intertrust®

White Paper

Intertrust PKI

Distributed trust management for app store diversity

An antidote to the risks of sideloading

Contents

Abstract

Apps provide a wide variety of new capabilities to computing devices. They have proven to be especially popular in smartphones.

Trusted diverse app stores and payment systems have been available for decades. Public Key Infrastructure (PKI) assures the authenticity and integrity of these systems. Mobile systems are some of the most secure ever created due to their combination of hardware and software systems. Together with PKI, they can support a plurality of hetrogenous systems, benefitting both app developers and consumers

Battle royale with the app stores

Epic Games is a studio best known for its incredibly popular and addictive game: Fortnite: Battle Royale. The largest gaming community in the world, as of May 2020, it boasts 350 million players and has been growing at a compound annual growth rate (CAGR) of 605% since it debuted in August 2017.[1]

The studio is known for the extensive Easter eggs[2] and trivia it builds into its game updates. From dances to gamer created icons, to thanking the bus driver for bringing gamers into the battle, these Easter eggs have become a cultural phenomenon. They are wildly popular and Fortnite players have made these into many viral memes.

In August 2020 Epic inserted a kind of Easter egg that was wildly unpopular, at least to Apple and Google. It included hidden code to enable the purchase of Fortnite currency "V-Bucks" directly from Epic. While the Fortnite community loved V-Bucks, Apple and Google weren't fans because it circumvented their payment systems. Shortly after the V-Bucks feature was released, both Apple and Google removed the game from their respective app stores. And that's when the real Battle Royale commenced—Epic filed lawsuits against both companies.

Fortnite players who currently use the app on Apple and Google mobile devices can no longer receive updates to their apps. This situation has played into a long-standing controversy around the power these two major app stores hold over app developers. One of the solutions that is being proposed is for both companies to allow "sideloading," that is, downloading apps from an app store not favored by the device maker.

Since then, there has been a lot of fear generated around sideloading. There is a security and privacy angle to all of this. There are claims that sideloading can adversely affect a user's privacy and device security since there are some risks from users inadvertently sideloading malware apps containing ransomware, spyware, and trojan horses.

In the absence of protection technologies, these risks are real. By combining cryptographic techniques with on-device security, it is possible to mitigate these threats and enable multiparty trusted systems and a plethora of trusted app stores.

Intertrust is the leading innovator in trusted systems and has been for over 30 years. We have a view on how to eliminate sideloading risks and enable multi-party trust among multiple app stores. This paper will discuss today's threat landscape, the mobile app eco-system, privacy, security, app stores, sideloading, and how Qualcomm® chipsets provide the device security required. Finally we offer some thoughts on how distributed trust systems may work to enable rich multiparty eco systems to benefit consumers and developers alike.

Today's threat landscape: mobile malware

Verizon's Mobile Security Index 2021 Report showed that 60% of companies thought mobile devices were their biggest security risk.

"Well-known problems like malware and ransomware remain major threats" … "Even apps downloaded from official stores can be compromised or introduce vulnerabilities due to poor coding practices".

Mobile malware is a threat, largely because it is effective. Even in the major app stores from Apple and Google, cyber criminals can evade detection. The app stores are continually evolving their protection efforts, but malicious code continues to get through.

Malicious actors employ numerous strategies. These include applying malware to updates rather than the initial version because updates receive less scrutiny. Or hiding within an entertainment app and remaining dormant for a period while working to infect other connected devices. Some malware even remains dormant until the smartphone's pedometer function identifies that a certain number of steps have been taken. This is a particularly good technique since security researchers usually don't walk around with the devices they are analyzing.

Mobile malware is a key attack vector into corporate and home networks. It has been used to harvest banking credentials and other sensitive information from consumers and corporations. Some malware simply show the user advertisements, while others will take over a device to enlist it in a botnet used for DDoS attacks, illicit crypto mining, or infecting other devices to affect a full ransomware attack.

Deploying counter measures against mobile malware is more important than ever. One thing is certain: the efforts taken to combat malware by Google and Apple are significant. They review apps, sign them at the app store and then verify those signatures using sophisticated security hardware and software at run time. We shall discuss these efforts more in the next section.

The mobile app eco-system: what sets it apart

Mobile device makers and carriers are fortunate to follow in the footsteps of previous computing developers, particularly the experiences of the personal computer. They were able to observe the risks of permitting the installation of arbitrary software and how malware could spread to desktops and servers. These systems have traditionally been "default open." That is, users can install and run arbitrary software from any source. This has allowed malware to penetrate and take root more easily.

