TAG

APPLE AND GOOGLE ARE SUPPRESSING INNOVATION IN MOBILE APP SECURITY: HERE IS WHY YOU SHOULD CARE

DR. EDWARD AMOROSO,
CHIEF EXECUTIVE OFFICER, TAG

TED MIRACCO,
CHIEF EXECUTIVE OFFICER, APPROOV

approov

APPLE AND GOOGLE ARE SUPPRESSING INNOVATION IN MOBILE APP SECURITY: HERE IS WHY YOU SHOULD CARE

EDWARD AMOROSO, CHIEF EXECUTIVE OFFICER, TAG INFOSPHERE[1] AND RESEARCH PROFESSOR, NYU[2]

TED MIRACCO, CHIEF EXECUTIVE OFFICER, APPROOV[3]

Apple and Google are exhibiting monopolistic behavior that is suppressing technical innovation in mobile app security.[4] With cyber threats growing, such behavior from these massive companies is not in the best interest of consumers. Alternative mobile app security approaches are discussed with emphasis on addressing the inevitable complications that arise with proposed changes to familiar systems and infrastructure.

[1] *TAG Infosphere provides research and advisory in cybersecurity, artificial intelligence, and climate science for enterprise teams and government agency practitioners and commercial vendors. See* https://www.tag-infosphere.com/.

[2] *NYU's Center for Cybersecurity (CCS) is an interdisciplinary academic center in which leading edge research, teaching, and scholarship are directed into meaningful real-world technology and policies. See* https://cyber.nyu.edu/.

[3] *Approov is a team of developers dedicated to making the future of mobile secure. With offices in Edinburgh, Scotland (UK), and Palo Alto, California, the company focuses on developing the world's most complete end-to-end solution for mobile app security from the device into the cloud. See* https://www.approov.io/ *for more information on the company and its mobile app security solutions.*

[4] *During the development and review of this article, the US Department of Justice sued Apple over its purported monopoly on smart phones. Obviously, this issue bears some relation to the arguments made here, but readers must understand that our focus here is on cybersecurity and we make concrete recommendations on how Apple (and Google) should take steps to fix the issues. The authors are not policymakers, but rather cybersecurity experts supporting practitioners. See* https://www.theverge.com/2024/3/21/24105363/apple-doj-monopoly-lawsuit.

INTRODUCTION

The thesis of this report – namely, that Apple and Google are increasing long-term consumer cyber risk through monopolistic behavior, is driven by two basic beliefs: The first is that bad actors have an inherent advantage over cyber defenders. Readers will recognize the aphorism that attackers need succeed only once, whereas defenders must succeed always.[5] This security concept is well-known and universally accepted by experts.[6]

The second belief is that monopolists tend to suppress innovation. One reason for this effect is that monopolists naturally prefer the status quo. Another is that monopolists are usually large, which tends to slow down the pace of change. Regardless of the justification, we view this claim as well-accepted. As an illustration, recall that AT&T was divested in 1984 for precisely this reason – namely, to increase innovation by nurturing competition in telecommunications.[7]

At first glance, our monopoly complaint might seem misplaced with respect to these larger companies. We all know, for example, that consumers knowingly buy into Apple's sandbox ecosystem, driven by Apple's strict policing of their environment to obsessively control what types of software are allowed and under which conditions.[8] Google also claims a strong security approach, albeit one based less on a controlled sandbox.[9]

Readers might be surprised that we agree that both companies, especially Apple, currently do a reasonable job with cybersecurity. The baroque measures that both companies take to ensure high integrity in mobile apps in their on-line stores is admirable and has been mostly successful addressing advances from outside adversaries. It is not easy, for example, to find major mobile app-related breaches that have occurred based on negligence from Apple or Google.[10]

We believe, however, that the relative success of Apple and Google addressing offensive pressure from nation states, criminal groups, and other capable threat actors is not likely to continue indefinitely. The conditions are too ripe, in our estimation, for the offense to not find seams, gaps, or other means (perhaps using AI) to break through the monoculture protection that emerges from any monopoly. Apple and Google should not be left alone to do this work, nor should they be allowed to set the security standards for what are considered safe apps.[11]

Furthermore, it should be evident that the mobile app security solutions from Apple and Google are specific to their respective closed ecosystems. As a result, there will not be great incentive for either company to support cross-platform initiatives that address mobile app security more comprehensively. This is despite the fact that developers and end-users are increasingly being held accountable for cross-platform breaches.

