Teknik-teknik Kriptografi untuk Menangkal Praktek Phishing

Imam Habibi, Keeghi Renandy, Yohanes Seandy Sunjoko

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if12042@students.if.itb.ac.id, if12026@students.if.itb.ac.id , if12038@students.if.itb.ac.id

Abstraksi

Dalam kegiatan berbisnis secara elektronik yang dikenal dengan nama *e-commerce,* aspek keamanan menjadi sebuah hal yang penting. Praktek-praktek kecurangan seperti *phishing* kerap terjadi. Pada makalah ini dipaparkan teknik-teknik yang dapat digunakan untuk menangkal praktek tersebut sehingga tingkat keamanan pengguna jaringan komputer terjaga dengan baik. Teknik-teknik tersebut adalah *strong website authentication*, *mail server authentication*, *mail authentication via digital signature.* Pada makalah ini dikemukakan pula keuntungan dan kerugian dari setiap teknik.

Kata kunci: authentication, phishing, digital signature.

1. Pendahuluan

Perkembangan teknologi informasi pada abad ke-21 ini telah memberikan kepraktisan bagi masyarakat modern untuk melakukan berbagai kegiatan komunikasi secara elektronik, salah satunya dalam bidang bisnis seperti perdagangan dan perbankan. Kegiatan berbisnis secara elektronik ini dikenal dengan nama *e-commerce*. Dengan teknologi informasi, khususnya dengan jaringan komputer yang luas seperti Internet, barang dan jasa dapat dipromosikan secara luas dalam skala global. Kepada calon konsumen pun diberikan pula kemudahan-kemudahan yang memungkinkan mereka mengakses dan membeli produk dan jasa yang dimaksud secara praktis, misalnya pelayanan kartu kredit.

Perkembangan ini rupanya membawa serta dampak negatif dalam hal keamanan. Praktek-praktek kejahatan dalam jaringan komputer kerap terjadi dan meresahkan masyarakat, misalnya pencurian sandi lewat dan nomor rahasia kartu kredit. Akibat dari hal seperti ini, aspek keamanan dalam penggunaan jaringan komputer menjadi hal yang krusial.

Kriptografi hadir untuk menjawab tantangan tersebut. Kriptografi merupakan sebuah ilmu dan seni yang bertujuan untuk menjaga kerahasiaan dan keamanan dari pesan. Yang dimaksud dengan kerahasiaan adalah bahwa pesan yang hendak dikirim disandikan terlebih dahulu ke dalam suatu bentuk yang tidak bermakna. Yang dimaksud dengan keamanan adalah bahwa

dalam hal penyampaian pesan dari pengirim kepada penerima, perlu diperhatikan keaslian pengguna, keaslian pesan, dan ketiadaan penyangkalan dari pengirim.

Pada makalah ini dipaparkan teknik-teknik kriptografi yang dapat digunakan untuk menangkal satu jenis kejahatan yang belakangan sering terjadi dalam dunia maya, yaitu *phishing*. Pemaparan tersebut mencakup pula keuntungan dan kerugian dari setiap teknik. Teknik-teknik tersebut adalah:

1. *strong website authentication*
2. *mail server authentication*
3. *mail authentication via digital signature*

2. Phishing

Menurut definisi dalam [1], *phishing* adalah usaha untuk mendapatkan suatu informasi penting, misalnya sandi lewat atau informasi kartu kredit, dengan cara memanfaatkan seseorang atau sebuah perusahaan bisnis yang sudah dikenal dan dipercaya oleh masyarakat, seperti bank, online retailer, dan perusahaan penerbit kartu kredit ternama. Sarana yang umumnya digunakan adalah pesan elektronik, pesan instan, dan situs jaringan palsu. Melalui sarana tersebut korban dikendalikan untuk menyerahkan informasi-informasi rahasia yang diinginkan. Karena itu, *phising* tergolong dalam bentuk *social engineering*. Nama ini sebetulnya merupakan akronim dari sebuah jargon, yaitu *password harvesting fishing*.

Serangan *phishing* menggunakan penipuan *e-mail* untuk memikat penerimanya menuju situs jaringan yang tidak benar. Penipuan *e-mail* merupakan teknik yang memanfaatkan pengubahan metadata/*header* email melalui protokol SMTP (*simple mail transfer protocol*) sehingga pengirim dapat memalsukan identitas dirinya menjadi pihak lain yang dikenal oleh penerima.

Masalah utama terjadinya praktek *phishing* adalah ketiadaan pemeriksaan asal *e-mail*. SMTP (*Simple Mail Transfer Protocol*) mengizinkan mengisi isian FROM dengan alamat apapun, sehingga *phishers* dapat memanfaatkannya untuk memperdaya penerima *e-mail* [1].

