Security
Solution Brief

Banking

IBM Security Trusteer mobile solutions: Meeting banking security threats

Build protection directly into mobile applications using the solution's mobile framework

Highlights

- Detect and assess mobile risks in real time
- Proactively detect malware and pharming attacks
- Silently operate in the background to help reduce undue customer friction
- Correlate device and account risk factors across online and mobile channels

The accelerated increase in mobile transactions[1] coupled with the free distribution of downloadable applications has created a significant security and management challenge for banks and other financial institutions. The combination of applications, sometimes installed from untrustworthy sources, and the constant increase in mobile malware[2] and mobile fraud poses a real threat to sensitive and confidential information that is received by, transmitted by and stored on end users' mobile devices.

As users increasingly adopt mobile devices, and financial institutions increasingly focus on delivering a seamless user experience, the opportunity for fraudulent activity lurks alongside the proliferation of legitimate banking applications. Forrester Research has estimated that US smartphone payments will top USD142 billion by 2019[3]—and it is the experience of security professionals, including the IBM® Security Trusteer® research team, that where there is growth, there is fraud.

To successfully combat evolving threats, banks and financial institutions need a different paradigm—one that provides secure and effective, nonintrusive, frictionless banking. This model must be easy to implement, manage and operate, require minimal operational support, and must be highly adaptable to address new threats. Coupled with a tiered approach, the solution must be able to incorporate new countermeasures without any intervention by bank security staff and without any noticeable impact to banking customers.

Understanding mobile fraud risk

In the more mature web channel, banks and other financial institutions have achieved the right balance between security, usability and performance. The mobile channel, however, often places the greatest emphasis on providing a seamless user experience that is not overwhelmed by authentication and security measures. This emphasis on customer experience and ease of use—coupled with a focus that can make acquiring and maintaining customers a priority over guarding against potential fraud losses—can open the door to the rapid growth of threats from malware and fraud.

Combining capabilities for improved security

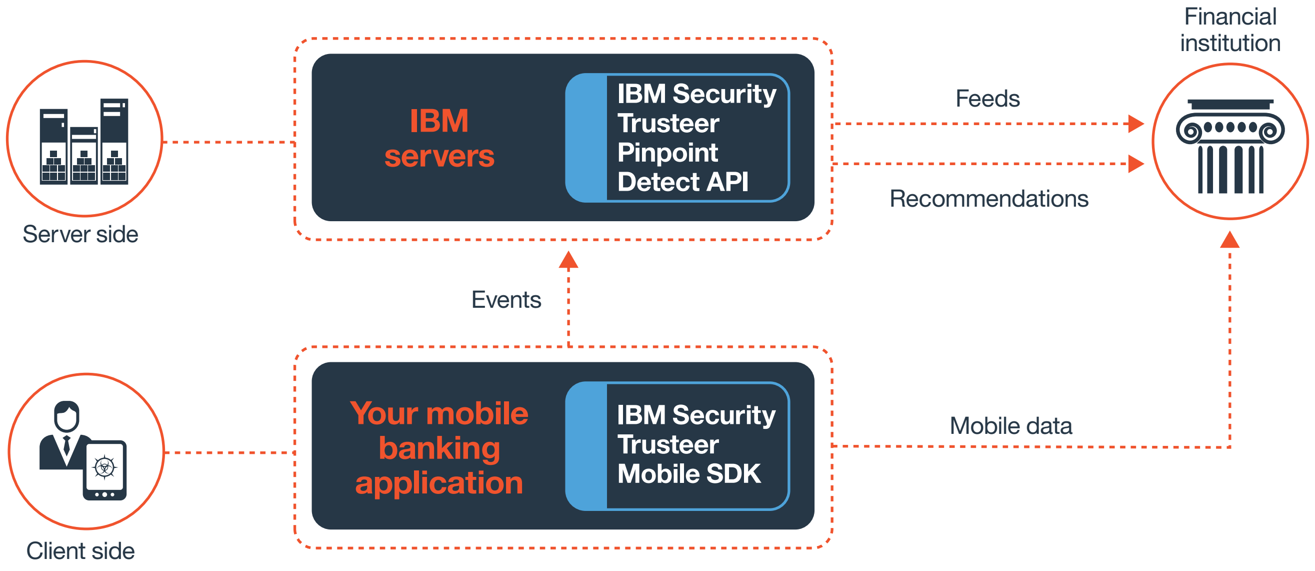
Financial institutions that offer mobile banking solutions need to accommodate several end-user access patterns, including dedicated applications and third-party mobile browsers. They also need to manage multiple authentication schemes, such as short message service (SMS), out-of-band (OOB) data, one-time password and others.

The proposed solution should also help to prevent multiple attack vectors that target user devices, such as man-in-the-middle (MitM) exploits, Domain Name Server (DNS) spoofing, certificate forging and mobile malware variants—including keyloggers, overlay attacks and banking Trojans. By defending against these attack vectors, financial institutions can help protect against client-side mobile threats that attempt to steal personal information and execute fraudulent transactions on behalf of legitimate users.

