周囲の状況に適応する統合的認証方式での状況判定法の精度向上について

周囲の状況に適応する統合的認証方式での状況判定法の精度向上について

山場　久昭 [a)]・長野　裕孝 [b)]・高塚　佳代子 [c)]・久保田　真一郎 [d)]・岡崎　直宣 [e)]

On Accuracy Improvement in Surroundings Estimation for Surroundings Adaptable Integrated Authentication Method

Hisaaki YAMABA, Hirotaka NAGANO, Kayoko TAKATSUKA,
Shin-Ichiro KUBOTA, Naonobu OKAZAKI

Abstract

At the present time, mobile devices come to be widely used. Since such devices store many kinds of important data, it is necessary to guard the devices using a personal authentication method. On the other hand, higher usability is also needed for such a authentication method. So, is is a hard task to guard mobile devices using a single authentification method. To overcome this problem, the integrated authentication method was proposed in the previous study to adapt multiple situations that have various kinds of requiremnets of security and usebility. However, the method to identify correct situation a device was plaeced was not good enough. In this study, a situation estimation method using GPS was investigated using a simple app developed by the authors and the method showed promise.

Keywords: mobile device, user authentication, shoulder surfing attacks, usability

1. はじめに

近年、個人が所有するモバイル端末を業務で使用するBYOD(Bring Your Own Device) の普及が進んでいることもあり [1)]、モバイル端末の中に個人情報だけでなく、業務上秘密にしなければならない重要な情報が格納されたり、端末を通じてこれらの情報にアクセスできるようになりつつあり、これらの情報の漏洩を防ぐことが強く求められるようになってきている。

モバイル端末は、パソコンなどに比べ場所を選ばずに使用できるのが利点である。そのため、ロック画面の解除認証は、人の目や録画機器に晒された環境で行われることが多い。その際に、第三者が認証操作を覗き見することでパスワードなどの認証情報を得てしまうこと (以下、覗き見攻撃) や、ビデオカメラなどの録画機器により認証操作を録画、解析することにより認証情報を得られてしまうこと (以下、録画攻撃) に晒されやすい。

また一方では、モバイル端末の個人認証方式には、解除認証の手間がかからないこと（以下、ユーザビリティ) への配慮も重要である。

ここで、覗き見耐性と録画攻撃耐性を含む安全性とユーザビリティの間には、トレードオフの関係がある。認証操作を複雑にすると覗き見攻撃への耐性は強くなるが、ユーザビリティは低くなってしまう。そのどちらを優先すべきであるかについては、モバイル端末を使用する環境や、端末に格納されている情報の重要度に応じて異なる。

本研究では、和斉が提案した統合的認証方式 [2)] で用いられる、状況を判定する手法の改善を、位置情報を利用して行う。具体的には、端末の現在地の位置情報から、そこがどのような場所であるのかを判定し、それに応じて、状況判定のための閾値として異なった値を用いる。モバイル端末の操作が無かった時間が、その閾値を超過しているか否かにより、モバイル端末をユーザが所持しているか否かを判定する。

2. 研究背景

2.1 モバイル端末における個人認証

現在の多くのモバイル端末には、端末を紛失したり、盗難にあった場合などに、端末内の情報の漏洩や改竄を防ぐため、画面をロックし操作不可能となる機能が搭載されている。これは、あらかじめ設定した時間内にマウスや、キーボードなどからの入力がなかった場合、または、ユーザが明示的に指示した場合に、端末の操作が可能な状態から不可能な状態にし、端末を再び操作可能にするためには、パスワードや Personal Identification Number(PIN) などの個人認証を必要とするというものである。

モバイル端末の個人認証方式の特徴の一つとして、タッチパネル液晶を活用した個人認証方式が多く採用されていることがある。代表的なものには、Android Password Pattern(以下、APP)[3)] がある。

また、モバイル端末は場所を選ばず使用できるため、ロック解除のための認証操作が人の目に触れ易いという特徴があ

[a)]情報システム工学科助教
[b)]情報システム工学科学部生
[c)]教育研究支援技術センター技術専門職員
[d)]情報システム工学科准教授
[e)]情報システム工学科教授

る。モバイル端末にて、周りに人が多数いる状況下で、送信されてきたメールやかかってきた電話に即時に対応しようとすると、覗き見されないような状況を直ちに確保することは容易ではない。

