

Security experts found a way to break iPhone passwords on all versions without worrying about locking or deleting data

Matthew Hickey, a security researcher at Hacker House, recently figured out a way for brute force attacks to unlock any iPhone or iPad device, despite being updated to the latest iOS version.

Matthew Hickey, a security researcher at Hacker House, recently figured out a way for brute force attacks to unlock any iPhone or iPad device, despite being updated to the latest iOS version. Hickey's discovery made Apple once again have to review security technology on its iPhone and iOS devices.

Brute force is a technique to try to guess a user's password. Hackers use the list of the most popular usernames and passwords in the world to constantly send queries to the user's wp-login.php file until they log in.

```

File Edit View Terminal Help
[*] 192.168.0.197:3306 MYSQL - [56/72] - Trying username:'ashishi' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [56/72] - failed to login as 'ashishi' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [57/72] - Trying username:'ashishi' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [57/72] - failed to login as 'ashishi' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [58/72] - Trying username:'ashishi' with password:'hello'
[*] 192.168.0.197:3306 MYSQL - [58/72] - failed to login as 'ashishi' with password 'hello'
[*] 192.168.0.197:3306 MYSQL - [59/72] - Trying username:'gelowo' with password:'12121'
[*] 192.168.0.197:3306 MYSQL - [59/72] - failed to login as 'gelowo' with password '12121'
[*] 192.168.0.197:3306 MYSQL - [60/72] - Trying username:'gelowo' with password:'asdad'
[*] 192.168.0.197:3306 MYSQL - [60/72] - failed to login as 'gelowo' with password 'asdad'
[*] 192.168.0.197:3306 MYSQL - [61/72] - Trying username:'gelowo' with password:'asdasd'
[*] 192.168.0.197:3306 MYSQL - [61/72] - failed to login as 'gelowo' with password 'asdasd'
[*] 192.168.0.197:3306 MYSQL - [62/72] - Trying username:'gelowo' with password:'asdas'
[*] 192.168.0.197:3306 MYSQL - [62/72] - failed to login as 'gelowo' with password 'asdas'
[*] 192.168.0.197:3306 MYSQL - [63/72] - Trying username:'gelowo' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [63/72] - failed to login as 'gelowo' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [64/72] - Trying username:'gelowo' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [64/72] - failed to login as 'gelowo' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [65/72] - Trying username:'gelowo' with password:'hello'
[*] 192.168.0.197:3306 MYSQL - [65/72] - failed to login as 'gelowo' with password 'hello'
[*] 192.168.0.197:3306 MYSQL - [66/72] - Trying username:'root' with password:'12121'
[*] 192.168.0.197:3306 MYSQL - [66/72] - failed to login as 'root' with password '12121'
[*] 192.168.0.197:3306 MYSQL - [67/72] - Trying username:'root' with password:'asdad'
[*] 192.168.0.197:3306 MYSQL - [67/72] - failed to login as 'root' with password 'asdad'
[*] 192.168.0.197:3306 MYSQL - [68/72] - Trying username:'root' with password:'asdasd'
[*] 192.168.0.197:3306 MYSQL - [68/72] - failed to login as 'root' with password 'asdasd'
[*] 192.168.0.197:3306 MYSQL - [69/72] - Trying username:'root' with password:'asdas'
[*] 192.168.0.197:3306 MYSQL - [69/72] - failed to login as 'root' with password 'asdas'
[*] 192.168.0.197:3306 MYSQL - [70/72] - Trying username:'root' with password:'1212'
[*] 192.168.0.197:3306 MYSQL - [70/72] - failed to login as 'root' with password '1212'
[*] 192.168.0.197:3306 MYSQL - [71/72] - Trying username:'root' with password:'123321'
[*] 192.168.0.197:3306 MYSQL - [71/72] - failed to login as 'root' with password '123321'
[*] 192.168.0.197:3306 MYSQL - [72/72] - Trying username:'root' with password:'hello'
[*] 192.168.0.197:3306 - SUCCESSFUL LOGIN 'root' : 'hello'
  
```

Starting from iOS 8, all iPhone and iPad devices are equipped with advanced encryption security technology with a 4 or 6 digit password. The close connection between hardware and software makes it impossible to break these devices. In addition, the device also allows users to set the mode to manually clear all data in the device if the wrong password is entered too many times, making brute force harmless.

On the new generation devices of Apple is equipped with a closed processor integrated right on the hardware of the machine. This security system is called Secure Enclave, which has a secure bootloader and its own software update mechanism that can 'count' the wrong number of user passwords. After each wrong entry, it reduces the speed of the device's response until it receives the correct password.



Secure Enclave security system first appeared on Apple's A7 processor.

But Hickey with an iPhone turned on but the screen lock and a Lightning cable figured out how to bypass the 10-time password entry limit on almost every iOS version to be able to run brute force comfortably, even above New versions like iOS 11.3.

Hickey said that when the iPhone or iPad is connected to Lightning and receives an input signal from an external peripheral (in this case a keyboard), an intervention request should be prioritized to handle immediately. will be activated. This means, if you do not break down the password to enter it multiple times and enter a long multi-digit string, the iPhone will process the entire sequence but only count as a single entry. This entry is equivalent to hundreds of single entries. This way, hackers can freely conduct brute force.

For example, all passwords listed from 0000 to 9999 will be hacked by hackers to create continuity during the operation of the software and then iPhone will process the entire range from 0000 to 9999 before the software tells the user that the password was entered incorrectly if the password is not in the above sequence.

With Hickey's attack method, hackers can only enter more than 100 passwords of 4 digits per hour and for 6-digit passwords, it will take longer.

Hickey has sent an email informing its findings to Apple, but the technology company has yet to give a formal response to the issue.

Earlier, Apple had to launch a new feature called USB Restricted Mode in the new version of iOS 12 to disable the iPhone unlocking tool called Grayshift's GrayKey.

See more:

1. This is how this guy controls the iPhone with his eyes, not one touch
2. Check iOS 12 beta and iOS 11.4 on iPhone 5S to iPhone 8, should upgrade?
3. How to check the safety cable for your iPhone

You finished reading the article "**Security experts found a way to break iPhone passwords on all versions without worrying about locking or deleting data**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.