengoreksian yang seharusnya menjaga integritas isi pesan dimanfaatkan untuk mengubah isi pesan. Bentuk serangan ini tentu dapat diaplikasikan pada *barcode* 2 dimensi selain *QR code* seperti *Aztec code* karena *Aztec code* memiliki kemampuan untuk mengoreksi kesalahan juga.

Penelitian ini mengimplementasikan serangan *Malicious Pixels* pada *QR code*. Tahapan serangan dimulai dari pemindaian *QR code*, pemrosesan *QR code* masukan, lalu menampilkan hasil serangan berupa daftar teks yang merupakan hasil manipulasi dari teks masukan. Daftar hasil serangan dapat menjadi gambaran seberapa rentan *QR code* masukan terhadap serangan *Malicious Pixels*. Tahapan yang sama juga diterapkan pada *Aztec code*.

Beberapa pengujian dilakukan terhadap perangkat lunak yang melakukan serangan *Malicious Pixels* pada *QR code* dan *Aztec code*. Pengujian pertama menguji kemampuan perangkat lunak dalam membangun dan memindai *QR code* dan *Aztec code*. Pengujian kedua menguji serangan dengan parameter ukuran data dan jenis *error correction* pada *QR code*. Pengujian ketiga menguji apakah serangan serupa dapat diaplikasikan pada *Aztec code*. Pengujian keempat menguji serangan dengan parameter ukuran data pada *Aztec code*.

Hasil dari pengujian menunjukkan perangkat dapat melakukan pembangunan dan pemindaian *QR code* dan *Aztec code* dengan baik. Pengujian kedua menunjukkan semakin besar ukuran data dan semakin tinggi jenis *error correction* maka semakin kebal terhadap serangan *Malicious pixel*. Pengujian ketiga menunjukkan bahwa serangan serupa dapat diaplikasikan pada *Aztec code*. Pengujian keempat menunjukkan semakin besar ukuran data pada *Aztec code* maka semakin kebal terhadap serangan *Malicious Pixels*.

Kata-kata kunci: *QR code*, *Aztec code*, *Malicious pixel*

ABSTRACT

Quick Response Code (QR Code) is a 2-dimensional barcode that is used to store data. The popularity of using coded QR in storing data is the reason many parties want to attack the code. One form of attack is the Malicious Pixels attack. Malicious Pixels attack is an attack that changes several pixels in the image. If applied to a 2-dimensional barcode, the constituent modules will be changed. This attack results in a change in the content of the message on the barcode. The application of Malicious Pixels attacks on QR code utilizes the ability of the QR code to correct errors on QR codes. The correction feature that should maintain the integrity of the message content is used to change the message content. This form of attack can certainly be applied to 2-dimensional barcodes other than QR code such as Aztec code because the Aztec code has the ability to correct errors as well.

This study implements a Malicious Pixels attack on a QR code. Stages of attack starting from scanning the QR code, processing QR code input, then displaying the results of attacks in the form of a list of texts that are the result of manipulation of the input text. List of attack results can be a picture of how vulnerable QR code input is to Malicious pixel attacks. The same stage is also applied to the Aztec code.

Some testing is done on software that attacks Malicious Pixels on QR code and Aztec code. The first test tested the software's ability to build and scan QR code and Aztec code. The second test tests the attack with data size parameters and error correction types on the QR code. The third test tests whether a similar attack can be applied to the Aztec code. The fourth test tests the attack with the parameter data size on the Aztec code.

The results of the tests show that the device can properly develop and scan the QR code and Aztec code. The second test shows the bigger the size of the data and the higher the type of error correction, the more immune to Malicious Pixels attacks. The third test shows that a similar attack can be applied to the Aztec code.