Celakanya, sebesar 5% dari seluruh target *phishing* menanggapi penipuan *e-mail* ini. Akibatnya, banyak pengguna menderita berbagai kerugian berupa pemakaian kartu kredit oleh pihak yang tidak bertanggung jawab, pencurian indentitas, dan kerugian lainnya.

Di samping itu, pengguna jasa *e-commerce* juga merasa dirugikan oleh pihak perusahaan yang tidak dapat melakukan suatu tindakan pencegahan terhadap tindakan *phishing*. Mereka menuntut perusahaan tersebut untuk memakai teknologi baru yang dapat menjamin keaslian *e-mail* dan situs jaringan.

Statistik berikut menyatakan persentase pemasangan situs jaringan yang melakukan *phising* di berbagai belahan dunia [2]:

1.	Amerika Serikat	35.0 %
2.	Korea Selatan	16.0 %
3.	RRC	15.0 %
4.	Rusia	7.0 %
5.	Inggris	5.5 %
6.	Meksiko	4.5 %
7.	Taiwan	2.5 %

Kerugian akibat *phising* meningkat setiap tahunnya dan hal ini perlu ditangani secara serius. Terlebih lagi, bank dan pihak penerbit kartu kredit di Amerika Serikat

menderita kerugian dengan jumlah mendekati 1.2 milyar dolar pada tahun 2003 akibat *phishing* [1].

3. Persyaratan Teknik untuk Menangkal Phishing

Teknik-teknik yang digunakan untuk menangkal masalah *phishing* ini pada dasarnya harus memenuhi persyaratan berikut ini [3]:

1. Teknik tersebut harus mampu mengautentikasi alamat *e-mail* yang tercantum pada isian FROM.

2. Teknik tersebut tidak memerlukan banyak pelatihan kepada pengguna. Pengalaman membuktikan bahwa pelatihan kepada pengguna tidak begitu efektif. Alasannya adalah bahwa pengguna umumnya merasa bahwa *phishing* dapat dihindari cukup dengan menganalisis isi *e-mail*. Pembelajaran terhadap teknik baru dirasakan cukup membebani pengguna.

3. Teknik tersebut harus dapat diterapkan pada teknologi yang sudah ada dan sudah distandarkan oleh badan global, misalnya pada SMTP.

4. Teknik yang dimanfaatkan harus efektif secara biaya bagi pengirim, penerima, maupun penyedia infrastruktur Internet.

4. Strong Website Authentication

Teknik ini menggunakan suatu mekanisme yang mengautentikasi setiap pengguna yang mengunjugi situs jaringan melalui dua tahapan. Tahap pertama dapat berupa permintaan akun nama pengguna dan sandi lewat, sedangkan tahap kedua berupa proses *challenging* dari pihak *server* kepada *client* seperti pada *smart card*. Teknologi ini berusaha untuk membatasi/mengurangi proses pelatihan bagi pihak pengguna [2].

Keuntungan dari teknik ini adalah :

1. *Phisher* tidak dapat masuk ke dalam situs jaringan *e-commerce* tanpa objek autentikasi secara fisik seperti *smart card* walaupun informasi pengguna telah diperoleh melalui praktek *phishing*.

2. Pengguna mendapatkan jaminan keamanan utuh untuk melakukan transaksi pada situs jaringan *e-commerce*

Kerugian dari teknik ini adalah :

1. Proses yang dilakukan memakan waktu yang lebih lama (*time delay*)

2. Pada komputer pengguna perlu diinstalasi suatu perangkat lunak *desktop* demi kepentingan autentikasi tahap kedua tersebut.

3. Diperlukan biaya manajemen yang tinggi dari pengembang dan penyedia jasa *e-commerce.*

4. Dibutuhkan biaya yang besar yang harus dikeluarkan oleh setiap pengguna.

5. Pengguna diwajibkan membawa serta *smart card* tersebut setiap kali transaksi hendak dilakukan.

5. Mail Server Authentication

Teknik ini merupakan peningkatan kemampuan dari DNS (*Domain Name System*) *server* dengan melakukan pemeriksaan dan verifikasi alamat IP (*Internet Protocol*) *server* pengirim *e-mail* [2] [3].

Keuntungan dari teknik ini adalah :

1. *Server* pengirim *e-mail* mudah dikonfigurasi agar dapat menggunakan teknik ini.

2. Pihak *phisher* sulit mengirim *e-mail* sebagai *anonymous user* karena domain yang hendak dipakai untuk mengirim *e-mail* harus sesuai dengan IP *server* yang digunakan.

3. *E-mail* dari perusahaan yang sah dapat dengan mudah diidentifikasi sehingga dapat dicegah kemungkinan adanya tindakan *spamming*.