2.2 覗き見による認証情報窃取攻撃

ここでは、覗き見することによって認証情報を窃取する攻撃を次の 2 つに分類する。

2.2.1 (目視での) 覗き見攻撃

覗き見攻撃とは、ユーザが個人認証を行っているところを第三者が覗き見し、パスワードなどの認証情報を得てしまうことである。

認証方式に覗き見耐性を持たせるには、人間には記憶力と処理能力に限界があることを利用する。人間はある程度認証方式を複雑にするとすべての認証情報、認証操作を記憶することが困難になる。つまり、認証をある程度複雑にすることで、覗き見耐性が実現できる。ただし、認証操作を複雑にすることにより、ユーザビリティがある程度低下してしまうことは避けられない。

2.2.2 録画攻撃

録画攻撃は、ビデオカメラなどの録画機器を用いることにより、認証画面と認証操作の全てまたは一部を記録し、コンピュータを用いて解析することにより、認証情報を特定する攻撃である。実質的に記憶能力と処理能力に限界はないため、認証方式に録画攻撃耐性を持たせることは、覗き見耐性を持たせることよりも難しい。また、この攻撃への耐性を実現するには、認証方式を複雑にするだけでは困難であり、録画された情報から認証情報が特定されないために、冗長な情報などによって、認証情報の隠蔽を行うことを必要とする。そのため、録画攻撃への耐性を持たせるためには、認証操作をより複雑にする必要があり、それゆえ、ユーザビリティを低下させてしまう。

2.3 統合的認証方式

和斉 [2] では、モバイル端末を対象として、覗き見攻撃への耐性を持つ認証方式を提案した。そこで、求められるセキュリティ要件の厳しさにより、様々な場面に応じて求められるセキュリティレベルを設定した。その上で、設定したセキュリティレベルに対して、適切な認証方式を選定し、それらを組み合わせることにより統合的認証方式を構成した。

2.3.1 セキュリティレベル

[2] では、まず、複数回の録画攻撃耐性が考慮する必要があるか否かにより、2 段階に分けることとしている。これら 2 つの段階は、具体的には次の 2 つの状況を想定していると考えることができる

状況 1: 勤務先のオフィスビルなどで監視カメラが設置されており、そこで認証操作を繰り返し行うような環境

このような環境では、複数回の録画攻撃に晒されることを想定する必要がある。また、このような環境で用いられるモバイル端末は、業務上の特に秘匿すべき情報が格納されていることがあるため、高いセキュリティが求められる。

状況 2: 上記以外の日常生活全般の環境

このような環境では、監視カメラが存在しないか、存在しても、それらの管理者が別個であり、撮影された動画像の情報が集約されることが無いと期待されることを想定する。

また、認証情報が分からなくても、入力をランダムに選んだときに、確率的に誤って認証してしまうことを確率的誤認証と呼ぶ。この確率的誤認証について警戒すべき次のような状況が想定されている。

状況 3: モバイル端末が第三者の手に渡っている環境

このような環境では、紛失や盗難などにより、モバイル端末が第三者の手に渡り、偶然に認証を突破することが想定される。そのため、確率的誤認証に対する耐性について高める必要がある。

その上で、これら 3 つの環境それぞれに対応した 3 つのセキュリティ要件 (A1,A2,B) が導入されている。以下では、これら 3 つのセキュリティ要件について、想定する環境がいずれであるのか、満たすべきセキュリティ上の耐性、及びユーザビリティをどの程度確保すべきについて説明する (表 1)。

LEVEL.A1

このセキュリティレベルは状況 2 のような環境を想定する。必要なセキュリティ要件は、複数回の覗き見耐性と 1 回の録画攻撃耐性を持つことである。

LEVEL.A2

このセキュリティレベルは、状況 1 のような環境を想定する。必要なセキュリティ要件は複数回の録画攻撃耐性と複数回の覗き見耐性を持つことである。

LEVEL.B

このセキュリティレベルは、状況 3 のような環境に想定する。必要なセキュリティ要件は、確率的誤認証に対する耐性が高いことである。

2.3.2 統合的認証方式の構成

[2] では、モバイル端末における認証方式に必要である高いユーザビリティを持たせるために、Secret Tap 方式とそのいくつかの拡張方式を組み合わせることにより、前述した異なるセキュリティ要件に求められる複数の場面において適用可能な統合的認証方式を提案した。

Secret Tap 方式 [4] は、タッチパネル液晶を備えたデバイス向けに提案された、チャレンジ・レスポンス型の認証方式である。特徴として、覗き見耐性を持たせることに加え、認証操作にアイコンを採用したことによりユーザビリティを高めていることがある。また、Secret Tap 方式は覗き見耐性を備えること、1 回の録画攻撃耐性を備えることを実現している。但し、Secret Tap 方式は、確率的誤認証が起こり易いこと、複数回の録画攻撃に対する耐性は十分ではないという弱点を持っている。この 2 つの弱点それぞれに対処できる手法として、STDS 方式 [5] と Secret Vibe 方式 [6] が提案されている。しかし、それらの方式は、代償として、ユーザビリティの低下、確率的誤認証への耐性が向上した分、他の攻撃への耐性が悪化するなどといった副作用が生じてしまっている。

