Solution Brief

Location Spoofing Detection

Challenges

Mobile apps that rely on accurate location, including apps for gambling and gaming, social, dating, transportation and food delivery share one thing in common: the challenge of detecting location spoofing.

Location spoofing has many purposes, depending on the nature of the app, but the primary intent is to hide a user's true location.

Evading geo-blocking is a common use case for location spoofing. In this case the goal of location spoofing is to circumvent controls (often resulting from regulations) restricting access to apps, systems or other types of digital content based on the location of the user. Usually geo-blocking applies to services such as streaming, gambling, gaming and others.

Location spoofing for social networks and dating apps represents a trust and safety issue. For delivery and transportation apps, location spoofing is being used for fraud by drivers.

Because traditional location-based signals such as IP address and GPS are a common risk signal used by services for compliance, fraud, and authentication, a spoofed GPS location poses a clear security risk. Fraudsters have several ways to spoof location, including low tech techniques such a GPS spoofing app, which are now more commonly used to bypass certain security features and commit certain types of mobile fraud, such as account takeover or SIM swap attack.

Location spoofing fraud is on the rise as fraudsters adopt new techniques, resulting in financial losses, and high false-positive rates that negatively impact legitimate users, low customer satisfaction and damaged brand reputation.

Solution

GPS spoofing alters the signals or data associated with the Global Positioning System to produce different position, navigation, or timing (PNT) information. It's a way to trick the GPS receiver and its applications, allowing it to consider that the user is in another location. Incognia is highly effective in detecting GPS spoofing in two ways:

01

The initial action is to search for the presence of GPS spoofing apps on the operating systems. They will indicate whether a GPS spoofing app is present and enabled.

02

To detect more sophisticated GPS spoofing techniques, Incognia verifies the existence of inconsistencies between GPS and other signals, including Wifi, cellular network, and IP. Based on that, if a fraudster is attempting to spoof a user's location, it would be required to obtain a recent Wifi scan to bypass this detection layer.

The Incognia SDK collects anonymous location data from mobile devices through its proprietary location technology, using GPS, Wi-Fi, cellular, and Bluetooth sensors data, unlike fraud detection based on IP and GPS alone. Each user's location behavior pattern is unique and made up of frequently visited locations, classified as Trusted Locations. Whenever a user tries to log in or perform a sensitive transaction in the app from a new or existing device, Incognia provides a risk score and associated evidence through Incognia's API, based on the correlation of current and historical user location behavior and device intelligence data. Incognia maps and correlates the unique signature of GPS coordinates and available network signals of each location to create unique environments with high accuracy and precision to identify a location and detect location spoofing. It is efficient because the environments are very dynamic. The addition of a Wi-Fi router nearby changes the environment fingerprint and the conditions that were at first considered for that activity. In addition to requiring the most updated location fingerprint, Incognia also processes the sensor data, which makes it even harder to spoof the location signal.

In addition, Incognia maintains a watchlist of over 150 million devices previously associated with fraudulent activity, including devices accessing multiple accounts, emulator usage, and location spoofing. Incognia also performs several additional real-time device integrity checks at login or transaction events, such as looking for compromised software configuration, presence of VPNs, proxies, GPS spoofing apps, root/jailbreak, use of mobile emulators, and app installation from unofficial app stores.

Key Benefits

Resistant to all location spoofing techniques

In addition to GPS spoofing, Incognia detects and informs in each risk assessment the usage of VPNs and Proxies, emulators, instrumentation tools and app tampering.

