GRID CARD: MODEL OTENTIKASI UNTUK MENCEGAH PENCURIAN DATA OTENTIKASI

Muhammad Affandes
Jurusan Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau
Jl. HR. Soebrantas Km.15 No.15 Panam, Pekanbaru, Riau
affandes@uin-suska.ac.id

Abstrak –Ancaman terhadap pencurian data otentikasi sebuah akun merupakan ancaman yang berkelanjutan. Faktor penyebab utama seringkali datang dari faktor manusia sebagai pengguna sistem tersebut. Sehingga dengan memanfaatkan kekurangan pengetahuan tentang teknologi, pelaku memperdaya pengguna lain untuk memberikan data otentikasinya tanpa mereka sadari. Salah satunya adalah penggunaan data pribadi seperti tanggal lahir sebagai *password* atau PIN kartu ATM mereka yang memudahkan orang lain untuk menebak. Banyak penelitian yang membahas dari segi keamanan sistem otentikasinya menggunakan *hardware based authentication*. Disamping cara ini sangat efektif, namun membutuhkan biaya dalam implementasinya. Penelitian ini memberikan pengenalan tentang mekanisme *non-hardware based authentication* yang sama efektifnya dengan biaya yang sangat murah.

Kata Kunci: *grid card*, *non-hardware based authentication*,otentikasi.

I. PENDAHULUAN

Proses otentikasi (*Authentication*) merupakan proses untuk mengetahui identitas seorang saat berinteraksi pada suatu sistem informasi [**1**]. Mekanisme ini digunakan oleh sebuah sistem untuk mengatur hak akses seorang pengguna pada sebuah sistem. Salah satu metode otentikasi yang paling banyak digunakan saat ini adalah *username* dan *password*. Metode ini tergolong praktis karena pengguna

hanya perlu mengingat kedua kombinasi *username* dan *password* tersebut dan menginputkannya pada saat otentikasi ke sistem.

Pencurian akun pada sistem yang menggunakan metode otentikasi seperti ini sering terjadi [**2**]. Karena metode ini hanya menggunakan satu elemen otentikasi (*single-factor authentication*). Biasanya pengguna menggunakan data-data pribadi sebagai *password*-nya, antara lain tanggal kelahiran, nomor telepon, bahkan nama orang tertentu. Dengan demikian, akan memudahkan bagi orang lain untuk menebak *password* pengguna tersebut.

Tidak sulit untuk mencari data pribadi seseorang, salah satunya bisa menggunakan situs jejaring sosial. Survei terhadap lebih dari 2500 pengguna internet antara umur 18-19 tahun menjelaskan bahwa sebagian besar pengguna internet tidak peduli dengan *privacy setting* yang ada pada web Facebook [**3**].

Hasil survei terhadap 3.126 pengguna yang memiliki akun jejaring sosial menjelaskan bahwa jejaring sosial merupakan pengaruh paling besar dalam mendapatkan informasi identitas seseorang, sekitar 55% tanggal kelahiran (bulan dan tanggal) dapat dijumpai pada akun tersebut, sekitar 51% terdapat nama sekolah menengah atas dan 47% terdapat alamat *email* mereka pada akun jejaring sosial. Selain itu, informasi seperti tanggal kelahiran yang lengkap, nomor telepon, profil saudara kandung, profil ibu kandung, *screenname* bahkan nama hewan peliharaan juga dapat dijumpai pada akun mereka [**4**].

Selain dengat cara menebak *password* berdasarkan data pribadi, ada juga metode *phising* yang masih efektif digunakan untuk menjebak seorang pengguna untuk memberikan *username* dan *password* mereka tanpa mereka sadari. Target *phising* yang paling banyak adalah web yang bergerak disektor finansial (47%) dan *payment service* (25%). Sedangkan web *social network* (4,2%) terletak pada peringkat 6 (enam) setelah *gaming* (6,1%), *retail* (6,1%) dan *auction* (4,3%) [**5**].

Berikutnya juga dapat menggunakan *tool keylogger* dan *sniffer* yang dipasang pada komputer pengguna. Biasanya pengguna tidak akan mengetahui keberadaan kedua aplikasi ini saat dijalankan di komputer. Kedua aplikasi ini mampu mencatat kode-kode apa saja yang diketikkan pada *keyboard*. Sehingga dapat diketahui *password* yang diketikkan oleh pengguna sistem.

