Twitter Thread by Matthew Green



Matthew Green
@matthew_d_green

My students @maxzks and Tushar Jois spent most of the summer going through every piece of public documentation, forensics report, and legal document we could find to figure out how police were “breaking phone encryption”. 1/

> ACLU is suing the FBI over its efforts to break into encrypted devices. https://t.co/TN8X0Slmnf
>
> — Zack Whittaker (@zackwhittaker) December 22, 2020

This was prompted by a claim from someone knowledgeable, who claimed that forensics companies no longer had the ability to break the Apple Secure Enclave Processor, which would make it very hard to crack the password of a locked, recent iPhone. 2/

We wrote an enormous report about what we found, which we’ll release after the holidays. The TL;DR is kind of depressing:

Authorities don’t need to break phone encryption in most cases, because modern phone encryption sort of sucks. 3/

I’ll focus on Apple here but Android is very similar. The top-level is that, to break encryption on an Apple phone you need to get the encryption keys. Since these are derived from the user’s passcode, you either need to guess that — or you need the user to have entered it. 4/

Guessing the password is hard on recent iPhones because there’s (at most) a 10-guess limit enforced by the Secure Enclave Processor (SEP). There’s good evidence that at one point in 2018 a company called GrayKey had a SEP exploit that did this for the X. See photo. 5/



There is really no solid evidence that this exploit still works on recent-model iPhones, after 2018. If anything, the evidence is against it.

So if they can't crack the passcode, how is law enforcement still breaking into iPhones (because they definitely are)? 6/

The boring answer very likely is that police *aren't* guessing suspects' passcodes. They're relying on the fact that the owner probably typed it in. Not *after* the phone is seized, in most cases. Beforehand. 7/

You see, iPhones can be in one of two states, which are respectively known as "Before First Unlock" (BFU) and "After First Unlock" (AFU). This is pretty self-explanatory.

When you turn your phone on and enter the passcode in the morning, you switch your phone from BFU->AFU. 8/

When you first unlock your iPhone after power-on, it uses your passcode to derive several sets of cryptographic keys. These stay in memory inside your phone, and are used to encrypt the file system. 9/

When you lock your iPhone (or press the button on the side, or leave it alone until the screen goes blank), exactly *one* set of keys gets “evicted”, ie erased from memory. Those keys are gone until you enter your passcode or use FaceID.

All of the other keys stay in memory. 10/

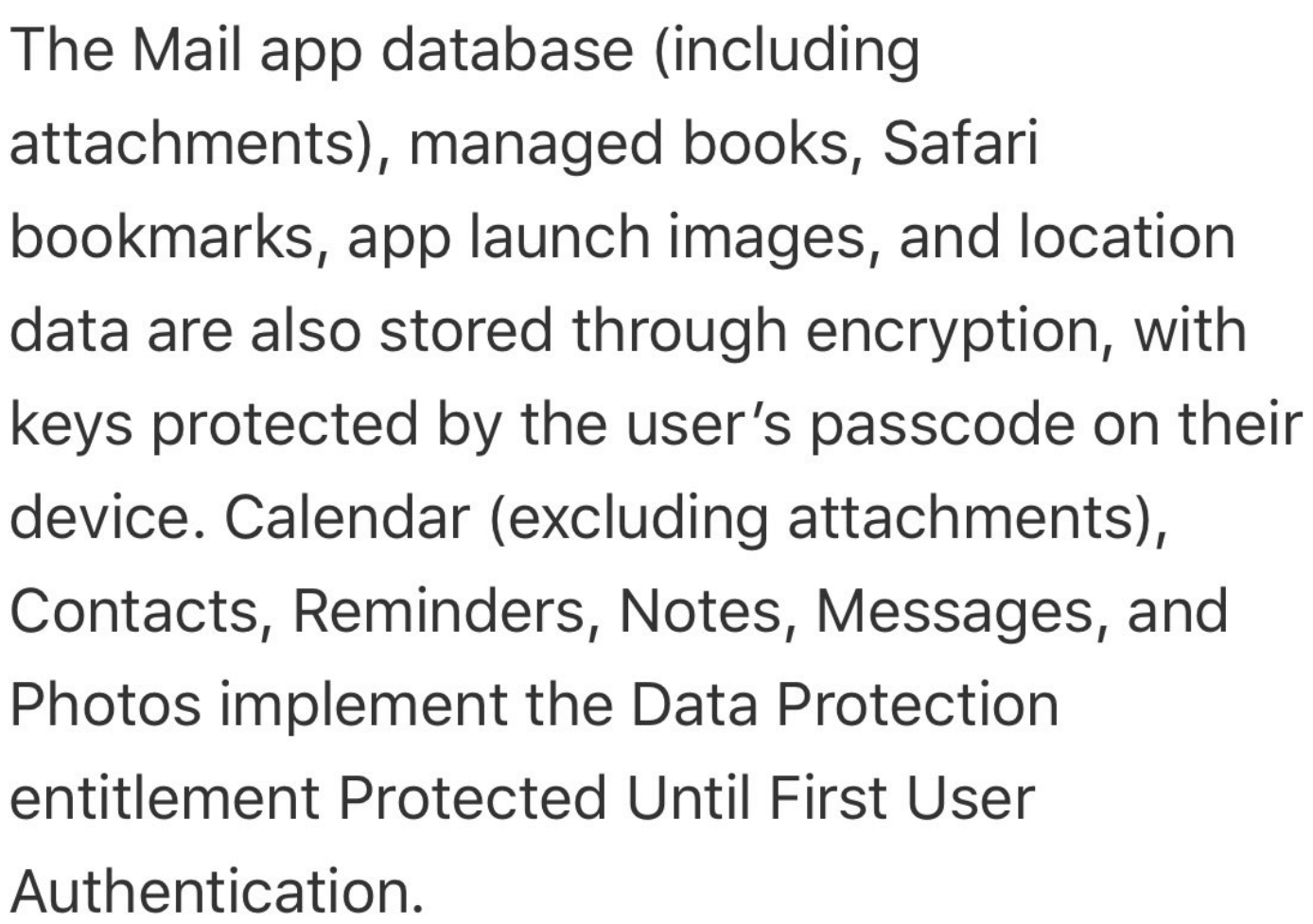
The key that gets evicted on lock is used to decrypt a subset of the files on the filesystem, namely the ones that have a specific protection class (NSComplete). The keys that don’t get evicted can be used to decrypt all the other files.

