JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 11 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 *DOI: https://doi.org/10.23960/ jitet.v11i3.3312*

ANALISIS SERANGAN MALWARE DALAM PERBANKAN DAN PERENCANAAN SOLUSI KEAMANAN

Kaira Milani Fitria[1*]

[1]Magister Teknik Informatika, Fakultas Ilmu Komputer, Institut Informatika dan Bisnis Darmajaya

Riwayat artikel:
Received: 11Juli 2023
Accepted: 30 Juli 2023
Published: 1 Agustus 2023

Keywords:
Serangan Malware;
Keamanan Jaringan;
Mobile Banking.

Corespondent Email:
kairaamilanii@gmail.com

How to cite this article:

Doe, J. (2021). Judul Artikel. *Jurnal Informatika dan Teknik Elektro Terapan*, 6(2), 156-168.

Abstrak. Penelitian ini mengeksplorasi ancaman serangan malware perbankan yang terus meningkat dan solusi keamanan yang dapat diterapkan untuk mengurangi risikonya. Makalah ini dimulai dengan memberikan gambaran umum tentang berbagai serangan malware perbankan, termasuk metode penyebaran dan kerusakan yang dapat ditimbulkannya. Kemudian membahas berbagai langkah keamanan yang dapat diambil untuk mencegah dan mendeteksi serangan ini, seperti perlindungan titik akhir, segmentasi jaringan, dan edukasi pengguna. Makalah ini juga membahas tantangan dan keterbatasan dari solusi keamanan ini dan potensi perkembangan di masa depan di lapangan. Secara keseluruhan, makalah ini memberikan analisis komprehensif tentang serangan malware perbankan saat ini dan solusi keamanan yang dapat digunakan untuk melindungi dari serangan tersebut. Penelitian ini bertujuan untuk menganalisis secara komprehensif berbagai jenis serangan malware perbankan dan solusi keamanan yang dapat mengurangi risikonya. Dengan memahami sifat dari serangan-serangan ini dan efektivitas dari berbagai langkah keamanan, penelitian ini dapat membantu lembaga keuangan mengembangkan strategi yang lebih efektif untuk melindungi diri mereka sendiri dan pelanggan mereka dari ancaman siber.

1. PENDAHULUAN

Latar belakang penelitian ini berakar dari meningkatnya prevalensi dan kecanggihan serangan siber yang menargetkan industri perbankan. Dalam beberapa tahun terakhir, telah terjadi peningkatan yang signifikan dalam serangan malware yang ditujukan pada lembaga keuangan, dengan penjahat siber menggunakan berbagai teknik untuk mencuri data sensitif, mengkompromikan sistem, dan melakukan transaksi penipuan. Serangan ini dapat menimbulkan konsekuensi yang parah, termasuk kerugian finansial, kerusakan reputasi, dan tanggung jawab hukum. Akibatnya, bank dan organisasi keuangan lainnya berada di bawah tekanan yang semakin meningkat untuk menerapkan langkah-langkah keamanan yang kuat untuk melindungi sistem dan pelanggan mereka dari ancaman-ancaman ini. Industri perbankan telah menjadi target utama penjahat siber, dengan serangan malware yang menjadi ancaman signifikan bagi lembaga

keuangan dan pelanggan mereka. Serangan ini dapat mengakibatkan pencurian data sensitif, kerugian finansial, dan kerusakan reputasi, di antara konsekuensi lainnya. Akibatnya, bank dan organisasi keuangan lainnya berada di bawah tekanan yang semakin meningkat untuk menerapkan langkah-langkah keamanan yang kuat untuk melindungi sistem dan pelanggan mereka dari ancaman ini.

Serangan malware perbankan telah menjadi semakin umum dalam beberapa tahun terakhir, yang menimbulkan ancaman signifikan bagi lembaga keuangan dan pelanggan mereka. Serangan ini dapat mengakibatkan pencurian informasi sensitif, kerugian finansial, dan kerusakan reputasi. Berbagai solusi keamanan telah dikembangkan untuk mengurangi risiko yang terkait dengan malware perbankan. Makalah ini mengulas solusi keamanan ini dan efektivitasnya dalam mencegah dan mendeteksi serangan malware perbankan. Dengan menganalisis kekuatan dan kelemahan dari solusi-solusi tersebut, makalah ini berusaha untuk memberikan wawasan tentang praktik terbaik untuk mengamankan lembaga keuangan dari jenis serangan ini. Makalah penelitian ini bertujuan untuk menganalisis secara komprehensif berbagai jenis serangan malware perbankan dan solusi keamanan yang dapat digunakan untuk mengurangi risikonya. Makalah ini akan dimulai dengan memberikan gambaran umum tentang serangan malware perbankan lainnya, termasuk metode penyebaran dan kerusakan yang dapat ditimbulkannya. Kemudian akan membahas berbagai langkah keamanan yang dapat diambil untuk mencegah dan mendeteksi serangan ini, seperti perlindungan titik akhir, segmentasi jaringan, dan edukasi pengguna.