Keywords: QR code, Aztec code, Malicious pixel

Dipersembahkan untuk Bapak, Mama, dan Matthew

KATA PENGANTAR

Puji syukur penulis sampaikan kepada Tuhan Yang Maha Esa karena atas berkat dan rahmatNya penulis dapat menyelesaikan penyusunan skripsi dengan judul "Analisis Serangan Malicious Pixels Pada QR Code dan Aztec Code". Penulis menyadari bahwa di dalam skripsi ini masih terdapat banyak kekurangan. Penulis juga menyadari bahwa penyusunan skripsi ini tidak terlepas dari bantuan berbagai pihak. Pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Kedua orang tua dan adik yang selalu mengingatkan kewajiban sebagai mahasiswa, serta selalu sabar dan terus memberi semangat kepada penulis dalam menyelesaikan tugas akhir.
2. Ibu Mariskha Tri Adithia selaku dosen pembimbing yang telah memberikan waktu, ide, kritik, dan nasihat selama proses penyusunan skripsi ini sehingga skripsi ini dapat terselesaikan.
3. Muhammad Hilman, Muhammad Irfan, dan Vinieta Abhinandaniya yang sering membantu penulis dalam proses penyusunan skripsi ini dan memberikan masukan yang dibutuhkan oleh penulis.
4. Abdiel, Adrian, Calvin, Fadhlan, Faza, Ihsan, Obrien, dan Osfaldo yang membantu meringankan beban perkuliahan yang penulis alami.
5. Haga, Efan, Egia, dan Bobby yang selalu memberikan semangat dalam menjalani perkuliahan dan menyelesaikan tugas akhir kepada penulis.
6. Keluarga UKM Listra UNPAR yang selalu membantu penulis terutama menyediakan ruang untuk penulis mengerjakan tugas akhir.
7. Semua pihak yang tidak mungkin disebutkan satu-persatu yang sudah memberikan bantuan dan dukungan dalam pengerjaan skripsi ini.

Akhir kata, penulis memohon maaf jika terdapat kesalahan dan kekurangan dalam skripsi ini. Semoga skripsi ini dapat bermanfaat bagi pihak yang membutuhkan.

Bandung, Desember 2018

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Quick Response Code atau yang biasa dikenal dengan *QR code* adalah kode batang berdimensi 2 yang dibangun oleh sebuah perusahaan di Jepang bernama Denso Wav[1]. Jika diartikan dalam bahasa Indonesia, quick response berarti respon cepat, dengan maksud informasi dalam QR code dapat diuraikan dalam kecepatan tinggi. *QR code* dapat memuat berbagai informasi seperti alamat URL, nomor telepon, hingga informasi spesifik suatu produk. Untuk membaca *QR code* dibutuhkan perangkat dengan pemindai khusus maupun perangkat dengan kamera dan perangkat lunak khusus. *QR code* memiliki mode masing-masing dalam menyimpan data. Pada *QR code* mode yang umum dalam menyimpan data ada tiga yaitu numerik, alfanumerik, dan 8-bit. Perbedaan dari ketiga mode tersebut adalah jenis data yang dapat disimpan di dalam *QR code*.

QR code semakin populer karena kemudahan dalam penggunaannya dan kemampuannya dalam menyimpan banyak informasi tanpa memakan banyak tempat. *QR code* juga digunakan oleh berbagai macam jenis perusahaan seperti perusahaan pengantaran barang, penyimpanan barang, hingga iklan. *QR code* bahkan dapat dimanfaatkan untuk keperluan pribadi seperti menyimpan data diri. Ditambah lagi sudah banyak pembangkit *QR code* yang dapat digunakan secara gratis.

Kepopuleran penggunaan *QR code* menjadi salah satu alasan mengapa *QR code* dijadikan sasaran penyerangan oleh pihak-pihak tertentu. Dengan memanfaatkan kemudahan penggunaan *QR code*, pihak-pihak penyerang dapat membuat pengguna *QR code* melakukan apa yang diinginkan penyerang tanpa disadari oleh pengguna tersebut karena *QR code* tidak dapat dipahami oleh manusia hanya dengan melihatnya. Hanya dengan mengubah beberapa piksel pada *QR code* isi informasi pada *QR code* dapat diubah sehingga tidak berfungsi sesuai tujuan awal pembuatannya.

Kode batang berdimensi 2 yang biasa digunakan selain *QR code* adalah *Aztec code*. *Aztec code* adalah kode batang berdimensi 2 yang diciptakan oleh Andrew Longracre, Jr. dan Robert Hussey[2]. Kode batang ini biasanya digunakan untuk menyimpan data teks yang lebih sedikit dari kapasitas terkecil pada *QR code* sehingga kode batang terlihat lebih ringkas. *Aztec code* yang digunakan untuk menyimpan data yang tidak banyak disebut *Aztec code* kompak. Tetapi kode batang ini tetap dapat menyimpan teks dalam jumlah yang besar dengan dampak ukuran dimensi kode juga lebih besar.

Malicious Pixels adalah sebuah serangan yang mengarah pada beberapa piksel pada suatu gambar[3]. Pada kasus serangan yang mengarah kepada kode batang berdimensi 2, serangan *Malicious Pixels* akan mengubah beberapa piksel pada kode batang seperti mengubah piksel yang berwarna hitam menjadi putih atau sebaliknya. Tujuan dari serangan ini adalah untuk mengubah isi informasi dari suatu *QR code* sehingga informasi tersebut dapat menjadi sebuah gangguan atau ancaman kepada penggunanya.

