3W-02

打鍵ミスを考慮したおとり付きパスワード管理ツールの提案

那須川至† 小倉加奈代† Bhed Bahadur Bista† 高田豊雄†
岩手県立大学ソフトウェア情報学部†

1. はじめに

近年，パスワードリスト攻撃による不正アクセス対策として，パスワード管理ツールがしばしば利用される．パスワード管理ツールの安全性を高めるために，おとりを用いて Master Password(MP)を防御する研究[1]があるが，ユーザが MP を入力ミスすることでユーザ自らがおとりに嵌るという問題がある．

本稿では，ユーザの打鍵ミス傾向に基づいた打鍵ミスが起こりにくい MP を生成するおとり付きパスワード管理ツールを提案し，その有用性を検証するとともに，生成されたおとりパスワードの看破困難性を評価する．

2. 関連研究

Chatterjee et al.[1]は，正規 MP と異なるパスワードを入力しても，もっともらしいアカウント情報を表示する NoCrack と呼ばれるおとりを用いたパスワード管理ツールを提案した．このツールでは，どのような文字列を入力してもそれらしいアカウント情報のリストが表示されるため，攻撃者はどの情報が正規のアカウント情報なのか推測することが困難である．しかし，正規ユーザが MP を入力ミスした場合も，もっともらしい結果が出力されるため，ユーザ自身が気づかないうちにおとりに嵌るという問題を孕んでいる．

藤原[2]は，ユーザの打鍵ミスの傾向を特定し，その傾向に基づいたパスワード生成手法を提案した．この手法により，ユーザの打鍵ミスの起こりにくいパスワードの生成が可能である．

3. 提案手法

提案手法は，次節より説明する独立した以下 2 つの機能からなる．

(1)おとり用パスワードの生成

NoCrack[1]の関連研究である ManWeir et al. [3]の手法を参考にし，正規パスワードからおとり用パスワードを生成する．

(2)打鍵ミスを考慮したパスワードの生成

システムが提示する文字列をユーザが入力するタイピングテストを実施し，その結果から打鍵ミスの傾向を特定する．特定した打鍵ミスパターンに基づき，打鍵ミスを起こしやすい文字を除外したパスワードを生成する．

3.1 おとり用パスワード生成

おとり用パスワードは以下の 3 つの手順で生成する．なお，2009 年に yahoo よりリークされたパスワードリスト yahoo-withcount.txt[4]をデータセットとして利用する．

(1)yahoo-withcount.txt 内にあるパスワードの特徴量を計算する．この時の特徴量の導出方法は以下の通りである．

- a~z, A~Z : 1 ~ 26
- 0~9 : 30 ~ 39
- その他記号 ：99

(2)ユーザが入力した正規パスワードにも同様の処理を行い，特徴量を抽出する．

(3)正規パスワードの特徴量に近似する値のパスワードを yahoo-withcount.txt から検索し，それをおとり用パスワードとして出力する．

3.2 打鍵ミスを考慮したパスワードの生成

打鍵ミスを考慮したパスワードは，以下の 4 つ手順で生成する．

(1)ユーザにタイピングテストを課す．ユーザが入力する文字列はアルファベット中心の 30 語，記号中心の 10 語の計 40 語で構成される．

(2)(1)のテスト結果よりユーザの打鍵ミスの傾向を以下の 5 つに分類し，特定する．

1. R_L：キーボード上で隣接するキーを押し間違える
2. Shift：Shift キーを押し間違える
3. Twice：必要のないところで同じ文字を 2 回入力する
4. Omit：入力すべき文字が抜ける
5. Miss：入力すべき文字と別の文字を入力する

(3)ユーザにパスワード生成のもととなる単語を 5 つ入力させる．

(4)入力された 5 つの中から，(2)で特定した打鍵ミス傾向を含まない単語を抽出し，それらを組み合わせてパスワードを生成する．

4. 評価実験

本章では，おとり用パスワードの看破困難性を評価する実験と，打鍵ミスを考慮し生成した MP に関する評価実験

A Proposal of Password Management System with Decoy Password Considering Typing Mistakes
† Itaru Nasukawa, Kanayo Ogura, Bhed Bahadur Bista, Toyoo Takata
† Iwate Prefectural University, Faculty of Software and Information Science