As a result, in the realm of personal computers we have been suffering from significant attacks for decades. These have ranged from the Melissa Virus causing severe destruction to hundreds of companies in 1999, to NotPetya in 2017 causing over $10 billion in direct economic harm.

For a long time, the solution was simply to monitor systems closely with anti-malware scans.

Realizing that such a compute intensive approach would be both insufficient and drain battery life from the mobile device, the mobile device industry took a different approach to updating features on mobile devices.

Mobile systems are designed around the principle of least privilege—and default closed is the key principle. Innovators like Google and Apple apply two key strategies for ensuring continued trust for their devices while expanding device functionality through app downloads.

The first are app security reviews. These are extensive, with both automated and manual procedures. Apps are tested not just for malware, but for well-known vulnerabilities. This latter is a key element, because for many vulnerabilities there are exploit kits available for trade or purchase in many hacker markets, in particular the dark web. These exploit kits allow malicious actors to mount very sophisticated attacks without necessarily having the expertise normally required.

Once an app is reviewed, how does an organization ensure their app hasn't been modified and is the one that a user downloads? How can the user ensure that app originates from a trusted source? Digital signatures combined with highly effective security mechanisms in chipset hardware provide that assurance.

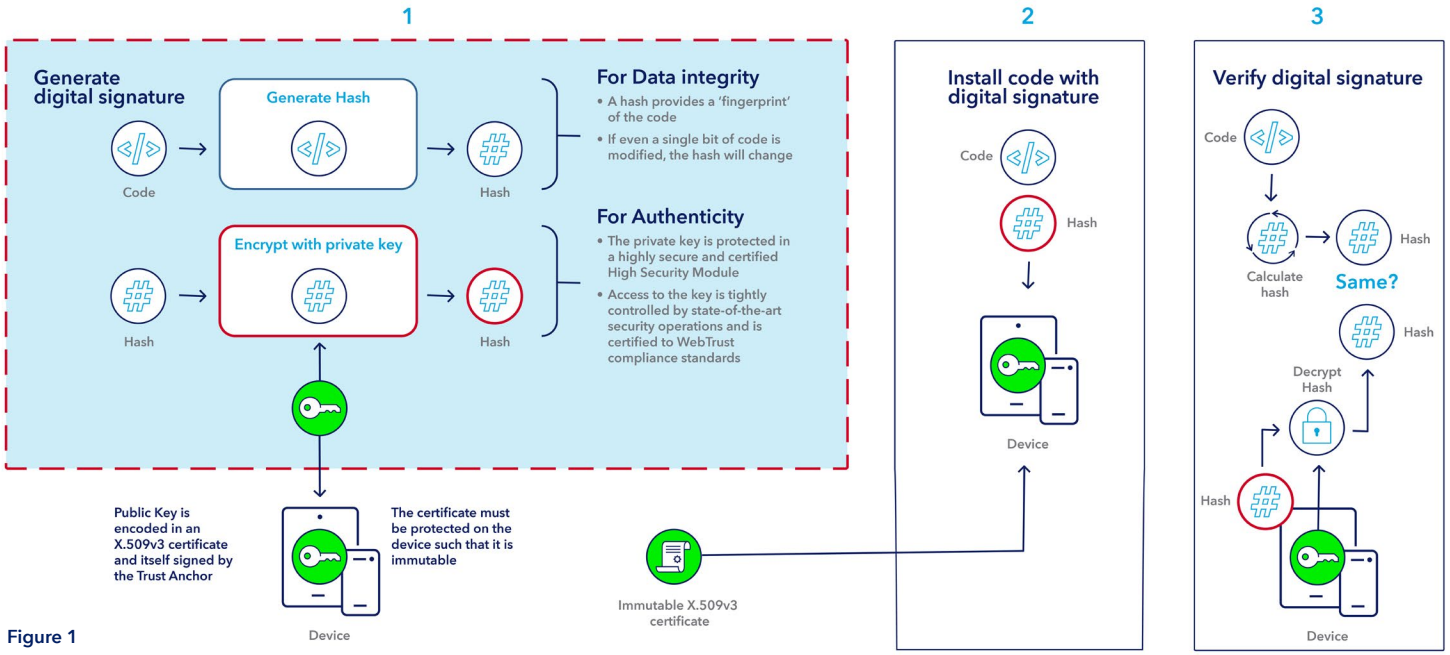


Figure 1

How does a digital signature provide protection?

