International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359

Research Article | **February 2013**

The Security of Customer-Chosen Banking PINs

RAJESHWARI SANGOLLI*
Dept of Computer Applications
CMJ University
Bangalore, India

Dr. G MAHADEVAN
Dept of Computer Applications
AMC Engineering College
Bangalore, India

BADRI H.S
Dept of Computer Applications
Presidency College
Bangalore, India

Abstract:

Here the paper provides the first published estimates of the difficulty of guessing a human-chosen 4-digit PIN. The paper begins with two large sets of 4-digit sequences chosen outside banking for online passwords and smartphone unlock-codes and uses a regression model to identify a small number of dominant factors influencing user choice. Using this model and a survey of over 1,100 banking customers, are estimated the distribution of banking PINs as well as the frequency of security-relevant behavior such as sharing and reusing PINs. Here the paper finds that guessing PINs based on the victims' birthday, which nearly all users carry documentation of, will enable a competent thief to gain use of an ATM card once for every 11{ 18 stolen wallets, depending on whether banks prohibit weak PINs such as 1234. The lesson for cardholders is to never use one's date of birth as a PIN. The lesson for card-issuing banks is to implement a denied PIN list, which several large banks still fail to do. However, blacklists cannot effectively mitigate guessing given a known birth date, suggesting banks should move away from customer-chosen banking PINs in the long term

Keywords: Guessing, PIN, Online Passwords, ATM Card, Birth Date

I. INTRODUCTION

Personal Identification Numbers, or PINs, authenticate trillions of pounds in payment card transactions annually and are entrenched by billions of pounds worth of infrastructure and decades of customer experience. In addition to their banking role, 4-digit PINs have proliferated in a variety of other security applications where the lack of a full keypad prevents the use of textual passwords such as electronic door locks, smartphone unlock codes and voice mail access codes. In this work, provide the first extensive investigation of the security implications of human selection and management of PINs.

A STANDARDS AND PRACTICES IN PIN SELECTION

Published standards on PIN security provide very brief treatment of human factors. The EMV standard [1] requires support for PINs of 4{12 digits, in line with earlier Visa standards, but makes no mention of PIN selection. Separately, Visa maintains Issuer PIN Security Guidelines with several recommendations for users specifically that they never write down their PIN or use it for any other purpose. The document is neutral between issuer-assigned PINs or customer chosen PINs, providing one sentence about PIN selection [2]: “Select a PIN that cannot be easily guessed (i.e., do not use birth date, partial account numbers, sequential numbers like 1234, or repeated values such as 1111)." ISO 9564 [3] covers PIN security and is largely similar to Visa's guidelines, mostly focusing on PIN transmission and storage. It adds a recommendation against “historically significant dates," and PINs chosen as words on the keypad. Neither standard mentions using a “denied PIN list" to blacklist weak PINs, as is recommended in standards for text passwords [8]. As a result of the vague standards, PIN requirements vary significantly but the minimal 4-digit length predominates. PIN length appears integrated into cultural norms: there is rarely variation within competitive regions, while in some locales most card issuers require PINs longer than 4 digits. Similarly, most banks allow user-chosen PINs, with a few regional exceptions such as Germany. Because denied PIN lists aren't publicly advertised, evaluated several banking cards by requesting the PIN 1234.4 In the UK, this was denied by Barclays, HSBC and NatWest but allowed by Lloyds TSB and The Co-op Bank. In the USA, this was denied by Citibank and allowed by Bank of America, HSBC and Wells Fargo. The paper only identified card-specific denied PIN lists; and found no ATM implementing local restrictions. At one bank the study tested, Chase in the USA, self-service PIN changes are not possible and changes must be made in-person. Banks's policies may vary with time or location (note the inconsistency of HSBC between the USA and UK), but denied PIN lists are clearly not universal.