表 1. セキュリティレベルにおける認証方法の分類

セキュリティレベル	セキュリティ要件	ユーザビリティ	認証方式
LEVEL A1	1 回の録画攻撃耐性 複数回の覗き見耐性	高いユーザビリティ	Secret Tap
LEVEL A2	複数回の録画攻撃耐性 複数回の覗き見耐性	ユーザビリティが高いことは問わない	Secret Vibe
LEVEL B	1 回の録画攻撃耐性 複数回の覗き見耐性 確率的誤認証に対する耐性が目標の強度	ユーザの許容回数で目標の強度	STDS

各セキュリティ要件を満たす認証手法として、具体的には、LEVEL.A1 には Secret Tap 方式、LEVEL.A2 には Secret Vibe 方式、LEVEL.B には STDS 方式が採用されている。

Secret Tap 方式とその拡張方式を選んだ理由として、いずれも共通の認証情報 (自分が選択した数個のパスアイコンとシフト量) と認証画面を用いることができるので、ユーザの負担が軽減できることがあげられる。認証情報のパスアイコンとして、ユーザが記憶することができるアイコンの数は 4,5 個が限界であることがわかっている [4]。そこで、全ての認証方式においてパスアイコン数を 4 個に設定されている。

なお、本方式を採用するにあたり、以下が前提とされている。

1. ユーザは、認証操作を行う環境や格納される情報などの条件から、必要なセキュリティレベルを判断することができる。
2. 認証方式に使用される認証情報の設定の時点で、攻撃者に認証情報が知られることはない。

2.3.3 個別の認証手法の切り替え

モバイル端末の盗難や紛失の危険性を考慮すると、常に LEVEL.B に適した認証方式を使用することが望ましい。しかしそれでは、本来 LEVEL.A1 に適した認証方式で十分な場合でも、ユーザビリティの低い手法を採用してしまうことになる。そこで、一定時間モバイル端末の操作が無かった場合に、ユーザがモバイル端末を紛失した、もしくは盗難にあったとみなし、LEVEL.B に対応した認証方式を利用するという方法をとる。この時間の長さはユーザが選択できるものとする。

基本的には比較的短い時間を用いるものとする。長くしてしまうと、状況 3 である場合でも、認証方式が確率的誤認証に弱い認証方式を利用することが増え、危険だからである。なお、状況 3 ではないと判定された場合は、状況 1 か 2 かの判定はユーザが行うものとされている。

3. 関連研究

モバイル端末がおかれた状況に応じて、複数の認証手法の中から適した認証手法を利用する認証方式の研究に、CASA[7] や、プログレッシブ認証 [8] がある。

CASA は、現在地がどれくらい安全であるのか、認証手法がどれくらい安全であるのかを値として表し、それぞれの場所に適した認証手法を選択する手法であり、本来デスクトップ型 PC を対象とした方式であるが、モバイル端末であっても有用である。また、いくつかの場所でモバイル端末を使用した時間を計測し、モバイル端末の 1 日の使用時間の半分以上が、いくつかの限られた場所での使用であったことが分かった。このことにより、状況判定の際の位置情報を用いることが有用であることを示した。

プログレッシブ認証では、モバイル端末をユーザが所持していることの確からしさを、ユーザの顔画像や音声などから判定し、その確からしさの度合いに応じて、モバイル端末の使用できるコンテンツを制限するという提案を行った。高いレベルの確からしさが必要なコンテンツにアクセスしようとするときに、確からしさが低かった場合には、能動的な認証の操作が必要となる。このように、確からしさがが十分に高い場合は、能動的な認証の操作を免除することにより、認証操作を行った回数を減少させることに成功した。

4. 提案手法

本研究では、和斉の提案 [2] における状況判定を、端末の位置情報を用いて改善する方法を提案する。

[2] では、状況 3 かそうではないのかの判定を、端末がスリープしてからの経過時間だけを用いて行っているため、その判定結果が十分に適切ではないことが考えられる。例えば端末が自宅にある場合は、それが第三者の手に渡っている可能性は極めて低いと考えられるが、就寝などにより端末を使用していない時間が長くなると、この手法の下では状況 3 であると判定されて、LEVEL.B の認証手法が選択されてしまう。