The process of signing an app assures the app comes from a trusted source and that it has not been modified. Public Key Infrastructure (PKI) is the enabling technology, and it underpins much of the digital trust infrastructure of today's internet. Figure 1 above depicts the process described below.

App signing works in two steps. First a fingerprint (a hash) of the app's bits is created, and then that hash is encrypted using the Root of Trust (RoT). The hash uniquely identifies the bits of the app. If a single bit is changed, so is the hash (H1). The signature is encrypted to keep H1 secret while in transit to the user's device.

At run time, the app's digital signature is verified by reversing these two steps. First, a hash is calculated (H1'). Then the original hash (H1) is decrypted. If H1' = the original (decrypted) H1 then the system knows the app has not been modified. Since the public key can only decrypt a digital signature generated by its paired private key, the system also knows the app came from the holder of the RoT.

As one can imagine, trust in the system is underpinned by the RoT, the private key, remaining private. That means it needs to be extensively protected, in very secure facilities, with access to these facilities strictly controlled. Intertrust provides such facilities ensuring the private key will not be disclosed.

While these are difficult processes to maintain in a sufficiently secure fashion without causing undue effort, they are not unique. How the public key infrastructure hierarchy is designed and deployed also affects trust and performance. So while implementations and secure processes might differ somewhat, at its core, this is the same technology Apple and Google use to provide authenticity and data integrity to the apps coming from their stores.

Trust also depends on the device hosting an immutable public key. This is essential because one common attack to is to simply sign a malicious app with the attacker's own key and provision their own public key in the device. This rogue public key will happily verify the authenticity and integrity of the app. But it is essentially verifying this toxic app is authentically what it claims to be.
This is where Qualcomm® security solutions provide the resilience needed to assure verification. The correct public key must be provisioned, stored, and used in a trusted manner.

Not just anyone can provision their public keys into a handset. Trusted parties make use of Qualcomm® Wireless Edge Solutions (WES) for provisioning. They can do this without special provisioning in the OEM factory and it is based on the hardware Root of Trust.

In addition, Qualcomm® chipsets have several mechanisms for ensuring the integrity and immutability of sensitive key materials with secure storage. At run time, there might be a possibility of a Man In The Middle (MITM) attack by disrupting the verification process. But using process isolation and Trusted Execution Environment makes this a very difficult attack indeed.

The protection of the private key's secrecy in Intertrust highly secure facilities along with public key assurance from the Qualcomm® based device represents a highly resilient trusted system for data of all sorts, including sideloaded apps.

App sideloading: definitions and implications

Both Apple and Google have removed Fortnite from their app stores. Both claim that downloading the Fortnite app directly from Epic constitutes "sideloading" and makes a device more vulnerable to malware. Even signed apps from a non-reputable source can raise critical concerns. There are plenty of rogue app stores that sign their malware-infested apps and ought not be trusted.

What exactly is sideloading?

Sideloading has emerged as a generic term for installing an app that is not approved by the device maker. Physically the app can be delivered by a memory card, over USB, or downloaded over the internet.

But not all sideloading responses are the same. Apple IOS blocks apps that aren't signed, whereas Android allows users to dive deep into settings to adjust permissions to allow sideloading if they wish. Since Android 8 (Oreo), these settings have been made more granular and may be set on an application basis rather than as a policy for the entire device.

