CCS'17-Pearman-Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat

优点：① 从用户实际使用角度研究口令重用和口令行为

② 比起Wash'16的研究，增加了口令音附重用的讨论

③ 指出Wash'16研究使用熵作为口令强度评估方案的不妥

问题：① 可进一步研究PM真实对口令强度和重用的影响

② 可以探究不同浏览器用户输口令行为的区别与原因

③ 可通过对用户编号用于后续研究后采访，研究重用行为的原因

▲研究背景

1> 之前针对于口令安全(口令重用、口令行为)的研究更多集中于用户自己报告的研究(用户调研)，间接评估的研究或只关注用户的一个口令(泄漏的数据集，或为研究创建的口令)

⇒ 查看一个用户日常在线活动中使用的口令，以及使用的范围，对理解口令的安全属性是必要的

例如：用户重用口令的程度、重用口令的数目，用户是否区分高价值、低价值帐户，以及PM对口令强度的作用

2> 目前很少有研究定量、实际考察地研究全部或大多数的口令.

一个相关研究：Wash SOUPS'16的研究(6周134名参与者)，研究了在不同网站重用口令的情况，且发现输入更频繁和更复杂的口令是重用更频繁的，未讨论的：未检查音附重用的情况.

另外Wash研究以熵作为口令强度评估，不够严谨.

▲研究问题

1> 通过全面、长期、实地考察、收及收行为，利用Security Behavior Observatory (SBO)对用户行为做长期纵向研究，具体讲：我们在平均1件天内仔细检查了154名参与者的口令使用信息和口令哈希，另外收集了计算机使用信息，包含PM、安全隐私扩展、恶意软件及软件更新等.

2> 具体探索的问题.

① 用户在网站间完全/部附重用口令的情况？

② 口令的特定属性与重用是否有关？

③ 强口令和弱口令与重用是否有关？

④ 不同类型帐户的口令重用程度如何？

⑤ 其它安全行为是否与口令强度重用有关？

收方法

①完全重用：查看口令哈希

②部附重用：长度大于3的子串的哈希

③强度：使用开源密码强神经网络口令猜测探索

④其它信息：长度、熵值、域、字符类型.

▲数据收集

1> 使用SBO收集的数据对Windows计算机用户的安全行为做纵向研究.

在Chrome、Firefox和Vivaldi浏览器更新SBO扩展，收集口令哈希、口令长度、字符种类和长度多于3个字符的子串的哈希值，口令强度.

共收集154名参与者的数据.

2> 口令自动填充的数据只收集了7周的数据.

3> 网站域和类型通过code方式区分部分仅为同一域的变体)，最终分析了154个用户在207个不同域上的口令集.

4> 第三方数据：通过Google Safe Browsing API收集的黑名单和VirusTotal检测恶意软件 (25%以上程序标记)

▲结果分析

1> 口令特征(包括口令行为和口令重用

①观察到154名参与者提交给207个不同域名的476个口令，若一个参与者只计算唯一的口令，有1522个

②每天提交1个口令1.4次，平均口令长度9.2个字符，字符种类2.7种，平均强度抗10^{12}次猜测

③有一半口令为购物或教育网站创建.

2> 重用特征.

①参与者平均使用9.88个口令，提交到26.3个不同的域.

②唯一的口令共1678个，511(32%)直接重用，833(53%)部分重用，951个(60%)存在某种重用

总体看，67%完全重用，63%部分重用，79%重用口令.

③部附重用口令中，有603个不同的共享子串，长度为4~20个字符，603个子串在833个口令中出现1704次.

大部附部分重用口令只涉及少数几个字符的改动，1个字符最常见

682(61%)用作前缀，530(52%)用作后缀.

④ 2.64%在同类网站重用，85.08%在金融帐网站的口令重用，这些口令95.5%被其它类型网站重用

3> 口令重用的类型(用户超50%属于的口令)

①Unique Password Creators：101(65%)人；帐户数少，参与在线活动少.

②Partial Password Re-users：53(32%)人；口令数少，活跃天数少

③Exact Password Re-users：17(11%)人；活跃时间差别很大；平均维护16个重用口令，平均用于9个域 (分别提此类的重用)

④Exact-and-partial Password Re-users：94(61%)人，非常活跃，平均2千帐户，33个口令用于74个域

⑤Mixed Strategy Users：28(18%)人，较活跃，平均22个不同在线帐户，

4> 口令强度分布

采用kolmogorov-Smirnov test计算两个用户口令强度分布之差，分为4类.

5> 有关口令重用的结论

① 口令存在数字更可能重用(12.20倍)，有特殊字符也更可能重用(2.69倍)

② 购物、工作相关帐户的口令更可能重用(3倍)

③ 猜测口令数目增加一个数量级，重用几率降低9%(强度与重用几率负相关)

④ 带数字的口令会在更多域重用，较长、更强、输入更频繁、有大写字母会在较少域重用

6> 与其它安全行为的关系

① 用户每天浏览网页的数目越多，重用会增多，使用PM、其它安全插件无明显作用关系

② 使用PM、安全插件等与口令强度无明显关系