そこで本研究では、より適切な判定が行えるようにするために、端末が第三者の手に渡っている状況か否かを判断する閾値の大きさを、端末のおかれた場所に応じて、異なった値にする手法を提案する (図 1 を参照)。すなわち、端末が第三者の手に渡っている可能性が高いと考えられる場所では、閾値の値は比較的短い時間に、可能性が低いと考えられる場所では、比較的長い時間にすることにより、判定の精度向上を目指す。なお、第三者の手に渡りにくいと考えられる場所とそれ以外の場所は、予めユーザが選定しておくものとする。今回は、ユーザが所持している可能性が高い場所としては家と職場を選び、それ以外の場所はユーザが所持している可能性が低い場所とした。

どちらの場所であるのかの判定には、GPS で取得した位置情報を用いる。場所の判定を行うにあたり、選定した場所それぞれの中心点と判定距離を予め登録しておく。中心点は、それぞれの場所の範囲のおおよその中心位置の緯度と経度、判定距離は中心点からその場所の範囲の端までの距離の最大値とする。認証を行おうとする際には、GPS でモバイル端末の

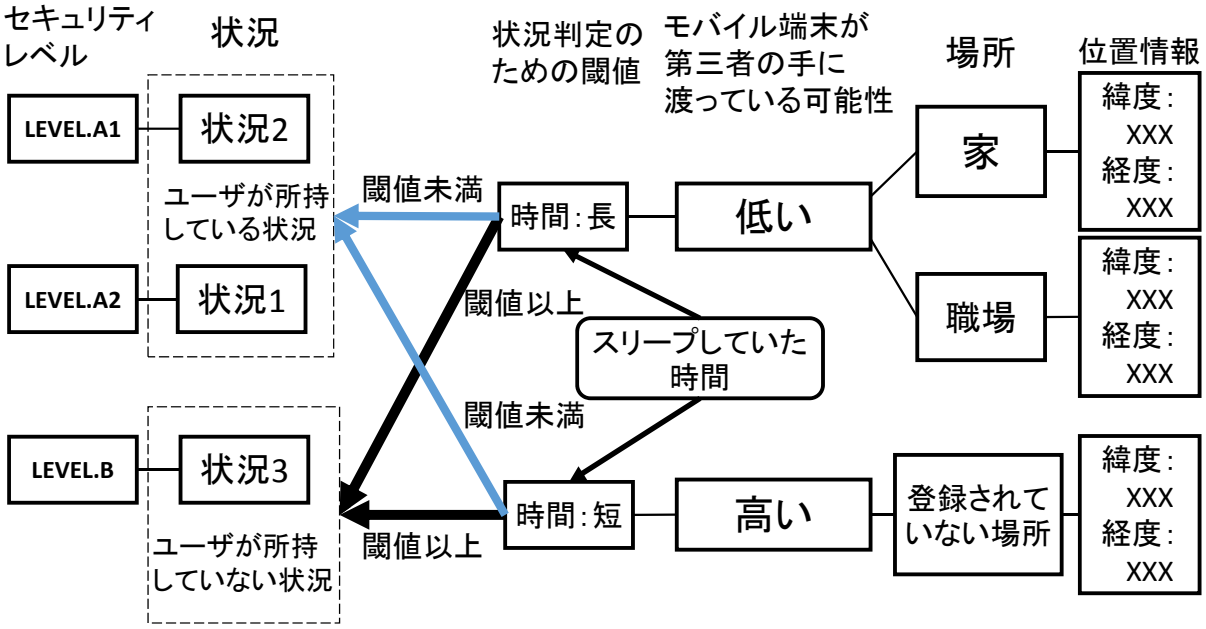

図 1. 位置情報からセキュリティレベルの判定

位置を測定し、各場所の中心点との距離を測定する。その距離が判定距離＋精度誤差の範囲内であれば、モバイル端末はその場所にあると判定する。範囲内と判定された場所がなければ、登録されていない場所であると判定する。後述する実験では、GPS の精度誤差は 5m とした。

本手法で認証を行う過程を以下に示す。

1. GPS で現在地の位置情報を取得する。
2. 取得した現在地の位置情報から、現在地が家か職場か、それ以外の登録された場所であるのかを判定する。
3. 判定された場所に応じた値を今回の閾値として選ぶ。
4. モバイル端末がスリープしてからの経過時間を取得する。
5. 経過時間が 3 で選ばれた閾値を超過していれば、モバイル端末は第三者の手に渡っているものと判定し、LEVEL.B に対応した認証手法の認証画面を表示する。
6. そうでなければ、モバイル端末はユーザが所持しているものと判定し、LEVEL.A2 に対応する認証手法の認証画面を表示する。
7. ユーザは表示された認証画面を用いて認証を行う。

