Google also now managing app sigining keys, like F-Droid

hans #1 May 18, 2017, 8:34am

Lol, so after all those raging debates and flames, it turns out that F-Droid was a pioneer and innovator, years ahead of Google. “With Google Play App Signing, you can securely manage your app signing keys for new or existing apps. Keys are stored on the same secure infrastructure Google uses to store its own keys.”

https://support.google.com/googleplay/android-developer/answer/7384423

Anyone hear anything about Google’s motivations for doing this?

3 Likes

nutomic #2 May 19, 2017, 1:10pm

From the article on Android Police (on mobile so no link), this is just to make things easier for developers. And also make it less likely that developers accidently lose their signing key.

2 Likes

hans #3 June 23, 2017, 1:49pm

That’s one consideration. But I’m guessing that’s just their public reason. I’ll bet they did it for very different reasons. It basically is a reversal of the driving idea behind APK signatures since the beginning of Android: decentralized cryptography and Google Play never modifying the binaries.

2 Likes

sesam #4 June 30, 2017, 11:06am

Probably for pragmatic, data-based reasons. Originally, being minimally centralised was better, but in fact developers and users are in general better served by having to do less, and the legal viewpoint is still that the key belongs to the developer, not Google, so they don’t have to “sign off” on that any Play store app is not complete crap or that it won’t kill kittens.

1 Like

relan #5 October 8, 2017, 6:46pm

Old thread, but topic is very relevant.

Amazon has always been re-signing apps you submit with their own key (just like Apple). They inject their code into apps: **https://developer.amazon.com/docs/app-submission/understanding-submission.html#amazons-code-wrapper**

Google hardly needs any dirty tricks as they control the whole platform. But keys give them power, who knows how they'll use it.

1 Like

hotlittlewhitedog #6 October 8, 2017, 6:53pm

And how they resign an application without the source?
They decompile it?

1 Like

relan #7 October 8, 2017, 7:02pm

> And how they resign an application without the source?
> They decompile it?

App is just a ZIP file where code, resources and signature are files with fixed names. "Re-signing" simply replaces signature files in the ZIP.

1 Like

hans #8 October 9, 2017, 12:40pm

thanks for bringing up Amazon, **@relan** . It is a scary example of what's to come.

2 Likes

NicoAlt closed #9 April 15, 2018, 3:10pm

Licaon_Kter #10 June 17, 2020, 10:08am

Oops: **https://nitter.net/ByteHamster/status/1272244176290275330#m**

2 Likes

hans #11 June 17, 2020, 10:51am

Yup, more info here:

Google introduces Play Billing Library version 3 and plans to make App Bundles...

Google has announced the Play Billing Library v3 and plans to make Android App Bundles a requirement for new apps uploaded to the Google Play Store in 2021.

2 Likes

Bubu opened #12 June 17, 2020, 1:27pm

Licaon_Kter #13 September 25, 2020, 9:23am

Uncomfortable Questions About App Signing

5 Likes

Licaon_Kter #14 November 20, 2020, 12:34pm

“new apps” for now?

New Android App Bundle and target API level requirements in 2021

Posted by Hoi Lam , Developer Relations Engineer, Android Platform In 2021, we are continuing with our annual target API level up...

Mahem #15 November 20, 2020, 9:15pm

Just like local branded but good quality product packets are repacked with big brands packets 🙂

1 Like

Licaon_Kter #16 July 1, 2021, 10:18am

Full circle as expected

Android App Bundles are replacing APKs – why it matters

Google Play Store is constantly evolving to meet the growing needs and demands of Android users and developers. Many of those improvements rely on automated systems powered by AI and machine learni…

2 Likes

justsomeguy #17 July 1, 2021, 11:21am

“This means that developers switching from APK to App Bundles can no longer provide the exact same package or experience on other app sources unless they opt to maintain a separate APK version. This naturally puts third-party app stores at a disadvantage, but Google will most likely play up the Play Store’s security…”

Time to take our eggs out of 666gle’s basket?

