IBM Security Trusteer Mobile SDK

Embedded security library for native mobile apps

Highlights

- **Reliable fraud detection:** combines multiple parameters such as device, session, and account risk factor to reliably detect fraud
- **Active protection**: active protection against financial malware, pharming attacks, and fake websites
- **Easy integration:** quick and simple integration with out-of-the-box options and parameters

IBM® Security Trusteer Mobile SDK overview

Trusteer Mobile SDK protects organizations' native mobile applications by performing device risk factors analysis and also provides a persistent mobile device ID. Trusteer Mobile SDK offers a library that enables application security services for mobile applications. This library can be used to build your custom application with Trusteer Mobile SDK's advanced security features. The core functionality provided by the library is as follows:

- Device risk detection.
- Active protection.
- API interface to IBM® Security Trusteer Mobile Risk Engine.
- Distinct and persistent device ID creation.

Benefits of using Trusteer Mobile SDK

- Detects device, session, and account risk factors to reliably detect fraud.
- Easy to integrate into the bank's existing application.
- Delivers a seamless user experience with enhanced security, without compromising on application usability.
- Helps proactively detect and prevent fraud, even in the face of active malware.
- Available as part of the IBM Security Trusteer suite of mobile fraud-prevention solutions fraud prevention solutions or as a standalone solution.

Key features

Device risk detection

Risk detection may be based on a variety of indicators such as jailbroken/rooted device detection, malware infection detection, and Wi-Fi network security state. The granular risk data is provided to the mobile application.

Persistent device ID

Trusteer Mobile SDK creates a persistent mobile device ID allowing organizations to distinctly identify any device using the native mobile banking application. The persistent device ID is associated with the end user's account and distinctly identifies the device, even after the phone is re-imaged. This helps ensure that new devices are identified, login attempts from known devices are unchallenged, and potential fraudster devices are flagged.

Trusteer Mobile SDK provides functions to retrieve the risk score for the risks listed in the following table:

Risk name	Threshold details
Wi-Fi	Indication that the device is using secure Wi-Fi.
Trusteer Mobile SDK up-to-date	Indicates whether the currently installed version of Trusteer Mobile SDK has the latest configuration version.
OS up-to-date	Indicates whether the OS on the device is the latest version.
Malware	Indication that the device is infected with malware.
Rooted/jailbroken	Rooted/jailbroken device or not.
Restrict	(Android only) Indication that only Android app-market applications are allowed on the device. The device risk is higher when non-Android marketplace apps are allowed.
Suspicious system	(Android only) Indication that there are high-risk system configurations, such as unknown SMS listeners.
Root evasion	Allows detection of root evasion techniques such as root hiders and active hiding techniques.
SSL certificate validation	Allows whitelisting and blacklisting of certificates.

Based on the specific risk attributes, the risk score, and your specific business policy, the embedding application can implement security policies, such as disabling high-risk activities like wire transfers or adding payees from jailbroken devices.

Active protection

Trusteer Mobile SDK provides protection of IP and SSL communication performed by the application against pharming attacks. Protected websites are pre-configured into the system, and Trusteer Mobile SDK validates both IP address and the SSL certificate any time a protected website is accessed. Protection is provided through a combination of reconfigured data and validation with a secured DNS server. Protection is performed invisibly to the application and requires no work by the application developer, except determining the protected addresses.

High-risk access detection

Trusteer Mobile SDK provides a technological framework which enables you to integrate it into your native app so that it is automatically invoked when the end user launches it. The product also actively collects various device risk factors which are fed back to the bank's mobile banking application to allow the bank to restrict functionality based on the device risk level. For example, the solution can limit specific application functions – such as adding a payee or transferring money on a modified, jailbroken/rooted device.

Why IBM?

IBM Security solutions are trusted by organizations worldwide for fraud prevention and identity and access management. The proven 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, services and business partner solutions. 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 Security fraud-prevention solutions and IBM® Security Trusteer Apex Advanced Malware Protection, please contact your IBM representative or IBM Business Partner, or visit the following website:
ibm.com/security

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

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
August 2014

Trusteer was acquired by IBM in August of 2013.

Please Recycle

WGD03036-USEN-00