Increased account security

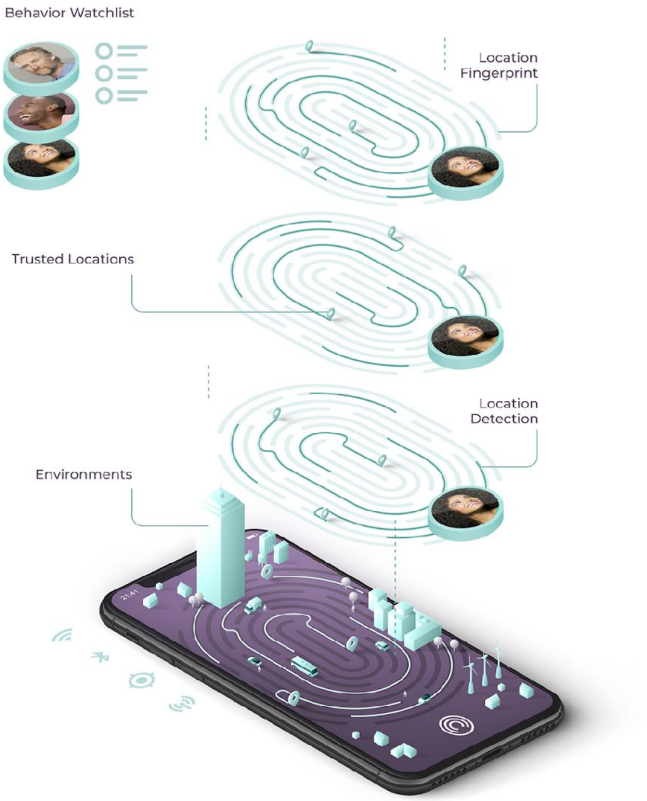
Reduce financial losses from location spoofing fraud, account takeovers and protect the complete user in-app journey, easily identifying bad actors and optimizing legitimate users' experience.

Zero friction authentication for trusted users

Working silently in the background, Incognia requires no action from users, instead relying on their unique location behavior and device data.

Highly Effective

- Highly resistant to location spoofing
- **Low fraud rate:** Below 1 in 100,000,000
- **Low false-positive rate:** Less than 0.001%.
- **Low false-negative rate:** Less than 0.003%



Key Capabilities

Incognia uses multiple location-related signals, beyond GPS, to detect location spoofing, while assessing a user's location in real-time. Additionally, Incognia's location and device watchlist enables immediate re-identification of bad actors and locations previously associated with fraud, verifying the usage of spoofing techniques such as spoofing apps, VPNs, Proxies and Emulators. All this detection evidence that supports the risk scoring is delivered in Incognia's easily consumable APIs, providing transparency and enabling a more clear and secure risk decision making process. The risk assessments delivered are dynamic due to the improvement of the Incognia algorithms and can result in a user or device becoming part of a watchlist after fraud or suspicious location spoofing behavior detection. The algorithms consider a holistic and proactive approach that combines risk and anomaly detection at both the location and the device layers to help businesses solve several types of challenges related to location spoofing.

Incognia's signals for increased account security against location spoofing

With Incognia, realize frictionless, passwordless authentication to reduce fraud and friction for legitimate mobile users, while protecting accounts against location spoofing and bad actors. Utilizing dynamic location and device fingerprinting, robust analysis like Operating System-level evidence that indicates source of location signal, the mismatch between signal environment and GPS and scan of known GPS spoofing and VPN apps are key differentiators. Incognia enables fast integration of the SDK and APIs that deliver actionable intelligence from day one through highly precise risk scoring in real-time, with minor false-negative rates. Incognia's Zero-Factor Authentication provides a superior defense to application accounts, highly resilient to location spoofing techniques, distinguishing legitimate users from fraudsters through its unique location technology and device intelligence data.

Key Features

Frictionless continuous mobile authentication

- Supports iOS and Android mobile devices

Highly accurate risk-assessments

- Location fingerprint and location analytics
- Device fingerprint and device integrity
- Behavior watchlist and network effect

Lightweight SDK

- 415 KB (Android)
- 1.5 MB (iOS)
- Battery usage: ~0.5% per day

Easy to integrate and use APIs & Webhook

- REST & JSON Response
- Average response time: 60 ms
- Low latency of the Incognia APIs
- Integration time: 1 hour

Use as stand-alone authentication solution or integrate to your risk-engine

Advanced technical support

- Open documentation
- API reference
- How-To Guides
- Developer Portal

Privacy and Security

- GDPR, CCPA and SOC 2 Compliant

About Incognia

Incognia is a privacy-first location identity company that provides frictionless mobile authentication to banks, fintech and mCommerce companies, for increased mobile revenue and lower fraud losses. Incognia's award-winning technology uses location signals and motion sensors to silently recognize trusted users based on their unique behavior patterns and is a key enabler for Zero-Factor Authentication. Deployed in over 100 million devices, Incognia delivers a highly precise risk signal with extremely low false positive rates.