B ACADEMIC RESEARCH

Research on authentication systems involving human-chosen secrets consistently finds that people favor a small number of popular (and predictable) choices. Strong bias has been analyzed for textual passwords starting with Morris and Thompson in 1979 [15] and confirmed in many studies since [19]. Similar bias been identified in responses to personal knowledge questions [6] and in graphical password schemes [20]. Despite their wide deployment, there exists no academic research about human selection of PINs. The best-known research on PINs, such as Murdoch et al.'s \no-PIN attack" [16], has identified technical flaws in the handling and verification of PINs but not addressed PIN guessing. Kuhn identified in 1997 that the use of unbalanced decimalization tables introduced a bias into the distribution of PIN offsets which could be exploited by an attacker to improve PIN guessing [13]. Bond and Zielinski developed further

decimalization-based attacks in 2003 [5]. Both attacks can be improved with knowledge of human tendencies in PIN selection.

II. SURVEYING BANKING PIN CHOICES

The low frequency of many PINs in the RockYou dataset means a survey of hundreds of thousands of users would be needed to observe all PINs. Additionally, ensuring that users feel comfortable disclosing their PIN in a research survey is difficult. The study aims to address both problems by asking users only if their PINs fall into the generic classes captured by the regression model. The study deployed the survey online using the Amazon Mechanical Turk platform, a crowd-sourcing marketplace for short tasks. The study was advertised as a "Short research survey about banking security" intended to take five minutes. Further, deliberately displayed the University of CMJ as the responsible body to create a trust effect. To reduce the risk of re-identification, no demographic or contact information was collected. The design was approved by the responsible ethics committee at the University of CMJ. The survey was piloted on 20 respondents and then administered to 1,351 respondents. 1,337 responses were kept after discarding inconsistent ones.8 Respondents were rewarded between US $0.10{0.44 including bonuses for complete submission and thoughtful feedback. Repeated participation was prohibited.

A PIN USAGE CHARACTERISTICS

The 1,177 respondents with a numeric banking PIN were asked a series of questions about their PIN usage. A surprising number (about 19%) of users rarely or never use their PIN, relying on cash or cheques and in-person interaction with bank tellers. Several participants reported in feedback that they distrust ATM security to the point that they don't even know their own PINs. Many others stated that they prefer signature verification to typing in their PIN. However, 41% of participants indicated that PINs were their primary authentication method for in-store payments, with another 16% using PINs or signatures equally often. Of these users, nearly all (93%) used their PINs on at least a weekly basis. Over half of users (53%) reported sharing their PIN with another person, though this was almost exclusively a spouse, partner, or family member. This is consistent with a 2007 study which found that about half of online banking users share their passwords with a family member [18]. Of the 40% of users with more than one payment card, over a third (34%) reported using the same PIN for all cards. This rate is lower than that for online passwords, where the average password is reused across six different sites [11]. The rate of forgotten PINs was high, at 16%, although this is again broadly consistent with estimates for online passwords, where about 5% of users forget their passwords every 3 months at large websites [11]. Finally, over a third (34%) of users re-purpose their banking PIN in another authentication system. Of these, the most common were voicemail codes (21%) and Internet passwords (15%).

B PIN SELECTION STRATEGIES

The study invited the 1,108 respondents with a PIN of exactly 4 digits to identify their PIN selection method. This was the most sensitive part of the survey, and users were able to not provide this information without penalty, removing a further 27% of respondents and leaving us with 805 responses from which to estimate PIN strength. The study presented users with detailed descriptions and examples for each of the selection strategies identified in the regression model. Users were also able to provide free-form feedback on how they chose their PIN. The largest difference between the survey results and the regression models was a huge increase in the number of random and pseudo-random PINs: almost 64% of respondents in our survey, compared to 23% and 27% estimated for our example data sets. Of these users, 63% reported that they either used the PIN initially assigned by their bank or a PIN assigned by a previous bank.9 Another 21% reported the use of random digits from another number assigned to them, usually either a phone number or an ID number from the government, an employer, or a university (about 30% for each source).Of users with non-random PINs, dates were by far the largest category, representing about 23% of users (comparable to the iPhone data and about half the rate of the RockYou data). The choice of date formats was similar to the other datasets with the exception of 4-digit years, which were less common in our survey. We also asked users about the significance of the dates in their PINs: 29% used their own birth date, 26% the birth date of a partner or family member, and 25% an important life event like an anniversary or graduation. Finally, about 9% of users chose a pattern on the keypad, and 5% a numeric pattern such as repeated or sequential digits. The study sample size was insufficient to provide an accurate breakdown of users within these categories

