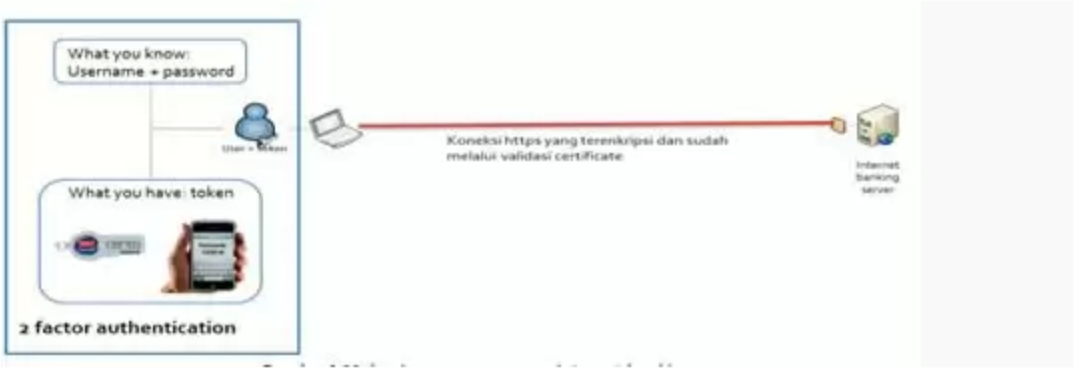
Memoles e-Banking Guna Menangkal Serangan Sinkronisasi Token

Posted by Detik | Date: April 14, 2015 | Leave a comment | 16 Views



Jakarta – Pada awal tahun 2015, dunia perbankan di Indonesia diresahkan serangan *cyber fraud* yang menyasar layanan internet banking beberapa bank papan atas. Metode serangannya cukup unik, yaitu mengintervensi proses transaksi internet banking yang tengah berlangsung. Nasabah yang sedang melakukan transaksi diminta mengentri token berulang kali, melalui pop-up window yang meminta sinkronisasi token.

Setelah menjalankan perintah pop-up window ini, seorang korban dilaporkan mendapati rekeningnya terdebit sebesar Rp 13 juta karena terjadi transfer secara tidak sah ke tujuan rekening yang tidak dikenalnya. Mengenai jumlah korban, pihak BCA sempat menyebutkan adanya seribu nasabah yang menjadi korban serangan ini (sumber: 1.000 Nasabah Terkena “Sinkronisasi Token”, kompas online, 6/3/15), yang kemudian diralat menjadi hanya 43 nasabah. (sumber: Hanya 43 Nasabah yang Terkena “Sinkronisasi Token”, kompas online, 6/3/15). Selain BCA, nasabah Bank Mandiri juga menjadi korban dari serangan ini. (sumber: Nasabah Mandiri juga Terkena Malware Pencuri Uang, CNN Indonesia Online, 6/3/15).

Sangat menarik dikaji, celah rawan apakah dalam sistem internet banking yang berhasil dieksploitasi penyerang. Pihak BCA menyatakan, serangan dapat terjadi karena nasabah menggunakan personal computer (PC) yang sudah terinfeksi virus. Pun demikian, sistem token sendiri dinyatakan tetap aman. Sebagai respons kasus ini, Otoritas Jasa Keuangan (OJK) telah meminta bank mengaudit ulang pengamanan IT untuk fasilitas internet banking, menyusul maraknya kasus pembobolan rekening nasabah akibat mengakses fasilitas tersebut.

Bank sebagai penyedia layanan telah menerapkan langkah mitigasi menurunkan risiko berulangnya insiden serangan di atas. Ini terutama dilakukan dengan memberikan sejumlah tips, yang ditampilkan dalam halaman web internet banking, agar nasabah memastikan keamanan transaksi internet banking dengan cara; (1) membersihkan personal computer yang digunakan dari infeksi virus, (2) menghentikan transaksi ketika muncul permintaan sinkronisasi token dan segera

melaporkan kejadian tersebut kepada customer service, dan (3) memeriksa bahwa alamat web internet banking adalah alamat yang benar.

