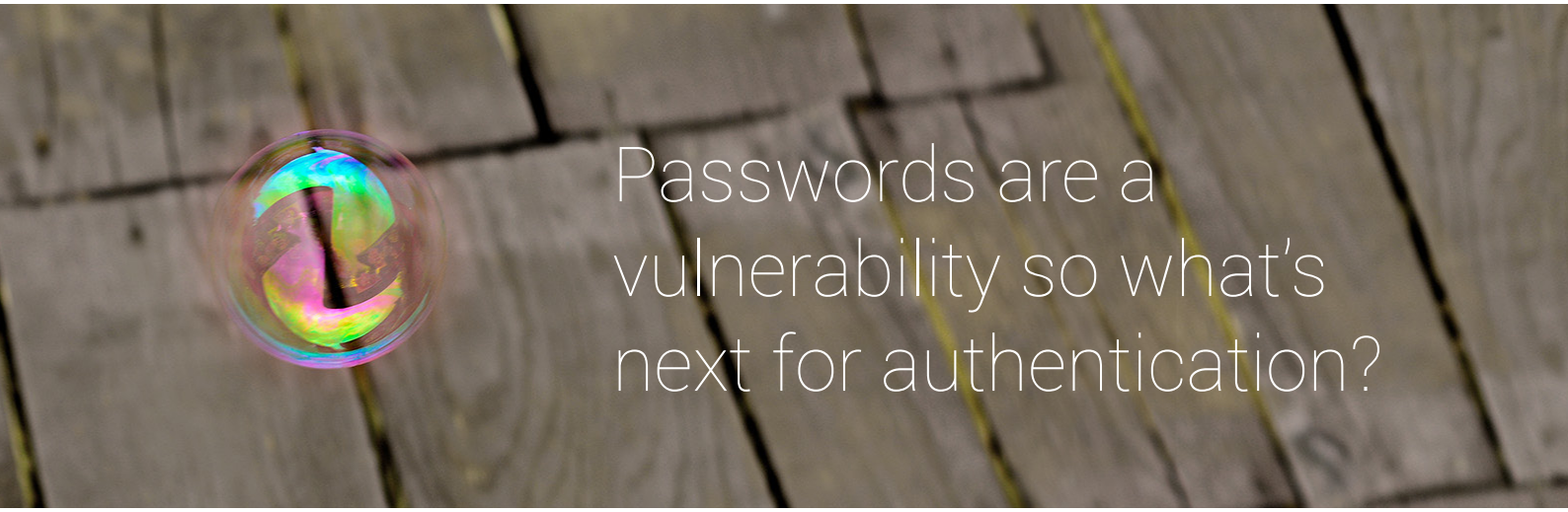
SECRET DOUBLE OCTOPUS



Passwords are a vulnerability so what's next for authentication?

Why passwords are a vulnerability?

In 2016 the second most stolen password was, ironically, "password" – right behind "123456."[1] It doesn't take much for a hacker to guess some of the most common passwords – and for the ones they can't guess, there's the option of extracting the relevant information via a phishing attack.

For years, organizations have sought to educate employees about the importance of secure passwords[2] and of resisting phishing attacks. Both efforts have failed.

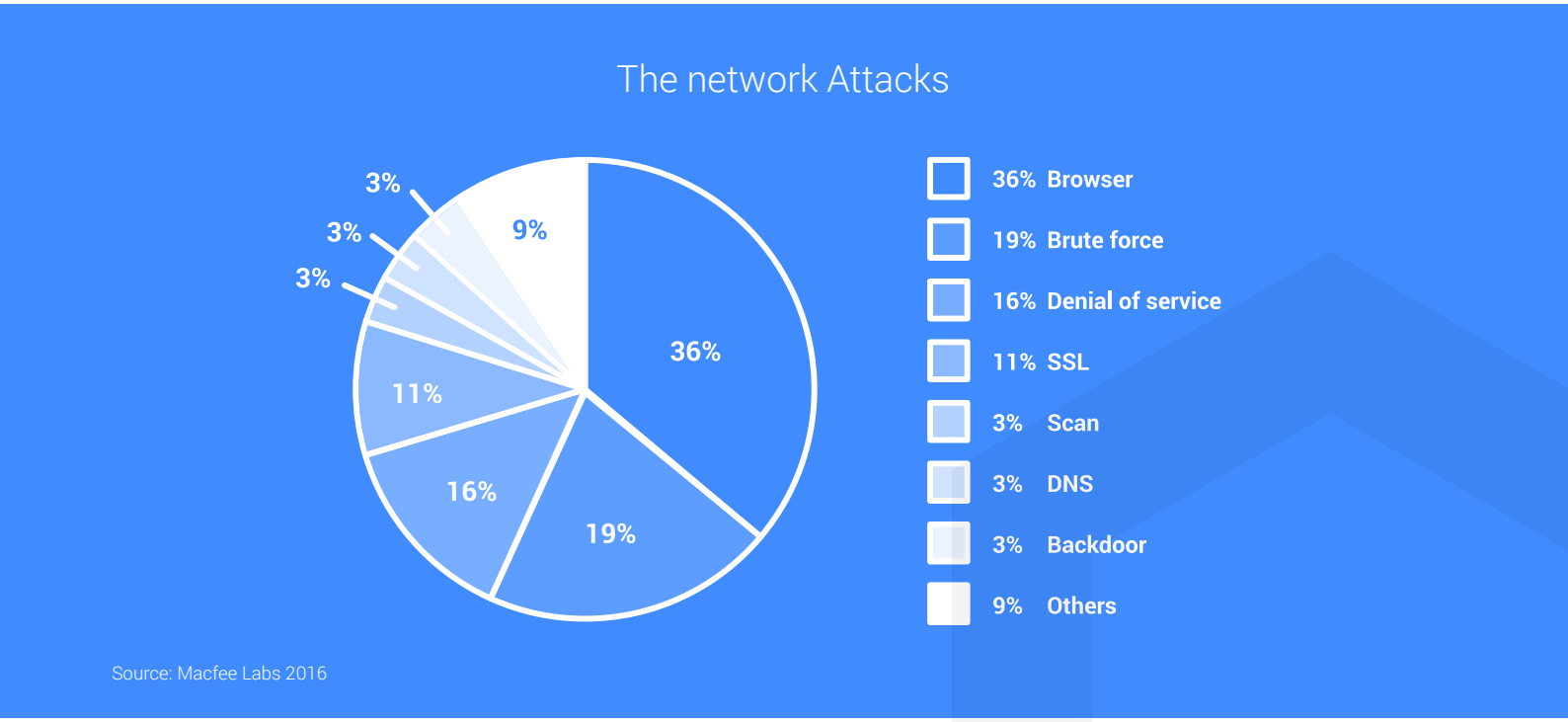
No less than 63 percent of confirmed data breaches involve leveraging weak, default or stolen passwords , while phishing and similar attacks using email were up 45 percent in the last quarter of the same year[3]. Clearly, the constant haranguing by security teams to employees to abide by best-practices for password use (regular changes, requisite complication, etc.), as well as their pleads not to click on suspicious links and attachments, aren't sinking in.