[5] This belief is generally viewed as an informal observation, but more formal government-funded reports have analyzed the offensive and defensive balance and have pretty universally concluded that it is much easier to attack than defend when it comes to cybersecurity. See https://cyberdefensereview.army.mil/Portals/6/Documents/2022_summer_cdr/08_Valeriano_CDR_V7N3_Summer_2022.pdf, for example.

[6] We are hardly the first business commentators to suggest that Apple and Google are intentionally behaving as monopolists. See https://www.wired.com/story/googles-app-store-monopoly-ruled-illegal-jury-epic/, for example, which explains that a court recently came to the same conclusion. Our perspective here is on the cyber security implications of such behavior, a perspective that we believe has been underrepresented in most discussions on this topic.

[7] Many articles, books, and lectures are available on this topic. The following report from the Department of Justice is interesting and reviews the rationale and results of the 1984 AT&T decree: https://www.justice.gov/archives/atr/att-divestiture-was-it-necessary-was-it-success.

[8] Apple does an excellent job with its sandbox approach for software and we admire the focused attention on ensuring that software is properly reviewed and vetted. See https://www.apple.com/business/docs/site/AAW_Platform_Security.pdf, for example.

[9] Google also provides world-class cybersecurity with a team of experts who are focused on making certain the cyber risk is properly minimized. See https://safety.google/stories/micklitz-pietraszek/, for example.

[10] Of course, there have been serious mobile app security breach incidents. Vendors such as NowSecure, which supports mobile app security testing, have aggressively pointed these out. See, for example, https://www.nowsecure.com/mobile-app-breach-news/.

[11] By way of comparison, consider that the OWASP® Foundation works to improve the security of software through its community-led open- source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences. See https://owasp.org/www-project-mobile-top-10/.

In this report, we make the specific case that the monopolistic behavior for mobile app security exhibited by Apple and Google must cease immediately. We explain how this behavior is occurring today, and we examine its ramifications. We also look at some alternative approaches, being careful to reference the geopolitical and other challenges (mostly related to Chinese manufacturers) that could result from such change.

ILLUSTRATIONS OF MONOPOLISTIC BEHAVIOR

A reasonable definition of monopoly is the exclusive possession or control of the supply of, or trade in, a commodity of service.[12] The general notion here involves an entity or group of entities restricting the ability of competing entities to participate in some desirable activity such as mobile applications. An interesting paradox is that real monopolies do everything possible to claim the opposite, whereas startups try to claim exclusive control of some target area.[13]

The problem with monopolies is that the drive to innovate diminishes because there is little or no fear of competition. They can also control scarcities, drive prices up, and decide on the level of quality that best suits their needs. Admittedly, Apple and Google are wonderful companies with amazing products that consumers generally love. The problem instead is an emerging issue, one that can create problems as the intensity of offensive methods increases.

The general issue we reference here is that Apple and Google essentially control the entire mobile app ecosystem. As a non-security-related illustration, consider that when Spotify mobile app users download music, a fee of between 15% and 30% is paid from Spotify to Apple. This might seem fair (tenants pay landlords) until one recognizes that Apple also competes with Spotify – and thus maintains a significant and seemingly unfair advantage.[14]

Another example is the on-going battle between video game developer Epic and Apple, and the issue is roughly the same as with Spotify. That is, when Epic innovates to develop new games or features, the profit margin is obviously squeezed by Apple taking its cut of the fees from consumers. Antitrust probes led right up to the Supreme Court, but we suspect that this issue will continue to reappear and cause problems for consumers.[15]

EFFECT ON MOBILE APP SECURITY VENDORS

The reason we care about such behavior has nothing to do with the philosophy of business or the attendant legal considerations. We leave that debate for others, but we have come to recognize that monopolies are not good for cybersecurity – and this is, in fact, our area of expertise and focus. Hence, it makes sense to review our security concerns about how Apple and Google might be placing consumers and society at risk.

