5W-4

打鍵署名を利用したパスワード認証の強化について

山村　直也(中京大学 情報科学部)*, ラシキア　ジョージ(中京大学)

１．研究背景

現在、個人認証の方法としてパスワード認証や生態認証などがあげられる。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洩れてしまう場合がある。生態認証では、コストがかかることや偽造されてしまった場合に鍵を変更できないなどの問題点がある。そこで、本研究では従来のパスワード認証に打鍵署名を新たな鍵として加えることにより万が一パスワードが洩れた場合でも容易に認証できないシステムの実現を目指す。

２．従来研究

打鍵署名を利用した研究として JG 法[1]、新 JG 法[1]、アルペジオ手法[2]などがある。ここでは、代表例として、新 JG 法と Fabian(2002)の手法の説明をする。

新 JG 法では、パスワードを入力する時に打鍵間時間を取得する。初めに数回パスワードを入力し、その時間の平均を基準署名と言い、認証をしたい時に入力した時間を入力打鍵書名と言う。入力打鍵署名と基準署名の差の絶対値をノルムと言う。ノルムが標準偏差の 1.5 倍より小さければ本人と認証されるようになっている。

Fabian(2002)の手法はパスワードを入力するときにあるキーを押してから 2 つ先のキーを押すまでの時間を取得し、特徴ベクトルを作成する。初めに数回パスワードを入力し、そのベクトルを学習データとする。学習データのベクトルの属性を小さい順に並び替える。Fig.1 のように学習データ間の差の平均と、テストデータと各学習データとの差の平均を求める。それぞれの平均を m(A)、md(A,X)とする。md(A,X)が m(A)と学習データ間の差の標準偏差の間に含まれていれば認証されるようになっている。

新 JG 法や Fabian(2002)の手法などによって生成される認証ルールは propositional rule である。つまり、入力打鍵署名は定数の比較によって認証される。こういったシステムは定数の選び方に依存し、かなり敏感である。定数を小さくすると本人であっても認証されなくなり、大きくすると誰でも認証されるようになってしまう。

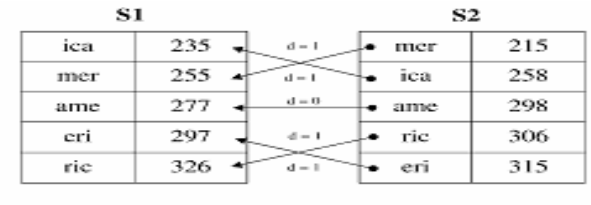

Fig.1 Distance of two typing sample of the same text

３．研究内容

本研究では propositional rule ではなく First-Order rule を生成し、もっとロバストなシステムの構築を目指す。また、いくつかの手法を提案し、評価をする。

第 1 の手法はパスワード入力時に入力時間情報(打鍵間時間、接鍵時間、非接鍵時間)を取得し、特徴ベクトルを作成する。取得したベクトルを小さいほうから順にラベルを付ける。ユーザに数回入力してもらい、それを学習データとする。学習データからルールを検出する。ラベル付きデータから共通パターンを取り出し、First-Order rule を作成する。共通パターンに当てはまらない残りの部分はタイピングの特徴を現す部分ではないと考え、従来の手法を適用する。例えば、Fig.2（打鍵間時間のグラフ）の user1 の場合では、k1 から k4 までが特徴的な部分で k5 から k8 までが順番がよく変わる部分である。生成される First-Order rule は次の通りである。

If k3 = 2 and k4 = 8 and k7 = 1 and k8 = 3

つまり k3 が 2 番目に小さく、k4 は最大値であり、k7 は最小値で、k8 は 3 番目に小さい。残りの部分に対しては従来の新 JG 法による propositional rule を作成し、First-Order rule に追加する。

第 2 の手法はパスワード入力時に入力時間情報を取得しベクトルを作成する。ベクトルからラベル付きデータを作成し、特徴ベクトルを生成する。生成した特徴ベクトルから共通部分を取り出し、第 1 の手法のような First-Order rule を作成する。共通分に当てはまらない部分は、テストデータのラベル付きデータが、特徴ベクトルのの平均から標準偏差の 1.5 倍の範囲に含まれているかという rule を作成し、先ほど作成した First-Order rule に追加する。

第 3 の手法は、パスワード入力時に打鍵間時間を取得し、ベクトルを作成する。ベクトルの属性間の差を求める。差データに対して小さい順にラベル付け、特徴ベクトルが生成される。ユーザに数回入力してもらい、それを学習データとする。学習データから平均を求め、それを認証ルールとする。テストデータも同様に項目間の差を求め、小さい順にラベルを付ける。ラベル付きデータと認証ルールを比較する。

