

AttestLens: A Large-Scale Measurement of Play Integrity Adoption in Android Apps

Collin MacDonald & Stephen Herwig
William & Mary | Williamsburg, Virginia, USA

ACM WiSec 2026



Background

- Modern smartphones contain many high-value applications, ranging from banking and government services to social media and premium games.
- At the same time, Android faces growing threats year-over-year.
- How do developers (and the companies who back them) know their app and your device is trustworthy and hasn't been tampered with?
- One solution is to use an **Attestation Framework**, which acts as a kind of "health check" for your phone.

What is an Attestation Framework?

- A way for an app's server to evaluate if the app it is interacting with is trustworthy.
- Checks three things:
 1. App Integrity – Is this the real, unmodified app?
 2. Device Integrity – Is the device genuine and not rooted?
 3. Account Integrity – Is the user's Google account legitimate?
- SafetyNet (2017–2025): Google's first attestation framework for Android.
- Play Integrity (2022-Present): The replacement, with stronger security.
- Google claims apps using the Play Integrity attestation framework see 80% less unauthorized usage, but public data is less clear.

Research Questions

1. How widely is Play Integrity adopted in real-world apps?
2. What factors predict whether an app uses it?
3. Are developers migrating from SafetyNet to Play Integrity?
4. When apps use Play Integrity, is it their own code or external code?
5. Do developers combine Play Integrity with other security measures?

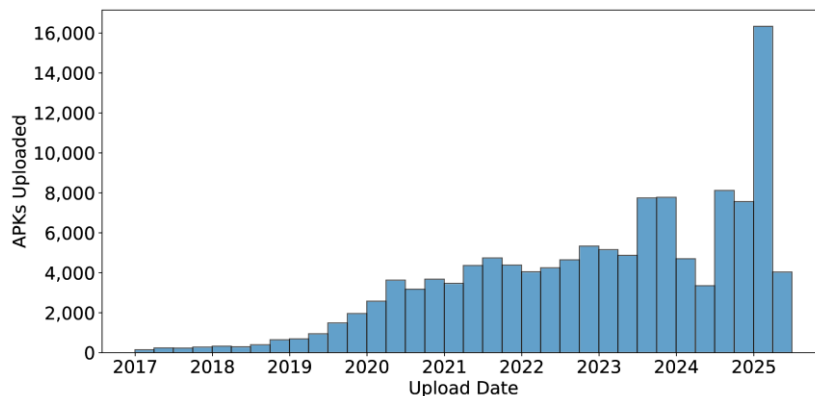
Data & Methodology

Dataset: 125,000 Android APKs from AndroZoo (University of Luxembourg).

Methodology: Multi-stage static code analysis on all downloaded APKs.

Usage Detection: Decomplied 7,334 apps with Play Integrity to understand usage.

Migration: Analyzed 814 government apps over time to assess longitudinal impacts of SafetyNet shutdown and Play Integrity migration.



App Categories

- **Popular:** 69,312 apps with 1M+ downloads.
- **Banking:** 12,847 apps (package name contains 'bank').
- **Crypto:** 4,371 apps (package name contains 'crypto').
- **Government:** 814 apps (package name starts with 'gov.'), all versions.
- **Gaming:** 20,000 published games.
- **Random:** 20,000 randomly sampled apps.

Adoption Findings

~90% of Apps Use No
Attestation

Adoption Findings

Category	Total Apps	No Attestation	SafetyNet	PI			SafetyNet + PI (Either)
				Classic	Standard	Both	
Popular	69,312	60,100 (86.7%)	2,788	1,800	92	4,005	527
Banking	12,847	11,521 (89.7%)	1,005	143	6	98	74
Crypto	4,371	3,957 (90.5%)	320	35	0	48	11
Government	814	710 (87.2%)	88	6	1	6	3
Games	20,000	19,003 (95.0%)	748	93	1	141	14
Random	20,000	18,170 (90.9%)	1,433	175	1	88	133

Attestation by Category

Popular: 69.7% of attestable apps use Play Integrity (often in combination with SafetyNet).

