L-056

打鍵署名を利用したパスワード認証の強化について

User Verification Based on Password Keystroke Information

山村　直也†　　ラシキア　ジョージ‡
Naoya Yamamura　　George V. Lashkia

１．研究背景

現在、個人認証の方法としてパスワード認証と生態認証などがあげられる。パスワード認証はユーザ ID とパスワードを使用して簡単に認証を行う事が出来る。しかし、パスワード認証では、容易に推測されてしまう場合や、クラッキングや過失によってパスワードがもれてしまう場合がある。生態認証はコストが高く、偽造された場合に鍵を変更できないという問題がある。打鍵も生体認証であるが、特別なハードウェアを使用しないため有用な認証技術として注目されてきた。しかし、打鍵が変わりやすいため、現在の打鍵認証では精度が不十分である。そこで本研究では従来のパスワード認証システムの改善が目的である。パスワードと打鍵を利用する手法について研究を行う。いくつかの手法を提案し特性を議論する。

２．従来研究

打鍵署名を利用した代表的な研究として、Joyce [1]と Bergadano [2]、Robinson [3]の手法があげられる。

[1]の手法はログイン時にだけ認証を行うため、短いテキストを扱う。これはいわゆる静的認証である。署名として digraph からなるベクトルを使用する。digraph は、ログイン時にあるキーを押してから次のキーを押すまでの時間である。リファレンス署名とテスト署名を比較し、差が閾値より小さければ本人であると認証される。この手法は打鍵時間と閾値を比べるため打鍵の変動の影響を受けてしまう。よって、精度が悪くなることが多い。

[2]の手法はユーザのタイピングを常に監視するため、長いテキストを用いる。これはいわゆる連続認証である。ユーザのタイピング時に trigraph を取得する。trigraph はあるキーを押してから 2 つ先のキーを押すまでの時間である。リファレンス署名とテスト署名を比較する時は並び替えた各時間の位置を比較する。この手法は打鍵の変動にロバストであるが、認証に長いテキストを必要とする。

[3]は３つの静的認証手法を提案している。ここでは、その中で一番精度が良かった手法について述べる。署名として digraph と接鍵時間の２つのベクトルを使用する。接鍵時間とはあるキーを押している時間である。初めに、有効なユーザと無効なユーザのデータを集める必要がある。ログイン時にテスト署名を与え、有効なユーザと無効なユーザのどちらのクラスに近いかを求め認証を行う。この手法は高い精度の認証が出来が、有効なユーザの他に無効なユーザの情報を必要するので、その情報の収集は困難である。

†　中京大学 大学院 情報科学研究科 情報科学専攻
‡　中京大学

３．研究概要

本研究の目的は既存のパスワード認証の強化であるため、短いテキストであるパスワードのみによって認証を行う。また、取得時間には一般的に利用される digraph を使用する。提案された多くの打鍵署名を利用したシステムは propositional rule を用いて digraph と定数(閾値)との比較を行う([1]など)。しかし、タイピングの時に digraph をミリ秒単位でコントロールする事よりリズムのコントロールの方が簡単であると考えられる。そこで本研究ではリズムを検出するために relational rule を使用して属性と属性を比較する。relational rule 用いる事によって、よりロバストなシステム構築を目指す。ここでは、M1,M2,M3 の 3 つの手法を提案し、[1]と[2]と比較する。

提案手法での処理の一般的な流れを示す。取得した digraph ベクトルから特徴を抽出し、特徴ベクトルを作成後、リファレンス署名を生成する。リファレンス署名は初回に数回タイプした特徴ベクトルから作成し、その後動的に更新される。ユーザのログイン時にパスワードが正しい場合は、digraph ベクトルから特徴ベクトルを生成しリファレンス署名と比較し認証を行う。

４．研究内容

打鍵時間は様々な要因で変化するため認証において時間データより順序関係の方が重要である。そのため提案する 2 つの手法は順序関係を使用する。時間ベクトルを昇順に並べ、ラベルを付ける。ラベルベクトルを使用する手法の場合、時間データの単調な変化に左右されない。例えば、9 文字のパスワードの場合、取得したミリ秒単位の時間ベクトルが以下であったとする。

（1156, 1089, 1360, 906, 478, 235, 758）

それに対応するラベルベクトルは以下のとおりである。

（7, 6, 3, 8, 5, 2, 1, 4）

M1 は digraph ベクトルをラベル付し、それを特徴ベクトルとする。アクセスしたい時には ID とパスワードをタイプし、パスワードが正しければ、取得した digraph ベクトルをラベルベクトルに変換し、テスト署名とする。リファレンス署名とテスト署名を比較する事で認証を行う。

M2 は digraph ベクトルの隣あう属性の差を求める。その結果をラベルベクトルに変換し、特徴ベクトルとする。ログイン時に同様の手順でテスト署名を生成し、リファレンス署名と比較する。

M3 は他の手法と違い、順序データを使用しない。より独特な認証手法を提案する。まず、digraph ベクトルの隣あう属性の差を求める。差データのシステムへの影響を少なくするために差データを equal interval width 法を用いて離散化し、それを特徴ベクトルとする。時間の差がマイナスなら特徴ベクトルの値もマイナスになる。ログイン時にテスト署名を作成し、リファレンス署名と比較し、認証する