SuperSapien64 #18 July 1, 2021, 6:41pm

This sucks thanks a lot Google if its not broke don’t fix it. 😡

ecxod #19 July 5, 2021, 1:54pm

Come on Hans, this is obviously to inject apps with binary code after compiling. Do you remember the viruses in the 80’s? the cascade virus for example … something like that…

relan #20 July 5, 2021, 7:17pm

> this is obviously to inject apps with binary code after compiling

What for? Google already has an official backdoor called Google Play Services and can do whatever they want with a device.

1 Like

hans #21 July 6, 2021, 7:29am

I agree that Google Play Services has backdoor like powers, I still think installing targeted malicious apps has its advantages. It is easier to target, all Google devices have Play Services, not all have a specific app. Also, it would be a lot easier to install a small malicious update, then insert an implant then uninstall the update. Google having the signing keys gives anyone who has username/password to the account the possibility to push out updates.

This could in theory be useful to disable malware, for example, malware gets into Play. Without the signing key, Google cannot push out an update to that malware. With the signing key, they could push out an update to that APK that disables it. I'll bet that's part of the thinking behind them requiring this feature, but they don't want to publicly announce that since they would get a ton of flak from security and privacy people. They do already have the power to do remote uninstalls, so this would be only useful if they actually want to tap into the running software, like in botnet scenarios.

2 Likes

ecxod #22 August 15, 2021, 5:35am

Because the normal DAU usually inputs different data in different apps. It is more simple to have a function in the same class or namespace that steals the data, then complicatedly sniffing the app traffic of the apps via play services.

Tryder #23 August 16, 2021, 12:40am

> hans:
>
> "…Keys are stored on the same secure infrastructure Google uses to store its own keys."

Sorry, just thought this line was pretty funny.

As secure as the infrastructure used by the world’s largest manufacturer of SIM cards in which the encryption keys were stolen by American and British spies? Or maybe as secure as the US Treasury department’s servers which were hacked and had encryption keys stolen off of them.

I always find it funny when a company boasts about their “secure” infrastructure.

So… If you had ten million apps with ten million signing keys all stored on different computers you’d have to hack roughly ten million computers if you wanted to compromise a significant selection of apps. Let’s just take those ten million keys and put them all in one basket. Who is Google conveniencing here anyway?

hans #24 August 20, 2021, 11:34am

Google does have a good track record of defending against unwanted intrusion.
China was able to hack in pretty deep years ago. But well resources state
actors always get in if they are committed to it. The open question with Google
is the kinds of things they do willingly and in secret, like PRISM.

1 Like

Moz #25 August 20, 2021, 2:24pm

Dragnet surveillance implemented through Google would drag so many people that it would take years to sift through it all and then cancel out false positives, some people will have probably emigrated or died by the time they get looked at. Plenty of terrorists running around undetected.

Tryder #26 August 20, 2021, 4:11pm

I think more likely such dragnet surveillance would be used to start building profiles on anyone that shows, let’s call it, undesireable behaviour. Then, should the need arise, the data on the subject is already there and ready for use.

So if the subject eventually proves effective at inspiring protests or something they already have a psychological profile worked up, they probably already have dummy accounts in their social media friends list ready to be activated, names, addresses, phone numbers of family members and known associates, etcetera…

Moz #27 August 20, 2021, 4:41pm

If would be difficult to say whats deemed “undesirable” and disprove the risk of false positive by direct investigation. It’s like how OONI Probe is purposely designed to trigger blocks in order to see which blocks exist, it doesn’t mean you directly went and did something worthy of triggering a block, it’s just a test. That would only be discovered if they looked deeper, directly and likely with need for a warrant which requires evidence to be granted in the first place.
And as I said at the end of my last post, countless terror attacks from domestic and international actors continue to happen and most of them are using Telegram, they could and should get sucked up, profiled, identified and arrested yet they hardly ever are.

Tryder #28 August 20, 2021, 4:54pm

Yes, but none of those attacks are effective in accomplishing their goals. If an international terrorist’s goal is to dismantle western imperialism and the domestic terrorist’s goal is to bring down the police state then none of their actions actually accomplish those goals or even nudge their ideologies even the slightest bit closer to becoming reality.

Quite the opposite really, domestic and international terrorist actions have only served to give reason to strengthen the very devices the terrorists wish to destroy. Therefore they’re not really national security threats, they’re more like assets even if they wish to believe otherwise.

