SEC575 | Mobile Device Security and Ethical Hacking

SANS

iOS 11.4.1 USB Restricted Mode Notes

Some notes on the iOS 11.4.1 USB restricted mode.

Joshua Wright
@joswr1ght
jwright@hasborg.com

GRAYKEY BY GRAYSHIFT

Grayshift sells the GrayKey to unlock iOS devices through USB

- $15K for online version, limited to 300 phone unlocks
- $30K for offline version, unlimited phone unlocks

Grayshift claims success against iOS 10-11 including iPhone 8 and X

Cellebrite offers unlocking features, but unlocks in-house only

- *Supports 4-digit, 6-digit, and complex passcodes*
- *Complete file system extraction*
- *Supports disabled iOS devices*
- *Continually updated for new iOS versions*

https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/

GrayKey by Grayshift

Grayshift is a digital forensics company run by an ex-Apple employee and US intelligence agency contractors (https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack). The flagship product at Grayshift is the GrayKey, a "technology that provides lawful access to iOS devices." (http://www.technosecurity.us/mb/exhibitors/grayshift) Selling to local, state, and federal law enforcement agencies, GrayKey is designed to bypass the lock screen on iOS devices, supporting iOS 10, iOS 11, and many different devices including the iPhone 8 and iPhone X.

Exploiting an undisclosed vulnerability in the USB interface of iOS devices, the GrayShift sells for $15K for a hardware device that requires internet access, limited to 300 phone unlocks. For $30K, the same capabilities are also available in an offline mode, unlocking an unlimited number of devices.

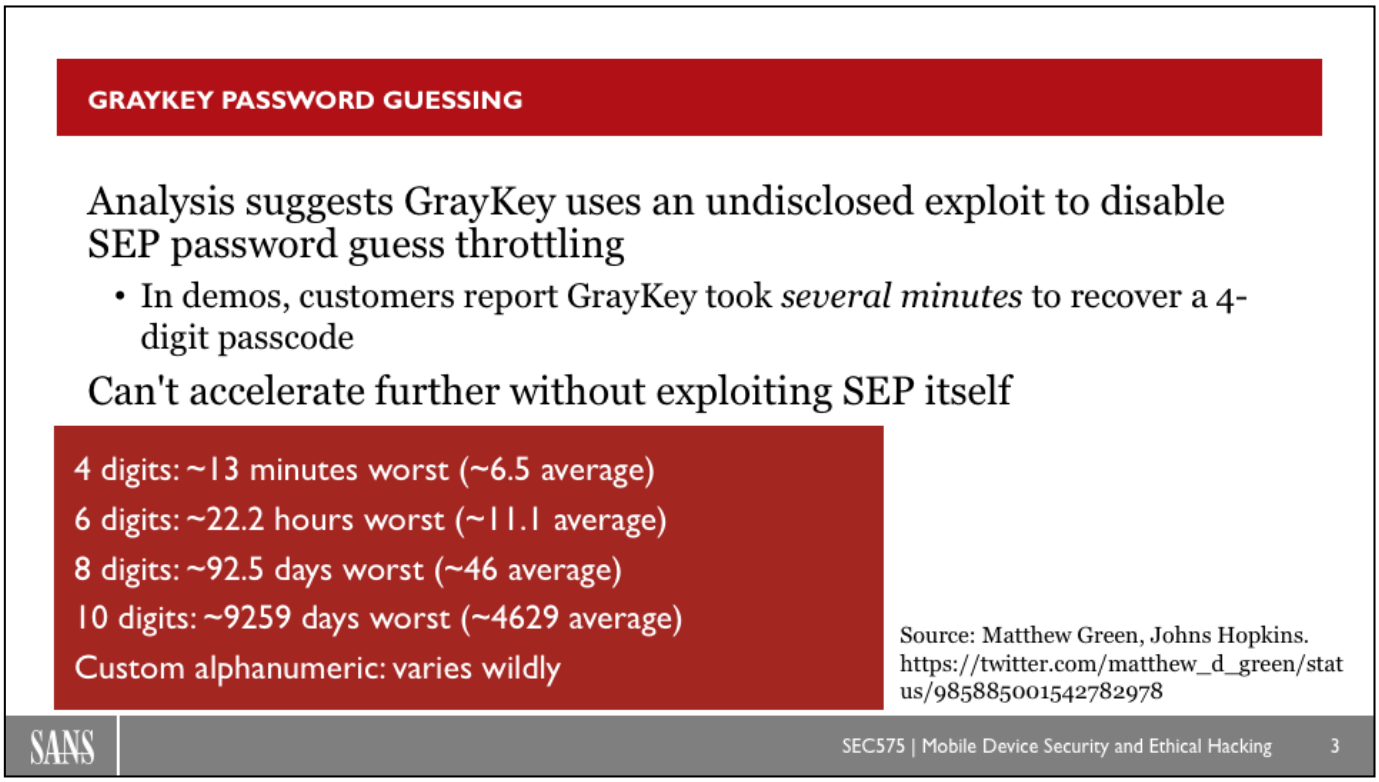
The GrayShift device offers several capabilities that are valuable to forensic analysis of iOS devices, including:

- Bypass of 4-digit, 6-digit, and complex passcodes (alphanumeric)
- Complete file system data extraction (reportedly exceeding the capabilities of a *logical acquisition* through an iTunes backup)
- Can bypass disabled iOS devices (e.g. devices that are in recovery mode, or are disabled due to prior incorrect password guesses)
- Ongoing support for new iOS software versions

Similar capabilities have been available through a *device unlock service* at the mobile forensics company Celebrite, but in a very different deployment model. Where Grayshift sells a physical device for phone unlocking to the customer, Cellebrite requires that law enforcement sends in the device to be unlocked for their handling. Celebrite maintains a more restricted level of control over what devices can be unlocked by which

customers, while Grayshift lacks similar controls, particularly in the more expensive *offline* GrayKey device.

Image: https://www.macobserver.com/columns-opinions/editorial/grayshift-data-breach/

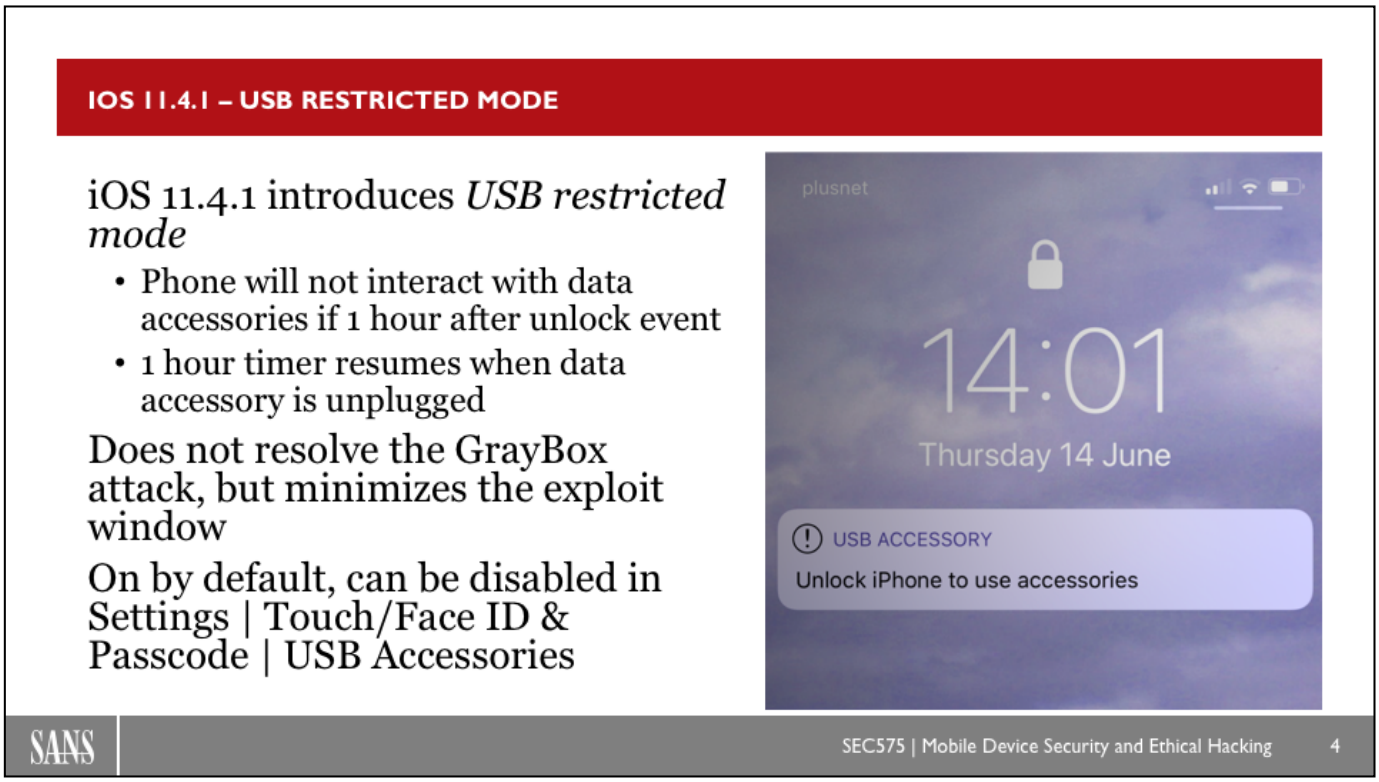


GrayKey Password Guessing

Although the GrayKey device is not widely available for analysis, there is sufficient reporting about the efficacy of the device to draw some conclusions about how it works. Analysis indicates that the GrayKey uses an undisclosed vulnerability in the USB data interface of iOS devices to disable the Secure Enclave Processor (SEP) password guess throttling capability (the feature in iOS that allows you to make 6 incorrect guesses before a delay of 1 minute, a 7th guess introduces a 5 minute delay, 8th incorrect guess introduces a 15 minute delay, and the 9th incorrect guess introduces a 60 minute delay before a data wipe). Even with the password guess throttling, there is a delay for each guess on the SEP itself, preventing the GrayKey from instantly recovering the password.