Furthermore, having the server-side capability to correlate and aggregate critical fraud indicators—phishing attacks, malware infections, compromised credentials and advanced evasion methods—can help to identify fraudulent behavior.

All of these building blocks, which are meaningful as standalone capabilities, can be combined to provide real-time recommendations and a comprehensive risk assessment based on a user's activity—including online and mobile activity. Financial institutions can then use this information to take immediate action to mitigate potential fraud losses.

Assessing mobile device risk: IBM Security Trusteer Mobile SDK


Server side
IBM servers
IBM Security Trusteer Pinpoint Detect API
Feeds
Recommendations
Financial institution
Events
Client side
Your mobile banking application
IBM Security Trusteer Mobile SDK
Mobile data

IBM Security Trusteer Mobile SDK

IBM Security Trusteer Mobile SDK transparently collects and helps assess mobile device risk. Trusteer Mobile SDK helps maintain the integrity of the application in which it has been embedded and continues to analyze the device and report on malicious activity or potential threats. This allows banks and other financial institutions to meet the critical balance between security and user experience.

High-risk access detection

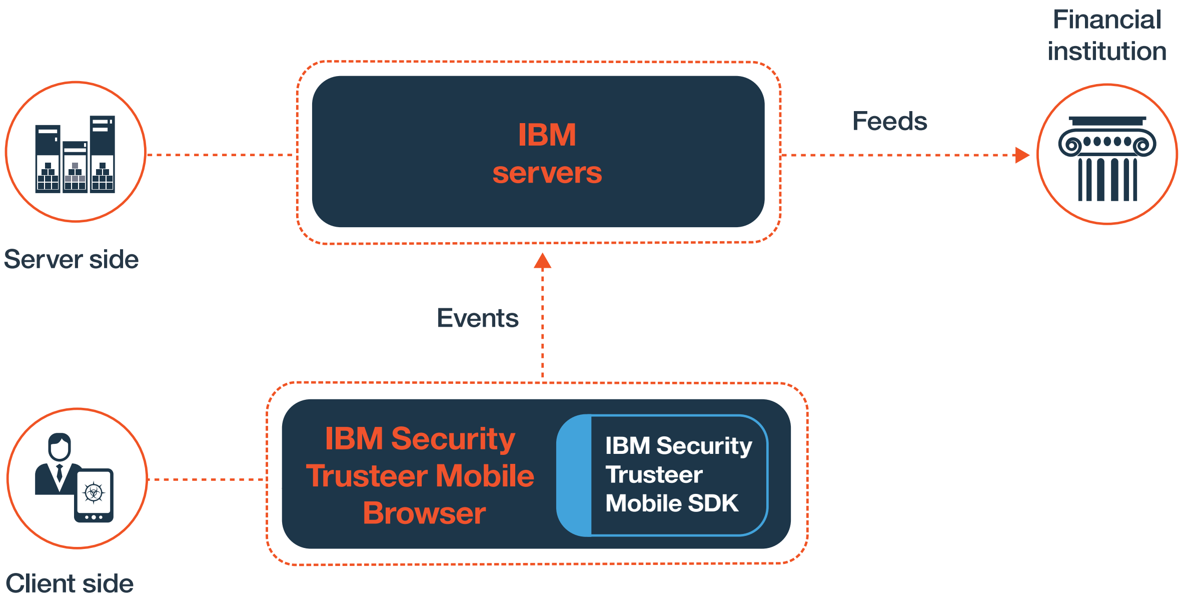
Trusteer Mobile SDK provides visibility into potentially high-risk activities to alert banks about the detection of potential threats, malware or malicious activities, and to enable making real-time decisions about security actions. Trusteer Mobile SDK enables the bank to maintain the balance between security and user experience while analyzing and providing real-time indicators to the banking application to assist the bank in taking appropriate action.

The banking application can take immediate action (on the device itself), it can send data to back-end systems for further investigation and future use, or it can do both for complete cross-channel coverage. For example, Trusteer Mobile SDK can detect a user attempting to access an online banking application from a jailbroken or rooted device. The banking application can consequently limit high-risk functionality—such as adding a new payee or transferring large sums of money.

IBM Security Trusteer Mobile Browser

For customers who do not have a native mobile banking application, IBM Security Trusteer Mobile Browser provides secure access to the banking website. It provides protection layers that enable secure browsing and protected transactions. Trusteer Mobile Browser includes a secure browser leveraging the security provided by Trusteer Mobile SDK to help detect malware, device vulnerabilities, pharming attacks, validation of Secure Sockets Layer (SSL) certificates and other threats. Organizations can provide banking websites that are accessed only through Trusteer Mobile Browser using a unique user agent that is defined for Trusteer Mobile Browser.

Providing secure access: IBM Security Trusteer Mobile Browser


Financial institution
IBM servers
Feeds
Server side
Events
IBM Security Trusteer Mobile Browser
IBM Security Trusteer Mobile SDK
Client side

A better way to address mobile challenges

IBM Security Trusteer solutions are trusted by more than 450 organizations worldwide for fraud prevention and protection. These proven technologies enable organizations to protect their customers and business-critical resources from the latest security threats. As new threats emerge, IBM Security Trusteer solutions help organizations protect against the ever-changing threat landscape and attack tactics that cybercriminals use in attempting to conduct online fraud.