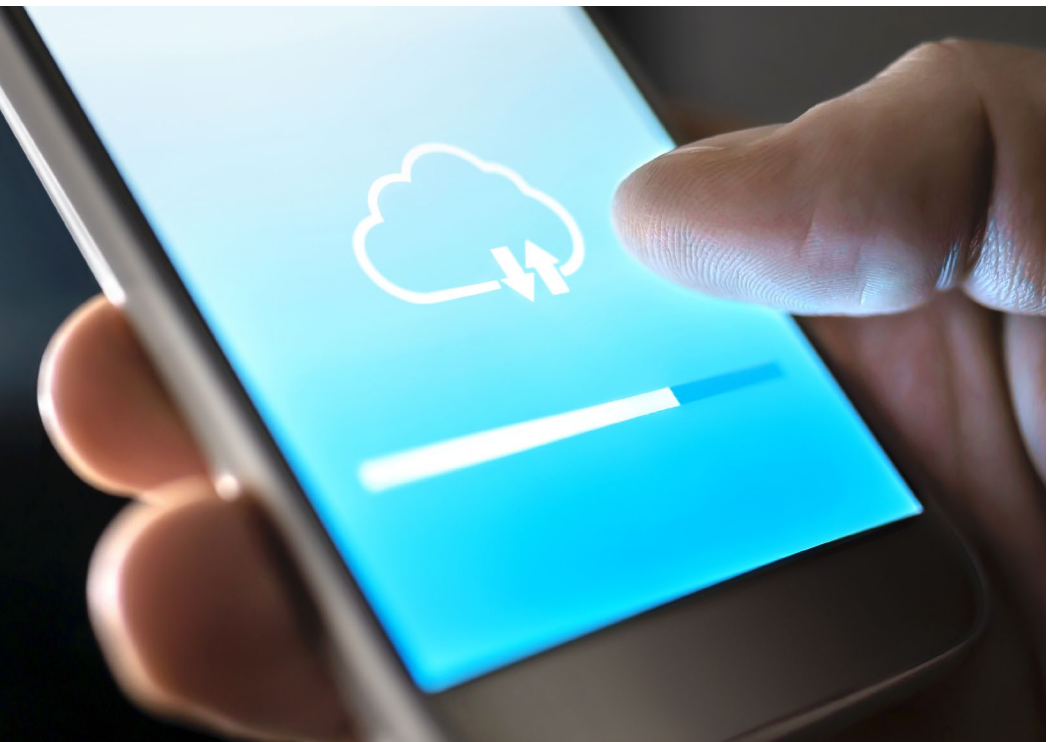
For MacOS, Apple takes a different and more common approach to app sideloadking. Unlike iOS, Apple gives the user choice.

Since signed apps are more trusted than unsigned, MacOS informs the user if an app is not signed. It enables other features as well, including admin settings to disallow unsigned apps.

Generally, MacOS offers its users choice with comprimising their security.

Enterprise apps

Both Apple and Google support enterprise app stores for businesses who wish to develop and distribute their own proprietary apps across their organizations. The process is like the app store model except instead of Apple or Google reviewing the app, it is done by the organization itself.



Alternative trust models and app stores

An app from a reputable source such as Epic, properly reviewed and signed, should not cause such concerns if the user trusts Epic or an alternative app store and the app is properly signed.

The Samsung Galaxy app store is a good example. They continue to offer Fortnite for download, and in fact, Epic has incentivized Samsung Galaxy app store users by offering a 20% discount on V-Bucks. It is possible to have multiple app stores that operate through multiple independent trust management providers for apps.

Trust roots for these providers can be embedded in the OS, and strongly protected by chipset hardware, just as TLS trust roots are embedded in browsers.

This model has existed almost since the beginning of e-commerce on the web, starting with Netscape browsers. Apple and Google use multiple independent trust roots with their browsers.

The concept has proven to be viable. It's also been applied at scale in the market for protected media for decades now.

Ensuring privacy and security with enabling technology

Chipset hardware protections

All device security is derived from the chipset at its core. Most software security can be circumvented. Hardware-based security combined with software security is one of the best ways to effectively resist malicious apps. As one example, Qualcomm® chipsets offer deeply integrated security systems that have been proven to be highly resilient and enable smartphone-based app store eco-systems around the world.

