19 May 2015, 11.36am BST

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

AUTHOR

Bill Buchanan

Head, Centre for Distributed Computing, Networks and Security at Edinburgh Napier University

DISCLOSURE STATEMENT

Bill Buchanan does not work for, consult to, own shares in or receive funding from any company or organisation that would benefit from this article, and has no relevant affiliations.

Edinburgh Napier UNIVERSITY

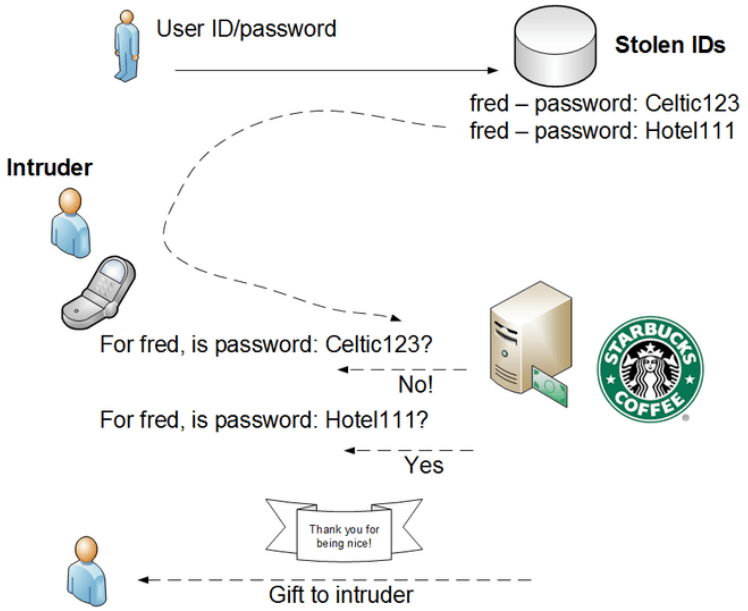
Provides funding as a Member of The Conversation UK.
napier.ac.uk/Pages/home.aspx

Hack attack. Shutterstock

Apple and Starbucks are two of the worldÕs 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 Òbrute-forceÓ 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 AppleÕs 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).

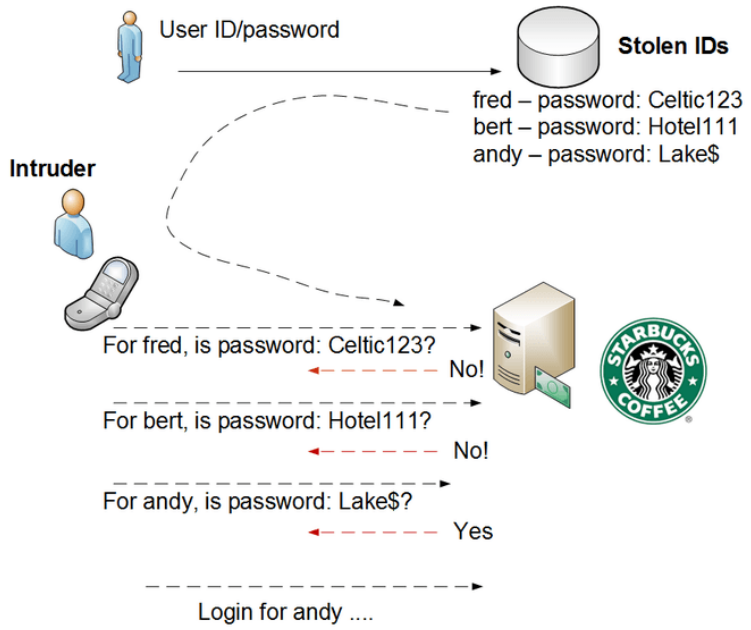


Brute force from a stolen account Author Provided

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.



Intruder trying lots of accounts Author Provided

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.

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 canÕt be completed by automated bots (for example: Captcha)

Stopping attacks at source

The problem in cybersecurity is often as simple as a developerÕs 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

Online voting is convenient, but if the results aren't verifiable it's not worth the risk

World War II is long over, but the fight against oppressive, invasive state laws continues

Big Data is useful, but we need to protect your privacy too

not wait for the general public to find the weaknesses.

Starbucks has made massive advances in getting users to trust mobile payments Ð 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.

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 phoneÕs 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, thereÕs nothing else for it but to employ managed security services with highly trained staff who can pick-off threats as they occur.