Designing with Location as a Factor in Zero-Trust Architectures

Patterns for incorporating location assurance alongside identity, device health, and behavior - with examples spanning high-value access, remote work controls, and regulated operations.

Executive Summary

Zero-trust security architectures have matured around three verification axes: identity, device posture, and behavioral analytics. Yet these frameworks share a fundamental gap-they cannot reliably establish the physical location from which access originates. This limitation stems not from oversight but from the absence of commercially viable location verification technologies resistant to adversarial manipulation.

This brief examines location verification through the lens of signal physics and geophysical constraints. We analyze why dominant positioning technologies-GPS/GNSS, IP geolocation, and Wi-Fi fingerprinting-remain vulnerable to spoofing, and outline integration patterns for incorporating robust location assurance into zero-trust implementations. Our assessment is deliberately conservative regarding current capabilities while identifying the physical principles that could enable genuinely spoof-resistant positioning.

The Physics of Position Determination

All positioning systems exploit physical phenomena that vary predictably with location. Understanding their vulnerabilities requires examining the underlying signal physics.

GNSS Signal Characteristics

Global Navigation Satellite Systems-GPS, GLONASS, Galileo, BeiDou-operate by measuring time-of-arrival differences from satellites at known orbital positions. The fundamental vulnerability lies in signal power: GPS satellites transmit at approximately 20-50 watts from an altitude of 20,200 km, arriving at Earth's surface at roughly -130 dBm (10^{-16} watts). This places GNSS signals below the ambient RF noise floor; receivers extract positioning data only through correlation with known pseudorandom codes.

The civilian L1 C/A signal uses publicly documented spreading codes and navigation message structure. An adversary with a software-defined radio and a modest amplifier can generate counterfeit signals that overpower authentic transmissions by 10-20 dB-sufficient to capture receiver lock and inject arbitrary position solutions. The required equipment costs under $500; open-source spoofing software is freely available.

In contested electromagnetic environments, this vulnerability has moved from theoretical to operational. Open-source analyses of flight-log data (e.g., GPSJam) reported more than 46,000 flights experiencing GNSS issues over the Baltic region between August 2023 and spring 2024, a scale consistent with EASA’s own advisories about rising interference. Maritime analysts report GPS spoofing affecting thousands of vessels quarterly in the Black Sea, Arabian Gulf, and South China Sea. These incidents demonstrate that state and non-state actors routinely exploit GNSS vulnerabilities at scale.

Terrestrial RF Positioning

Wi-Fi and cellular positioning estimate location through received signal strength indication (RSSI) or time-difference-of-arrival (TDOA) measurements from known access points or base stations. While less susceptible to distant spoofing than satellite signals, these approaches carry their own limitations.

Wi-Fi fingerprinting databases can be poisoned through systematic submission of false access point locations. Portable access points can replicate MAC addresses and SSIDs of distant networks, causing

devices to report incorrect positions. Cellular positioning degrades significantly indoors and in urban canyons where multipath propagation dominates. All RF-based approaches that depend on external infrastructure (public cellular, Wi-Fi) fail entirely in shielded environments, underground facilities, and many GPS-denied contexts - precisely where robust positioning may matter most - unless you deploy dedicated in-situ beacons.

IP Geolocation Constraints

IP-based location infers position from network topology databases mapping address blocks to geographic regions. This approach suffers from both accuracy and authenticity limitations. Commercial IP geolocation services typically achieve country-level accuracy above 95%, but city-level accuracy drops to 50-80% depending on region and ISP. More critically, IP geolocation provides no resistance to proxying: VPN services, Tor exit nodes, and residential proxy networks trivially defeat any location inference. These tools are widely deployed, often for legitimate privacy purposes, making IP geolocation unsuitable as a security control.

Toward Geophysically-Grounded Positioning

The vulnerabilities above share a common root: they rely on signals that can be generated, replayed, or manipulated. Spoof-resistant positioning requires anchoring to physical phenomena that an adversary cannot fabricate - measurements that reflect genuine properties of the local environment.

Earth's Magnetic Field

The geomagnetic field presents one such opportunity. The main field, generated by convection in Earth's liquid outer core, varies smoothly with position according to well-characterized spherical harmonic models (IGRF, WMM). Superimposed on this are crustal anomalies-local variations of tens to hundreds of nanotesla caused by magnetized geological structures, ferromagnetic building materials, and infrastructure.

Unlike RF signals, the quasi-static magnetic field cannot realistically be generated at a distance. To counterfeit a field signature matching a distant location, an adversary would need to place ferromagnetic masses or electromagnets in the immediate vicinity of the device with the right geometry—impractical for most attack scenarios. The field penetrates structures where GPS fails: indoors, underground, in urban canyons, and within Faraday-shielded environments.

Practical magnetic positioning faces challenges. Crustal anomaly data coverage varies geographically; some regions are well-surveyed while others lack reference measurements. Temporal variations from solar activity and ionospheric currents introduce noise that must be modeled or filtered. Sensor calibration requires care, particularly on mobile devices where hard and soft iron distortions from device components affect measurements. These are engineering challenges rather than fundamental barriers, but they constrain achievable accuracy and availability.

Gravitational Signatures

Local gravitational acceleration varies with subsurface density structure, from approximately 9.78 m/s² at equatorial sea level to 9.83 m/s² at the poles, with smaller variations from terrain and geology. Gravimetry has a long history in geophysical surveying and could theoretically contribute to position determination.

In practice, gravity-based positioning remains confined to specialized applications. Detecting position-diagnostic gravity variations requires sensors with micro-gal (10^{-8} m/s²) resolution-laboratory instruments rather than mobile devices. Consumer MEMS accelerometers lack several orders of magnitude of the required precision. Gravity may eventually contribute to high-security positioning through quantum gravimeters or future sensor advances, but current technology does not support widespread deployment.