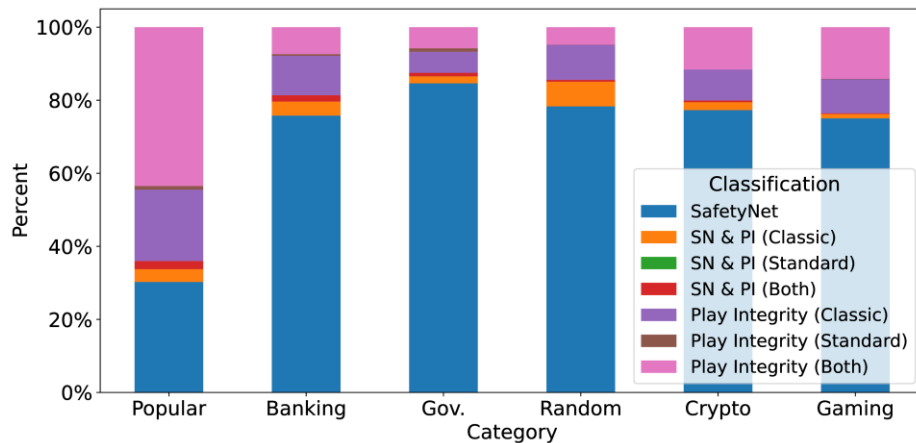
Banking: 75.8% only use SafetyNet.

Government: 84.6% only use SafetyNet, the *highest* among all six app categories.

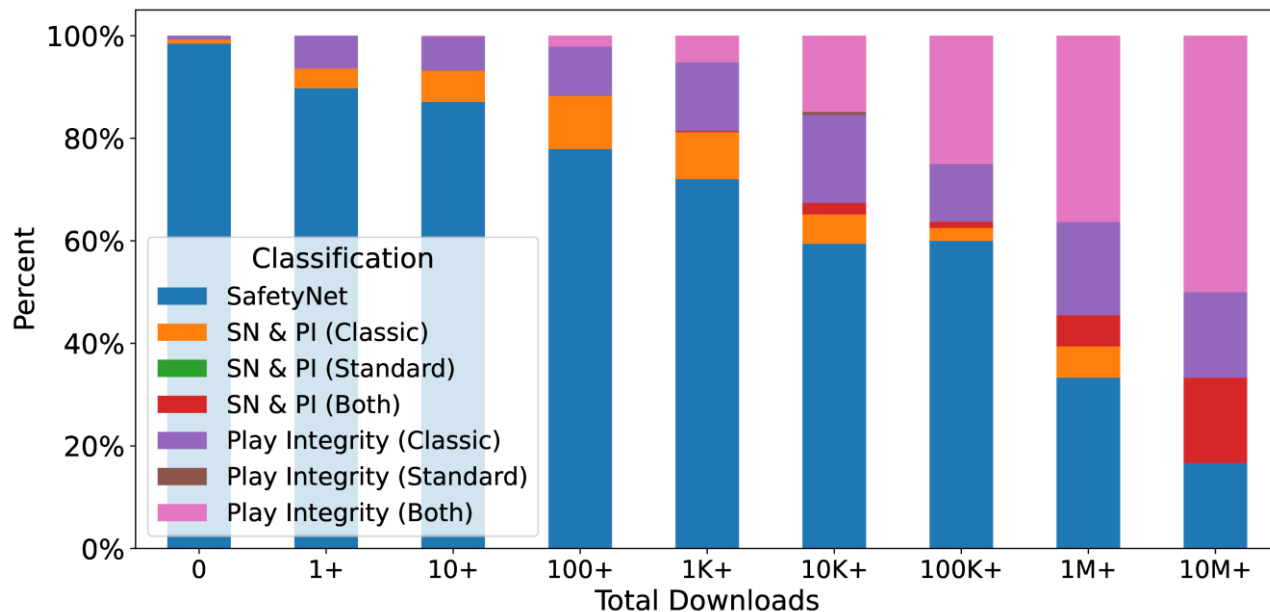
Random: 78.3% only use SafetyNet.

Crypto: 77.3% only use SafetyNet.