The first hint that there is a problem is the honest observation that innovative startups and entrepreneurs in mobile app security are struggling. Where we have observed commercial vendors in adjacent areas such as cloud and API security reaching significant levels of growth and valuation, we have seen the mobile app security vendors struggle to reach similar levels of accelerated sales and customer adoption.

[12] *Any number of definitions of monopoly can be found on the Internet (ignoring references to the board game). A good sample definition of a monopoly is available here:* https://www.merriam-webster.com/dictionary/monopoly.

[13] *One of the authors (Amoroso) has noticed this behavior in his research and advisory work at TAG Infosphere where cybersecurity startups desperately try to convince observers that they essential dominate a particular area (usually proof that they do not) whereas legitimate monopolies such as Apple and Google in the context presented here, will do everything they can possibly muster to demonstrate that they compete with everyone (usually proof that they do not).*

[14] *Our attention in this report is on the cybersecurity of mobile apps and how Apple and Google are misbehaving in this context, but the Spotify case offers useful insight into the problem. While we are not experts in this music debate, we do follow the narrative – and here is a typical post explaining the seeming back-and-forth between the companies and regulators:* https://forums.appleinsider.com/discussion/233654/spotify-speaks-out-against-apples-30-commission-fee-again.

[15] *We also do not purport to be experts in the gaming battles between Apple and companies like Epic, but we encourage readers to dive in to learn more. Here is a typical post:* https://appleinsider.com/articles/20/08/23/apple-versus-epic-games-fortnite-app-store-saga-the-story-so-far. *If this interests you, spend some time reviewing both sides of the story and hopefully come to your own conclusion. Our interpretation is that Apple is clearly exhibiting the behavior of a typical monopoly. It looks textbook to us, but again, our primary interest is on security.*

An analysis of cybersecurity vendors reveals high valuations for companies such as Wiz, Crowdstrike, CyberArk, Palo Alto Networks, SentinelOne, Fortinet, Check Point, Vectra, Obsidian, Okta, Fastly, and more. These companies address security for cloud, endpoints, privileged access, networks, and related enterprise assets – but despite the central role that mobile apps play in our lives – none of the truly major cybersecurity vendors work in this area.[16]

The reason this situation matters is rooted in the importance of mobile apps for consumers, as well as business, government, and general society. We have learned that malicious actors target the most valued assets, and we believe this increasingly involves mobile apps. By placing the bulk of security responsibility to provide attendant protection in this area on two monopolies, we are following a path that misses the value of open competition and innovation.

The implication, we believe, is that unless we take a different approach toward mobile app security, one that encourages fair use, competitive development, and entrepreneurial risk, then we will run the risk of placing our defensive eggs into one basket (in this case, two baskets) and that if we expect this to sufficiently cover the growing threat from nation state-sponsored actors, then we believe we have misplaced our hopes and trust.

CASE STUDY: GOOGLE MOBILE SERVICES

To illustrate our point, let's review how Google Mobile Services (GMS) maintains a lock on Android mobile apps, which in turn makes life difficult for external mobile app security vendors. Again, the issue is not the current state of GMS or whether Google does an acceptable job providing security. Our issue is that by stifling competition, innovation slows (or ceases) and the gap between offense and defense will widen.

GMS is a reference to a collection of Google applications and services that are preinstalled on Android devices.[17] These services provide functions such as Google Play Store, Google maps, Gmail, Google Drive, and so on. Our observation and experience are that these are solid utilities and applications, and that Google consistently provides excellent software and support. They have even improved their update process for their suite of apps.[18]

The problem comes when a device is used without GMS, perhaps because a mobile user or organization would prefer that Google not have access to their private data or because they would like to make use of non-Google apps for functions such as location or data storage from non-Google app stores. The mobile app experience is immediately less integrated, and the range of apps available becomes limited with the device connected into GMS.