Inertial Navigation and Sensor Fusion

Inertial measurement units (IMUs)-accelerometers and gyroscopes-provide self-contained position tracking through dead reckoning. Modern MEMS sensors offer sufficient short-term stability for pedestrian and vehicle tracking over limited intervals. However, integration drift accumulates rapidly; consumer IMUs exhibit position errors growing at meters per minute without external correction.

The value of inertial sensing lies in fusion with other modalities. IMU data can validate or reject GPS position jumps inconsistent with physical motion. Sensor fusion architectures-typically Kalman filters or particle filters-combine measurements from multiple sensors, weighting each according to its uncertainty characteristics. A well-designed fusion system leverages the strengths of each input while remaining robust to individual sensor failures or attacks.

Integration Patterns for Zero-Trust Architectures

Assuming availability of location verification technology meeting an organization's accuracy and spoofing-resistance requirements, the following patterns describe how location assurance integrates with existing zero-trust infrastructure.

Pattern 1: Location as Authentication Factor

Incorporate verified location as a fourth authentication factor alongside knowledge (passwords), possession (tokens), and inherence (biometrics). At authentication time, the system confirms the user's physical presence within an authorized geographic zone before granting access. This differs from IP-based "location" checks in that it resists proxying and VPN circumvention.

Implementation notes: Define authorization zones at appropriate granularity-building, floor, or room level depending on use case and technology capability. Consider time-of-day policies (office hours versus after-hours access). Establish fallback procedures when location cannot be verified.

Pattern 2: Continuous Session Verification

Extend location verification beyond initial authentication to periodic re-verification throughout active sessions. If location becomes unverifiable or changes unexpectedly, trigger re-authentication or session termination. This addresses credential handoff scenarios where an authenticated user transfers their device to an unauthorized party.

Implementation notes: Balance verification frequency against power consumption and user experience. Consider risk-adaptive intervals-more frequent verification for sensitive operations, less frequent for routine access. Define acceptable location uncertainty bounds.

Pattern 3: Geofenced Resource Access

Associate data classifications or application permissions with geographic boundaries. Certain resources become accessible only when the requesting user is physically within designated areas. This creates defense-in-depth: even with valid credentials, an adversary cannot access geofenced resources from unauthorized locations.

Implementation notes: Align geofencing policies with data classification frameworks and regulatory requirements. Consider scenarios where legitimate access is needed outside normal boundaries (travel, emergencies) and design exception workflows accordingly.

Pattern 4: Location Anomaly Detection

Log verified location alongside access telemetry to enable retrospective analysis. Identify physically impossible patterns-authentication from New York at 09:00 and Singapore at 09:30, for instance-that

indicate credential compromise. Correlate location anomalies with other threat indicators in SIEM platforms.

Implementation notes: Establish baseline location patterns for users and roles. Define alert thresholds accounting for legitimate travel. Preserve location logs for forensic and compliance purposes while addressing privacy considerations through appropriate access controls and retention policies.

Pattern 5: Attestation for Remote and Field Operations

For distributed workforces and field operations, verify that personnel are physically present at claimed locations-home offices, client sites, inspection points, or operational areas. This supports compliance with remote work policies, validates field service activities, and provides audit evidence for regulated industries.

Implementation notes: Register authorized work locations during onboarding. Accommodate location changes through defined update procedures. Consider accuracy requirements for each use case-city-level for remote work policy, meter-level for safety-critical field operations.

Deployment Considerations

Organizations evaluating location verification technologies should assess capabilities against operational requirements:

- **Accuracy:** Match positioning precision to use case requirements. Continent or country verification differs fundamentally from building or room-level assurance. Specify accuracy as a statistical distribution (e.g., 95th percentile error bound), not a single nominal value.
- **Environment coverage:** Verify performance across actual operating environments-indoors, underground, in urban canyons, and in RF-contested settings. Technologies that work well in open outdoor conditions may degrade significantly inside buildings.
- **Spoofing resistance:** Evaluate adversary capabilities and attack costs. If commodity hardware defeats the positioning system, security value is limited. Prefer approaches requiring physical presence to falsify-not merely software manipulation or signal generation.
- **Sensor requirements:** Understand what device hardware is necessary. Solutions requiring specialized sensors limit deployment scope; those leveraging standard smartphone components enable broader adoption.
- **Reference data dependencies:** Some positioning approaches require pre-surveyed reference databases. Assess geographic coverage of available data and procedures for extending coverage to new areas.
- **Privacy architecture:** Design for minimum necessary data collection. Consider whether verification can produce binary authorized/unauthorized results without logging precise coordinates. Address data retention, access controls, and regulatory requirements.

Conclusion

Zero-trust security has advanced substantially in verifying identity, device integrity, and behavioral patterns. Location remains the underdeveloped fourth dimension-not for lack of recognition, but because dominant positioning technologies offer insufficient resistance to adversarial manipulation. GPS was designed for navigation, not authentication; its civilian signals were never intended to resist spoofing.

The path forward lies in positioning approaches grounded in geophysical phenomena that adversaries cannot practically falsify. Earth's magnetic field, gravitational variations, and multi-sensor fusion offer

foundations for spoof-resistant location verification-though each carries implementation challenges that constrain current accuracy and availability. As these technologies mature, organizations should prepare integration architectures that treat location as a first-class security primitive alongside identity, device, and behavior.

The stakes are significant. Credential theft, insider threats, and location-dependent fraud increasingly exploit the gap between where access *claims* to originate and where it *actually* originates. Closing this gap requires moving beyond signal-based positioning to verification anchored in the physical world.