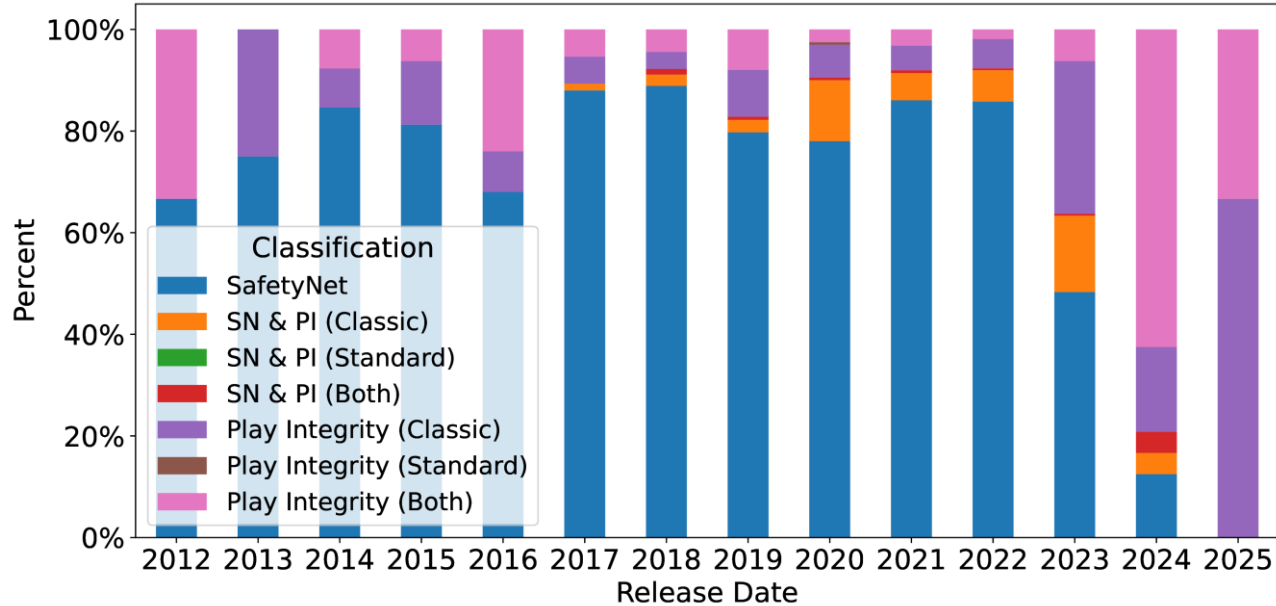
Gaming: 75.0% only use SafetyNet.



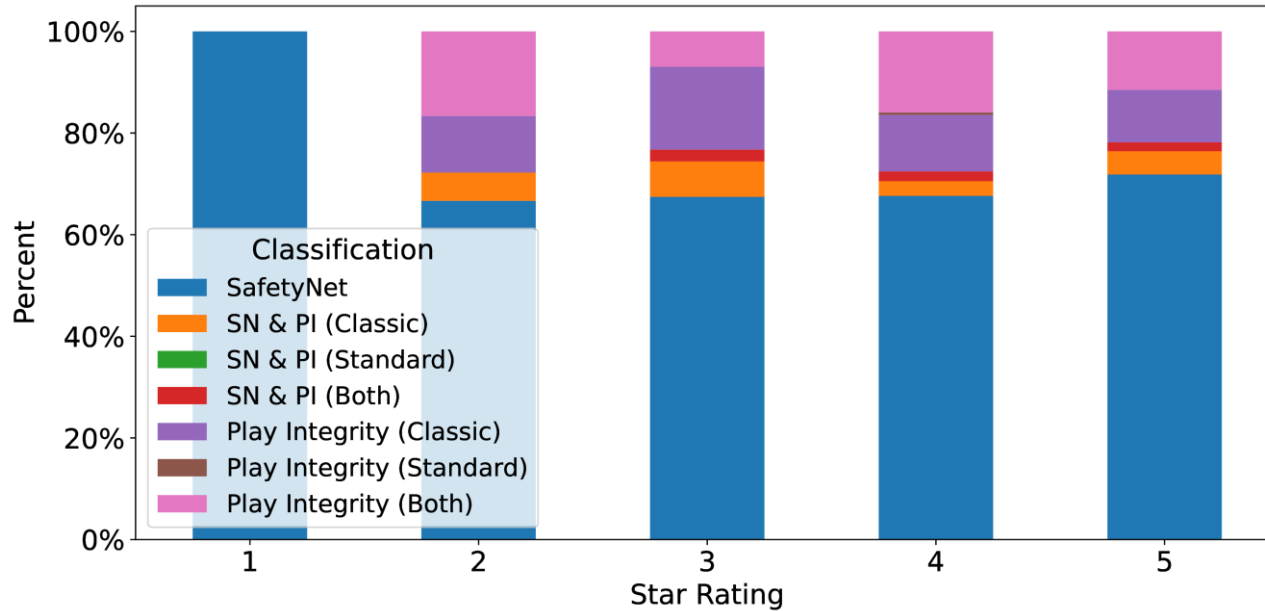
Adoption Factors: Total Downloads



Adoption Factors: Release Date



Adoption Factors: Star Rating



Longitudinal Analysis: Government Apps

We tracked 814 government apps across all versions (over 4,000 APKs).