Third-party developed versions of Android which are generally referred to as custom ROMs (they also known as Android skins) are also available to users. Usually created from the source code of the Android Open-Source Project (AOSP), which is the same base that Google uses for Android, these custom ROMs are intended to support a range of new features and to enhance the performance, capabilities, and features of the device.[19]

[16] *Readers are welcomed to review any number of cybersecurity valuation estimates available on the Internet or privately. There must be dozens of good analysis reports and they all show comparable results – namely, that commercial mobile app security vendors are literally nowhere to be found on leaderboards of corporate valuation, growth, revenue, sales, or any other financial metric. The report that we reference above is here:* https://www.finrofca.com/news/cybersecurity-startups-valuation-and-multiples-2024.

[17] *Here is something funny. We were looking for a nice reference on GMS and found a decent explanation on the website of Hong Kong-based HONOR, which is a provider of smart devices. The reason it's funny is the obvious use of ChatGPT to generate their article. It has phrases like "In the ever-evolving landscape of mobile technology, GMS stands as a cornerstone . . ." and so on. We have no quibble with this, but it's funny that non-English speakers cannot sense the subtle awkwardness that comes with Generative AI. We have nevertheless used their AI-generated document to help explain GMS. We thought you'd enjoy that – and no, this article (and this footnote) was not generated by AI, but rather by living, breathing, and biased humans. Here is the site in case you need a chuckle:* https://www.hihonor.com/sa-en/blog/what-is-gms/.

[18] *One of the authors (Amoroso) was directly involved as CISO of AT&T for two decades in the early days of Android apps on iPhones and other devices. Things were bad in those early days in terms of the long process of getting software updated on a smartphone. It's beyond the scope of this article but suffice it to say that the Android process has improved. Apple, as you'd guess, always did this well because they control the entire ecosystem, which does bode as points for them in the context of security. Monopolists always control their end-to-end experience better than non-monopolists. We will give them that.*

[19] *See* https://medium.com/@theentrepreneurreview/7-best-custom-roms-for-android-f091d5caee90/ *for a description of custom ROMs for Android.*

It would thus seem like GMS should not be necessary in every Android device. The difference would be that a non-GMS Android device would omit apps such as Google Maps, Google Chrome, YouTube, and other Google apps. Alternatives do exist for these apps (an argument against the monopoly) and many of these GMS apps aren't required in an Android device supporting a specific function such as in certain industrial settings.[20]

The problem, however, as was evident in a recent court case that found Google to be a monopoly,[21] is that mobile app security companies operate at a significant disadvantage when having to deal with GMS. Consumers and businesses might not expect this to be relevant, since it doesn't have a near-term financial impact for them, but our concerns for emerging threat coverage will most certainly have security consequences for mobile app users of all types.

ALTERNATIVES TO GMS

When one begins to consider alternatives to GMS, one finds (especially American readers) that the options begin to look somewhat foreign and perhaps even uncomfortable. That is, most of the activity that is currently on-going to address such monopoly behavior in the mobility ecosystem are being done in countries such as China, the Middle East, and Africa. These are markets that are generally considered non-relevant to the typical US consumer.

For example, one leading manufacturer of non-GMS mobile phones is Transsion, a Chinese smartphone manufacturer known for brands like Tecno, Itel, and Infinix.[22] Transsion has grown to become the world's fifth-largest smartphone manufacturer, focusing on markets in Africa, the Middle East, Latin America, Asia, and Oceania. They have a strong presence in Africa and offer affordable smartphones while also venturing into new technologies like foldable devices.

Similarly, Huawei, Xiaomi, and Oppo are Chinese manufacturers of non-GMS mobile phones. Huawei, despite facing challenges due to U.S. sanctions, continues to produce phones like the Mate 60 Pro and is striving to re-establish itself in the global market.[23] Xiaomi, known for its affordable phones, has a strong presence worldwide, shipping millions of phones annually. Oppo, Vivo and Xiaomi have been gaining market share globally especially with young buyers.[24]

These various companies, most of whom will be largely unknown to American buyers, are all part of a group of vendors focused on competing against the Google Play Store by allowing developers to upload apps simultaneously to their app stores. Overall, Huawei, Xiaomi, and Oppo are the most prominent manufacturers of non-GMS mobile phones that offer a diverse range of devices catering to different market segments.