Moz #29 August 20, 2021, 5:00pm

I see your point but I think that’s a very large scale strategic view, many terrorists attack for the sake of showing they’re still capable of doing so despite these strengthened devices you mentioned. Look at the IRA in the 1980s, they used to place explosives in a public area and then phone the police to report themselves and initiate evacuation. It was done to show they could still operate despite everything Scotland Yard and MI5 had. There are many documentaries about it on YouTube.

Tryder #30 August 20, 2021, 5:10pm

Yes, but how much closer are they to pushing out the Brits now than they were thirty years ago? Not at all.

Sure they pose a threat to the citizenry with their bombs, but they pose no threat to the state. The only thing they’ve been able to accomplish is strengthening British rule by giving reason for the widespread deployment of surveillance technologies and equipment.

Moz #31 August 20, 2021, 5:13pm

The Brits probably have less surveillance than the USA due to all the alphabet agencies yet look at the narwhal from yesterday who was targeting the Capitol, a government building, nobody saw him coming (other than ivory poachers)

Tryder #32 August 20, 2021, 6:16pm

The UK just legalized everything that Snowden warned us about

The UK is about to become one of the world's foremost surveillance states, allowing its police and intelligence agencies to spy on its own people to a degree that is unprecedented for a...

“The UK is about to become one of the world's foremost surveillance states, allowing its police and intelligence agencies to spy on its own people to a degree that is unprecedented for a democracy. The UN's privacy chief has called the situation ‘worse than scary.’ Edward Snowden says it's simply ‘the most extreme surveillance in the history of western democracy…’”

That was 2016. Of course there's also the close surveilance relationship between the US and the UK. As I understand it the relationship is so close that GCHQ has been performing NSA tasks and vice versa.

P.S. I don't know to which narwhal you refer. I don't read or watch the news.

Moz #33 August 20, 2021, 6:23pm

I'm certainly very glad not to live there, if I did it would be premium cash VPN for everything +Tor for anything important. Although I have noticed some UK based exit nodes with CIA directly in the name. Operating safely in the UK could be a self set challenge, if they have one the highest surveillance levels in the world and you go about undetected then you could definitely go undetected anywhere else as their surveillance will be to a lesser extent.

I believe 5 eyes is still a think but one country was going to or actually did leave (Canada I think) so they will continue to work for each other. Germany seems to be a country rather heavily involved with privacy but they too are in 5 eyes.

The NSA has physical stations in the UK and some old ones have been abandoned so it's fair to assume GCHPOO and Johnny English both have buildings in America.

All this monitoring to miss or willingly ignore deadly threats in order to arrest people who post political leaflets, winning.

Aforementioned narwhal

August 19, 2021 US Capitol bomb threat news

A suspect who claimed to have an explosive device in a truck near the US Capitol has surrendered to authorities, two law enforcement sources tell CNN. Follow here for the latest news.

I try not to read it either but it still intrudes somehow, even the front page of YouTube has a news section dedicated to suffering.

Tryder #34 August 20, 2021, 6:31pm

Last I checked Germany was a member of the 9 eyes surveillance alliance so, you know, cooperative, but not to the same level as the 5 eyes. The UK and the US should really be called the two eyes, or the one eye really.

So you have the twins, US/UK, the 5 eyes, the 9 eyes and the 14 eyes all with differing levels of cooperation. I believe it was, what, six or seven years ago when the US was caught spying on the German govenment. The German's didn't seem too surprised or even really that concerned. Probably because they're doing the same thing.

Despite a few proxy wars, the Cold War wasn't fought with F-14s and Mig-22s. The Cold War was fought with propaganda and psychological manipulation. Now the Soviet Union's KGB, et al, were good, they were damn good. But they didn't win that war.

P.S. I found out about Afghanistan through New Pipe when getting ready to look up some music.

1 Like

Licaon_Kter #35 August 20, 2021, 7:30pm

Can we get back on track though? 🙂

2 Likes

justsomeguy #36 August 20, 2021, 8:46pm

Aren't you glad you reopened this topic so Tryder could host his blog here? 😆

1 Like

Moz #37 August 20, 2021, 9:02pm

Yes, sorry for getting a bit off track with it

1 Like

Moz #38 August 20, 2021, 9:03pm

Maybe block him too you discount shill

1 Like