CACM'18-Florencio-Pushing on string: the "don't care" region of password strength

亮点：①提出攻击饱和点和在线-离线的鸿沟

②通过举RSA和NSA的例子说明企业中一个帐户泄漏带来的危害

问题：①可考虑从用户的角度评测口令的强度，涉及口令管理方式PM等

②当涉及到猜测时，管理员应采用的措施需改变，黑名单可能效果减小

③nudge用户提升口令强度仍是有效的，应用户和server共同努力抵抗猜测

④可评估blacklist的有效性的影响因素。

▲研究背景

企业，政府或大学的管理员需采用合理的策略保护用户的帐户，防止对口令的攻击。

目前没有准则提供实际的指导，例如评估口令强度的方法和口令策略。

许多实际的方法或策略是不合理的(例如要求用户选择尽可能强的口令)。

⇒本文通过分析指出现有方法的局限性，并指出部分增强口令强度的方法是无用的，给出部分改进措施 ↳分析现有抵抗口令猜测攻击策略的有效性。

▲研究问题

本文主要从管理员的角度考虑，旨在讨论以下几个问题：

1>通过分析及引用文献，指出两个抵御口令猜测攻击的"don't care"区域，在这两个区域提高口令强度是无意义的，类似于pushing on string，两个区域分别是：

①the compromise saturation point ②the online-offline chasm

2>根据上述分析，指出管理员可以从哪些方面进行改进以及相应的措施。

▲研究问题1>的子问题 compromise saturation point.

1>问题来源：当系统帐户出现泄漏时，管理员需确定帐户泄漏的方式，例如是否通过猜测攻击以及口令文件是否被敌手获取？若管理员根据泄漏帐户的数目决定是否重置所有帐户，这个数目应为多少？

2>分析过程：α代表攻击者控制的凭证的比例，管理员何时认为网络已被破坏取决于网络本质

①对于1个企业来说，泄漏1个帐户就可能能够访问许多服务具有滚雪球效应。

②当攻击者攻破一定比例的帐户时就可以访问所有的资源，再攻破的帐户对攻击者的收益的提升可忽略不记。(此处指出攻击者的目标可能只是在网络世界中立足foothold)

认为达到饱和点 α_{sat}。在攻破部分帐户后，攻击者有许多方法攻击其它帐户，列举RSA和NSA的实例。

③企业环境通常有最低的α_{sat}，但其它环境如银行一定比例的泄漏将影响信誉度。

④从系统的角度看，在超过α_{sat}的部分中，即使口令强度高也不会有什么效果。

口令强度(抗猜测数目)更多是一种用于防止攻击者访问网络资源的工具。

管理员需从系统的整体角度考虑，而从个人角度，口令强度高仍有许多益处。

3>阶段性结论：对于系统管理员和攻击者来说，存在一个攻破比例的饱和点，在此之外的攻击对系统整体无明显效果。

▲研究问题1>的子问题：online-offline chasm

1>问题来源：探究抵抗在线猜测和离线猜测攻击的不同，以及对现实防御的方法。

2>分析过程：在线猜测总是可行的，而离线猜测必须获取加盐哈希的口令文件。

T_0为期待在线猜测次数的最大值，T_1为未知真实离线次数的最小值。

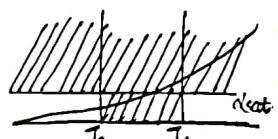
T_1通常应远远大于T_0。

3>阶段性结论：猜测攻击只有offline和online，中间无连续，故出现了online-offline chasm，导致处于之间don't care region的口令 too much and not enough.

▲研究问题1>的总结

1>以上两个部分组成的区域为don't care region，即使付出努力提高口令强度也无用。

2>在阴影区域的内容是口令分布无法更改的，口令分布只能影响非阴影的部分，



3>α_{sat} T_0，T_1可以改变区域的大小，而真正受口令强度影响的区域与口令分布有关，管理员可尝试缩小don't care region的大小。

▲研究问题2>的子问题：管理员可进行的优化

1>问题：理想情况，泄漏帐户的数目在T_1处低于α_{sat}，最好更低。但实际中用户口令离此目标很远，若选$\alpha=0.1$，$T_1=10^{14}$，则几乎无法抵抗离线猜测攻击？管理员应采用什么措施。

2>分析过程：stronger passwords are always better 不一定是对的，即较强的口令可以使曲线下降一些，但若发生在"don't care region"则无意义。

→一个合理的目标，以合理的代价最大化抗猜测的能力，尽可能使T_0和T_1的取值小。

▲研究问题2>的子问题：优化的方法。(α_{sat}，T_0，T_1以及分布的形状)

1>α_{sat}很大程度上由网络拓扑决定，且在给定的环境中难以控制或改变，认为使用基本原则

2>改善T_0：限制在线猜测的方法包括throttling mechanism (rate-limiting)，以及IP address blacklisting。其中DoS攻击可通过whitelist来处理。

3>改善T_1：技术的进步有助于攻击者，且硬件是攻击者操作的，因此可以通过slow hash让一次计算的消耗更多，例如hash iteration；另外还有GPU-unfriendly的设计。

需调整iteration以防给用户带来过多负担。

4>消除离线攻击：①防止口令文件泄漏，利用HSM中的key计算加盐哈希的MAC存储用验证

②限制认证server与hash server的带宽，限制离线猜测的速率。

5>改善口令分布(使曲线下降一些)。

问题：①所有的建议都需要用户听从才能奏效。②无法对某个部分改善，无法保证付出是有效的

影响用户选择的通用估效法。

①Password blacklisting：显式屏蔽常见的口令，阻止不好的选择，且只对不好选择的用户影响

②Composition Policies：很少真正奏效；目的是为一个更具防御性的口令分布，实际上是否改善对管理员不可见。