The problem, obviously, is the geopolitics associated with these companies. The authors here, both Americans, clearly understand the awkwardness and implausibility of shifting toward Huawei from Google and GMS to improve security.[25] This would be a ridiculous recommendation, and it is hardly our intent here. That said, we do offer these foreign use-cases to illustrate the type of focus required to build non-GMS mobile app ecosystems.

[20] *See* https://emteria.com/blog/gms-vs-non-gms/ *for a more detailed information and useful discussion on the topic and implications of non- GMS Android apps.*

[21] *See* https://www.theverge.com/23994174/epic-google-trial-jury-verdict-monopoly-google-play *for an excellent explanation of the case, its details, and its implications.*

[22] *For more information on Transsion, see* https://www.transsion.com/?lang=en.

[23] *Many interesting articles are available on the Internet that explain and comment on business-related issues for companies such as Huawei in the context of US restrictions. See, for example,* https://www.cnet.com/tech/mobile/huaweis-2023-revenue-soars-despite-us-sanctions/.

[24] *See* https://www.mi.com/us/ for more information on Xiaomi.

[25] *It should be pointed out that one of the authors of this report (Miracco) is the Chief Executive Officer of an international mobile app security company (Approov) that is headquartered in Edinburgh, Scotland (UK) and Palo Alto, California (USA). See* https://approov.io/info/company.

THE CYBER THREAT THAT ARISES WITH MONOPOLY

Perhaps the best way to understand the type of threats that arises when a large company behaves in a monopolistic manner regarding cyber is to compare the mobile app security ecosystem with the cloud security ecosystem. The resulting comparison helps to explain how and why we are so concerned that Apple and Google are operating as they are, despite doing an acceptable job of security today.

If we begin with the cloud security ecosystem, we must baseline the three massive services – namely, Amazon Web Services (AWS), Microsoft Azure, and (ironically) Google Cloud Platform (GCP). The vast majority of enterprise cloud usage scenarios start with these cloud services, which in many cases must be used in the context of a multi-cloud architecture requiring coordination, integration, and orchestration of workloads and applications.

Into this multi-cloud ecosystem, the security industry has enjoyed a plethora of highly successful and valuable companies such as Palo Alto Networks and Wiz, which address the cloud security needs of buyers based on tough competition, high demands for innovation, and the on-going need to track threats from malicious actors ranging from hackers to well-funded nation-states. The resultant diverse cloud security ecosystem is represented as in Figure 1.