Kerugian dari teknik ini adalah :

1. Diperlukan adanya *sender* dan *recepient gateway*.

2. SMTP pengirim tetap tidak terlihat pada penerima. Alamat *e-mail* pada isian FROM masih dapat disamarkan.

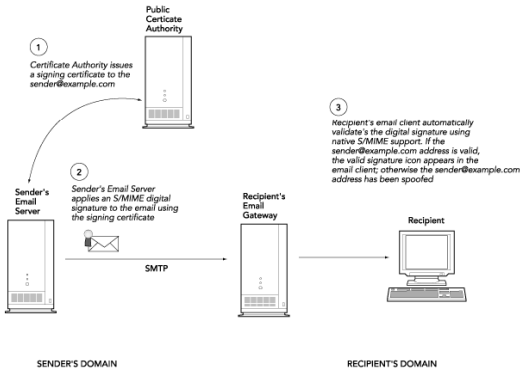
3. Terdapat masalah kompatibilitas bagi pengguna yang memakai fasilitas *e-mail* dari pihak ketiga.

4. Kebutuhan *e-mail forwarding* tidak dapat diakomodasi.

6. Mail Authentication via Digital Signature

Teknik ini menggunakan tanda tangan digital S/MIME untuk memastikan bahwa *e-mail* yang dikirim telah diverifikasi oleh penerimanya pada *gateway* atau *e-mail client* [2] [3].

S/MIME menggunakan teknik kriptografi asimetri untuk mengautentikasi pengirim dan menyediakan semantik tanda tangan digital yang cukup kuat.



Gambar 1. Mail Authentication via Digital Signature

Berikut ini adalah langkah-langkah autentikasi e-mail melalui tanda tangan digital S/MIME:

1. Pihak yang berwenang dalam hal sertifikasi publik (contohnya VeriSign, Thawte, GlobalSign, dsb) menerbitkan sertifikat digital bagi alamat *e-mail* tersebut.

2. E-mail yang dikirimkan melalui alamat yang telah disertifikasi akan dibubuhkan tanda tangan digital dengan kunci privat. Tanda tangan digital ini menyediakan sebuah cara untuk membuktikan keabsahan alamat *e-mail* pada isian FROM.

3. Penerima e-mail yang dilengkapi dengan fitur S/MIME memvalidasi tanda tangan digital tersebut. Jika tanda tangan tersebut valid, alamat *e-mail* pada isian FROM dinyatakan sah dan penerima dapat mempercayai isi *e-mail* tersebut.

Keuntungan dari teknik ini adalah :

1. Teknik ini dapat dijalankan tanpa membutuhkan instalasi software tambahan

2. Alamat FROM tidak mungkin dapat disamarkan karena selalu dilakukan validasi tanda tangan digital.

3. *Phisher* harus terdaftar dan memiliki *certificate authority* untuk bisa mengirim *phishing e-mail*. Akan tetapi hal tersebut tidak akan bermanfaat karena identitas dapat dilacak dan diaudit sehingga mudah dituntut ke pengadilan

4. *E-mail* dari perusahaan legitimasi dapat dengan mudah diidentifikasi oleh pihak *end-user*

Kerugian dari teknik ini adalah :

1. Tidak semua *e-mail client* mendukung teknologi S/MIME

2. Terdapat kemungkinan bahwa penerima *e-mail* tidak memeriksa *certificate revocation status*.

3. Teknik ini menuntut biaya yang cukup tinggi bagi pengguna.

4. Harus ada informasi tentang tanda tangan digital pada *gateway* dari pihak pengirim dan penerima.

7. Kesimpulan

Hingga saat ini belum ada satu metode yang bebas dari kelemahan untuk menangkal praktek *phishing*. Teknik *strong website authentication* menyediakan tingkat autentikasi yang tinggi, tetapi tidak memberikan kepraktisan bagi pengguna. Teknik *mail server authentication* memeriksa domain pengirim, tetapi tidak mengautentikasi isian FROM dan tidak mengakomodasi *e-mail forwarding*. Teknik *mail authentication via digital signature* sebetulnya mengakomodasi secara baik autentikasi alamat e-mail dan pencegahan praktek *phishing* dan *spamming*, namun tidak efektif dari segi biaya yang diperlukan. Dari segi kepraktisan bagi

pengguna pada umumnya, *mail server authentication* adalah teknik yang disarankan. Walaupun demikian, pengguna yang mengandalkan teknik ini tetap perlu memeriksa keabsahan dari isi *e-mail*.

8. Referensi

[1] http://en.wikipedia.org/wiki/Phishing, diakses pada tanggal 4 Januari 2006 pukul 10.00
[2] http://www.antiphishing.org/, diakses pada tanggal 6 Januari 2006 pukul 12.00
[3] http://www.itpapers.com/whitepaper.aspx?scname=Digital+Signatures&docid=130185, diakses pada tanggal 31 Desember 2005 pukul 18.00