Analysis by Matthew Green of Johns Hopkins University indicates that the GrayKey can recover a 4-digit PIN in approximately 6.5 minutes (which seems to align with public reports of demonstrations of the GrayKey device where a password was recovered after *several minutes*. A 6-digit PIN is recovered in 11.1 hours on average, and an 8-digit PIN is recovered after 46 days on average.

A 10-digit PIN seems impractical (4629 day average), and a custom alphanumeric password will vary wildly. Using the same password guessing statistics (approximately 128 guesses/second), a password in the rockyou.txt file of 14.3 million words could be recovered in 16 hours on average, though a complex password of sufficient length would likely evade password cracking attempts at this rate.



iOS 11.4.1 – USB Restricted Mode

In iOS 11.4.1 released on July 9, 2018, Apple introduced the USB restricted mode feature. Turned on by default, iOS devices will not interact with data accessories (including PCs, Macs, or anything else using data USB pins; charging is not affected) if the device has not been unlocked within one hour. If you plug in a data peripheral and the iOS device has not been unlocked, it will display the error "Unlock iPhone to use accessories" as shown on this page (https://9to5mac.com/2018/07/09/ios-11-4-1-unlock-iphone-to-use-accessories-explained/). The one hour timer restarts when the data accessory has been unplugged from a locked device.

With this feature, an iOS device can still be exploited using the GrayBox, but it minimizes the opportunity for a threat actor to exploit the device. If the GrayBox user receives a device that is locked, and has not been unlocked within an hour, then the iOS device will not interact with the GrayBox device, precluding the opportunity to exploit the platform.

Apple indicates that some third-party devices may not interact well with the USB restricted mode feature, and offers users the ability to disable this capability altogether. (https://support.apple.com/en-us/HT208857)

"BYPASS" USB RESTRICTED MODE

Any connected data device will keep the USB restricted clock timer from restarting