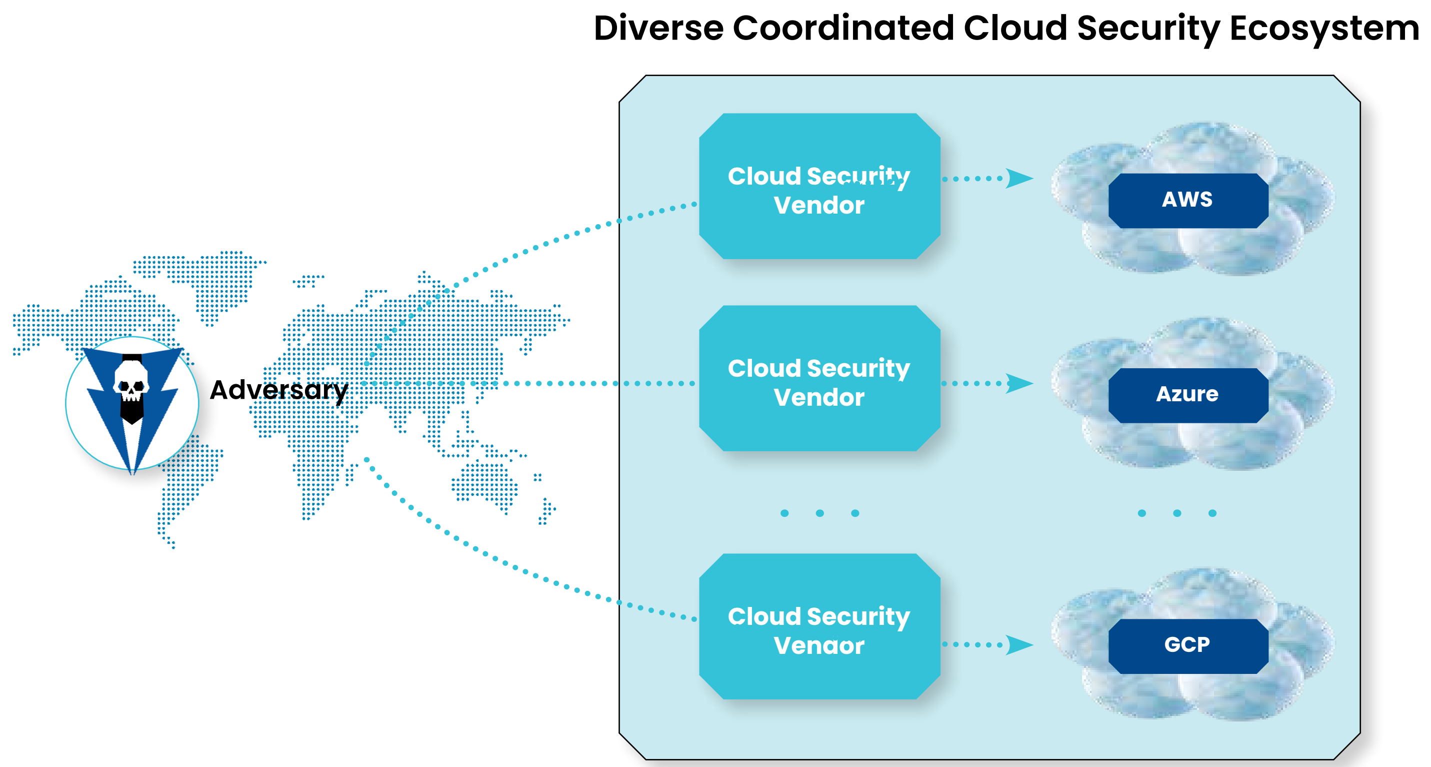

Figure 1. Diverse Cloud Security Ecosystem

Similarly, the mobile app security ecosystem also must be baselined with large companies – namely, the two focused on in this report: Apple and Google. Whereas, however, the three cloud service providers (which, as mentioned above, includes Google) provide a basis for security vendors like Wiz and Palo Alto Networks to sell products and services, the manner in which this is done for mobile app security stifles establishment of similarly successful vendors.

That is, what we see are two powerful mobile operating systems companies bundling the majority of security themselves. The perceived success of Apple and Google provides comfort to consumers who seem satisfied with present levels of security.[26] Our concern, however, is that in any monopolistic monoculture, the adversary need only exceed the capability of one company, rather than a diverse ecosystem of successful vendors and providers (see Figure 2).