5. 状況の判定実験

状況の判定に位置情報を加えることにより、スリープしていた時間の長さのみを利用していた場合に比べ、どの程度性能を向上できるのかを調べる実験を行った。

実験を行うにあたり、実験のための Android アプリを実装した。これは、GPS から取得した位置情報を取得が、登録しておいた場所のいずれであるかを判定し、その場所に応じた閾値によって、ユーザが端末を所持しているのかどうかを判定する。実装はプログラミング言語 Java と Android SDK を用いて、統合開発環境 Eclipse で行った。このアプリを起動すると、スリープしていた時間、モバイル端末の位置情報 (緯度と経度)、そこから判定した現在の場所 (登録した場所のいずれであるのか、あるいは、それらの場所以外であるのか)、その場所に対応した閾値を表示する。今回、閾値の長さは、状況 3 になっている可能性が低いとした場所 (家と職場) では 8 時間、それ以外の場所では 1 時間とした。8 時間は一般的な就寝時間から、1 時間は 8 時間と比較して十分短い時間から選択した。これを閾値を 1 時間に固定した従来法と比較する。

本実験では、宮崎大学工学部の学生 6 人を被験者とした。被験者には、家と研究室において、モバイル端末が起動する度に実装したアプリを起動してもらい、表示されるスリープしていた時間を記録してもらった。記録は家か研究室にいた時間の総和が 24 時間になるまで続けてもらった。家と研究室の中心位置と判定距離は Google Map を用いて測定した。

スリープしていた時間が提案法での状況 1 と 2 での閾値 (8 時間) を超過した回数と、[2] の方法 (従来法) での閾値 (1 時間) を超過した回数を数え上げ、比較した。

記録した 139 回のスリープしていた時間から、閾値が 1 時間であった場合、超過した回数は 59 回、閾値が 8 時間であった場合の超過した回数は 6 回であった (表 2)。閾値を 1 時間とした場合は、記録した回数の 42.4 %で超過していた。それに対して、閾値を 8 時間とした場合は、記録した回数の 4.3 %で超過していた。このことから、提案手法が従来法よりも良い判定を行えていると考えられる。

表 2. それぞれの閾値における超過比率

閾値	超過した回数	超過した比率
従来法	59 回	42.4 %
提案法	6 回	4.3 %

6. まとめ

本論文では、以前に提案された統合的認証方式における状況の判定手法について、位置情報を用いてその精度を上げる手法を提案した。また、この判定手法を Android アプリとして実装し、それを用い実験を行うことにより、以前の手法に比べ、より適切に状況の判定ができることを示した。また、今後の課題として、次のことが考えられる。

1. 実際に家や職場であっても、状況 3 である可能性はあるので、スリープしていた時間と位置情報以外の情報も利用してさらなる改良を行う。
2. 場所の判定には GPS を用いたが、屋内では誤差が無視できないので、屋内での場所を判定する際には、位置情報の取得には GPS 以外を利用することを検討する。

参考文献

1) Cisco：BYOD 世界各国の動き-従業員が引き起こすイノベーションを生かす (online) <http://www.cisco.com/web/JP/ibsg/howwethink/pdf/BYOD_Horizons-Global.pdf>(2016.2.6)
2) 和斉薫「モバイル端末向け個人認証方式における柔軟な安全性強度の実現に関する研究」, 宮崎大学修士論文 (2015)
3) Google: Android-open source project,http://source.android.com/
4) 菅井, 他: アイコンとタッチパネル液晶を用いた覗き見耐性を持つ認証方式の提案, マルチメディア, 分散, 協調とモバイル (DICOMO)2012 シンポジウム, pp.2402_2409(2012).
5) 喜多, 他: モバイル端末における覗き見耐性を持つ認証方式の提案と実装, コンピュータセキュリティシンポジウム (CSS2012),2D2_1,pp1_8(2012).
6) 和斉, 他:モバイル端末に適したアイコンを用いた個人認証方式の録画攻撃耐性とユーザビリティに関する考察、コンピュータセキュリティシンポジウム (CSS2013),3D1_3,pp700_707(2013).
7) E.Hayashi,et al: CASA:Context-Aware Scalable Authentication,Symposium on Usable Privacy and Security (SOUPS)2013, July 24-26,2013, Newcastle, UK
8) O.Riva,et al: Progressive authentication: deciding when to authenticate on mobile phones, Proceedings of the 21st USENIX Security Symposium,2012