(This is all well-known so far BTW.) 11/

So the upshot of this is that, if police can capture your phone in the AFU state (yours is almost certainly in that state for 99% of its existence) *and* they have a software exploit that allows them to bypass the OS security measures, they can get most of the files. 12/

The real question is: what exactly does “most of the files” mean, and the corollary is “why not protect *more* than just a few of the files with that special key (the one that gets evicted)”. That’s where things get depressing. 13/

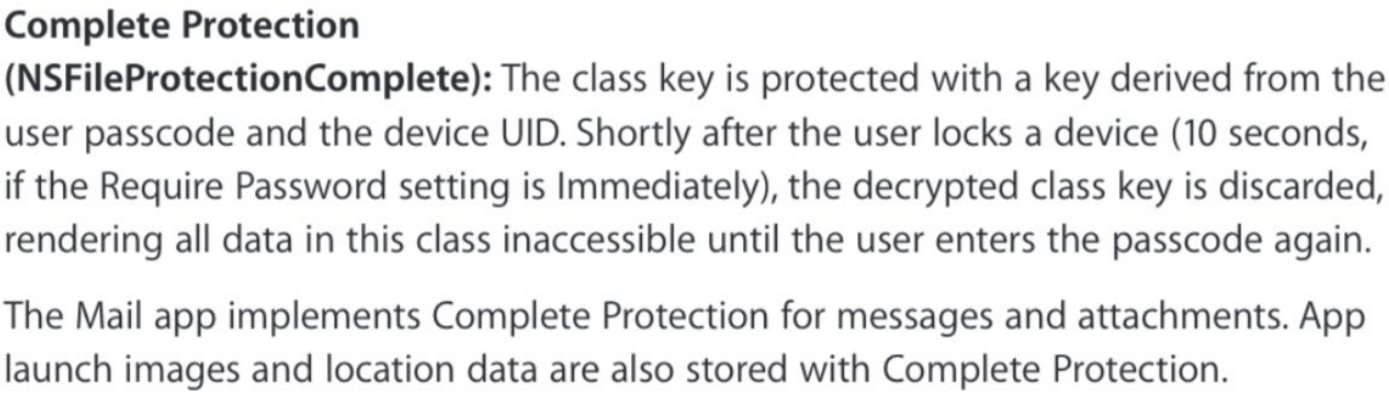
Apple *sort of* vaguely offers a list of the apps whose files get this special protection even in the AFU state. But notice how vague this language is. I have to actually decode it. 14/



Notice how this text simply reports that some app data is "protected through encryption" (this is vague and meaningless, since it doesn't say whether it's AFU or BFU) and other app data is explicitly only protected in the BFU state (before you first unlock.) Why so vague? 15/

Here is a version of the same text from back in 2012. Notice how it explicitly states that "Mail, App Launch images, and Location Data" are protected using the strongest type of encryption.

So it seems that Apple is actually protecting *less* data now than in 2012. Yikes. 16/



(Our most likely guess: Apple has weakened the protections on location data in order to enable fancy features like “location based reminders”. So they had to weaken the language in the security guide. This isn’t great.) 17/

But whether you look at the 2012 or 2020 data, the situation sucks. The built-in apps that definitely use strong AFU protection are:

Mail (which probably already exists on a server that police can subpoena, so who cares.)

App launch data (■■■■)

That’s not great. 18/

3rd party apps can opt-in to protect data using the strongest type of encryption, so this isn’t necessarily the whole story. But let’s list some data that *doesn’t* get AFU protection:

Photos
Texts
Notes
Possibly some location data

Most of what cops want. 19/

So this answers the great mystery of “how are police breaking Apple’s encryption in 2020”. The answer is they probably aren’t. They’re seizing unlocked phones and using jailbreaks to dump the filesystem, most of which can be accessed easily since keys are in memory. 20/

Oh my god my thumbs. 21/

Anyway, this leaves basically only one remaining question:

Why is so little of this data encrypted when your phone is AFU and locked? And the answer to that is probably obvious to anyone who develops software, but it still sucks. 22/

Most apps like to do things in the background, while your phone is locked. They read from files and generally do boring software things.

When you protect files using the strongest protection class and the phone locks, the app can’t do this stuff. It gets an error. 23/

Apple provides some tools to make this less painful: for example, they have a “write only” protection class.

But for the most part it’s annoying for software devs, so they lower protections. And if Apple *isn’t* using strong protection for its in-house apps, who will? 24/

If I could tell Apple to do one thing, I would tell them to figure this problem out. Because without protection for the AFU state, phone encryption is basically a no-op against motivated attackers.

Maybe Apple's lawyers prefer it this way, but it's courting disaster. 25/

For those who would prefer to read this thread in the form of a 65-page PDF that also discusses cloud backup systems and Android, here is our current paper draft: https://t.co/k3Qw0DNIoI

This will be on a pretty website soon. Thanks for not blocking me after this thread. // fin