II. PENELITIAN TERKAIT

Banyak solusi yang telah diterapkan untuk mencegah terjadinya pencurian *id* dan *password*, salah satunya rekomendasi dari Javelin Strategies & Research antara lain (1) *update firewall, antivirus* dan *antispyware*, (2) kenali dan gunakan web yang terpercaya, (3) hati-hati terhadap lampiran pada *email*, dan (4) cari tahu bagaimana membuat *password* yang aman dan tidak mudah ditebak.

Ada dua jenis metode otentikasi menggunakan *one-time password*, yaitu *password-generating token device* dan *non-hardware one-time password*.

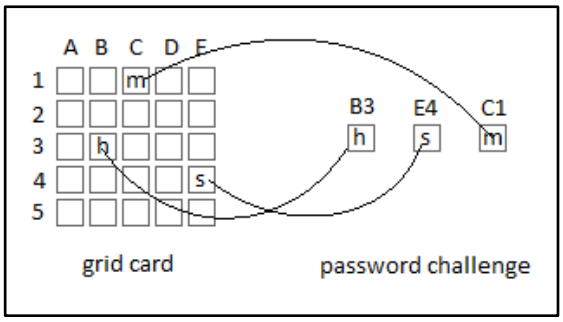
Password-generating token device telah diproduksi oleh berbagai manufaktur antara lain RSA Security (www.rsasecurity.com), VeriSign (www.verisign.com) dan ActivIdentity (www.actividentity.com). Salah satu produknya adalah RSA SecurID.

III. GRID CARD

Grid card atau *scratch card* merupakan versi lain dari *one-time password* dalam bentuk kartu. Pada umumnya kartu tersebut terdiri dari karakter angka dan huruf yang disusun dalam bentuk kolom dan baris atau *grid* [**2**].

Grid card termasuk unsur *something a user has*. Namun pada implementasinya digabungkan dengan *username* dan *password* (*something a user knows*) sehingga termasuk ke dalam *multi-factor authentication*[**2**].

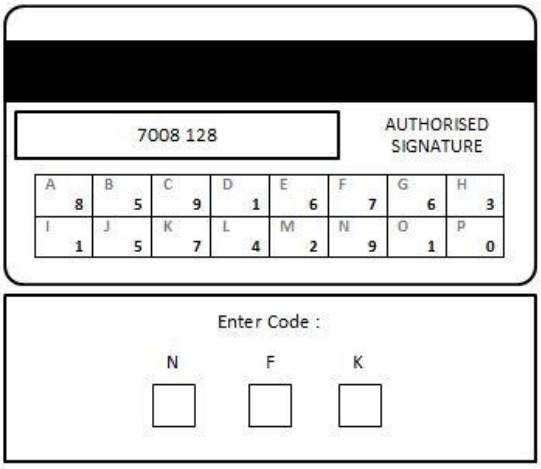
Pada saat proses otentikasi, sistem akan meminta pengguna untuk memasukkan kode yang terdapat pada beberapa sel tertentu secara acak. Penamaan sel berdasarkan label kolom dan diikuti oleh label baris.



Gambar 1. Cara kerja grid card

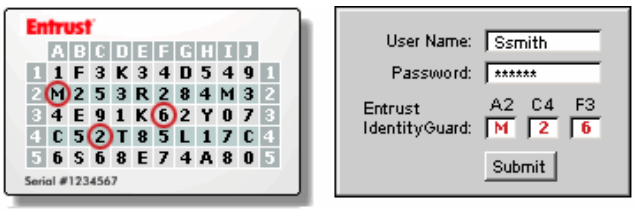
Ada beberapa model *grid card*, antara lain pada kartu kredit/debet sebagai tambahan untuk melakukan transaksi secara *online*. Beberapa bank menyertakan

kode dalam bentuk *grid* pada kartu kredit/debet yang dikeluarkan, sebagai contoh ICICI Bank. Masing-masing pengguna memiliki kombinasi kode yang berbeda satu sama lainnya. Kode tersebut akan diminta pada saat melakukan transaksi keuangan secara *online*. Pada ICICI Bank, *grid card* tersebut digunakan untuk melakukan aktifasi layanan.



Gambar 2. Grid card pada kartu debit/kredit [6]

Selain pada kartu kredit/debet, beberapa bank memang menggunakan kode berbentuk *grid* sebagai otentikasi tambahan untuk melakukan transaksi keuangan. Penyedia jasa keamanan Entrust menggunakan *grid card* dengan ukuran 10x5 yang disebut Entrust IdentityGuard. Setiap kali proses otentikasi menggunakan Entrust IdentityGuard, sistem akan meminta 3 kode secara acak yang terdapat pada grid card pengguna [**7**].