Imbauan dan sosialisasi tips pengamanan tersebut sudah baik, mengingat tingkat pemahaman dan kepedulian pengguna merupakan faktor kunci dalam keamanan internet banking. Namun demikian, jelas efektifitas upaya mitigasi tersebut sangat bergantung kemampuan nasabah memahami dan juga menjalankan berbagai tips yang disampaikan pihak bank.

Dengan memperhatikan hambatan-hambatan di atas, penulis memperkirakan masih terdapat peluang kegagalan yang signifikan dari langkah mitigasi yang sudah dijalankan. Bank masih perlu memikirkan strategi mitigasi lain yang tidak hanya bergantung pada kapabilitas dan kepatuhan nasabah.

Secara internal, di mata penulis, bank perlu melakukan analisis dan mencari solusi terhadap serangan internet banking yang telah terjadi, antara lain mencakup: Mengidentifikasi (a) titik kerawanan yang mana yang berhasil dieksploitasi penyerang dan juga (b) mekanisme keamanan yang mana yang berhasil dipatahkan atau tidak berjalan dengan efektif?. Mengidentifikasi skenario dasar serangan yang ada dan mengkaji berbagai alternatif kemungkinan serangan yang dapat dibangun berdasarkan skenario dasar tersebut, dan merumuskan alternatif solusi perbaikan keamananan sistem internet banking yang dapat menangkal skenario dasar serangan di atas.

(ash/ash)

Artikel ini selanjutnya akan membahas langkah-langkah di atas dengan maksud membantu institusi perbankan dan juga regulator mencegah terjadinya serangan serupa di masa datang.

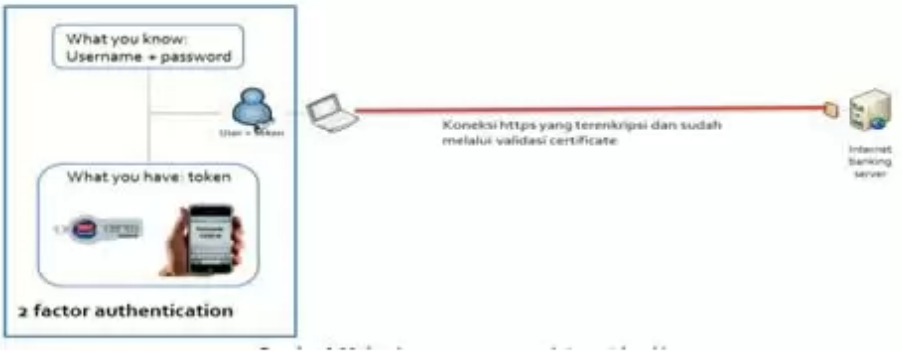
Prinsip Dasar *Security*

Untuk mengambil pelajaran dari kasus serangan yang sudah terjadi, kita perlu mengingat kembali salah satu prinsip dasar menganalisis keamanan sistem teknologi informasi, yaitu keamanan total suatu sistem dapat dipandang sebagai sebuah rantai yang dibentuk sekumpulan mata-rantai yang saling berhubungan. Untuk mematahkan keamanan, penyerang cukup mencari dan memutuskan mata-rantai yang paling lemah.

Metode serangan sinkronisasi token yang terjadi sepenuhnya sejalan prinsip di atas. Penyerang mengarahkan serangannya ke titik paling lemah dari rangkaian keamanan, yakni pengguna serta perangkat (PC, tablet) dan juga lingkungan di sisi pengguna. Serangan ini memiliki aspek teknis, yakni penggunaan malware ataupun tool serangan lainnya, dan sekaligus aspek social engineering, yakni strategi mengecoh pengguna.