IBM Security Trusteer Mobile solutions help address a wide range of security business challenges faced by banks and other financial institutions as described in the following table:

Business challenge	IBM Security Trusteer solution
Proactively detect online fraud for both mobile applications and mobile browsers	Supports both browser-based and application-based access via Trusteer Mobile Browser and Trusteer Mobile SDK, providing financial institutions with complete coverage for both access paths. Trusteer Pinpoint Detect collects and assesses session performance via Trusteer Mobile Browser or any native browsers on tablets or smartphones, thus detecting and correlating risks from possible access paths.
Manage access to an account via multiple device types including tablets, PCs and smartphones	Supports major mobile operating systems; continually adds new features and enhanced capabilities to help mitigate the latest and most prevalent threats.
Correlate online and mobile banking risk data for reliable mobile risk detection	Incorporates account risk factors including persistent mobile device ID, device location, malware infections and phishing incidents while providing risk data that helps detect account takeover attempts from mobile devices using compromised credentials.
Minimize friction for valued and reliable customers	Transparently operates behind the scenes to allow the bank or financial institution to control the flow of the online banking application as a result of risk data, device data and account data parameters.
Detect malware on compromised mobile devices	Provides visibility into potentially high-risk activities; alerts the bank to potential threats and the detection of malware or malicious activities to enable real-time security decisions.
Improve differentiation of user devices	Creates a persistent mobile device ID that allows organizations to identify any device using the mobile banking application. The persistent device ID is associated with the end user’s account and uniquely identifies the device.
Augment certificate authority security	Verifies the financial institution’s server certificate against trusted validation data as an effective way to detect and block potential man-in-the-middle attacks.
Enhance active protection	Actively detects the existence of root evasion techniques on Google Android devices such as root hiders and active hiding techniques.
Help enable compliance with guidelines and regulations	Analyzes sessions and correlates user behavior indicators such as geolocation and information, along with device attributes to create evidence-based detection.

IBM Security Trusteer Pinpoint Detect

IBM Security Trusteer Pinpoint™ Detect delivers cutting-edge cybercrime detection and analysis. It incorporates evidence-based indicators to deliver a comprehensive view across the entire fraud lifecycle on both PC and the mobile channel. Trusteer Pinpoint Detect provides a real-time mobile channel risk assessment that helps organizations stop fraud in its tracks while mitigating the risk on the endpoint. This is achieved by producing accurate, reliable and actionable recommendations such as allowing a transaction, restricting access to certain features on high-risk devices or denying end-user access. Organizations can use these recommendations to apply stepped-up authentication or extended transaction review for high-risk end users, sessions and transactions.

Detect high-risk devices based on multiple data sources

Trusteer Pinpoint Detect collects detailed risk information from the mobile device, including evidence of malware infections, information on jailbroken and rooted devices, accurate geolocation, and Wi-Fi security status, allowing the solution to generate accurate actionable recommendations.

Using a dedicated Trusteer Pinpoint Detect application programming interface (API), aggregated session information and real-time mobile device data is fed back to Trusteer Pinpoint Detect, which in turn provides a full risk assessment based on multiple collected indicators. As a result, Trusteer Pinpoint Detect provides the bank with recommendations of how to best handle the specific evaluated session.

Correlate online and mobile banking risk data for reliable mobile risk detection

To address complex cross-channel attacks, Trusteer Pinpoint Detect correlates a wide range of critical fraud indicators—including malware infections, phishing attacks, compromised credentials, and advanced evasion methods as collected by IBM client-side and clientless fraud-prevention solutions. Trusteer Pinpoint Detect leverages this risk data to help detect account takeover attempts from mobile devices that are using credentials that have been compromised on other channels.

Why IBM?

The IBM Security platform provides the security intelligence to help organizations holistically protect their customers, data, applications and infrastructure from security threats. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations.

For more information

To learn more about Trusteer Pinpoint Detect or Trusteer Fraud Protection Suite, please contact your IBM representative or IBM Business Partner, or visit the following websites: **ibm.com**/security or **ibm.com**/software/products/en/trusteer-fraud-protection-suite

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2016

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Recycle

[1] “Global mobile payment transaction volume from 2015 to 2019 (in billion U.S. dollars),” *Statista*, 2016. Accessed April 19, 2016. http://www.statista.com/statistics/226530/mobile-payment-transaction-volume-forecast/

[2] “2015 Mobile Threat Report – The Rise of Mobile Malware,” *Security Intelligence*. Accessed April 19, 2016. https://securityintelligencecom/events/the-current-state-of-mobile-threats/

[3] “US Mobile Payments To Reach $142 Billion By 2019,” *Forrester Research*, November 17, 2014. https://www.forrester.com/US+Mobile+Payments+To+Reach+142+Billion+By+2019/-/E-PRE7454