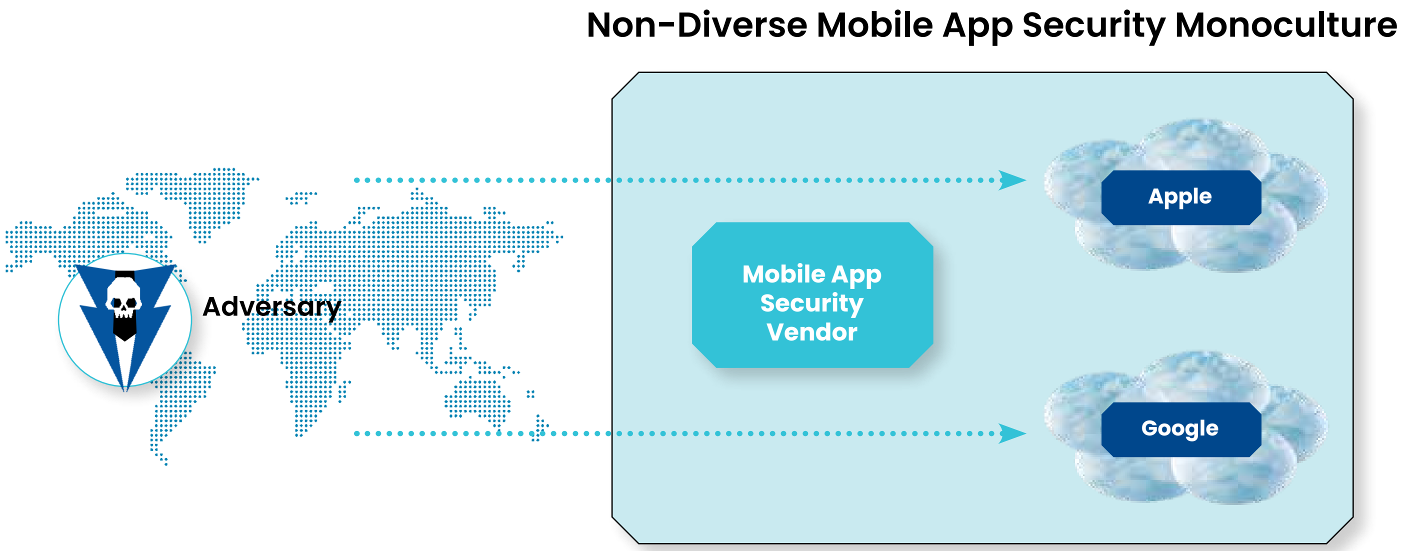
Non-Diverse Mobile App Security Monoculture
Adversary
Mobile App Security Vendor
Apple
Google

Figure 2. Monoculture Mobile App Security Ecosystem (Bypassing Security Vendors)

Recommendations for Mobile App Security

In this section, we make our series of five recommendations. We feel obliged to underscore that readers should understand our motivation as having nothing to do with geopolitics. That is, we are neither touting nor recommending shifts away from Apple and Google toward providers located in China. Instead, our motivation is to enhance the spirit of global competition to drive greater levels of innovation for all users, both inside the United States and out.

Each of our recommendations below is offered as an action statement, followed by a technical explanation and business rationale. We would hope that global policy influencers and corporate decision makers in both public and private organizations will read these recommendations and perhaps consider their suitability for government and business strategy. Both authors are available for comments, suggestions, and questions from readers.

Recommendation: Apple and Google must facilitate the use of third-party mobile app security vendors more effectively.

Apple and Google should open their ecosystems to third-party mobile app security solutions.[27] Such a strategic move, which could be associated with a vendor certification and review process, would enrich the security landscape with new and innovative approaches and would attract more specialized expertise. A partnership model could be established where certified vendors are recognized within the app stores, thus ensuring compliance with high standards.

[26] *We must mention that companies such as NowSecure and Approov have well researched reports showing that 85-95% of apps are leaking credentials and API keys. There are also long lists of privacy concerns where app developers are abusing access rights to contacts.*

[27] *Again, this is hardly the first time this suggestion has been mentioned or written about. Here, for example, is a typical article explaining the various means by which organizations such as the European Union have pushed for, or passed laws for, a more open app ecosystem:* https://www.bloomberg.com/news articles/2022-12-13/will-apple-allow-users-to-install-third-party-app-stores-sideload-in-europe.

If one wonders why Apple and Google would do this, we would offer three reasons: First, it would lower the sole burden for both companies of having to stay ahead of capable nation- state adversaries in cyber. Second, it would have zero impact on Apple and Google's bot-tom- line revenue. In fact, one could imagine it removing many barriers to mobile app usage (e.g., for future elections).[28] And third, it would remove the possibility for future legal action.[29]

Funding such ecosystem development and support should also be a simple process for two companies whose combined market capitalization is almost five trillion dollars.[30] That number, combined, is larger than the gross domestic product (GDP) of every country in the world except the US and China. These companies hold staggering valuations so asking them to enhance the mobile app ecosystem to avoid future threats is hardly unreasonable.

Recommendation: Apple and Google must financially incentivize developer-led mobile app security initiatives.

