# Apple and Starbucks could have avoided being hacked if they'd taken this simple step

May 19 2015, by Bill Buchanan



Credit: AI-generated image (disclaimer)

Apple and Starbucks are two of the world's most trusted companies, but they both recently fell victim to security hacks. Both set up systems that appear to have allowed hackers to break into customers' accounts by repeatedly trying different passwords, a procedure commonly known as a "brute-force" attack. It has been reported that neither firm employed

the simple tactic of automatically locking accounts after several failed attempts to enter a password.

Last week it was reported that these tactics allowed thieves to [steal money](#) from users of Starbucks' mobile app. In 2014, an [investigation](#) around the publishing of nude photos of celebrities taken from their iCloud storage accounts, identified that intruders could access Apple's Find My iPhone app by continually trying different login details.

In order to protect against this type of attack, many sites block login after a given number of incorrect attempts. The system can then go into a permanent lock-out mode (where the user must perform a lock-out procedure, such as calling the hosting company to verify their account), or lock out for a given time (known as the hold-down time).

The size of mobile keyboards can make it tricky for users to correctly enter their password on the first try, especially as it is increasingly common for companies to require [passwords](#) with non-alphabet characters. To counter this, developers now often support many more incorrect logins than was previously normal. But many just go for an infinite number of incorrect ones without the chance of a lock-out.

In the Starbucks case, and in many others, the hackers reportedly managed to gain stolen IDs and passwords and then try to brute-force the accounts on the Starbucks mobile app, trying hundreds of logins per second.

One tactic of intruders is to try many accounts rather than concentrate on a single one and try lots of passwords for it, which is more likely to trigger security measures. There is a high likelihood that there will be some user accounts that match from the stolen credentials.

Users will also typically use the same password for multiple accounts, so

if the intruder manages to gain the password against one compromised account, they will try the same password against other login systems. Often, the same email address is used as a login for different systems, so that it can be fairly easy for an intruder to try the same ID and password that has been used on another system against a new target.
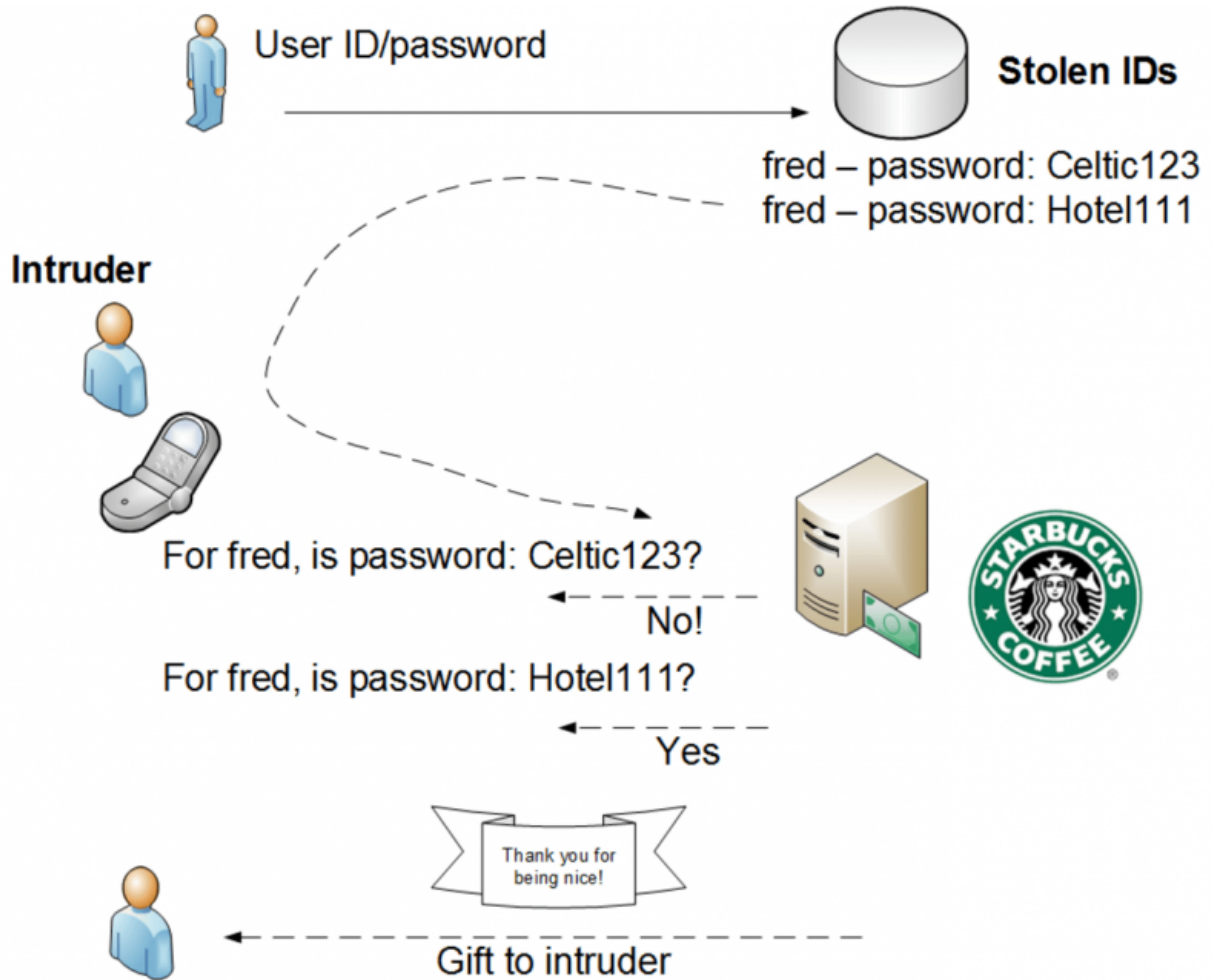


