Offensive AUP-RPE 均来自比 Defensive AUP-RPE 的密码强度更低的分布,可能导致最终计算得到的图形密码出现概率偏离于实际率.因此,当满足相同分布的训练集容量逐渐增大时,相同的猜测次数将达到更高的攻击率,也即同一性质的训练集样本容量越大,攻击者获得的信息就越多,也就越有利于提高攻击效率.

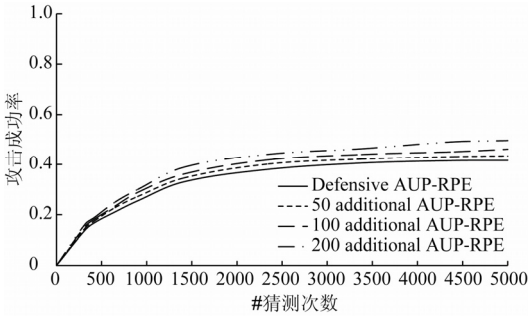


Fig.11 Impact of training set upon attack rate and attack frequency

图 11 训练集对攻击次数与攻击率的影响

综合以上分析,AUP-RPE 在图形密码设置所需时间、认证所需时间及成功率上都与 AUP 十分相近,在安全性分析中更具有远远大于 AUP-RPE 的密码熵值.这表明新方案在保持了与原方案几乎一致的可用性的基础上,极大地提高了图形密码的安全性,充分说明了 AUP-RPE 的良好实用性.

## 4 讨论与结论

AUP-RPE 是进行较大规模调查,基于用户数据建模并以熵值形式计算实际应用中密码强度的安卓图形解锁改进方案.它在认证阶段是普通的 4×4 点阵,在密码设置阶段,剔除 4×4 点阵四角处的点,剩余的 12 个点在每次设置密码时随机剔除其中两点,即每次参与密码设置的仅有 10 个点,这既保证了密码空间大于原方案,又在一定程度上规避了用户原具有安全隐患的使用习惯,避免了 AUP 中用户使用四角处点过多或过少的问题,而且 AUP-RPE 方案在攻击率达到 20%后,熵值明显大于 AUP,攻击者在攻击 AUP-RPE 时达到相同攻击成功率时通常比 AUP 需要更多的攻击次数,因而,AUP-RPE 的攻击难度更高,具有比 AUP 更高、更强的安全性.

AUP-RPE 着重于通过改变图形密码设置界面的布局,使用户规避具有安全隐患的使用习惯,所设置出的密码在密码空间上分布更均匀,使攻击者难以利用用户的使用习惯来加快字典攻击和暴力破解.因此,攻击者对某一系统用户密码了解得越少,实行字典攻击或暴力破解的难度越高,从而达到提高图形密码的熵值与安全性的目标.如果将 AUP-RPE 的大小再扩展到 5×5,6×6,那么,尽管密码空间越来越大,但设计出的图形也越来越多,密码强度也将随之增大,但考虑到手机屏幕的大小以及用户难以记住复杂的密码,如何在提高安全性的同时兼顾可用性又是一个值得探究的问题.AUP-RPE 在提高安全性的同时兼顾了可用性,具有良好的实用性.

**References**:

[1] Spafford EH. Opus: Preventing weak password choices. Computers & Security, 1992,11(3):273−278. [doi: 10.1016/0167-4048(92)90207-8]

[2] Hu XX, Zhang ZF, Liu WF. Universal composable password authenticated key exchange protocol in the standard model. Ruan Jian Xue Bao/Journal of Software, 2011,22(11):2820−2832 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3910.htm [doi: 10.3724/SP.J.1001.2011.03910]

[3] Standing L, Conezio J, Haber RN. Perception and memory for pictures: Single-Trial learning of 2500 visual stimuli. Psychonomic Science, 1970,19(2):73−74. [doi: 10.3758/BF03337426]

[4] Biddle R, Chiasson S, Van Oorschot PC. Graphical passwords: Learning from the first twelve years. ACM Computing Surveys, 2012,44(4):No.19. [doi: 10.1145/2333112.2333114]

[5] Qing SH. Research progress on Android security. Ruan Jian Xue Bao/Journal of Software, 2016,27(1):45−71 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4914.htm [doi: 10.13328/j.cnki.jos.004914]

[6] Passfaces Corporation. Passfaces. http://www.passfaces.com

[7] Brostoff S, Sasse MA. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In: People and Computers XIV—Usability or Else! London: Springer-Verlag, 2000. 405-424. [doi: 10.1007/978-1-4471-0515-2_27]

[8] Davis D, Monrose F, Reiter MK. On user choice in graphical password schemes. In: Proc. of the 13th Conf. on USENIX Security Symp., Vol.13. USENIX Association, 2004.

[9] Chiasson S, van Oorschot PC, Biddle R. Graphical Password Authentication Using Cued Click Points. Berlin, Heidelberg: Springer-Verlag, 2007. [doi: 10.1007/978-3-540-74835-9_24]

[10] Jermyn I, Mayer AJ, Monrose F, Reiter MK, Rubin AD. The design and analysis of graphical passwords. In: Proc. of the Usenix Security. 1999.

[11] Tao H, Adams C. Pass-Go: A proposal to improve the usability of graphical passwords. Int'l Journal of Network Security, 2008, 7(2):273−292.

[12] Tafasa. Patternlock. 2010. http://www.tafasa.com/patternlock.html

[13] Uellenbeck S, Dürmuth M, Wolf C, Holz T. Quantifying the security of graphical passwords: The case of android unlock patterns. In: Proc. of the 2013 ACM SIGSAC Conf. on Computer & Communications Security. ACM, 2013. 161−172. [doi: 10.1145/2508859.2516700]

[14] Castelluccia C, Dürmuth M, Perito D. Adaptive password-strength meters from Markov models. In: Proc. of the NDSS. 2012.

[15] Cachin C. Entropy measures and unconditional security in cryptography [Ph.D. Thesis]. Swiss Federal Institute of Technology Zürich, 1997.

[16] Massey JL. Guessing and entropy. In: Proc. of the IEEE Int'l Symp. on Information Theory. IEEE, 1994. No.204. [doi: 10.1109/ISIT.1994.394764]

[17] Bonneau J. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE, 2012. 538−552. [doi: 10.1109/SP.2012.49]

**附中文参考文献**:

[2] 胡学先,张振峰,刘文芬.标准模型下通用可组合的口令认证密钥交换协议.软件学报,2011,22(11):2820−2832. http://www.jos.org.cn/1000-9825/3910.htm [doi: 10.3724/SP.J.1001.2011.03910]

[5] 卿斯汉.Android 安全研究进展.软件学报,2016,27(1):45−71. http://www.jos.org.cn/1000-9825/4914.htm [doi: 10.13328/j.cnki.jos.004914]

**熊思纯**(1992－),女,湖南娄底人,硕士生,主要研究领域为网络与信息安全.

**马建峰**(1963－),男,博士,教授,博士生导师,CCF 会士,主要研究领域为网络与信息安全,密码学.

**杨超**(1979－),男,博士,副教授,CCF 专业会员,主要研究领域为网络与信息安全.

**张俊伟**(1982－),男,博士,副教授,CCF 专业会员,主要研究领域为密码学,网络安全.