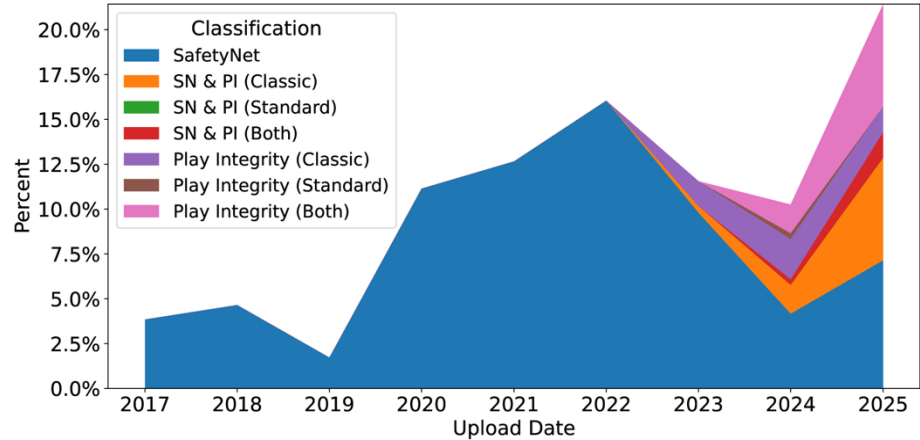
90 apps still reference SafetyNet (shut down Jan 2025).

Only 9 apps migrated from SafetyNet to Play Integrity.

7 apps removed SafetyNet with no replacement.

50%+ of government apps have not been updated in at least 2.5 years.

When a critical security service disappears, most developers do nothing.



Third-Party Libraries Drive Adoption

Only **5.4%** of applications exclusively use Play Integrity in their own code.

Most applications use Play Integrity through third-party code, of which Google-backed libraries dominate:

- Firebase Authentication (3,880 APKs)
- ReCaptcha (2,373 APKs)
- Google Mobile Services (1,220 APKs)

Metric	APKs
First-party	4,930
Third-party	6,982
Only First-party	341
Only Third-party	2,393
Only First-party & Third Party	4,589
Classic API	6,197
Standard API	1,492
Invoking Apps	6,281
Non-Invoking Apps	1,042

API	First-party	Third-party	Both
Standard	22	9	53
Classic	111	1295	3383
Both	9	417	982

Defense-in-Depth

Technique	APKs	%
Root Detection	5,682	90.5%
Runtime Checks	5,860	93.3%
Certificate Pinning	167	2.7%
None	363	5.8%
Only Root Detection	53	0.84%
Only Runtime Checks	231	3.7%
Only Certificate Pinning	2	0.032%

Technique	Marker	APKs	%
Root Detection	/system/xbin/su	5,579	88.8%
	/system/app/Superuser.apk	5,508	87.7%
	/system/bin/su	3,000	47.7%
	/sbin/su	2,913	46.3%
	/system/sd/xbin/su	2,891	46.0%
	com.noshufou.android.su	1,326	21.1%
	eu.chainfire.supersu	1,324	21.1%
	com.koushikdutta.superuser	1,293	20.6%
	com.thirdparty.superuser	1,290	20.5%
	com.yellowes.su	767	12.2%
	com.topjohnwu.magisk	761	12.1%
	isDebuggerConnected	5,764	91.8%
	ro.kernel.qemu	2,098	33.4%
	de.robv.android.xposed	899	14.3%
Runtime Checks	com.saurik.substrate	563	9.0%
	waitForDebugger	334	5.3%
	XposedBridge	188	3.0%
	frida-gadget	31	0.49%
Certificate Pinning	pin digest	213	2.9%
	pin-set	212	2.9%

Good news: Developers who invest in attestation tend to invest broadly in security!

Incidental Security Findings

- Even among apps using Play Integrity, we found security mistakes:
- 11 apps hardcoded private cryptographic keys in source code.
- 12 apps included secret API keys in plaintext config files.
- These apps collectively had 117+ million downloads.
- Adopting a framework doesn't guarantee overall security.
- Security requires a holistic approach throughout development.

Implications & Future Work

- **For Google:** Adoption barriers may be too high for smaller developers.
- **For developers:** Security-sensitive apps need to prioritize attestation.
- **For policymakers:** Government app maintenance practices need attention.
- **Future research:**
 - Dynamic analysis to verify runtime behavior at scale.
 - Study manufacturer-specific frameworks (Samsung Knox, Huawei, etc.).
 - Design and implement a new developer-focused framework.

AttestLens: A Large-Scale Measurement of Play Integrity Adoption in Android Apps



Most apps don't
use Play
Integrity

Government
Apps adopted
SafetyNet but
not Play Integrity

Adoption is
driven by 3rd
party code, not
developer intent