Makalah ini juga akan memeriksa tantangan dan keterbatasan solusi keamanan ini dan potensi pengembangan di masa depan di lapangan. Dengan memahami sifat dari serangan-serangan ini dan efektivitas dari berbagai langkah keamanan, penelitian ini dapat membantu lembaga keuangan mengembangkan strategi yang lebih efektif untuk melindungi diri mereka sendiri dan pelanggan mereka dari ancaman siber. Secara keseluruhan, makalah penelitian ini bertujuan untuk berkontribusi pada pengetahuan yang berkembang tentang serangan malware perbankan dan solusi keamanan, memberikan wawasan dan rekomendasi untuk membantu lembaga keuangan tetap terdepan dalam lanskap ancaman yang terus berkembang.

2. TINJAUAN PUSTAKA

Serangan malware perbankan baru-baru ini menjadi perhatian yang semakin meningkat bagi lembaga keuangan dan pelanggan mereka. Meningkatnya penggunaan layanan perbankan online telah mempermudah penyerang untuk mencuri informasi dan kredensial sensitif melalui vektor serangan seperti email phishing, malware, dan rekayasa sosial. Ekonomi malware bawah tanah telah mendorong pertumbuhan penipuan perbankan yang signifikan, dan bank telah meningkatkan keamanan mereka untuk melindungi transaksi dari penipuan [1], [2]. Memiliki solusi keamanan yang memadai untuk mencegah dan mendeteksi serangan malware perbankan sangatlah penting. Solusi mutakhir dengan melihat penipuan sebagai penyimpangan dari kebiasaan belanja pelanggan, tetapi mereka tidak memberikan perincian model yang mendalam dan analisis keamanan terhadap serangan yang sulit dipahami [1]. Pendekatan berlapis-lapis terhadap keamanan jaringan diperlukan untuk sistem respons intrusi berbasis jaringan guna mengamankan jaringan modern yang terdiri dari perangkat heterogen [3].

Serangan malware perbankan telah meningkat dalam beberapa tahun terakhir, dan beberapa insiden penting telah terjadi. Beberapa contoh serangan malware perbankan baru-baru ini adalah Emotet, malware ini aktif dari tahun 2014 hingga 2021 dan bertanggung jawab atas pencurian kredensial perbankan dan informasi sensitif lainnya dari para korban. Malware ini disebarkan melalui email phishing dan lampiran berbahaya [3]. Ransomware, jenis malware ini dirancang untuk mengenkripsi file korban dan meminta pembayaran sebagai imbalan atas kunci dekripsi. Dalam beberapa kasus, ransomware telah menargetkan lembaga keuangan dan pelanggan mereka [1]. Serangan lawan, serangan ini menggunakan algoritma pembelajaran mesin untuk menghasilkan malware yang dapat menghindari deteksi oleh sistem keamanan. Pembuat malware menggunakan serangan ini untuk melewati langkah-langkah keamanan dan mencuri informasi sensitif [4], [5]. Serangan berbasis

memori dimana serangan ini menggunakan forensik memori untuk mengidentifikasi dan melacak malware yang mungkin bersembunyi di dalam sistem korban. Serangan ini dapat digunakan untuk menemukan indikator kompromi dan mencegah kerusakan lebih lanjut [6]. Ini hanyalah beberapa contoh serangan malware perbankan dalam beberapa tahun terakhir. Karena lanskap ancaman terus berkembang, lembaga keuangan dan pelanggan mereka harus tetap waspada dan mengambil langkah-langkah untuk melindungi diri mereka sendiri dari serangan-serangan ini.

3. METODE PENELITIAN

Metodologi untuk makalah ini melibatkan tinjauan komprehensif terhadap solusi keamanan yang tersedia untuk mengurangi risiko yang terkait dengan serangan malware perbankan. Studi ini akan didasarkan pada analisis kekuatan dan kelemahan solusi-solusi ini serta efektivitasnya dalam mencegah dan mendeteksi serangan malware perbankan. Makalah ini akan membahas dampak kejahatan siber dan keamanan dalam transaksi perbankan online.

Dalam kegiatan transfer uang, memeriksa saldo rekening, melakukan pembayaran tagihan, dan melakukan tugas-tugas perbankan online lainnya ketika jauh dari komputer di rumah. Praktik ini dikenal sebagai mobile banking. Konsumen bank menyukai kemudahan yang ditawarkannya, tetapi infrastruktur untuk mobile banking rentan terhadap berbagai ancaman. Kami menguraikan perkembangan mobile banking, berbagai risiko yang menyertainya, dan beberapa serangan malware terbaru. Untuk mengaktifkan mobile banking yang aman, kami juga menganalisis beberapa solusi keamanan kontemporer.