とその結果について述べる．

4.1 おとり用パスワードの看破困難性評価

4.1.1 実験目的

提案手法によるおとり用パスワードの看破困難性，すなわち,おとりがおとりであると見破られないかを評価する．

4.1.2 実験手順

著者が用意した正規パスワード 10 個からそれぞれ 3 種類ずつ提案手法によるおとり用パスワードを生成する．被験者（情報系学部に所属する大学生 1-4 年生 146 名）は正規パスワード 1 つ，提案手法によるおとりパスワード 3 つの合計 4 つの中から正規パスワードを推測する問題(但し，「分からない」という選択肢を設ける）を 10 問回答する．

4.1.3 実験結果

計 1460 個のパスワードを出題し, 突破されたパスワードは 99 個であり, 約 93.2%の確率で正規パスワードが選択されることを防ぐことができた．

また，結果から「分からない」の回答を除くと，その回答数の合計は 556 個であり，約 82.2%の確率で正規パスワードの選択を防ぐことができた．この結果は，提案手法により作成されたおとり用パスワードの看破困難性が十分な性能を持っていることを示唆している．

4.2 打鍵ミスを考慮したパスワードの評価

4.2.1 実験目的

提案手法によりユーザの打鍵ミスを考慮した MP を生成し，それについて打鍵ミスの発生状況とパスワードの安全性を評価する．

4.2.2 実験手順

本実験では以下 3 つのパスワードを利用する．

A：3.2 節で説明した提案手法によるパスワード

B：適当な文字列で生成したパスワード

C：打ち間違えやすい文字で生成したパスワード

5 名の被験者は，提案手法によるパスワード A を生成するために，3.2 節の(1)の手順を実施する．この時，各被験者の打鍵ミス傾向に合わせパスワード B と C を作成する．次に，被験者は A，B，C のパスワードをそれぞれ 3 回ずつ入力フォームに入力する．この時の打鍵ミスの回数や所要時間を評価の指標とする．

また，パスワードの安全性については，パスワード A を入力されたパスワードを 0~4 の 5 段階で評価するパスワードチェッカーzxcvbn[5]を用いて評価する．zxcvbn は s→$や a→@などの文字の置き換えを考慮することや, 関係のない単語をランダムに並べ，十分な長さを保っているパスワードは強いと判定される特徴がある．

4.2.3 実験結果

実験結果を表 1, 表 2 に示す．表 1 より，どの被験者も，提案手法によるパスワードの打鍵ミスの回数が最も少なく，打鍵ミスが起こりにくいことが確認できた．また，提案手法によるパスワードの強度は平均で 4 段階中 3 以上と実用に問題のない強度であることが確認できた．さらに表 2 より，どの被験者も提案手法によるパスワードを最も速く入力できることが確認できた．この結果は，提案手法によるパスワードがスムーズに入力できる文字列で構成されたものであることを示唆している．

表 1　生成パスワードの打鍵ミスの回数/強度

Table 1　Number of key misses and strength of generated password.

	A	B	C	A の強度
被験者 1	1	2	6	4
被験者 2	0	2	3	2
被験者 3	1	3	7	3
被験者 4	0	1	0	3
被験者 5	3	7	5	4

表 2　生成パスワードの打鍵時間

Table 2　Keystroke time of generated password.

	A(平均)	B(平均)	C(平均)
被験者 1	4.20 秒	11.45 秒	17.70 秒
被験者 2	3.90 秒	16.50 秒	15.46 秒
被験者 3	6.19 秒	21.73 秒	14.65 秒
被験者 4	3.76 秒	14.21 秒	10.13 秒
被験者 5	7.93 秒	24.25 秒	15.21 秒

5. おわりに

本稿では打鍵ミスを考慮したおとり付きパスワード管理ツールを提案し，実験によりその有用性を確認した．

今後は提案手法で作成したパスワードの記憶保持性を調査する．

参考文献

[1]R. Chatterjee, J. Bonneau, A. Juels and T. Ristenpart : Cracking-Resistant Password Vaults Using Natural Language Encoders, Proc. of IEEE Symposium on Security and Privacy 2015, pp.481-498, 2015.

[2]藤原咲子: タイピングミスを考慮したパスワード生成手法の提案, 岩手県立大学ソフトウェア情報学部卒業論文, 2016.

[3]M.Weir, S.Aggarwal, B. D. Medeiros and B. Glodek : Password Cracking Using Probabilistic Context-Free Grammars, Proc. of IEEE Symposium on Security and Privacy 2009, pp.391-405, 2009.

[4]R. Chatterjee: Cracking-Resistant Password Vaults using Natural Language Encoders, https://pages.cs.wisc.edu/~rchat/projects/NoCrack.html (accessed 2017/06/25)

[5]zxcvbn:https://github.com/dropbox/zxcvbn(accessed 2017/12/20)