Separating people from passwords

OSIRIUM REPORTS

It seems the message about using 'strong' passwords is getting through. According to the Verizon DBIR reports, the instances of brute forcing are reducing year on year (3% in 2014). As always, if we fix one weakness the attackers shift their focus to the next.

Right now we're seeing how rigorous password policies are creating the exact opposite of their intended outcome. This is due to two factors: First, considering policy, humans need to remember passwords, so they are heavily biased towards patterns. A typical policy would state that a password needs to be more than 12 characters, contain upper and lowercase, some digits and a punctuation mark. Furthermore, our policy states that the users need to change their passwords every 30 days.

Humans tend to follow instructions serially. The first thing they do is to think of a long word, for example 'Manchester' that has upper and lower case and takes up 10 characters. 'ManchesterFC' would be a useful alternative taking up 12. For the digits, most users would start with the year, so 'ManchesterFC2017' works. For the punctuation character '.' is the most common choice, so we are at 'ManchesterFC2017.' After 30 days our user is faced with forced password change. Typically the user will choose 'ManchesterFC201710.' where the last two digits are the current month.

Now we have a solid 18 character password, beyond

cont. overleaf

Osirium is a UK software development team that has pioneered the concept of a virtual air gap for privileged account access. The team have delivered a virtual appliance that can recognise an incoming identity, create a connection to a system, device or application, perform single sign-on and enterprise class password lifecycle management, and then hand the pre-prepared session back to the incoming request ready for system management. The session can be recorded, subject to time windows and device group separation. We have delivered millions of privileged tasks and sessions for many of our blue chip clients. Osirium currently has four patents pending.

> "More accountability creates a greater deterrent"

the reach of the 14 character LM hash brute force, so all is good? Well, no it isn't. Football clubs are very popular choices for passwords, 'Manchester', 'Liverpool', 'Chelsea', 'Arsenal', 'Tottenham' quickly covers the top five. Year, month and '.' are commonly used. Therefore the combinations of all these are very easy to compute. However, there are still too many to directly brute force.

This is where the second element comes in. If we were to take all the common combinations of the above we could set a user's password and record the resulting hash. The hash is the result of passing the password through a complex one way algorithm. Now imagine that we've done this 131 billion times. If a hacker were to obtain a user's password hash they'd have a great chance of recovering the original password.

It is worth a moment to reflect on your password policy. How many of your users would have chosen one of those 131 billion passwords? Given this situation, it becomes difficult to prove the identity of who did what. This is of course amplified where several users are sharing a password to a particular device account.

So what's the solution? It's easy to say 'one cannot trust users with passwords', however, the vast majority of your users will use online banking. You can be sure that where their own money is concerned they chose strong passwords. The banking systems do not ask you to change your passwords every 30 days. Historically, banking systems have proven to be secure. Online banking authentication systems use a second factor of authentication. The key point here is that banking systems seek to prove identity. Identity is the real key to security. In the corporate world we really need to know who did what, where and when.