3.1. Peningkatan Pengguna Mobile Banking

Perbankan online dimungkinkan dengan memanfaatkan alat khusus (seperti keyboard, terminal, dan monitor) untuk mengakses rekening bank melalui sambungan telepon pada akhir 1980-an. Saat ini, perbankan online mencakup semua sistem pembayaran elektronik yang memungkinkan klien (pemegang rekening bank) dari sebuah lembaga keuangan (bank) untuk melakukan transaksi keuangan melalui situs web bank. Layanan perbankan online baru-baru ini telah menerapkan teknologi perbankan Internet seluler, seperti pembayaran dari orang ke orang yang dimungkinkan oleh beberapa aplikasi ponsel cerdas. Masalah-masalah berikut ini adalah beberapa penyebab utama peningkatan tajam jumlah orang yang menggunakan mobile banking [7].

- Faktor usia: Pertumbuhan penggunaan mobile banking didorong oleh mereka yang berusia antara 18 dan 32 tahun.
- Kegunaan: Orang-orang menggunakan berbagai program mobile banking yang mudah digunakan saat ini. Selain itu, aplikasi-aplikasi ini memberikan pengalaman yang komprehensif dan lancar bagi konsumen perbankan.
- Aksesibilitas: Pengguna mobile banking mendapatkan akses ke beberapa layanan, termasuk kemampuan untuk menambahkan penerima manfaat, memindahkan uang antar rekening, dan menerima notifikasi ketika saldo mereka berubah, semua dengan menekan satu tombol, kapan pun mereka mau, dari lokasi mana pun.
- Bank khusus seluler: Saat ini, perbankan tradisional telah berubah untuk memanfaatkan aplikasi seluler. Untuk berbagai fungsi keuangan, mayoritas bank-bank besar menggunakan aplikasi seluler.
- Beralih ke transaksi tanpa kertas: Banyak bank memberikan hadiah uang tunai untuk menggunakan mobile banking daripada transaksi berbasis kertas. Dalam waktu dekat mekanisme pembayaran nirsentuh berbasis teknologi komunikasi, dua kartu dapat berbicara satu sama lain dan mentransfer dana secara digital [8].
- Aktivitas penipuan dapat dengan mudah diidentifikasi secara online oleh pengguna mobile banking, yang juga dapat memantau rekening bank mereka. Menggunakan kata sandi sekali pakai dapat membantu mencegah transfer uang online yang tidak diinginkan dan melanggar hukum dalam situasi ini.

3.2. Evolusi Mobile Banking

Perkembangan perbankan Internet sejak tahun 1980-an telah mempermudah pengguna untuk mengelola uang di rekening mereka. Nasabah Nottingham Building Society pertama kali

mengetahui layanan perbankan Internet "Homelink" di Inggris oleh Bank of Scotland pada tahun 1983. Contoh awal internet banking dapat dilihat pada layanan Homelink. Perbankan online pertama kali ditawarkan oleh program keuangan pribadi Microsoft Money pada tahun 1994, dan dengan cepat mendapatkan popularitas. Stanford Credit Union meluncurkan situs web perbankan online pertama pada dekade yang sama. Delapan bank di Amerika masing-masing memiliki setidaknya satu juta pelanggan internet pada tahun 2001. Sebanyak 19 juta rumah di Amerika menggunakan internet banking pada saat itu. Dewan Pemeriksaan Lembaga Keuangan Federal menerbitkan pedoman dan norma pada tahun 2005 untuk membantu lembaga keuangan melakukan analisis berbasis risiko. Perbankan online pertama kali ditawarkan oleh bank-bank langsung, seperti ING Direct, yang tidak memiliki cabang fisik. Transaksi keuangan beralih dari komputer pribadi ke perangkat seluler seperti ponsel pintar setelah Apple memperkenalkan iPhone pada tahun 2007. 54 juta rumah tangga di Amerika mulai menggunakan komputer dan perangkat seluler untuk mengakses rekening bank online mereka pada tahun 2009. Perbankan online mulai digunakan secara luas pada tahun 2011. Jejaring sosial, internet banking, manajemen keuangan pribadi, pembayaran, dan hadiah menjadi satu pada tahun 2012 untuk mengantarkan era perbankan sosial.

3.3. Tren Serangan pada Mobile Banking

Sektor jasa keuangan telah mengakui janji mobile banking. Agar klien dapat menggunakan semua manfaat yang diberikan aplikasi ini, industri ini telah mengimplementasikan aplikasi mobile banking. Namun, risiko keamanan yang terkait dengan mobile banking telah membuat banyak pengguna enggan menggunakannya. Berikut ini adalah kekhawatiran mobile banking saat ini yang dimiliki oleh calon pengguna mobile banking:

- Malware seluler: Serangan dari malware berpindah dari sistem konvensional ke skema keuangan online. Para penyerang telah menciptakan malware yang menargetkan aplikasi mobile banking, dan lebih banyak lagi malware yang akan menargetkan aplikasi mobile banking.
- Penggunaan aplikasi pihak ketiga: Aplikasi dari pihak ketiga hanya sebagian yang dapat dipercaya. Penyerang jahat dan penipu menciptakan beberapa aplikasi.
- Penggunaan Wi-Fi yang tidak aman: Wi-Fi tersedia di sebagian besar tempat umum, seperti pusat perbelanjaan dan bandara, dan peretas serta penjahat siber dapat memperoleh akses ke ponsel pintar dan meluncurkan serangan man-in-the-middle dan serangan estafet.
- Perilaku pengguna: Karena pengguna cenderung mengunduh perangkat lunak pihak ketiga, memanfaatkan Wi-Fi yang tidak terlindungi, dan membuka serta mengeklik tautan dalam email dan layanan pesan singkat, mereka juga dapat membantu penyerang mencapai niat jahat mereka. Penyerang juga bisa mengakses sistem ketika perangkat pengguna salah tempat atau dicuri.