III. HUMAN CHOICE OF OTHER 4-DIGIT SEQUENCES

RockYou The leak of 32 million textual passwords from the social gaming website RockYou in 2009 has proved invaluable for password research [21]. The study extracted all consecutive sequences of exactly 4 digits from the RockYou passwords. There were 1,778,095 such sequences; all possible 4-digit sequences occurred. 1234 was the most common with 66,193 occurrences (3.7%), while 8439 was the least common with 10 occurrences (0.0006%). Though these sequences occurred as part of longer strings, a manual inspection of 100 random passwords which include a 4-digit sequence identified only 3 with an obvious connection between the digits and the text (feb1687, classof2007 and 2003chevy), suggesting that digits and text are often semantically independent. Users also show a particular affinity for 4-digit sequences, using them more significantly more often than 3-digit sequences (1,599,959) or 5-digit sequences

(497,791). iPhone. The study second dataset was published (in aggregate form) in June 2011 by Daniel Amitay, an iPhone developer who deployed a screen locking mechanism which requires entering a 4-digit sequence to unlock. This dataset was much smaller, with 204,508 PINs. It doesn't support reliable estimates of low-frequency PINs, as 46 possible PINs weren't observed at all. 1234 was again the most common, representing 4.3% of all PINs. The screen unlock codes were entered using a square number pad very similar to standard PIN-entry pads. Geometric patterns, such as PINs consisting of digits which are adjacent on the keypad were far more common than in the RockYou sequences.

IV. APPROXIMATING BANKING PIN STRENGTH

Using the survey data and regression model, estimated the distribution of banking PINs for the survey population. This was straightforward for random PINs and PINs based on dates. Within the other two categories, used the sub-distribution from the iPhone dataset due to lack of sufficient sample size. Banking PINs appear considerably more vulnerable against marginal guessing attacks. An attacker with 3 guesses will have a $\lambda 3 = 1.4\%$ chance of success and an attacker with 6 guesses a $\lambda 6 = 1.9\%$ chance of success, equivalent to $\lambda 6 = 8{:}3$ bits of security (2.5 dits). This is significantly better than the estimates based on the RockYou or iPhone distributions (Table 1), for which $\lambda 6 > 10\%$. The optimal guessing order is 1234 followed by 1990{1986.

A KNOWN BIRTH DATE GUESSING

Given the large number of users who base their PIN on their birth date (nearly 7% in total, or 29% of those using some type of date), the study evaluated the success of an attacker who can leverage a known birth date, for example if a card is stolen in a wallet along with an identification card. The exact effects vary slightly with the actual birth date: if variants of the date also correspond to common PINs such as 1212, the attacker's success rate will be higher. The study calculated guessing probabilities for all dates from 1960{1990 and report results for the median date of June 3, 1983. In this scenario, the attacker's optimal strategy shifts to guessing, in order, 1983, 6383, 0306, 0603, 1234, and 0683.

B EXPTECTED VALUE OF A STOLEN WALLET

The study calculated the guessing probability of a thief with multiple stolen cards, for example from an entire wallet or purse. Though most of the surveyed users own only one card with a PIN, on expectation stealing a wallet instead of a single card raises a thief's guessing chances by over a third. The survey results suggest that virtually all payment card users (99%) carry documentation of their birth date alongside their card. Thus, conclude that a competent thief will gain use of a payment card once every 11{18 stolen wallets, depending on the proportion of banks using a denied PIN list.