Dalam kondisi normal, sistem internet banking telah memiliki beberapa mekanisme pengamanan yang merealisasikan kriteria keamanan sebagai berikut:
1. Otentikasi server internet banking.

Pengguna, melalui personal computer (PC) yang digunakannya, harus dapat memastikan bahwa server internet banking yang dituju adalah benar-benar server yang valid.
2. Enkripsi komunikasi antara PC dan server.
Komunikasi antara PC pengguna dan server internet banking harus dijamin kerahasiaannya sehingga harus terenkripsi, dan
3. Otentikasi pengguna.
Server internet banking harus dapat memastikan bahwa pengguna yang menggunakan layanan adalah benar-benar pengguna internet banking yang sah.
Kriteria (1) dan (2) dipenuhi dengan menerapkan protokol HTTPS. Dalam protokol ini, pertama-tama, PC pengguna mengotentikasi server internet banking dengan cara memeriksa digital certificate-nya. Lalu, PC dan server membentuk jalur komunikasi yang terenkripsi untuk menjaga kerahasiaan data.

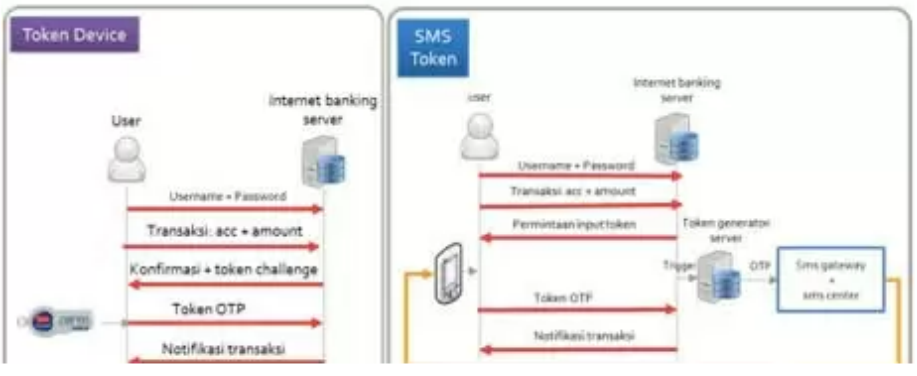


Gambar 1: Mekanisme pengamanan internet banking

Kriteria keamanan (3) direalisasikan dengan menggunakan *two-factor-authentication* yang terdiri dari faktor *what-you-know* dan *what-you-have*. Untuk faktor *what-you-know*, pengguna harus mengetahui dan memasukkan username dan password ke halaman login internet banking. Untuk faktor *what-you-have*, pengguna harus memasukkan password-token-sekali-pakai (token *one time password*, token-OTP) yang diminta.

(ash/ash)

Token-OTP ini sampai ke tangan pengguna dengan dua cara, yaitu (1) menggunakan token-device yang dapat membangkitkan token-OTP atau (2) menerima token-OTP dari Bank melalui SMS yang dikirim ke ponsel pengguna.
Gambar 1 memperlihatkan mekanisme pengamanan utama layanan internet banking. Gambar 2 memperlihatkan dua alternatif protokol keamanan untuk dua jenis sistem token, yaitu token-device dan SMS-token.



Gambar 2: Protokol keamanan internet banking untuk kasus token-device dan SMS-token.

Untuk melakukan login ke halaman internet banking, pengguna hanya perlu memasukkan username dan password yang merupakan faktor otentikasi what-you-know. Untuk melakukan berbagai jenis transaksi (pembayaran, transfer dll), pengguna memerlukan faktor otentikasi tambahan yakni token password yang merupakan faktor otentikasi *what-you-have*.

Username dan password dapat digunakan secara berulang untuk melakukan login sedangkan token-OTP hanya dapat digunakan untuk satu kali transaksi. Untuk transaksi berikutnya, pengguna harus membangkitkan kembali token-OTP (atau mendapatkan token-OTP yang baru melalui SMS).