3.4. Serangan Malware Mobile Banking

Beberapa jenis malware dapat membahayakan sistem mobile banking. Berikut ini adalah berbagai jenis serangan malware yang berpotensi menyerang mobile banking:

- Keylogger: Aplikasi jahat yang dikenal sebagai keylogger menangkap semua penekanan tombol pada sistem komputer. Aplikasi ini dapat digunakan untuk mencuri kredensial pengguna (seperti untuk akun perbankan online) dan data sensitif lainnya tentang bisnis.
- Mata-mata-mata (Spyware): Spyware adalah sebuah program yang melacak informasi penting dari sebuah sistem (misalnya, ponsel pintar). Data yang dicuri dapat digunakan dengan tidak semestinya, seperti menjual alamat email kepada pengirim spam.
- Virus: Virus adalah program menular yang terhubung ke perangkat lunak (atau program) lain dan kemudian mereplikasi setelah perangkat lunak tersebut mulai berjalan.
- Worm: Worm adalah perangkat lunak komputer yang menyebarkan dirinya sendiri ke seluruh sistem dan menghapus file dan data. Worm dapat menyebar ke seluruh jaringan komputer dengan memanfaatkan kelemahan dalam sistem operasi.

- Trojan: Program Trojan ditulis untuk mendapatkan data keuangan pengguna dan mendapatkan kendali atas sumber daya sistem. Ponsel cerdas yang terhubung dapat melakukan serangan lebih lanjut terhadap router menggunakan virus trojan yang terinfeksi Android.
- Rootkit: Rootkit adalah bentuk malware yang menggunakan aspek-aspek sistem operasi, seperti pengalihan fungsi antarmuka pemrograman aplikasi, untuk menyembunyikan keberadaannya atau keberadaan program lain (misalnya, spyware di ponsel cerdas).
- Hijacker (pembajak): Perangkat lunak berbahaya yang terutama berdampak pada peramban adalah pembajak atau pembajak peramban. Perangkat lunak ini mengalihkan aktivitas pencarian yang biasa dilakukan dan menampilkan hasil yang diinginkan oleh pembuatnya untuk dilihat oleh pengguna.
- Ransomware: Malware ini mengunci data pengguna atau mengunci layar sistem sampai atau kecuali jumlah tertentu (disebut "tebusan") dibayarkan. Perangkat lunak ini melarang pengguna untuk menggunakan perangkat yang mereka rancang (misalnya, ponsel pintar).

Pada sistem perbankan seluler/Internet, beberapa serangan virus dapat digunakan. Rincian serangan ini, termasuk nama, jenis, ciri-ciri, dan dampak malware, dirangkum dalam Tabel 1.

Tabel 1. Serangan malware pada mobile banking

Nama	Tipe	Karakteristik
Zbot	Trojan dengan Ransomware	Zbot, atau Zeus, pertama kali diidentifikasi pada bulan Juli 2007. Penggunaan malware ini untuk mencuri data perbankan dengan metode pencatatan keystroke man-in-the-browser
Faketoken	Trojan	Serangan berupa munculnya layar login palsu sehingga penyerang dapat mencuri kredensial login melalui beberapa aplikasi keuangan.
Tordow	Trojan	Menyusup ke dalam aplikasi populer (misalnya, Pokemon GO) dan mencuri informasi sensitive dari perangkat seluler dengan mendapatkan akses root.
Black Jack Free	Trojan	Program ini didasarkan pada malware ganas yang mencuri informasi pribadi dan perbankan pengguna serta kredensial login situs web online populer.
HijackRAT	Trojan	HijackRAT berperilaku seperti trojan perbankan seluler. Dia hadir dengan aplikasi Android berbahaya yang menyamarkan dirinya sebagai "Kerangka Kerja Layanan Google."
Tinba	Trojan	Tinba pertama kali menginfeksi sistem ketika pengguna mencoba masuk ke salah satu situs web bank yang ditargetkan. Kemudian, korban menerima pesan palsu dan formulir web yang meminta kredensial login.
TrickBot (Dyre)	Trojan	Pada tahun 2014-2015, Trickbot melakukan banyak kerusakan melalui aktivitas berbahaya (yaitu, spamming dan phishing). Malware ini berhasil mencuri sekitar US$5,5 juta dengan melakukan transfer kawat yang tidak sah.
SpyEye	Trojan	Malware pencuri data yang diciptakan untuk mencuri uang dari rekening bank online.
Shylock	Trojan	Malware perbankan ini dapat mencuri kredensial perbankan pengguna untuk melakukan transfer uang ilegal.

