DEVICE FINGERPRINTING AND BINDING

CARA MELINDUNGI NASABAH PADA TRANSAKSI MOBILE DENGAN CARA MENGIKAT DAN SIDIK JARI PADA PERANGKAT

Topik mengenai operasi seluler dan juga perlindungan nasabah yang menggunakan layanan mobile seluler sedang menjadi perbincangan saat ini. Meskipun banyak bank sudah menggunakan otentikasi berdasarkan kriptografi asimetris, pengikatan perangkat menjadi yang terdepan.

Pengikatan yang dimaksud di sini adalah pengikatan perangkat dengan kunci pribadi yang aman. Nasabah sangat mungkin untuk memperkuat keamanan di beberapa titik penting seperti jika kehilangan ponsel, mengganti ponsel baru dan nasabah punya hak penuh jika ada upaya masuk ke ponsel baru.

MASALAH UTAMA

- Sulit untuk mengidentifikasi perpindahan nasabah perbankan yang mempunyai perangkat baru
- Sulit melindungi dari akses tidak sah & pengambilalihan akun
- Sulit melindungi dari phishing melalui WA, SMS atau email
- Bermasalah dalam mengidentifikasi malware yang beroperasi secara tersembunyi

Salah satu komponen utama perlindungan nasabah yang menggunakan aplikasi mobile adalah PayConfirm. PayConfirm melindungi dengan cara adanya sidik jari yang digunakan untuk semua konfirmasi transaksi sebagai bagian dari tanda tangan otentikasi. Yang dimaksud dengan sidik jari perangkat adalah serangkaian parameter perangkat unik — totalnya mencapai 70. Parameter ini mencakup statis — seperti ID perangkat dan parameter teknologi pabrikan utama lainnya pada platform seluler — serta dinamis — seperti koneksi jaringan WiFi, operator jaringan seluler, dan parameter seperti apakah perangkat tersebut di-malware atau di-root, dan lain-lain. Semua parameter dinamis diidentifikasi sebagai peristiwa yang dapat ditangkap dan dikirimkan ke sistem back-end sebagai data mentah untuk memperkaya sistem anti-fraud di sisi bank.

Sidik jari perangkat memungkinkan untuk mengikat nasabah dengan perangkat yang tepat di mana aplikasi beroperasi. Poin pentingnya di sini adalah terhubung dengan kunci pribadi yang tidak dapat diekstraksi. Dengan demikian, bank dapat mengikat nasabah dengan perangkatnya dan kunci yang digunakan untuk masuk dan hanya bisa dioperasikan di perangkat tersebut.

BAGAIMANA PENGIKATAN PERANGKAT MENYEDERHANAKAN PENGALAMAN PENGGUNA

Jika pada bank umumnya menggunakan kredensial biasa seperti mPIN dengan Touch/Face ID untuk bisa mengakses mobile banking, sekarang bisa jadi adalah perangkat itu sendiri yang terhubung dengan kunci rahasia yang tepat dan penggunanya. Dengan demikian, nasabah bank tidak perlu menggunakan mPIN karena dua faktornya adalah:

Perangkat itu sendiri — **sesuatu yang Anda miliki**

Touch/Face ID — **sesuatu tentang diri Anda**

Pendekatan ini membuat proses menjadi lebih mudah untuk nasabah, dan tentunya lebih aman.

BAGAIMANA PERANGKAT DENGAN SIDIK JARI MEMBANTU UNTUK MEMINIMALISIR PHISING

Skenario phishing yang biasa terjadi adalah mengirimkan tautan phishing ke nasabah bank melalui saluran apa pun yang tersedia – messenger, SMS, atau email. Penipu mencoba membujuk nasabah bank untuk memasang aplikasi palsu untuk mendapatkan kredensial dan mengambil kendali atas operasi di aplikasi perbankan yang dipasang. Dengan sidik jari perangkat, setiap instalasi aplikasi akan dievaluasi sebagai suatu peristiwa, sehingga setiap aplikasi tersembunyi akan mudah diidentifikasi karena data ini akan diberikan kepada anti-fraud bank untuk dievaluasi sesuai dengan kebijakan keamanan bank.

