Mobile fraud prevention: IBM MobileFirst Platform and Trusteer Mobile SDK

Detect risks and help secure mobile transactions with an integrated, best-in-class platform

Highlights

- Help make mobile banking safe and secure by adding best-in-class security to your mobile banking applications
- Make your mobile banking application risk aware
- Allow, deny or restrict functionality of applications based on device risk scores
- Leverage persistent mobile device IDs to uniquely identify devices

As fraudsters have become increasingly savvy at tampering with transactions, capturing login credentials and taking control of device functions, securing mobile banking applications has become an item of paramount importance. The implications of security weaknesses are significant, as worldwide losses to cybercrimes of all sorts—including those on the mobile platform—have topped USD400 billion annually.[1] Meanwhile, compliance requirements are driving banking organizations to increase security across all channels.

With 33 percent of all mobile phone owners—and 51 percent of smartphone owners—now conducting financial transactions on their devices, mobile banking usage continues to grow.[2] Unfortunately, the growth in mobile banking activity has also increased the risk of mobile banking fraud. That's because as other platforms have become increasingly hardened against attack, fraudsters have been driven toward cross-channel and mobile attacks—with a new generation of malware designed to target mobile devices.

The result? Concerns over lack of security have become a significant deterrent to the financial industry's ability to grow the mobile channel, with both banks and their customers still reluctant to fully embrace the mobile banking options.[3]

To meet the challenge IBM® Security Trusteer® Mobile SDK is now integrated into IBM MobileFirst Platform, formerly known as IBM Worklight®, making it easier for banks to create secure, best-in-breed mobile banking solutions. Using IBM MobileFirst Platform, developers can integrate security capabilities into mobile banking applications to constantly keep up to date with the latest security features as they build, test, integrate and deploy applications—saving costs in development and maintenance, while achieving faster time to market.

Trusteer Mobile SDK enables developers to make mobile banking applications more secure by building in abilities to detect risk factors associated with devices attempting to access the institution's and its customers' resources. It enables organizations to block devices and restrict application functions based on risks, while maintaining a customer experience that delivers the convenience, ease and immediacy of mobile computing.

Quickly detect device risks to help secure mobile banking and prevent threats

With Trusteer Mobile SDK integrated into IBM MobileFirst Platform, developers can add robust security capabilities to their mobile banking applications, including real-time scanning for device risks such as:

- Malware infections
- Jailbroken or rooted devices (including the use of root hiders)
- Malicious or fraudulent applications
- Outdated operating system vulnerabilities
- Unsecured WiFi access

Detecting mobile malware infections

Defending against malware is a significant challenge for mobile banking. One study has reported, in fact, that malicious code infects more than 15 million mobile devices at any given time.[4] Mobile devices can be infected when users unintentionally access malicious or compromised websites targeting mobile browser vulnerabilities. In this scenario, a malicious application is downloaded and runs undetected, so the user never sees any suspicious activity.

For example, a customer's device with a banking application installed may become infected when the user opens or downloads a document received via email or accesses a website that was maliciously designed to infect the device. Once the device is infected, the fraudster can gain access to the mobile banking application and compromise the user's credentials. With Trusteer Mobile SDK installed as a feature of the mobile banking application, the existence of malware on a user's device can be detected immediately. Trusteer Mobile SDK then informs the mobile banking application, so the appropriate policy steps can be taken to secure the device.

New malware threats such as WireLurker pop up every day, so staying aware of the latest threats can be a challenge. By recognizing the unique fingerprints of malware, however, Trusteer Mobile SDK can detect both known and unknown malware culprits.

Detecting jailbroken or rooted devices

Jailbroken (Apple iOS) or rooted (Google Android) devices—in which many of the built-in defenses are disarmed—are extremely susceptible to malware attacks and credentials theft. This is because an altered device can allow installation of unauthorized applications from insecure sources and stealing of application data. Trusteer Mobile SDK can detect jailbroken or rooted devices. Trusteer Mobile SDK can also detect the use of sophisticated root hiders used by fraudsters in an attempt conceal their attacks.

Identifying suspicious applications

Malware often masks itself as legitimate software, making applications downloaded from alternative markets suspect, if not outright dangerous. An application might appear to be

legitimate, but when installed it may ask for unusual permissions such as administrative rights or access to emails—both of which are beyond the scope of a legitimate application.
In a common scenario, hackers take the original code for a popular game or application and add features that would give them control over the user's device and enable them to commit financial fraud. Trusteer Mobile SDK can detect this activity immediately, and the solution applies the appropriate device risk score to the mobile application to block access to sensitive data.

Managing operating system vulnerabilities

Trusteer Mobile SDK maintains an up-to-date repository of all known vulnerabilities in mobile operating systems versions. Each vulnerability is assigned a specific risk score, allowing financial institutions to control the level of functionality or access they would like to give to users with outdated operating systems.

Providing protection during unsecured WiFi access

Customers who bank while using unsecured WiFi access—such as in a coffee shop or other public place—open themselves up to fraud. If the user continues on a public network, however, Trusteer Mobile SDK can detect the risk, apply the appropriate risk score to the mobile banking application and take necessary action to prevent system compromise or man-in-the-middle banking fraud attacks.

Generate a unique ID for each device to help keep threats at bay

Trusteer Mobile SDK creates a persistent device ID allowing you to uniquely identify any device. The persistent device ID—along with the device's International Mobile Station Equipment Identity (IMEI) number and IDs for components including CPU, battery and chip—can be associated with the user's account in order to uniquely identify the device, even across removal and re-installation of the mobile application. This ensures that new devices are identified, login attempts from known devices are not challenged and potential fraudster devices can be flagged.

Powerful benefits for banks and customers

IBM MobileFirst Platform supports all development approaches (native, hybrid and web); connects to and synchronizes enterprise data, applications and cloud services more easily; and manages development of the financial institution's mobile application portfolio from one central control point.
Using the integrated Trusteer Mobile SDK component in IBM MobileFirst Platform enables institutions to better manage their mobile banking applications—because they can know and manage their mobile fraud risk and defend mobile applications against fraud with powerful, risk-aware capabilities.

Why IBM?

IBM provides mobile security solutions that are trusted by organizations worldwide for fraud and cybercrime prevention. Proven IBM technologies enable organizations to protect their customers, employees and business-critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products and services. IBM empowers organizations to reduce their security vulnerabilities and focus on the success of their strategic initiatives.

For more information

To learn more about IBM MobileFirst Platform, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/mobilefirstfoundation

To learn more about IBM Security Trusteer Mobile SDK, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security/trusteer

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

[1] Jeremy Kirk, "Cybercrime losses top $400 billion worldwide, study claims," IDG News Service, October 6, 2014. http://news.idg.no/cw/art.cfm?id=31CFC814-BA8E-4466-DBD8CAA511B5F1F6

[2] Board of Governors of the Federal Reserve System, "Consumes and Mobile Financial Services 2104," March 2014. http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf

[3] Kount, The Fraud Practice and CardNotPresent.com, "Mobile Payments & Fraud Survey: 2014 Report," *Kount*, 2014. http://www.paymentscardsandmobile.com/wp-content/uploads/2012/08/Mobile-Payments-and-Fraud-Survey-2014.pdf

[4] Alcatel-Lucent, "Kindsight Security Labs Malware Report – H1 2014." http://www.alcatel-lucent.com/solutions/malware-reports

Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
December 2014

WGS03045-USEN-00