Assignment 3

2014 Celebrity photo hack

What happend?

On August 31, 2014 a collection of almost 500 private pictures of various celebrities where post on image board 4chan and later on other social networks.

The images where obtained via Apple's cloud service. The attack was very targeted on account information and not on any specific security vulnerabilities Apple sad.

But 6 months before it was a guy called Balic who told Apple via mail he was able to try more then 20.00 passwords combinations with brute force attack. But he didn't get any response.

How could it happend?

Source: http://www.mirror.co.uk/3am/celebrity-news/jennifer-lawrence-leaked-nude-photos-4145139

Owen Williams from technology site The Next Web, who discovered the bug, said: "The Python script found on GitHub appears to have allowed a malicious user to repeatedly guess passwords on Apple's 'Find my iPhone' service without alerting the user or locking out the attacker.

"If the attacker was successful and gets a match by guessing passwords against Find my iPhone, they would be able to, in theory, use this to log into iCloud and sync the iCloud Photo Stream with another Mac or iPhone in a few minutes, again, without the attacked user's knowledge.

Source end.

So with this information we can note that Apple was wrong with they first speech. It was a vulnerability in both iCloud and "Find my Iphone" service and with this script who was found at Github it was easy to find a way in.

With brute force attack the hackers could easy find the matched passwords and with no lockout for wrong password.

Who it affect?

First of all it affected the celebrities people who had the private pictures on the Cloud service. But also their families and friends. So all the vulnerable people.

But it also affected Apple iCloud service itself. Can people really trust them after a big “bug” and leak like this? And how safe is iCloud service today?

What could be done with the vulnerability? (Code & service)

Like it seems in this case Apple had vulnerabilities in both iCloud and “Find my Iphone” service.

Via bug from Github “The Python script” you could use brute force attack on account without locking out the user.

Code: A user should never be able to use any brute force or other hacking program to a login system. (More knowledge and test)

Some sites I was reading on the information came from iCloud backups. And the data on iCloud backups is not encrypted, so this should be a thing for Apple to make.

Service: The Apple was mailed and knowledge about the problem and didn’t take it serious enough. I should say this is/was a big service mistake when people note the problem so early on.

How to avoid the problem? (Design)

I really don’t know how to avoid the problem in design way and can’t find any information about it on the web either.

Written by: Tim Emanuelsson (te222ds)