Gambar 3. Grid card dari Entrust [8]

Penelitian tentang otentikasi sangat banyak, ini dikarenakan model-model otentikasi yang sangat bervariatif. Namun, penelitian yang khusus membahas tentang otentikasi menggunakan *grid card* antara lain [**6**] yang memanfaatkan *model hidden Markov* untuk mendeteksi pola transaksi yang mencurigakan. Tentu fokus penelitian tersebut tidak pada model *grid card* nya, tetapi pada proses otentikasi dan pendeteksian dini terhadap transaksi yang mencurigakan.

Penelitian lainnya yaitu [**9**] yang membuat *password* dalam bentuk gambar. Teknik ini memanfaatkan perangkat USB untuk menyimpan algoritma enkripsi yang akan digunakan untuk proses otentikasi. *Password* yang dibentuk akan disimpan pada sebuah *image* dengan posisi tertentu. Penelitian ini juga tidak terlalu berkaitan dengan *grid card*.

IV. HASIL

Penambahan faktor otentikasi pada sebuah proses otentikasi harus mempertimbangkan segi kemudahannya serta biaya. *Grid card* merupakan salah satu solusi terbaik untuk faktor kedua pada proses otentikasi. Terbaik disini dinilai bukan hanya dari segi kemudahannya saja, namun juga mempertimbangkan segi biaya pengadaan dan perawatan. Jika dibandingkan dengan *fingerprint*dan alat pemindai lainnya yang cenderung mahal dari segi biaya, juga tidak dapat ditempatkan di semua tempat di mana saja. *Fingerprint* hanya bisa dipasang pada perangkat sistem yang menetap seperti absensi pegawai yang ditempatkan pada tempat tertentu. Sehingga untuk otentikasi pada sistem berbasis web yang bisa diakses dari mana saja tidak cocok.

Namun, *grid card* ini juga memiliki keterbatasan pada penggunaannya. Sebuah *grid card* hanya bisa digunakan beberapa kali tergantung jumlah sel yang dimiliki dan jumlah *password challenge* yang diminta oleh sistem. Apabila sebuah sel pada *grid card* diminta lebih dari satu kali oleh sistem pada saat otentikasi, akan menimbulkan resiko untuk dicuri dan digunakan kembali. Keterbatasan penggunaan kode pada *grid card* biasanya dipecahkan dengan menambahkan jumlah sel pada *grid card*. Cara ini sudah banyak digunakan oleh beberapa pengembang, namun tetap dinilai masih belum efektif.

V. PENELITIAN SELANJUTNYA

Penelitian yang sedang dikembangkan saat ini adalah mencari teknik untuk menggunakan kode pada sebuah sel lebih dari satu kali, sehingga jumlah sel pada *grid card* yang kecil mampu digunakan dengan jumlah yang jauh lebih banyak. Mekanisme yang diteliti bukan hanya bagaimana menggunakan sebuah sel pada lebih dari satu kali, namun juga bagaimana membangkitkan kombinasi

passwordchallenge agar kombinasi yang dihasilkan tidak menyebabkan resiko pencurian data otentikasi.

VI. REFERENSI

[1] William E. Burr et al., *Electronic Authentication Guideline*.: National Institute of Standards and Technology, 2011.

[2] Federal Financial Institutions Examination Council, *Authentication in an Internet Banking Environment*.: Federal Financial Institutions Examination Council, 2005.

[3] Danah Boyd and Eszter Hargittai, "Facebook Privacy Settings: Who cares?," *First Monday*, vol. 15, Agustus 2010.

[4] Javeline Strategies & Research, "2012 Identity Fraud Report: Consumers Taking Control to Reduce their Risk of Fraud," Javeline Strategies & Research, Pleasanton, 2012.

[5] Anti-Phising Work-Group, "Phising Activity Trend Report 1st Half 2011," 2011.

[6] Nayani Sateesh, "An Approach For Grid Based Authentication Mechanism To Counter Cyber Frauds With Reference To Credit Card Payments," *Global Journal of Computer Science and Technology*, pp. 59-61, 2011.

[7] Entrust, *Securing What's at Risk: A Common Sense Approach to Strong Authentication*.: Entrust, 2005.

[8] Gregory D. Williamson, "Enhanced Authentication In Online Banking," *Journal of Economic Crime Management*, 2006.

[9] John Charles Gyorffy, Andrew F. Tappenden, and James Miller, "Token-based graphical password authentication," *International Jurnal of Information Security: Springer*, no. 10, pp. 321-336, Oktober 2011.

[10] Alain Hiltgen, Thorsten Kramp, and Thomas Weigold, "Secure Internet Banking Authentication," *IEEE Security and Privacy*, pp. 24-32, 2005.