Solution: plug in any data accessory after seizing iOS device

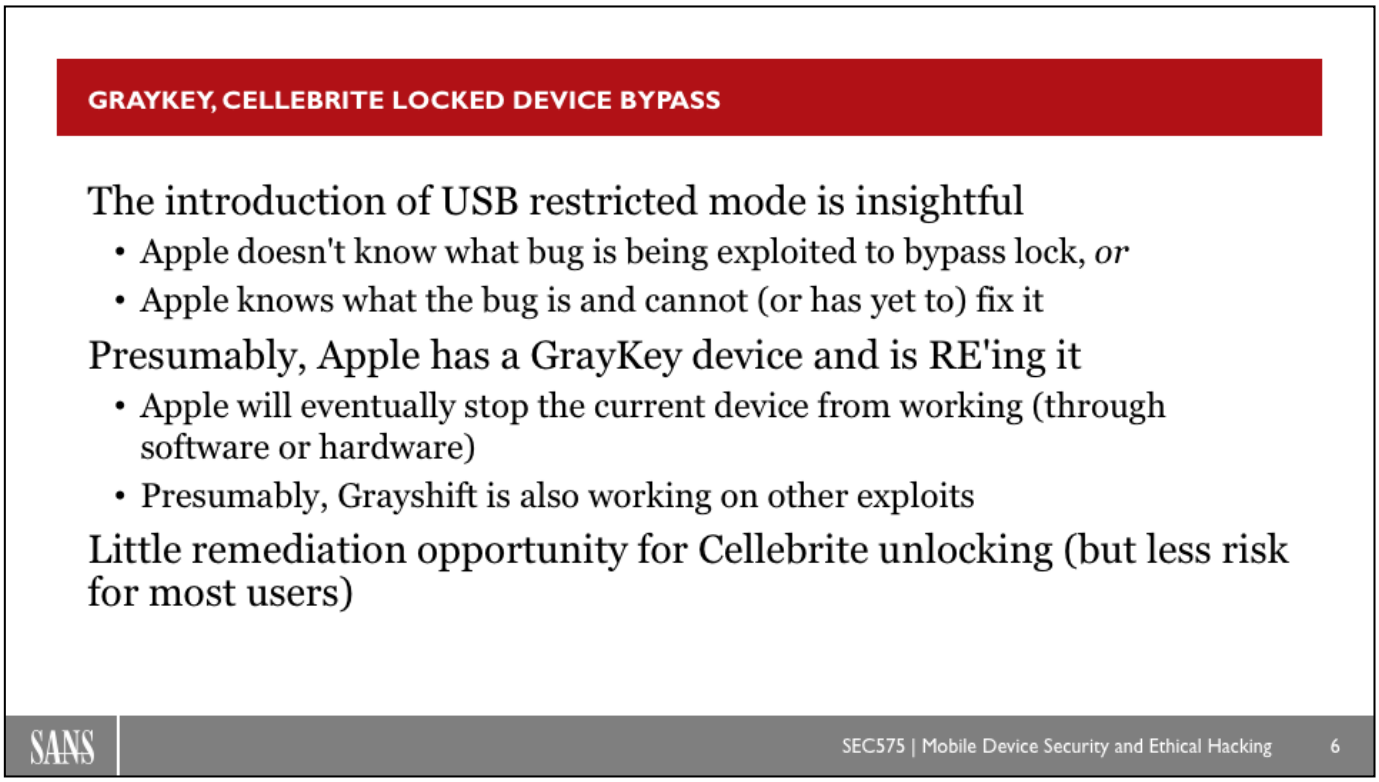
- Presumably, the user has unlocked it within the last hour
- Plugging in a data accessory restarts the USB restricted timer
- Keeping the device plugged in keeps the counter from resuming
- Allows *threat actor* leisure to crack passcode at a later time

Apple Lightning to USB 3 Camera Adapter, $39

"Bypass" USB Restricted Mode

First reported by Elcomsoft (https://blog.elcomsoft.com/2018/07/usb-restricted-mode-inside-out/), any USB data device that connects to an iOS device will reset the USB restricted mode clock timer. This presents an opportunity for a threat actor (e.g. law enforcement agencies, or anyone with access to a GrayKey) to overcome the USB restricted mode defense:

1. The threat actor seizes the target device; presumably, the user has unlocked the device with in the last hour
2. The threat actor plugs in any USB data device, such as the Apple Lightning to USB 3 Camera Adapter (shown on this page); this device is convenient because it can also power the device
3. Keeping the adapter plugged in keeps the USB restricted mode clock timer from restarting, allowing the threat actor time to relocate the target device to the GrayKey device
4. Attacker cracks the passcode as their leisure



GrayKey, Cellebrite Locked Device Bypass

Apple has not responded to requests for comment on the GrayKey device, but the introduction of the USB restricted mode feature is insightful. Apple has yet to resolve the vulnerability exploited by the GrayKey device, instead introducing a general workaround (with its own set of limitations), indicating that Apple does not yet know what bug is being exploited by Grayshift, or Apple knows what the bug is but cannot (or has yet to) fix it.

It seems reasonable to imagine that Apple has a GrayKey device in their possession and is attempting to reverse engineer (RE) it to identify the nature of the flaw being exploited. It also seems reasonable that Apple will work to resolve the vulnerability, either through a software update or a hardware replacement (e.g. the next iPhone model, if the vulnerability is related to a hardware flaw that cannot be resolved through a software update). However, one would assume that Grayshift's commitment to continued support for later iOS versions would indicate that they also continue to identify opportunities to exploit iOS devices with additional updates.

The Grayshift model of on-premises lock screen bypass device makes the technology more accessible to would-be threat actors (including law enforcement agencies, but also people who surreptitiously obtain a GrayKey device through other means), but it also creates an opportunity for Apple to evaluate the exploit(s) in use to resolve them. The Cellebrite on-premises data recovery model is perhaps less of a threat to a wide audience of iOS users, but will also likely evade Apple's ability to identify and resolve the exploits they have developed.