Brute force from a stolen account Author Provided

In the case of both Starbucks and Apple, the companies' authentication

systems are said to have failed to provide a locking mechanism for repeated attempts to enter usernames and passwords. This should have included:

- A lock-out on a certain number of tries
- A network detection system setup to detect multiple logins
- A task or question that can't be completed by automated bots (for example: Captcha)

## Stopping attacks at source

The problem in cybersecurity is often as simple as a developer's desire to quickly produce a solution and get it online, but forgetting to think through the processes that an adversary might take. In this case, it was a novice problem. Most system administrators would advise that a three-try system works best and will quickly knock out an automated agent. This lock can then be identified by the user and often reported by to the host company.

However, companies must also do their own penetration testing and not wait for the general public to find the weaknesses.

Starbucks has made massive advances in getting users to trust mobile payments – and this kind of sloppiness is unlikely to stop this trend. But it is the lack of due process that is the most worrying in such large firms.
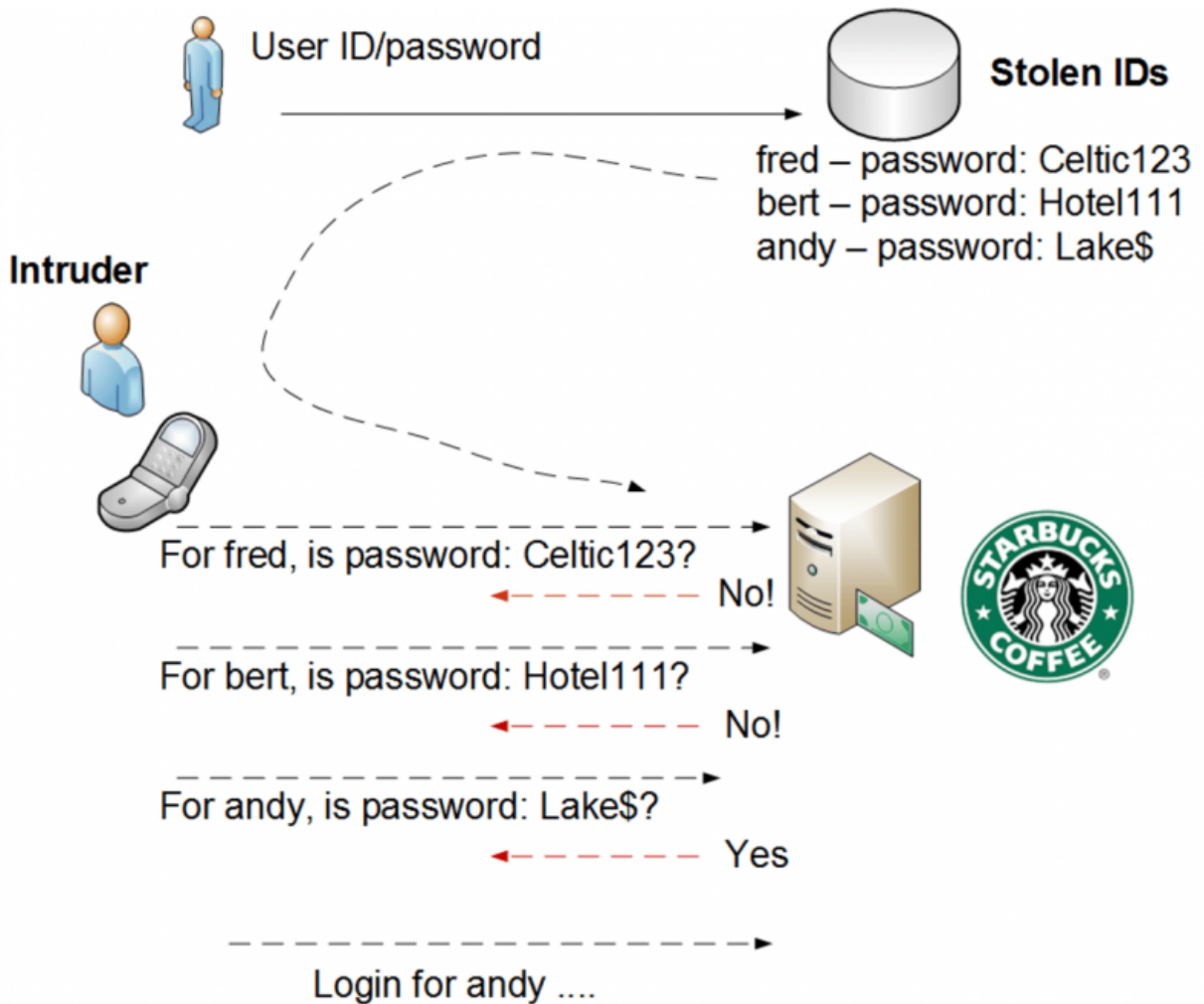
Intruder trying lots of accounts. Author Provided

These businesses perhaps have a great deal to learn from the finance sector, where companies often employ many network monitors to detect brute-force logins and stop attacks at their source.

We would never trust a bank not to implement an auto-lock-out on incorrect passwords. A simple email reset on three bad attempts seems a balanced approach. Obviously if someone compromises your main email account they can do the reset for you, but it is another hurdle in their

path. Also an intruder could trip a whole range of accounts on a network too.

Increasingly, multi-factor authentication is used, often involving location-tracking via a phone's GPS, to prove a user is who they claim to be. This means the best piece of security you have could actually be the mobile phone that goes everywhere with you (but please make sure to refresh your passwords on a regular basis).

For companies, however, there's nothing else for it but to employ managed security services with highly trained staff who can pick-off threats as they occur.

Bill Buchanan is Head, Centre for Distributed Computing, Networks and Security at Edinburgh Napier University .

*This story is published courtesy of* The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Apple and Starbucks could have avoided being hacked if they'd taken this simple step (2015, May 19) retrieved 26 June 2024 from https://phys.org/news/2015-05-apple-starbucks-hacked-theyd-simple.html