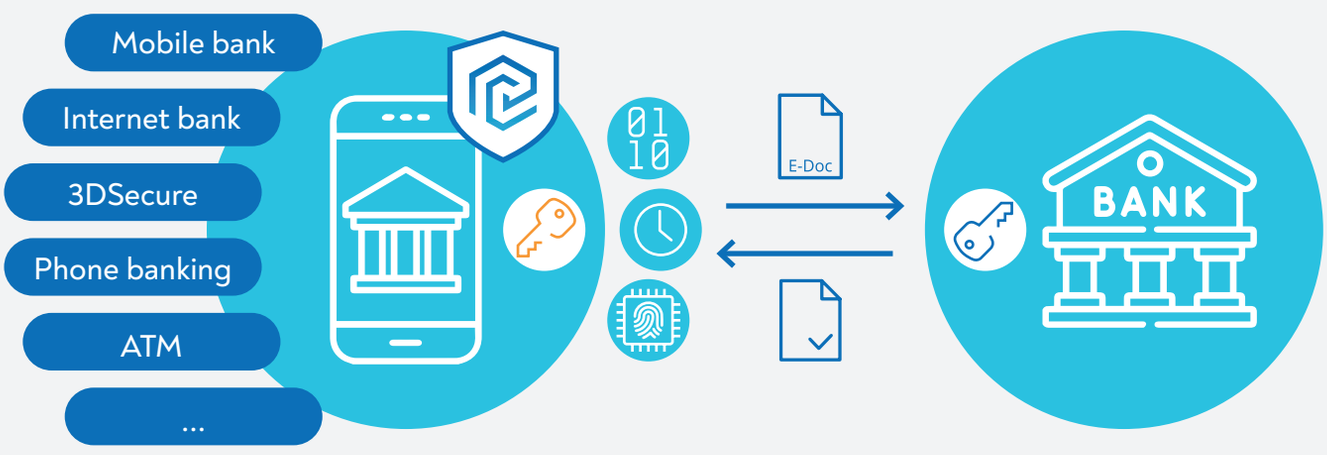
BAGAIMANA PENGIKATAN PERANGKAT MEMBANTU MEMINIMALKAN KASUS PENGAMBILALIHAN AKUN

Saat penipu mencoba mendapatkan akses dari perangkat lain menggunakan kredensial nasabah, sidik jari perangkat akan membantu mengidentifikasi upaya tersebut karena parameter perangkat bersifat unik dan perangkat persisnya terhubung dengan nasabah bank yang sama. Sesuai dengan kebijakan keamanan bank, verifikasi nasabah dapat dilakukan dengan benar jika ada upaya untuk mendapatkan akses dari perangkat baru atau upaya untuk melakukan transaksi dari perangkat baru.

Pada saat yang sama jika nasabah berpindah ke perangkat baru, akan mudah untuk mengonfirmasi langkah ini menggunakan sidik jari perangkat sebagai bagian dari alur autentikasi — cukup konfirmasi satu ketukan pada perangkat lama.

BAGAIMANA SIDIK JARI PERANGKAT MEMBANTU MEMPERKAYA SISTEM ANTI-FRAUD

Hingga 70 parameter tersedia untuk dikumpulkan dengan sidik jari perangkat oleh PayConfirm. Informasi ini dapat dengan mudah diberikan ke sistem anti-fraud yang dipasang di sisi bank. Dengan data mentah ini, lebih mudah untuk membuat otentikasi berbasis risiko yang akurat berdasarkan penilaian sistem anti-fraud. Jika tidak ada yang istimewa pada perangkat — tidak ada aktivitas mencurigakan, tidak ada akses dari perangkat baru, dan lain-lain, maka transaksi dapat dikonfirmasi secara rutin. Jika terdeteksi sesuatu yang mencurigakan, sistem perbankan digital mungkin akan meminta beberapa faktor lagi untuk melanjutkan transaksi.



KELEBIHAN PENGIKAT PERANGKAT NASABAH MELALUI PAYCONFIRM

- Cara mudah untuk mengidentifikasi peralihan nasabah ke perangkat baru
- Cara mudah mengidentifikasi kejadian instalasi aplikasi mencurigakan, misalnya dari phishing melalui WA, SMS, atau email
- Alat untuk memperkaya sistem anti-fraud bank
- Cara sederhana untuk mengidentifikasi upaya mengakses dari perangkat lain
- Sudah disertakan dalam autentikasi bersama dengan kriptografi asimetris dan prinsip «apa yang Anda lihat adalah apa yang Anda tandatangani» untuk meminimalkan risiko penipuan

TENTANG KAMI

Airome Technologies adalah pengembang solusi keamanan siber yang berbasis di Singapura, dan kami berfokus pada perbankan digital dan sistem manajemen dokumen elektronik. Kami menyediakan perangkat lunak server-klien yang aman untuk mengonfirmasi atau menandatangani semua jenis operasi secara digital, termasuk transaksi bank atau dokumen elektronik, pada perangkat seluler. Tujuan kami adalah memberikan solusi untuk menurunkan risiko transaksi tidak sah yang disebabkan oleh serangan man-in-the-middle, phishing, atau social engineering.

Recognized by Gartner

BERHUBUNGAN BERSAMA KAMI

airome.tech
info@airome.tech