4. HASIL DAN PEMBAHASAN

4.1 Persyaratan Keamanan Untuk Mobile Banking

Tingkat keamanan tertentu harus dijaga untuk menjaga keamanan nasabah mobile banking.

- Kerahasiaan (Confidentiality): Hanya mereka yang memiliki otorisasi yang tepat yang dapat mengakses informasi keuangan nasabah bank yang berbeda.
- Integritas (Integrity): Dalam situasi apa pun, entitas yang tidak berwenang (misalnya, penyerang) tidak boleh memodifikasi atau mengubah data keuangan bank.
- Ketersediaan (Availability): Setiap serangan denial-of-service terhadap sistem informasi keuangan, termasuk berbagai server perbankan, harus dicegah.

- Otentikasi (Authentication): Proses mengkonfirmasi identitas pengguna (yaitu pemilik rekening bank) dikenal sebagai otentikasi. Otentikasi dua faktor dan otentikasi tiga faktor adalah dua jenis teknik otentikasi multifaktor yang dibahas dalam artikel ini. Seorang pengguna menggunakan dua jenis kredensial, yaitu kata sandi dan perangkat seluler (kartu pintar), dalam autentikasi dua faktor. Ketika pengguna mendaftar ke server, kartu pintar atau perangkat seluler dapat menyimpan data yang diperlukan. Pada autentikasi tiga faktor, pengguna mengautentikasi dengan sistem menggunakan tiga kredensial yang berbeda, termasuk kata sandi, kartu pintar atau perangkat seluler, dan biometrik (sidik jari dan pengenalan wajah).
- Otorisasi (Authorization): Otentikasi memungkinkan seseorang untuk melakukan operasi yang disetujui. Hal ini mencegah pengguna mobile banking mengakses informasi yang disimpan di server perbankan yang telah diberi otorisasi (misalnya, tergantung pada posisi mereka dalam sistem).
- Pencurian perangkat secara fisik (Physical theft of devices): Perangkat seperti kartu pintar dan instrumen seluler (misalnya, ponsel pintar) menyimpan informasi berharga yang diperlukan untuk otentikasi yang aman dan efektif. Setelah pencurian perangkat ini, berbagai serangan, termasuk orang dalam yang memiliki hak istimewa dan serangan menebak kata sandi secara offline/online, dapat dilakukan.
- Nonrepudiation: Nonrepudiation mengacu pada ketidakmampuan pengguna untuk menyangkal keabsahan tanda tangan mereka pada dokumen atau pesan yang dikirimkan oleh mereka.
- Kesegaran (Freshness): Dalam sistem pembayaran mobile banking, kesegaran menjamin bahwa data yang ada adalah data terkini dan mencegah pihak lawan untuk mengulang pesan sebelumnya.
- Forward secrecy: Misalkan sebuah entitas meninggalkan jaringan. Setiap pesan yang dikirim setelah entitas yang pergi harus tidak dapat diakses oleh entitas tersebut.
- Backward secrecy: mengharuskan entitas baru yang bergabung dengan jaringan tidak memiliki akses ke komunikasi apa pun yang telah dikirim.

4.2 Solusi Keamanan Untuk Ancaman Mobile Banking

Beberapa langkah keamanan harus dilakukan untuk membatasi potensi risiko pada jaringan mobile banking.

- Kesadaran (Awareness): Penting untuk membuat program yang menginformasikan karyawan bank dan pengguna mobile banking tentang berbagai ancaman, termasuk malware, phishing, dan unduhan file berbahaya.
- Lampiran email berbahaya (Malicious email attachments): Pengguna mobile banking harus berhati-hati untuk tidak mengklik, mengunduh, atau membuka file yang diterima dalam lampiran email karena dapat mengandung malware.
- Pembaruan sistem operasi (Operating system updates): Kemampuan untuk mengunduh pembaruan perangkat lunak secara otomatis adalah salah satu fitur paling signifikan dari teknik modern (termasuk komputer desktop, ponsel cerdas, dan tablet).
- Perlindungan (Protection): Pengguna mobile banking harus melindungi diri mereka sendiri dengan menginstal perangkat lunak antivirus di komputer mereka.
- Penggunaan skema otentikasi yang solid (Use of solid authentication schemes): Untuk melindungi sistem mobile banking, diperlukan teknik otentikasi yang aman.

4.3 Keterbatasan Solusi Keamanan Mobile Banking

Terdapat beberapa batasan untuk aplikasi keamanan di mobile banking, bahkan dengan kesadaran dan kehati-hatian.

- Beberapa institusi menyediakan kursus kesadaran keamanan untuk pelanggan perbankan online atau mobile. Namun, untuk menginformasikan secara memadai kepada konsumen tentang risiko yang terkait dengan mobile banking, kita perlu melakukan program kesadaran keamanan secara lebih teratur baik dalam mode online maupun offline.
- Kartu pintar atau perangkat seluler dapat digunakan untuk melancarkan beberapa

jenis serangan. Strategi otentikasi yang aman harus dibuat untuk menahan serangan terhadap kartu pintar atau perangkat seluler.