Serangan sinkronisasi token yang terjadi baru-baru ini tidak secara langsung mematahkan berbagai mekanisme keamanan yang dijelaskan di atas. Yang terjadi adalah, serangan tersebut mencegah mekanisme pengamanan bekerja sebelum mekanisme tersebut berfungsi. Mengapa demikian?

Hingga saat ini, protokol HTTPS masih sangat aman digunakan untuk mengotentikasi server serta mengamankan jalur komunikasi antara klien dan server. Protokol ini menggunakan algoritma enkripsi standar yang kuat dan dijamin keamanannya. Kondisi yang sama juga berlaku pada mekanisme pengamanan token-OTP.

Mekanisme ini masih sangat aman karena token dibangkitkan dengan menggunakan algoritma kriptografi standar yang aman. Kelemahan yang ditemukan saat ini, baik untuk HTTPS ataupun sistem token, adalah kelemahan yang masih bersifat teoritis. Secara praktis, keduanya masih sangat aman untuk digunakan.

Jika dua mekanisme pengamanan (HTTPS dan sistem token) tersebut masih aman, lalu bagaimana penyerang dapat melakukan transaksi dengan menggunakan akun pengguna yang sah?

(ash/ash)

Pola Serangan Sinkronisasi Token

Dalam kasus serangan sinkronisasi token, penyerang dapat melakukan transaksi transfer dari rekening milik nasabah yang sah ke tujuan rekening yang dikehendakinya. Ini berarti penyerang dapat mengakses layanan internet banking dan bertindak seolah-olah sebagai nasabah yang sah. Bagaimana ini bisa terjadi? Untuk ini, penyerang harus mencuri seluruh faktor otentikasi pengguna, yaitu username, password dan token-OTP.

Dalam protokol internet banking, otentikasi terhadap pengguna dilakukan setelah

koneksi HTTPS terbentuk. Karena protokol HTTPS ini mengenkripsi data yang dipertukarkan antara PC pengguna dan server internet banking, maka penyerang tidak dapat mencuri username, password ataupun token-OTP dengan cara melakukan intercept terhadap komunikasi data yang sedang berlangsung.

Namun demikian, penyerang masih mungkin mencuri username, password ataupun token-OTP (selanjutnya kita sebut credential) dengan cara seperti menanamkan malware-keylogger ke PC pengguna. Keylogger ini akan mengintip dan merekam pengetikan credential dan kemudian mengirimkannya kepada penyerang. Keylogger ini berjalan di PC pengguna yang tidak terlindung oleh protokol HTTPS.

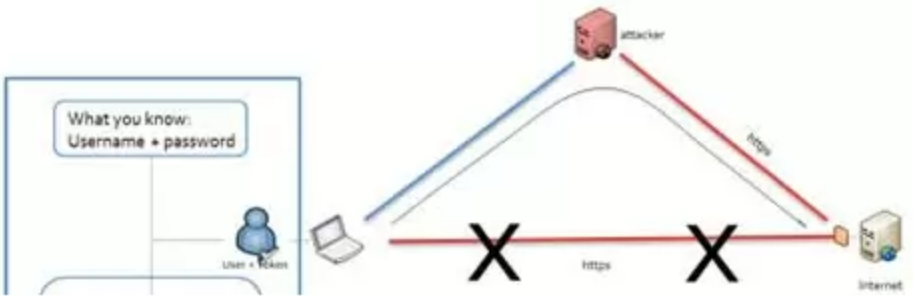
Atau cara *shoulder sniffing*, yaitu mengintip secara visual (atau menggunakan kamera) pengetikan credential yang dilakukan oleh pengguna, juga mencegah terbentuknya protokol HTTPS dan dengan demikian penyerang dapat mencuri credential pengguna dengan melakukan intercept terhadap paket data yang dikirimkan oleh PC pengguna.