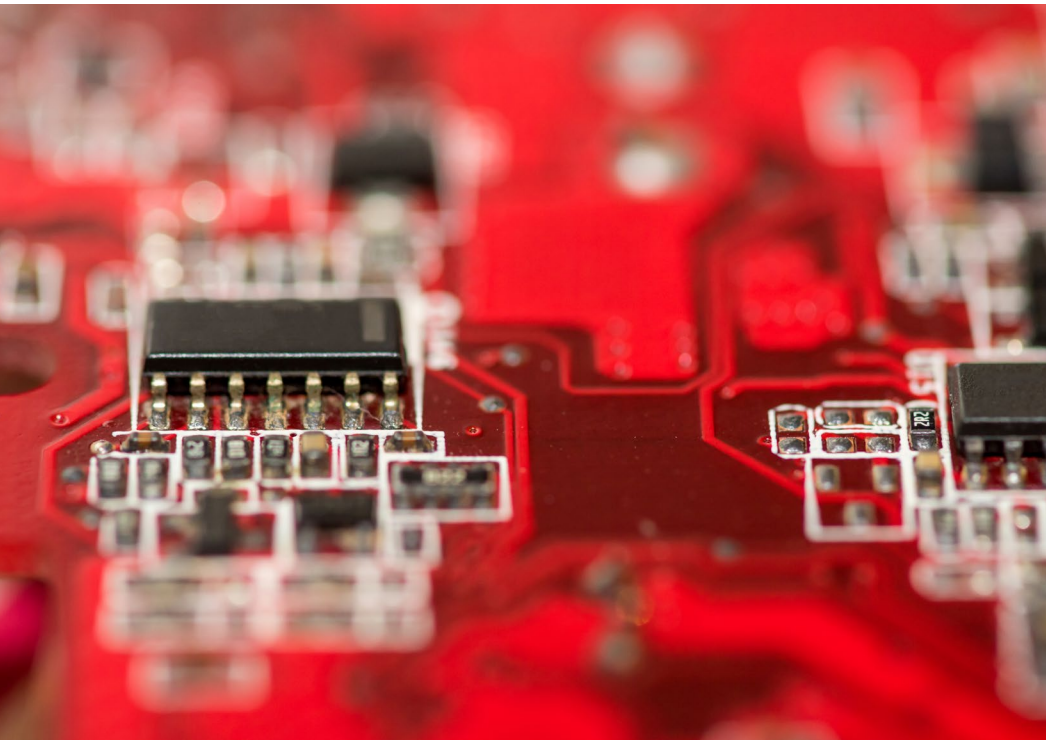
Qualcomm's Snapdragon™ Security Foundations are a collection of SoC-based (System on a Chip) hardware and software features that enable a system-wide approach to securing various use cases, such as ensuring app authenticity and integrity. It forms the essential security fabric used on 100s of millions of devices.

It includes critical features such as:

- Secure Processing Unit which provides both passive and active protection against side-channel attacks and forensic analysis
- Qualcomm® Trusted Execution Environment for processing highly sensitive material on chip in a fashion that is isolated from the rest of the device's systems
- Debug security with policy-based access control to protect against backdoor attacks throughout the device lifecycle
- FIPS (Federal Information Processing Standards) certified crypto engines to assure strong key derivation, ciphering and mod math functions for public key operations
- Qualcomm® Wireless Edge Services (WES) for risk monitoring, anomaly detection, and renewable security
- Bare metal (type – 1) hypervisor for multiple OS environments running isolated and concurrently
- Secure Boot to ensure software and configuration authenticity and integrity

Continual monitoring of device state is critical for maintaining a strong security posture. Qualcomm® WES (wireless edge services) provides an on-demand attestation service. This trusted attestation service reports on privacy state to preserve user identity, device health and context as well as enterprise application information. WES also provides highly trusted key provisioning services as described above in detail.

Together these security features provide a platform for resilient defense against even the most sophisticated attacks. With this platform, the essential functions needed to protect both cryptographic keys and processes such as apps' digital signature verification are in place.



Intertrust PKI (iPKI): device authenticity and data integrity rich personality for devices, digital signing of apps and certificates for secure communications

Intertrust has been developing innovative distributed trust systems for over 30 years. We're leaders in IoT security, digital and data rights management as well as protected content distribution. We have enabled countless premium content services and distributed trust architectures at massive scale. Recently a major video distributor demonstrated the live streaming of Indian Premiere League to 25 million concurrent users using Intertrust PKI and Intertrust ExpressPlay content protection.

We manage the root of trust for some of the largest cable companies in the world and have extensive expertise integrating with hardware security platforms such as Qualcomm®

Our Intertrust PKI (iPKI™) solution:

- Has operated securely for over 15 years
- Provisioned keys for trusted software and secure communications for over 2 billion devices
- Is WebTrust and ISO 9001 certified
- Is optimized for IoT systems and devices and CyberSecurity Mesh Architecture (CSMA)
- Enables zero trust for IoT
- Deeply integrated with chipsets' hardware security foundations

Distributed multi-party app eco-systems: a new dawn

Secure mobile systems, properly implemented, are some of the most trustworthy computing platforms ever designed. The early days of mobile app development have been largely driven through the distribution of trusted apps by two key innovators.

It has proved to be practical, resilient, trusted and incredibly popular with consumers and enterprises alike. However, this is only the beginning. There has been a presumption that openness implies vulnerability to breaches and malware infestations. This doesn't take into account the fact that the mechanisms for designing and deploying distributed multi-party trust eco-systems are well understood.