- Kelainan yang tidak diketahui, seperti serangan zero-day, dapat berdampak pada langkah-langkah keamanan. Oleh karena itu, anomali yang tidak teridentifikasi harus memiliki dampak minimal pada infrastruktur mobile banking.

4.4 Perbandingan Fitur Keamanan dan Fungsionalitas Skema Autentikasi

Penulis menguraikan beberapa persyaratan keamanan yang harus dipenuhi oleh autentikasi dua faktor dan tiga faktor untuk mempertahankan diri dari ancaman yang telah diketahui.

- Serangan pemutaran ulang (Replay attack): Dalam skenario ini, penyerang A mencoba mengelabui pengguna lain yang dapat dipercaya dengan menggunakan kembali pengetahuan yang diperoleh dengan mendengarkan data yang dikirimkan.
- Serangan Man-in-the-middle (Man-in-the-middle assault): Pada jenis serangan ini, A menempatkan dirinya di tengah-tengah dua pihak yang berkomunikasi, berpura-pura menjadi keduanya dan mengakses informasi yang mereka bagikan.
- Serangan dengan peniruan (Attack by impersonation): Pada jenis serangan ini, A menggunakan identitas pengguna yang sah pada jaringan untuk mengelabui pengguna lain. Tujuannya adalah untuk membujuk penerima dengan memodifikasi pesan yang sah atau menyisipkan berita palsu ke dalam komunikasi.
- Serangan pada tebakan kata sandi (Attack on password guessing): Dalam serangan menebak kata sandi, A mencegat beberapa pesan selama pertukaran komunikasi dan menggunakan metode serangan kamus kata sandi untuk mencoba menebak kata sandi pengguna, atau A menggunakan kartu pintar pengguna yang hilang atau dicuri, perangkat seluler, dan data yang dikumpulkan selama waktu pendaftaran untuk mencoba menebak kata sandi pengguna.
- Serangan pencurian kartu pintar/perangkat seluler (Smart card/mobile device stolen attack): Dalam serangan pencurian kartu pintar/perangkat seluler, A menggunakan informasi yang diperoleh dari kartu pintar/perangkat seluler yang hilang/dicuri, bersama dengan strategi seperti serangan analisis daya [9], untuk mencoba menebak kata sandi pengguna yang sah.
- Serangan orang dalam yang memiliki hak istimewa (Privileged insider attack): Dalam serangan orang dalam yang memiliki hak istimewa, orang dalam yang buruk (penyerang A, misalnya) dapat mengakses informasi registrasi pengguna. A kemudian mencoba menghitung kredensial rahasia, seperti kata sandi pengguna.
- Anonimitas pengguna (User anonymity and untraceability): Untuk melindungi privasi pengguna, A seharusnya tidak dapat menentukan identitas asli pengguna dari pesan yang disadap. Akan tetapi, A seharusnya tidak dapat menentukan aktivitas pengguna dari komunikasi yang disadap berkat atribut tidak dapat dilacak.

4.5 Perbandingan Teknik Otentikasi Dua Faktor dan Tiga Faktor

Pengujian pada aspek keamanan dan fungsional dari beberapa metode otentikasi dua faktor yang baru-baru ini disarankan [10]–[13] pada Tabel 2. Aspek keamanan dan fungsional yang berbeda dari metode otentikasi tiga faktor yang baru saja disarankan [14]–[17] ditampilkan pada Tabel 3.

Tabel 2. Perbandingan skema dua faktor

Fitur	[11]	[12]	[13]	[10]
Anonimitas pengguna & anti pelacakan	No	Yes	Yes	Yes
Otentikasi bersama	No	Yes	Yes	No
Otentikasi dan persetujuan kunci	No	No	Yes	No
Persetujuan kunci sesi	No	Yes	No	No
Serangan insider dengan hak istimewa	No	Yes	No	No
Serangan ulang	No	Yes	No	Yes
Serangan tebak kata sandi	No	No	No	Yes
Serangan peniruan pengguna	No	Yes	Yes	No
Serangan pencurian kartu pintar	N/A	Yes	No	Yes

Fasilitas pengubahan kata sandi yang aman	N/A	No	Yes	No
Serangan man-in-the-middle	No	No	Yes	Yes
Kerahasiaan maju sempurna	Yes	Yes	Yes	Yes
"Yes" berarti skema aman dari serangan tertentu atau mendukung fitur tertentu, dan "No" berarti sebaliknya				

Autentikasi dua faktor (2FA) dalam mobile banking adalah langkah keamanan yang menambahkan lapisan perlindungan ekstra dengan mengharuskan pengguna memberikan dua jenis faktor autentikasi yang berbeda saat mengakses akun mobile banking mereka. Metode ini meningkatkan keamanan di luar kombinasi nama pengguna dan kata sandi tradisional. Dua faktor yang biasanya digunakan dalam 2FA adalah:

- Faktor Pengetahuan (Knowledge Factor): Ini melibatkan sesuatu yang diketahui pengguna, seperti kata sandi, PIN, atau pola. Ini adalah bentuk autentikasi yang paling umum dan merupakan langkah pertama dalam proses verifikasi.
- Faktor Kepemilikan (Possession Factor): Faktor ini melibatkan sesuatu yang dimiliki pengguna, biasanya perangkat fisik seperti smartphone, tablet, atau token perangkat keras. Faktor kepemilikan menambahkan lapisan keamanan dengan mengharuskan pengguna untuk mengakses perangkat tertentu untuk menyelesaikan proses otentikasi.