Table.1 False alarm rate

Category	[1]	[2]	M1	M2	M3
1 (low-case)	37.00% ±7.73	3.80% ±1.99%	2.60% ±1.90%	0.00% ±0.00%	1.00% ±1.05%
2 (all keys)	31.84% ±9.28%	3.06% 1.67%	3.67% ±3.99%	0.00% ±0.00%	1.02% ±1.41%
3 (PIN)	29.89% ±13.27%	1.76% ±2.20%	4.40% ±7.41%	19.34% ±7.98%	17.80% ±7.85%
4 (free-style)	38.32% ±6.93%	4.99% ±2.72%	8.58% ±4.65%	37.13% ±4.91%	37.33% ±8.68%

Table.2 Impostor Pass Rate

Category	[1]	[2]	M1	M2	M3
1 (low-case)	0.00% ±0.00	7.41% ±19.0	0.00% ±0.00	0.00% ±0.00	0.00% ±0.00
2 (all keys)	0.00% ±0.00	8.06% ±21.3	0.00% ±0.00	0.81% ±4.35	7.26% ±27.1
3 (PIN)	0.00% ±0.00%	51.31% ±38.21%	24.09% ±30.45%	0.00% ±0.00%	0.37% ±1.84%
4 (free-style)	0.00% ±0.00%	38.03% ±40.85%	22.30% 27.82%	0.00% ±0.00%	0.00% ±0.00%

５．評価実験

本研究ではシステムの精度を false alarm rate と impostor pass rate を用いて評価する。false alarm rate (FAR)は正規のユーザがアクセスを拒否されてしまう確率である。impostor pass rate (IPR)は攻撃者に侵入を許してしまう確率である。提案したシステムを評価するために本研究ではパスワードを 4 つのカテゴリに分け、実験を行う。1 つ目のカテゴリは小文字の英字のパスワード、2 つ目のカテゴリは 1 つ目に大文字の英字と数字を加えたパスワード、3 つ目のカテゴリは文字数の少ないパスワードでキー同士が近いもの。これらのカテゴリはリズムを記憶している。最後のカテゴリはフリースタイルである。本研究では、各カテゴリにつき１０人の学生に実験に協力してもらった。実験にはほぼ同じパソコンを使用した。レファレンス署名は 1 人のユーザにつき 50 回分、全体で 2000 回から得られる。各カテゴリにつき 20 人の攻撃者が 10 人のユーザの中からランダムに選ばれた人へ攻撃を試みる。全体で 140 回の侵入を試みた。攻撃者にはユーザのログイン情報としてパスワードだけを与える。ユーザのトライアルは目撃していないとする。認証システムとして FAR は 5%以下、IPR は 1%以下が望ましい。実験結果の FAR を Table.1 に、IPR を Table.2 にそれぞれ示す。提案手法のカテゴリ 1,2 の FAR は許容できる。M1 はカテゴリ 1 , 2 で許容できる IPR である。M2 のカテゴリ 1,3,4 は妥当な IPR である。M3 はカテゴリ 1,4 で IPR が妥当である。[1]と M2,3 は IPR が低いが FAR が高い。[2]は FAR が低いが、IPR が高い。M1 は FAR も IPR も少し高い。1 つの方法で全てのカテゴリで許容できるものは得られなかった。カテゴリ 1,2 は M1,M2 が良い結果となったが、カテゴリ 3,4 に優れている手法は得られなかった。カテゴリ 3 で精度が極端に悪くなるのはパスワードが短すぎるためリズムが取りにくいからである。カテゴリ 4 が極端に悪いのはリズムを意識してなく、タイピングが一定ではないためであると考えられる。

６．まとめ

打鍵時間は様々な要因で大きく変化してしまう。そこで、本研究では、パスワード入力時に digraph を取得し、認証に使用する問題に取り組んだ。打鍵時間の変化に左右されないように、ユーザがタイプする時のリズムパターンを見つける事でユーザを特定する 3 つの手法を提案した。提案手法を評価するためにパスワードを 4 つのカテゴリに分け実験を行い、従来手法と比較した。提案手法は従来手法より優れた性能を発揮した。また、比較的長いパスワードを用いた場合、パスワードと digraph を用いる事により、セキュアなシステムを構築できる事を発見した。

精度が特に悪いカテゴリ 3 を改善する事が一番の課題である。また、より多くの人に実験に協力してもらい、実験回数を増やす事も必要である。手法の複合的な適用によって精度を改善できると考えられる。リズムの学習をするソフトの開発にも取り組みたい。

参考文献

[1] R.Joyce, G.Gupta : Idertity Authertication Based on Keystroke Latencies, Communications of the ACM, Vol.33,No.2,1990

[2] F.Bergadano, D.Gunetti, Claudia Picardi : User authentication through keystroke dynamics, ACM Transactions on Information and System Security, Volume 5, Issue 4, 2002

[3] John A. Robinson, Vicky M.M. Liang, J.A. Michael Chambers, and Christine L. Makenzie : Computer User Verification Using Login String Keystroke Dynamics, IEEE Transactions on Volume 28, Issue 2, Mar 1998