Developers who invest in robust security measures, either through third-party vendors or by implementing their own solutions, should be rewarded with reduced commission rates. This approach would not only encourage better security practices but would also provide financial relief to developers working in this area. A structured verification process, aligned with industry standards, could assess these security measures for efficacy and compliance.

It is clear to the authors that incentivizing developers has always been the best way for large companies to influence their industry. This point is made not just for individual developers who work in isolation or as consultants, but more so for ones who might make the decision to start new companies focused in this area. They must see a path to significant hyper-growth akin to vendors such as Wiz and Palo Alto Networks before they will take the risk.[31]

Apple and Google should also implement a tiered discount system on commission fees for developers using certified security solutions. These massive companies can easily create a financial incentive to prioritize high-quality security. This system would recognize and reward the efforts of developers to adhere to the highest security standards, thereby enhancing the overall security posture of apps within the ecosystem.

Recommendation: Apple and Google must adopt open standards for mobile app security evaluation.

Transitioning to widely recognized open standards, such as those developed by the Open Web Application Security Project (OWASP) for app evaluations would help to democratize the cybersecurity review process for mobile apps.[32] This strategy would ensure that security measures are being judged against a transparent and equitable benchmark, thus fostering trust among developers, security vendors, and users alike.

[28] *This point regarding elections is only mentioned in passing but is worth emphasizing. It is a sad fact that elections today do not utilize mobile apps, and the potential for hacking of these mobile apps is the primary reason for paper use. For future generations to truly trust the mobile app ecosystem, we believe an open and collaborative model must be in place to drive greater confidence amongst citizen voters. It seems inconceivable that without vibrant, well-incentivized startups and vendors supporting mobile app security with high valuations and growth that we will ever see public elections held using iPhone and Android devices. Obviously, these security issues would not be the sole factor in driving such a transition, but it would be a major one.*

[29] *The EU's Digital Markets Act was a strong move that produced an interesting non-response from the White House which included verbal response, but no substantive objection. See* https://www.washingtonpost.com/technology/2024/03/07/eu-digital-markets-act-biden-dma/.

[30] *Obviously, this goes up and down, but the number is directionally correct. See* https://www.businessinsider.in/stock-market/news/apples- market-cap-is-larger-than-all-but-6-of-worlds-top-economies/articleshow/106032676.cms.

[31] *One of the authors (Miracco) obviously understands the risks and challenges of building and operating a mobile app security company – and our request here for Apple and Google to incentive developers would certainly create more competition for Approov and other vendors working in this area. The suggestion is made here, nevertheless, because it is clear that such action would be in the best interest of the mobile app ecosystem and with greater competition will come a more vibrant market.*

[32] *The excellent app verification and review standard from OWASP that we would recommend for use in the mobile app security context is explained here:* https://owasp.org/www-project-application-security-verification-standard/.

Of all our recommendations, this one seems the most straightforward, since it drives the set of evaluation criteria to an open process. That said, we suspect that this recommendation might be the least welcome by Apple and Google, given their traditional focus on great secrecy in how they provide security. Every security expert knows, however, that security through obscurity, even when done by highly capable actors in strong organizations, eventually fails.3[3]

It is perhaps worth adding here that such standards adoption should extend to the mobile payment ecosystem. We believe that Apple and Google should allow developers to utilize alternative certified payment systems. Such action could reduce transaction costs for these third parties and would increase autonomy, provided that such systems adhere to stringent security and privacy standards.

[33] *Perhaps the greatest on-going experiment in security through obscurity lies in the global intelligence community, where classification and clearances are used to create legal walled gardens. Despite such baroque actions, organizations such as the National Security Agency (NSA) have had spectacular breaches, often from insider action, which call into question such means. We are not suggesting that NSA declassify their operations, but instead are pointing out that cybersecurity at the enterprise level benefits from open standards and community collaboration.*

ABOUT APPROOV

Approov creates advanced mobile app and API shielding security solutions for many leading global organizations with consumer and B2B applications being used by millions of customers annually across a wide range of industry sectors such as eCommerce, financial services, healthcare, gaming, and connected cars. For More information, please visit **www.approov.io.**

ABOUT TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science/sustainability.