Pengguna yang mengaktifkan 2FA untuk akun mobile banking mereka biasanya harus memasukkan nama pengguna dan kata sandi (faktor pengetahuan) sebagai langkah pertama. Setelah informasi ini diverifikasi, sistem akan meminta pengguna untuk memberikan faktor kedua, yaitu kode sandi sekali pakai (OTP) yang dihasilkan oleh aplikasi otentikasi di perangkat seluler mereka, yang diterima melalui SMS atau notifikasi. Dengan memasukkan faktor kedua ini, pengguna menunjukkan kepemilikan perangkat yang terdaftar, mengonfirmasi identitas mereka.

Tabel 3. Perbandingan skema tiga faktor

Fitur	[16]	[15]	[14]	[17]
Anonimitas pengguna & anti pelacakan	No	No	Yes	No
Otentikasi bersama	Yes	Yes	No	Yes
Serangan ulang	Yes	Yes	Yes	Yes
Serangan man-in-the-middle	No	No	Yes	Yes
Serangan pencurian kartu pintar	Yes	Yes	Yes	Yes
Serangan peniruan pengguna	No	No	No	No
Serangan peniruan server	No	No	Yes	No
Serangan orang dalam	Yes	Yes	No	No
Serangan tebak kata sandi	Yes	Yes	Yes	Yes
Kerahasiaan maju sempurna	No	Yes	Yes	Yes
"Yes" berarti skema aman dari serangan tertentu atau mendukung fitur tertentu, dan "No" berarti sebaliknya				

Autentikasi tiga faktor (3FA) dalam mobile banking mengacu pada langkah keamanan yang menambahkan lapisan autentikasi di luar kombinasi nama pengguna-kata sandi tradisional dan autentikasi dua faktor (2FA) yang umum digunakan. Ini melibatkan penggunaan tiga faktor untuk memverifikasi identitas pengguna yang mencoba mengakses akun mobile banking mereka. Tiga faktor tersebut biasanya meliputi:

- Faktor Pengetahuan (Knowledge Factor): melibatkan sesuatu yang diketahui pengguna, seperti kata sandi atau PIN. Ini adalah bentuk otentikasi yang paling umum dan penting.
- Faktor Kepemilikan (Possession Factor): Faktor ini melibatkan sesuatu yang dimiliki pengguna, biasanya perangkat fisik atau token. Dalam konteks mobile banking, ini dapat berupa perangkat seluler, kartu pintar, token perangkat keras, atau kunci keamanan.
- Faktor Warisan (Inherence Factor): melibatkan sesuatu yang melekat pada pengguna, sering disebut biometrik. Ini mencakup karakteristik fisiologis atau perilaku yang unik, seperti sidik jari, pengenalan wajah, pengenalan suara, atau bahkan pemindaian iris mata.

Dengan menggabungkan ketiga faktor ini, otentikasi tiga faktor memberikan lapisan keamanan tambahan, sehingga menyulitkan orang yang tidak berwenang untuk mengakses akun mobile banking pengguna. Bahkan jika salah satu aspeknya dilanggar, faktor lainnya

akan melindungi. Untuk mengimplementasikan otentikasi tiga faktor di mobile banking, pengguna mungkin diminta untuk memberikan nama pengguna dan kata sandi (faktor pengetahuan), menggunakan perangkat seluler atau token keamanan (faktor kepemilikan), dan memberikan data biometrik seperti sidik jari atau pemindaian wajah (faktor bawaan) untuk menyelesaikan proses otentikasi.

5. KESIMPULAN

Dalam review penelitian mengenai mobile banking, banyak topik yang dapat dibahas, termasuk kekuatan pendorong mendasar di balik pengadopsian suatu metode keamanan dalam mobile banking, risiko inheren yang dihadapinya, dan persyaratan keamanan penting pada masing-masing fitur. Selain itu, didapatkan hasil eksplorasi berupa variasi solusi keamanan yang dirancang untuk memerangi ancaman yang menargetkan mobile banking, dengan cermat menganalisis keterbatasannya dan mengeksplorasi jalan potensial untuk peningkatan sistem. Meskipun solusi keamanan ini memberikan dasar yang kuat untuk memerangi ancaman malware di mobile banking, penting untuk diketahui bahwa kemungkinan ancaman akan terus berkembang. Perlunya penelitian berkelanjutan, adaptasi teknologi baru, dan langkah-langkah keamanan proaktif sangat penting untuk tetap selangkah lebih maju dari para penjahat siber dan melindungi integritas sistem perbankan seluler

1. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Bapak Sriyanto, PhD dan pihak-pihak terkait yang telah memberi dukungan terhadap penelitian ini.