Such systems hold the promise of catalyzing a new ecosystem of multiple app stores that can help incentivize new innovative, trusted and very popular apps with unique utility. A new dawn of resilient systems promises to chase away the clouds of risky malware and continual breaches.

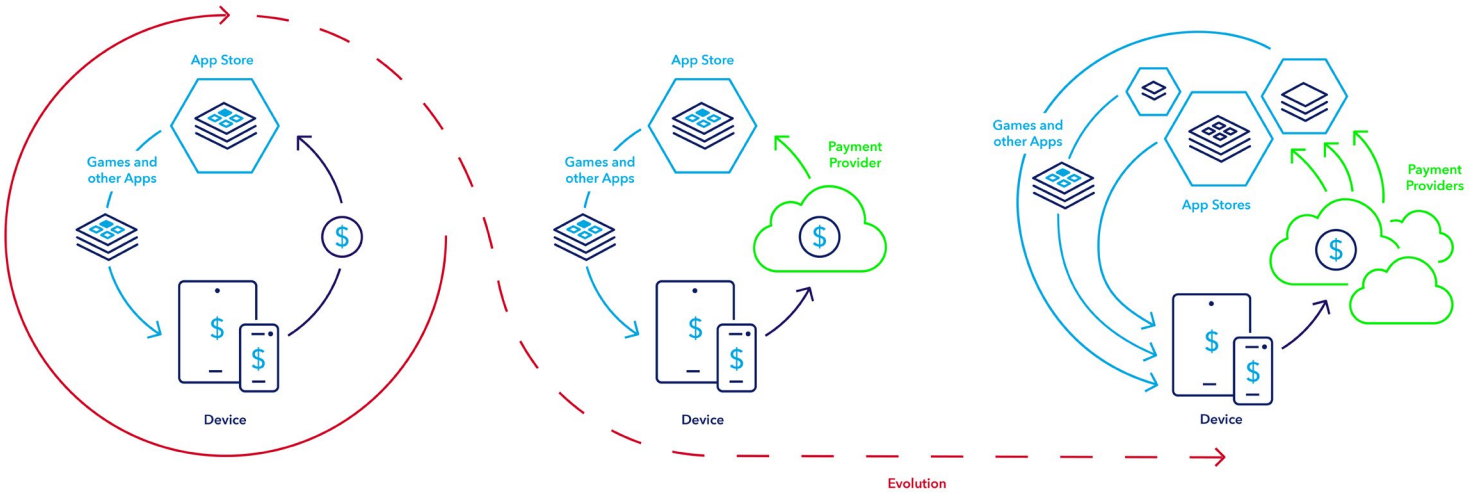


Figure 2

One path towards a trusted ecosystem supporting multiple app stores
Currently the major app stores control both the distribution and payment systems for mobile apps (left), giving them an outsized influence on the mobile app economic ecosystem. To evolve towards a more equitable system, the payment provider could be separated from the app store (center). The next step would be to have multiple payment providers working with multiple trusted app stores, creating a more competitive ecosystem (right) which will ultimately benefit both the app developers and consumers.

About the Author

Julian Durand is VP of Intertrust Secure Systems and product owner of Intertrust PKI (iPKI). He earned his engineering degree from Carleton University and his MBA from the University of Southern California (USC). He is also a Certified Information Systems Security Professional (CISSP) and inventor with 10 issued patents.

Try Intertrust Platform™ free for 14 days: intertrust.com/intertrust-platform-14-day-free-trial

Footnotes

1. VGChartz. (2020). Registered users of Fortnite worldwide from August 2017 to May 2020 (in millions). Statista. Statista Inc.. Accessed: October 21, 2021. https://www.statista.com/statistics/746230/fortnite-players/
2. An Easter egg is a message, image, or feature hidden in software, a video game, a film, or another, usually electronic, medium. https://en.wikipedia.org/wiki/Easter_egg_(media)
3. Mobile Security Index 2021 Report: https://www.verizon.com/business/resources/reports/mobile-security-index/2021/foreword/
4. Mobile Security Index 2021 Report: https://www.verizon.com/business/resources/reports/mobile-security-index/2021/foreword/

intertrust®

Building trust for the connected world.

Learn more at: intertrust.com/pki-for-iot
Contact us at: +1 408 616 1600 | iPKI@intertrust.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035