Pada skripsi ini, akan dibangun perangkat lunak untuk membangkitkan kode batang berdimensi 2 yaitu *QR code* dan *Aztec code* dari masukan pengguna, memindai kode batang masukan, dan membangkitkan kode batang baru hasil implementasi serangan *Malicious Pixels*. Hasil dari implementasi tersebut akan diuji dan dianalisis. Tujuan dilakukannya analisis adalah untuk mengetahui celah yang digunakan untuk penyerangan dan bagaimana cara mencegah serangan tersebut.

1.2 Rumusan Masalah

Berdasarkan pemaparan pada latar belakang, rumusan masalah yang akan dikaji adalah sebagai berikut :

- Bagaimana cara kerja serangan *Malicious Pixels*?
- Bagaimana cara mengimplementasikan serangan *Malicious Pixels* pada *QR code*?
- Bagaimana cara mengimplementasikan serangan *Malicious Pixels* pada *Aztec code*?

1.3 Tujuan

Berdasarkan pada rumusan masalah, tujuan yang ingin dicapai adalah sebagai berikut :

- Mempelajari cara kerja serangan *Malicious Pixels*.
- Mempelajari serangan *Malicious Pixels* yang diimplementasikan pada *QR code*.
- Mempelajari serangan *Malicious Pixels* yang diimplementasikan pada *Aztec code*.

1.4 Batasan Masalah

Batasan masalah pada penelitian ini adalah :

1. Mode yang digunakan untuk mengodekan data pada *QR code* adalah mode byte.
2. Jenis *Aztec code* yang digunakan adalah *Aztec code* kompak.
3. Jumlah pengubahan karakter pada pesan di dalam *QR code* maupun *Aztec code* maksimal 2 karakter.

1.5 Metodologi

Bagian-bagian pengerjaan skripsi ini adalah sebagai berikut :

1. Melakukan studi literatur mengenai *QR code*, *Aztec code BCH code*, *Barcode* 1 dimensi, dan *Malicious Pixels*.
2. Mencoba serangan *Malicious Pixels* pada *QR code* dan *Aztec code* secara manual.
3. Melakukan analisis kebutuhan perangkat lunak yang melakukan serangan *Malicious Pixels* pada *QR code* dan *Aztec code*.
4. Membuat diagram kelas dan diagram aktivitas perangkat lunak yang melakukan serangan *Malicious Pixels* pada *QR code* dan *Aztec code*.
5. Melakukan perancangan perangkat lunak yang melakukan serangan *Malicious Pixels* pada *QR code* dan *Aztec code*.
6. Membangun perangkat lunak yang melakukan serangan *Malicious Pixels* pada *QR code* dan *Aztec code*.
7. Melakukan pengujian perangkat lunak yang melakukan serangan *Malicious Pixels* pada *QR code* dan *Aztec code*.
8. Melakukan analisis serangan *Malicious Pixels* pada *QR code* dan *Aztec code*.
9. Menulis dokumen skripsi.

1.6 Sistematika Pembahasan

Pembahasan dalam penelitian ini dilakukan secara sistematis sebagai berikut :

1. Bab 1 Pendahuluan
   Berisi latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi, dan sistematika pembahasan.

2. Bab 2 Landasan Teori
   Berisi dasar-dasar teori yang digunakan dalam melakukan analisis. Dasar-dasar teori tersebut meliputi penjelasan tentang *QR code*, *Aztec code*, serangan *Malicious Pixels*, dan *library* yang digunakan dalam membangun perangkat lunak yang mengaplikasikan serangan *Malicious Pixels*.

3. Bab 3 Analisis
   Berisi analisis kasus dengan beberapa studi kasus sebagai objek penelitian. Studi kasus tersebut meliputi serangan yang diaplikasikan pada *QR code* dan *Aztec code*.

4. Bab 4 Perancangan Perangkat Lunak
   Berisi analisis dan perancangan perangkat lunak yang dapat melakukan serangan Malicious Pixels pada *QR code* dan *Aztec code*. Rancangan meliputi rancangan antarmuka dan rancangan perangkat lunak yang melakukan serangan *Malicious Pixels*.

5. Bab 5 Pengujian Perangkat Lunak
   Berisi proses pengujian perangkat lunak dan analisis hasil uji. Bab ini diawali dengan hasil implementasi rancangan antarmuka perangkat lunak yang dibangun. Pengujian yang dilakukan berupa pengujian secara fungsional dan eksperimental.

6. Bab 6 Kesimpulan
   Berisi kesimpulan dan saran.