2. DAFTAR PUSTAKA

[1] M. Carminati, M. Polino, A. Continella, A. Lanzi, F. Maggi, and S. Zanero, "Security Evaluation of a Banking Fraud Analysis System," ACM Transactions on Privacy and Security (TOPS), vol. 21, pp. 1–31, 2018.

[2] G. Lakshmi, S. E. Ovia, and A. D. Sre, "The Impact Of Cyber Crime And Security In Online Banking Transaction," International Journal Of Management And SOCIAL SCIENCES, vol. 8, pp. 28–31, 2018.

[3] K.-P. Grammatikakis, I. Koufos, N. Kolokotronis, C. Vassilakis, and S. Shiaeles, "Understanding and Mitigating Banking Trojans: From Zeus to Emotet," CoRR, vol. abs/2109.01610, 2021, [Online]. Available: https://arxiv.org/abs/2109.01610

[4] W. Hu and Y. Tan, "Generating Adversarial Malware Examples for Black-Box Attacks Based on GAN," CoRR, vol. abs/1702.05983, 2017, [Online]. Available: http://arxiv.org/abs/1702.05983

[5] X. Qi, Y. Tang, H. Wang, T. Liu, and J. Jing, "Adversarial Example Attacks Against Intelligent Malware Detection: A Survey," 2022 4th International Conference on Applied Machine Learning (ICAML), pp. 1–7, 2022.

[6] T. Proffitt, "Indicators of compromise in memory forensics GIAC (GCFA) Gold Certification," 2013.

[7] S. Kiljan, K. Simoens, D. De Cock, M. C. J. D. van Eekelen, and H. P. E. Vranken, "A Survey of Authentication and Communications Security in Online Banking," ACM Computing Surveys (CSUR), vol. 49, pp. 1–35, 2016.

[8] S. Ghosh, A. Majumder, J. Goswami, A. Kumar, S. P. Mohanty, and B. K. Bhattacharyya, "Swing-Pay: One Card Meets All User Payment and Identity Needs: A Digital Card Module using NFC and Biometric Authentication for Peer-to-Peer Payment," IEEE Consumer Electronics Magazine, vol. 6, no. 1, pp. 82–93, 2017, doi: 10.1109/MCE.2016.2614522.

[9] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Transactions on Computers, vol. 51, no. 5, pp. 541–552, 2002, doi: 10.1109/TC.2002.1004593.

[10] I. Memon, I. Hussain, R. Akhtar, and G. Chen, "Enhanced Privacy and Authentication: An Efficient and Secure Anonymous Communication for Location Based Service Using Asymmetric Cryptography Scheme," Wirel Pers Commun, vol. 84, no. 2, pp. 1487–1508, 2015, doi: 10.1007/s11277-015-2699-1.

[11] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi, "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks," Math Comput Model, vol. 55, no. 1, pp. 214–222, 2012, doi: https://doi.org/10.1016/j.mcm.2011.04.036.

[12] Q. Xie, B. Hu, X. Tan, M. Bao, and X. Yu, "Robust Anonymous Two-Factor

Authentication Scheme for Roaming Service in Global Mobility Network," Wirel Pers Commun, vol. 74, no. 2, pp. 601–614, 2014, doi: 10.1007/s11277-013-1309-3.

[13] D. Zhao, H. Peng, L. Li, and Y. Yang, "A Secure and Effective Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks," Wirel Pers Commun, vol. 78, no. 1, pp. 247–269, 2014, doi: 10.1007/s11277-014-1750-y.

[14] D. He and D. Wang, "Robust Biometrics-Based Authentication Scheme for Multiserver Environment," IEEE Syst J, vol. 9, no. 3, pp. 816–823, 2015, doi: 10.1109/JSYST.2014.2301517.

[15] H. Lin, F. Wen, and C. Du, "An Improved Anonymous Multi-Server Authenticated Key Agreement Scheme Using Smart Cards and Biometrics," Wirel Pers Commun, vol. 84, no. 4, pp. 2351–2362, 2015, doi: 10.1007/s11277-015-2708-4.

[16] L. A. N. D. Y. X. A. N. D. Y. Y. Lu Yanrong AND Li, "Robust Biometrics Based Authentication and Key Agreement Scheme for Multi-Server Environments Using Smart Cards," PLoS One, vol. 10, no. 5, pp. 1–13, Jul. 2015, doi: 10.1371/journal.pone.0126323.

[17] X. A. N. D. Z. Z. Wang Chengqi AND Zhang, "Cryptanalysis and Improvement of a Biometric-Based Multi-Server Authentication and Key Agreement Scheme," PLoS One, vol. 11, no. 2, pp. 1–25, Jul. 2016, doi: 10.1371/journal.pone.0149173.