第 4 の手法はパスワード入力時に打鍵間時間を取得し、ベクトルを作成する。属性間の距離を求め、離散化し特徴ベクトルを作成する。ユーザに数回入力してもらい、それを学習データとする。学習データの平均を認証ルールとす

Table.1 Results in User Authentication

Category	手法 1	手法 2	手法 3	手法 4	Fabian (2002)	Rick (1990)
Category1	92.00% ±1.63%	96.67% ±1.89%	100.00% ±0.00%	98.67% ±0.94%	96.67% ±2.49%	58.00% ±4.32%
Category2	87.33% ±0.94%	93.33% ±4.71%	100.00% ±0.00%	98.00% ±1.63%	96.00% ±0.00%	72.00% ±4.32%
Category3	95.05% ±2.00%	97.03% ±4.00%	96.04% ±5.00%	95.05% ±0.00%	96.04% ±1.00%	64.36% ±7.00%
Category4	89.00% ±5.00%	97.00% ±1.00%	50.00% ±26.0%	100.00% ±0.00%	98.00% ±2.00%	72.00% ±6.00%

る。テストデータに対しても同じように特徴ベクトルを求め、認証ルールと比較する。

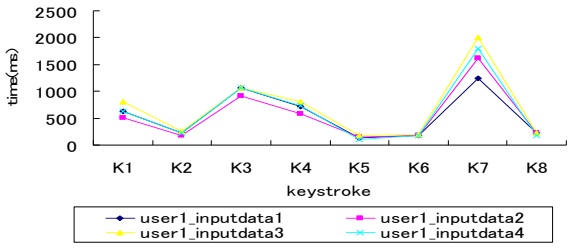

Fig.2 Keystroke Dynamics

４．評価実験

考案した各認証ルールと従来の認証ルールの様々なデータでの精度を比較することにより、考案した認証ルールの利点、欠点を調べる。実験ではパスワードの種類などによって入力データを４つの Category に分類する。Category1 は小文字の英字だけのパスワードのもの。Category2 は小文字、大文字の英字と数字を含むパスワードのもの。Category3 は ATM などのようにタイプするキーが近く短いパスワードのもの。Category4 はリズムを意識せずにタイプしたもの。

評価実験では 10 人（現在実験中である）のユーザにタイピングしてもらった。本研究は、パスワード入力時に入力時間情報を 5ms の幅で取得し、システム開始時８回の入力を求め、その後は、最大３０回のデータよりルールを作成し、入力された入力時間情報がそのルールの条件を満たしているかで個人の認証を行う。各 User がどのくらい認証されるかで評価する。Table.1 に各考案手法と従来手法の Category 別の認証率と偏差を示す。Table.2 に各考案手法の全体の認証率と偏差を示す。リズムを意識してタイプすれば、高い認証率を上げることが出来た。

Table.1 Results in User Authentication

Rate	手法 1	手法 2	手法 3	手法 4
All	90.22% ±3.81%	95.91% ±3.52%	89.22% ±22.91%	98.00% ±1.98%
Rithm only	91.02% ±3.33%	95.51% ±3.84%	99.00% ±2.65%	97.51% ±1.91%

５．まとめ

考案手法 1、2 は共通パターンを多く取ることが出来れば、従来手法に比べ精度が向上することがわかった。Category3 のような場合、共通パターンが取り易く適しているといえる。しかし、共通パターンがあまり取れない場合は精度が上がらない。考案手法 1 は 2 に比べ顕著に現れる。考案手法 3、4 はリズムを意識してタイプすれば、高い精度を上げる。しかし、リズムを意識せずにタイプした場合キー間の差があまりなく、適切なルールを作成できないため精度が上がらない。特に考案手法 3 では顕著に現れる。考案手法 4 ではリズムを重要であり、一部のキーだけがリズムをはずすと認証が失敗してしまう。

６．課題

認証精度を向上させるために認証ルール検出法を見直すこと、評価をより確かなものにするために実験を行うこと、他の従来研究と比較することなどが今後の課題である。

文　献

[1] Rick Joyce, Gopal Gupta : Identity Authentication Based on Keystroke Latencies, Communication of the ACM,Vol.33,No.2,1990

[2] 粕川 正充．他：アルペジオ打鍵列を利用した個人認証手法の提案，情報理学会論文誌,Vol.34,No.5,1993

[3]Francesco Bergadano, Daniele Gunetti, Claudia Picardi:User authentication through keystroke dynamics, ACM Transactions on Inforormation and System Security,Volume 5,Issue 4,2002

Identity Authentication through Keystroke Dynamics based on rule Induction

†Naoya Yamamura (Chukyo University)

‡George V. Lashkia (Chukyo University)