Indeed, the only way passwords can be effective, according to NIST[4], the US National Institute for Standards and Technology, is by requiring users to come up with 16 letter/digit (preferably a mix, with some capital letters and/or alphanumeric symbols thrown in) standard passwords, allowing for as many as 64 characters, instead of the 8 to 16 character range most organizations require for passwords currently.

And what about two-factor authentication? It's improvement, says NIST[4], but not if you are going to rely on SMS as the second factor; SMS is nearly as insecure as passwords, and NIST recommends staying away from it. And even if a more secure second factor is utilized (like biometrics), it still does not solve the security problem inherent in the first factor.

1 Announcing our Worst Passwords of 2016, TeamsID, March 30, 2017
2 Data Breach Investigations Report, Verison, 2016
3 BEC attacks up 45% and gaining in sophistication: Proofpoint, SC Media, March 23, 2017
4 NIST Special Publication 800-63B Digital Identity Guidelines
5 Threats Report, McAfee Labs, March 2016

A report from McAfee[5] highlights the top seven network attack types in Q4 2016. The second highest attack type (19 percent of the total) is Brute force attacks, wherein a hacker tries to decode a password or pin number through trial and error. Almost a fifth of cyber-attacks in Q4 2016 were perpetrated by brute force, which involves automated software generating guesses to try and crack the password. The guesses are taken from a dictionary that contains common passwords and combinations of letters and numbers.



Source: Macfee Labs 2016

If we look at 2015 and 2016, we see a massive increase in the number of account breaches. According to the ITRC Data Breach Reports from 2015 & 2016[6][7], there were over 170 million personal records exposed that were held by financial institutions, educational institutions, health or medical institutions, businesses, the military, or the government. These records were exposed across 780 breaches in 2015 alone.

What can be done?

One option, adopted lately by Microsoft[8] , is to shift the security burden from your memory to your mobile device with push authentication. Instead of typing in a password, which can be forgotten, phished, or compromised, users can simply respond to a push notification when they try to access their account.

How push notification works

Whenever a user types their password, they go to the app to either approve a notification or receive a verification code. With no-password sign-in, you skip the password and do all of your identity verification on your phone. This still works similar to two-step verification, which asks for a thing you know and a thing you have. The phone is still the thing you have, but now we ask for you to enter your phone's PIN or biometric key as the thing you know.

6 Data Breach Reports, Identity Theft Resource Center, 2015 EOY Report
7 Data Breach Reports, Identity Theft Resource Center, 2016 EOY Report
8 No password, phone sign in for Microsoft accounts, Microsoft, April 18, 20

Why signing in with a phone is more secure than typing a password

Today most people sign into web sites or apps using a username and password. Unfortunately, passwords are often lost, stolen, or guessed by hackers. When using a no-password sign-in app, it generates a key on your phone that can unlock your account. This key is protected with the PIN or biometric that the user already uses on their phone. When a user signs in with their phone, this key is used to prove one's identity securely with two factors – the phone itself, and your ability to unlock it.

Strong authentication is required in password-free environments

Octopus authenticator uses secret sharing for multi-route protection. If a single secret is stolen from the device – or captured in motion – there's no compromise to security. The platform is resilient.

This is the industry's first comprehensive platform to replace passwords and keys with multi-shield protection that does not depend on any single protection mechanism – and uses algorithms classified as unbreakable within the field of mathematics information-theory.

Features include:

A tough authenticator app – secure enough to reliably turn the phone from a second to a first factor of authentication.

Complete protection of user lifecycle from physical enrollment through to revocation.

An open platform upon which all authentication solutions converge, including SAML, Radius, OpenID, FIDO, Active Directory, etc.

Secret Double Octopus has developed the world's only keyless multi-layer authentication technology to protect identity and data across cloud, mobile and IoT environments. Based on Secret Sharing algorithms, originally developed to protect nuclear launch codes, Secret Double Octopus' technology prevents cyber attackers from accessing enough critical information to be useful for attacks, eliminating brute force, man-in-the-middle, PKI manipulation, key theft and certificate authority weaknesses.

SECRET DOUBLE OCTOPUS

For more information, contact us:
contact@doubleoctopus.com
www.doubleoctopus.com