V. CONCLUSION

The widespread security role assigned to 4-digit PINs is a historical accident which has received surprisingly little scrutiny. While complete analysis is impossible without access to a huge list of real banking PINs, it appears that user choice of banking PINs is not as bad as with other secrets like passwords. User management of PINs is also comparatively good, with lower rates of reuse and sharing and many users reporting serious thought about PIN security. However, the skew introduced by user choice may make manual guessing by thieves worth while|a lost or stolen wallet will be vulnerable up to 8.9% of the time in the absence of denied PIN lists, with birthday-based guessing the most effective strategy. Blacklisting appears effective only if a thief doesn't know the user's date of birth (or users stop using this to choose their PIN). The study advise users not to use PINs based on a date of birth, and those banks which do not currently employ blacklists to immediately do so. Still, preventing birthday-based guessing requires a move away from customer-chosen PINs entirely.

ACKNOWLEDGMENT

I am indebted to Dr. G. MAHADEVAN for his valuable insights and guidance.

REFERENCES

[1] EMV Integrated Circuit Card Standard for Payment Systems version 4.2. EMVco, 2008.
[2] Issuer PIN Security Guidelines. Technical report, VISA, November 2010.
[3] ISO 9564:2011 Financial services { Personal Identi_cation Number (PIN) man-agement and security. International Organisation for Standardisation, 2011.
[4] B. B_atiz-Lazo and R. J. Reid. The Development of Cash-Dispensing Technology in the UK. IEEE Annals of the History of Computing, 33:32{45, 2011.

[5] M. Bond and P. Zieli_nski. Decimalisation table attacks for PIN cracking. Technical Report UCAM-CL-TR-560, University of Cambridge, Jan. 2003.
[6] J. Bonneau, M. Just, and G. Matthews. What's in a name? Evaluating statistical attacks against personal knowledge questions. FC '10: The Fourteenth Interna- tional Conference on Financial Cryptography and Data Security, 2010.
[7] S. Boztas. Entropies, Guessing, and Cryptography. Technical Report 6, Department of Mathematics, Royal Melbourne Institute of Technology, 1999.
[8] W. E. Burr, D. F. Dodson, and W. T. Polk. Electronic Authentication Guideline. NIST Special Publication 800-63, April 2006.
[9] C. Cachin. Entropy measures and unconditional security in cryptography. PhD thesis, ETH Z□urich, 1997.
[10] S. Drimer, S. J. Murdoch, and R. Anderson. Optimised to Fail: Card Readers for Online Banking. FC '09: The Thirteenth International Conference on Financial Cryptography and Data Security, 2009.
[11] D. Flor^encio and C. Herley. A large-scale study of web password habits. In WWW '07: Proceedings of the 16th International Conference on World Wide Web, pages 657{666, New York, NY, USA, 2007. ACM.
[12] A. Ivan and J. Goodfellow. Improvements in or relating to Customer-Operated Dispensing Systems . UK Patent #GB1197183, 1966.
[13]M. Kuhn. Probability Theory for Pickpockets|ec-PIN Guessing . Technical report, Purdue University, 1997.
[14] J. L. Massey. Guessing and Entropy. In Proceedings of the 1994 IEEE International Symposium on Information Theory, page 204, 1994.
[15] R. Morris and K. Thompson. Password security: a case history. Commun. ACM, 22(11):594{597, 1979.
[16] S. J. Murdoch, S. Drimer, R. Anderson, and M. Bond. Chip and PIN is Broken. Security and Privacy, IEEE Symposium on, 0:433{446, 2010.
[17] J. O. Pliam. On the Incomparability of Entropy and Marginal Guesswork in Brute- Force Attacks. In Progress in Cryptology-INDOCRYPT 2000, 2000.
[18] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong. Password Sharing: Implications for Security Design Based on Social Practice. In CHI '07:
Proceedings of the SIGCHI Conference on Human factors in Computing Systems, pages 895{904, New York, NY, USA, 2007. ACM.
[19]E. Spa_ord. Observations on Reusable Password Choices. In Proceedings of the 3rd USENIX Security Workshop, 1992.
[20] P. C. van Oorschot and J. Thorpe. On Predictive Models and User-Drawn Graphical Passwords. ACM Trans. Inf. Syst. Secur., 10(4):1{33, 2008.
[21] M. Weir, S. Aggarwal, M. Collins, and H. Stern. Testing metrics for password creation policies by attacking large sets of revealed passwords. In Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS '10,
pages 162{175, New York, NY, USA, 2010. ACM.