Sekali penyerang berhasil mencuri username dan password, maka ia dapat menggunakannya kapanpun untuk melakukan login ke halaman internet banking sepanjang pengguna tidak mengubah username dan password tersebut. Kasus token-OTP sangat berbeda. Token-OTP ini hanya berlaku untuk satu transaksi saja, sehingga penyerang tidak dapat menggunakannya untuk mengeksekusi transaksi yang lain. Token-OTP yang valid adalah token-OTP yang dibangkitkan at-the-moment oleh pengguna dengan menggunakan device token pada saat pengguna melakukan transaksi (atau yang dikirimkan at the moment juga pada saat transaksi berlangsung).

Konsekuensinya adalah, untuk dapat melakukan transaksi atas nama pengguna yang sah, penyerang harus memiliki kendali terhadap token-device yang dipegang oleh pengguna yang sah. Teknik serangan yang memungkinkan hal tersebut terjadi adalah tipe serangan man-in-the-middle-attack (MITM). Dalam teknik ini, penyerang harus dapat melakukan *intercept*, modifikasi, membuat pesan baru, dan juga me-*replay* pesan.

(ash/ash)

Karena protokol HTTPS dirancang untuk menangkal serangan MITM, maka penyerang harus melancarkan serangan MITM sebelum protokol HTTPS antara PC-pengguna dan server internet banking terlaksana. Gambar 3 memperlihatkan apa yang dilakukan oleh penyerang yaitu mencegah berjalannya protokol HTTPS dan kemudian melakukan MITM.



Gambar 3: Penyerang mencegah terlaksananya protokol HTTPS dan kemudian melakukan serangan MITM.

Seperti yang sudah dijelaskan di bagian sebelumnya, serangan sinkronisasi token ini tidak mematahkan mekanisme keamanan internet banking, namun ia hanya mencegah mekanisme tersebut bekerja sejak dari awal. Prinsipnya adalah, penyerang sejak awal akan membelokkan (*redirect*) paket data dari PC pengguna untuk berkoneksi dengan server/PC penyerang dan bukan berkoneksi dengan server internet banking. Setelah itu, penyerang akan melanjutkan dengan serangan MITM. Pembelokan paket data ini dapat dilakukan dengan berbagai cara, di antaranya adalah:

1. Menanamkan tool di dalam proxy server

Ini dapat dilakukan jika koneksi internet harus melalui proxi server. Penyerang akan menggunakan proxy server sebagai sarana untuk melakukan MITM. Tool yang tertanam dalam proxy server akan bertindak sebagai *man-in-the-middle*.

2. Menyerang DNS server (DNS Poisoning)

Serangan ini akan me-redirect permintaan koneksi ke alamat web internet banking yang valid ke arah server/PC penyerang.Serangan ini dapat dilakukan terhadap DNS server di lingkungan perusahaan. Serangan mungkin juga dilakukan terhadap DNS server yang dijalankan oleh ISP. Selanjutnya, server penyerang akan berfungsi sebagai *man-in-the-middle*.

3. Memodifikasi perangkat user (PC, smartphone, tablet).

Penyerang akan mengubah file system tertentu dalam perangkat pengguna untuk me-redirect alamat web internet banking valid yang diketikkan oleh user ke server attacker. Serangan jenis ini dapat dieksekusi dengan dua cara; (a) mengakses perangkat pengguna secara fisik dan kemudian memodifikasi perangkat tersebut, dan (b) menggunakan virus untuk memodifikasi perangkat pengguna. Selanjutnya, server penyerang akan berfungsi sebagai *man-in-the-middle*.

