

WHITEPAPER

TrustDefender™ Mobile

Fraud Screening for Mobile Devices

ThreatMetrix™ Cybercrime Defender Platform



Overview

Consumers have embraced mobile devices in a big way; smartphones have outsold personal computers since the last quarter of 2010. Mobile transaction volumes across the ThreatMetrix™ global network grew by 500% in 2011 alone. Companies and organizations have capitalized on this trend by offering online services tailored for mobile devices.

While this growing mobility is convenient for end users, it has increased the complexity of managing online services. Multiple front end entry points need to be developed and maintained. This is a particular challenge for organizations that support both a traditional browser-based interface as well as a mobile application (app-based) front end. Multiple application front ends means multiple versions of application code to support.

Often overlooked is the associated complexity of fraud management across these disparate front ends. Ideally, organizations could use a common platform to automatically screen all transactions for fraud – regardless of originating device – yet still detect anomalies specific to the device type.

This paper describes how ThreatMetrix TrustDefender™ Mobile SDK, used in conjunction with ThreatMetrix™ Cybercrime Defender Platform, provides comprehensive, real-time fraud screening of all online transactions, whether originating from a PC browser, a mobile browser, a smartphone, or a tablet.

Device Verification and Identification Challenges for Mobile

Mobile devices present unique challenges for device identification when compared to personal computers and other traditional endpoints.

Changes in User Behavior and Expectations

Transactions originating from mobile devices may have very different characteristics from those on laptops. Traditional fraud detection techniques that rely on manual review may conflict with the user's expectation of immediate gratification.

Limited Options for Browser Identification

For years, the advertising industry has relied on Flash cookies to retarget users even when they cleared their regular cookie cache. No such luxury is available for Apple's iOS, which does not support Flash. For most users, third-party browser cookies are blocked by default. And on iOS devices, the Safari browser limits fingerprinting of browser attributes.

Lack of Consistent Hardware Identifiers

The various mobile OS libraries do not provide a common, consistent API that can be used to uniquely identify a device. (In 2011, with the release of Apple iOS 5, Apple deprecated its UDID that applications developers had been using to uniquely identify a phone). Various unique attributes are associated with a phone, including the phone number, a serial number, and an IMEI number. However, due to privacy concerns, these attributes are not generally available through a native API. Those that are tend to be easily subverted by fraudsters if used as a single authentication factor.

Changeable Application IDs

Mobile application developers commonly generate a unique ID when the application is installed to aid in device identification. Then, whenever the mobile application needs to communicate with the back end service, it provides the application ID that was established at install time.

For use in application logic, this approach works well. But for use in fraud screening, this approach is limited because it is not a true device identifier; it is an application + device identifier. Uninstalling the application and reinstalling it would yield a new identifier. Also, these identifiers are not global – there is no way to correlate suspicious transactions from two different applications on the same device.

Privacy and Usability Concerns

Recent privacy scandals demonstrate that users are becoming more educated and concerned about applications that leak their identity and location. For effective fraud screening, any device identifiers should be anonymized prior to leaving the customer's handset. In addition, fraud screening should only use attributes that do not require the explicit consent of the device owner.

Mobile Malware

Cybercriminals have recently started targeting mobile devices given the popularity of SMS one-time-passwords as a second authentication factor for online banking. This trend will only increase as mobile wallets and stored-value payments make the mobile device even more attractive for online fraud.

Lack of Integrated Fraud Screening Tools and Processes

Enterprises are struggling to glue together data supplied from their mobile application developers, dedicated HTML5 optimized mobile sites and traditional PC-oriented websites to make fraud decisions in real-time.

TrustDefender Mobile

TrustDefender Mobile provides a software developer kit (SDK) that leverages the broader ThreatMetrix Cybercrime Defender Platform for detecting fraud originating from mobile devices in real time.

TrustDefender Mobile provides mobile application developers with OS specific libraries that generate device identifiers for use with the ThreatMetrix Cybercrime Defender Platform. Used in combination with TrustDefender™ ID and TrustDefender™ Cloud, TrustDefender Mobile provides real-time risk screening through three separate techniques:

- **Hardware Fingerprinting:** a method that collects non-personal attributes directly using the TrustDefender Mobile SDK to generate device identifiers and checksums to detect subversion. The mobile application can transmit the identifiers to your back end server application and the ThreatMetrix standard HTTPS API.
- **Browser and Connection Fingerprinting:** a method that loads the standard TrustDefender ID HTML tags inside a hidden, embedded browser within the mobile application. This initiates web profiling with the ThreatMetrix device profiling service, collecting information from the TCP/IP packets and setting browser cookies.
- **Page Fingerprinting:** a method that loads the TrustDefender Cloud HTML tags inside a hidden, embedded browser within your mobile application. This initiates the page fingerprinting and verification that can instantly detect transaction modifications made by Trojans.

After these methods are called within the mobile application, the response, along with a transaction, is passed to your back end server for processing. Within your transaction processing code, an API call is made to the cloud-based TrustDefender Cybercrime Defender Platform for real time evaluation against a customizable fraud screening policy to inform your process whether to accept, reject or review the transaction.

The ThreatMetrix Cybercrime Control Center rules engine allows for the flexible definition of custom risk factors for mobile application vs. mobile browser vs. PC browser transactions. For example:

- Detect high velocity of cookie wiping with respect to hardware configuration
- Detect UDID tampering via jail breaking
- Detect use of scripts, PCs or virtual machines disguising themselves as mobile phones via changes to browser and HTTP headers
- Detect mobile apps being accessed from multiple devices
- Detect suspicious high velocity spend amounts
- Detect account hijacks based on access from multiple time-zones
- Detect use of hidden proxies
- Detect suspicious page injections by mobile malware or man-in-the-middle attacks

Conclusion

The age of mobile has arrived, and with it a new set of challenges and complexities for safely managing online access and transactions without degrading the user experience. TrustDefender Mobile as part of the ThreatMetrix Cybercrime Defender Platform is the first industry solution that integrates sophisticated malware detection and advanced device identification technologies in a single, unified platform across all device platforms.

Contact Us

USA Corporate Headquarters:

ThreatMetrix Inc.
160 West Santa Clara Street
Suite 1400
San Jose, CA, 95113
Telephone: +1.408.200.5755
Fax: +1.408.200.5799

EMEA Headquarters:

ThreatMetrix B.V.
Laan van Vredenoord 33-39
2289 DA Rijswijk
The Netherlands
Telephone: +31 (0)70 8200 508

www.threatmetrix.com

www.threatmetrix.com/fraudsandends