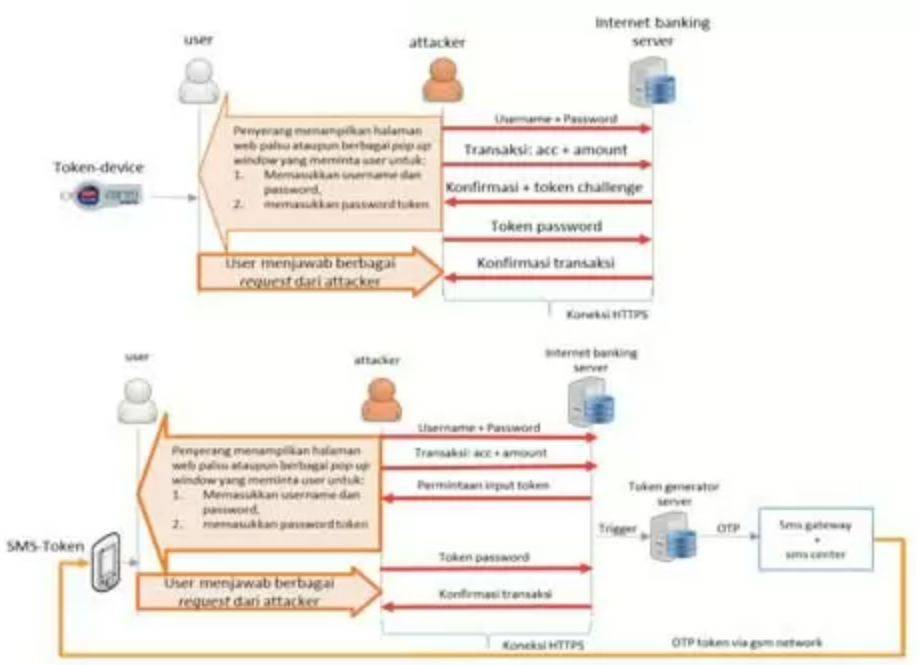
Setelah berhasil menempatkan dirinya di antara PC pengguna dan server internet banking (sebagai *man-in-the-middle*), penyerang selanjutnya akan melakukan prosedur transaksi internet banking atas nama pengguna dengan cara memintausername, password dan token-OTP kepada pengguna ketika diperlukan.

Penyerang berinteraksi dengan pengguna melalui tampilan halaman web internet banking palsu yang dibuat sedemikian rupa, sehingga pengguna tidak menyadari bahwa koneksi layanan internet banking yang dia lakukan sedang diintervensi oleh penyerang. Gambar 4 menunjukkan bagaimana penyerang dapat melakukan langkah-langkah transaksi normal atas nama pengguna yang sah dengan menggunakan credential milik pengguna. Berikut ini adalah langkah-langkah yang dilakukan oleh penyerang:

1.Penyerang mencegah protokol HTTPS berjalan dan kemudian melakukan MITM.
2. Berikutnya, penyerang mencuri username dan password dengan cara meminta pengguna untuk memasukkan keduanya ke halaman login internet banking palsu

yang dibuat semirip mungkin dengan halaman yang asli.
3. Berbekal username dan password ini, penyerang melakukan login ke halaman internet banking.
4. Penyerang terus berinteraksi dengan pengguna dengan teknik social engineering sedemikian rupa sehingga pengguna tidak menyadari bahwa ia sebenarnya sedang berkomunikasi dengan penyerang, bukan dengan server internet banking.
5. Melalui interaksi ini, penyerang kemudian melakukan transaksi ilegal atas nama pengguna. Untuk otentikasi token, penyerang dapat meminta token-OTP kepada pengguna dengan menampilkan halaman palsu untuk me-request atau melakukan challenge-and-response token-OTP. Dalam kasus serangan baru-baru ini, penyerang menggunakan pop-up window sinkronisasi token untuk meminta token-OTP dari pengguna.

Lantas seperti apa solusi penangkalannya? Ikuti di bagian artikel kedua.



Gambar 4: Serangan MITM terhadap protokol keamanan internet banking.

**) Penulis, Dr. Budi Sulistyo CISA adalah Security Expert dari Lembaga Riset Telematika Sharing Vision, Bandung. Dapat dihubungi pada surel di budi@sharingvision.biz.*