Vol.2013-SPT-7 No.3
2013/11/11

“CASA: Context-Aware Scalable Authentication”の紹介

望月 翔太[1,a)]　高田 哲司[1]

概要：本稿では 2013 年 7 月に英国で開催された Symposium on Usable Privacy and Security で発表された論文“CASA:Context-Aware Scalable Authentication”[1] についてその研究内容を紹介する．

1. はじめに

この論文では，CASA:Context-Aware Scalable Authentication と呼ぶ個人認証の強化と単純化を目指した新たな枠組みを提案している．スマートフォンなどの普及により一般化したセンサー群とそこから得られるデータから構築できる人物モデルを個人認証に応用することで，リスク状況に応じた認証手法を利用者に提供する枠組みである．

CASA は 2 つの概念を含んでいる．概念 1 ）センサー情報による場所や人の“モデル”は，ユーザの本人性検証における passive factor になるという点である．passive factor とは，ユーザの居場所や最終ログイン時刻からの経過時間など明示的に対話処理をしなくても得られる情報を指す．一方，active factor は暗証番号の入力や指紋のスキャン等，明示的に対話処理を要求することで得られる情報のことを指す．概念 2 ）passive factors はユーザに行わせる個人認証の強度を調節するのに利用可能という点である．例えば「passive factors が高い確率で正規のユーザらしいことを示している状況では，簡単な検証方法で認証を行う.」といった仕組みである．

この実現に向けて，この論文では 3 つの研究成果が述べられている．第一に，一般的なベイジアンフレームワークにより，得られた passive factor から active factors を選択できることを示す．第二に，利用者の位置情報を passive factor の一つとして適用可能かについて検証する．第三に，2 回の被験者実験を通じて行った CASA の設計/実装とその評価について述べる．

2. フレームワーク

Hayashi らのアプローチは，passive factor など複数の要因を組み合わせ active factor の適切なレベルを決定するために，単純ベイズ分類機を使用して「リスク評価」の値を算出することである．ユーザ u(正当ユーザ；u=1，非正規ユーザ：u=-1) を判別するために，式 1 を使用する．

$$u = sign\Big[\log(a\frac{P(u=1)}{P(u=-1)})+\sum_{i=1}^{n}\log\frac{P(s_i|u=1)}{P(s_i|u=-1)}\Big] \quad (1)$$

ここで，P(u=1)，P(u=-1) は認証される人が正規ユーザまたは非正規ユーザである事前確率を示し，$P(s_i|u=1)$，$P(s_i|u=-1)$ は i 番目の観測 s を与えられた際の正規ユーザまたは非正規ユーザである確率を示している．

表 1　携帯電話使用状況 (出典:[1])

場所	時間 [%]	起動時間 [%]
1 (自宅)	38.9	31.9
2 (仕事場)	18.7	28.9
3	9.9	18.5
4	5.5	10.8
5	4.3	5.2
他	22.6	4.5

3. 実験

3.1 実験 1 ：移動パターン解析

128 人の被験者を集め，5 ヶ月間実験を行った．携帯電話にアプリケーションを入れてもらい，被験者の位置情報と携帯電話の起動状況のデータを収集した．表 1 は，被験者が過ごした時間と携帯電話起動時間の分布である．結果は，被験者が (自宅と仕事場と仮定した)2 箇所で 1 日の 57.8%を過ごすことを示した．この 2 箇所にはデスクトップまたはラップトップ等のネットワーク接続可能な装置があると思われるため，これほど頻繁に携帯電話を使用するか不明慮であった．しかし，このデータは，人が自宅および仕事場で携帯電話を頻繁に使用することを示している．

以上の結果より，位置情報が非常に有効な passive factor

[1] 電気通信大学
The University of Electro-Communications
[a)] m1010143@edu.cc.uec.ac.jp

表 2　active factor 選択 (出典:[1])

条件	自宅	仕事場	その他
PIN	なし	なし	PIN
Password	PIN	PIN	Password

であるかもしれないことを示唆しており，携帯電話を使用することで強固な認証が必要であることを証明できる．よって，位置情報に基づき active factor を調節すれば，有用性とセキュリティのバランスを調節することできる．

3.2　実験２：CASA 試作システムの評価

32 人の被験者を集め，CASA フレームワークの試作機の実験を行った．この試作機は，ユーザの位置情報に基づいて active factor を選択する機能を持つ．被験者は，携帯電話でのセキュリティ・ロックの使用経験に基づき，PIN 条件 (使用経験なし，19 人)，パスワード条件 (使用経験あり，13 人) の 2 つに分割した．この実験では，ユーザが active factor が変更されることへの反応を調査した．

表 2 は，PIN 条件およびパスワード条件の各位置における active factor である．ユーザが PIN またはパスワードを忘却する可能性が懸念されたが，それらの記憶を保持するほど被験者が頻繁に PIN やパスワードを入力することがわかった．

ポスト調査で，試作機の使用についての認識を調査した．その結果，被験者は試作機を有用であると考えたが使用することには中立であった．また，仕事場でユーザ認証を必要としないことに懸念を示していた．自宅にいる人を信頼する人は 68%存在したが，仕事場にいる人を信頼する人は 18%しか存在しなかった．

3.3　実験３：改良版 CASA システムの評価

18 人の被験者を集め，改良版システムの評価を行った．以前とは異なり，位置情報トレーニング期間と評価期間を分離した．改良点は 2 つある．第一に，仕事場では第三者が入る可能性があるため自宅ほど信用できる場所と言い切れないため，仕事場での計算機利用状況を passive factor として追加した．第二に，携帯電話盗難時に盗難者に自宅や仕事場を探索されない対策として，携帯電話をアクティブにしたにもかかわらず PIN を入力しない状況を 5 回以上発生した場合，以降は必ず PIN を入力するようにした．

実験の結果，被験者は仕事場において，平均で携帯電話を 5.5 回起動した．5.5 回のうち 2.9 回は PIN を要求しなかった．

ポスト調査で，コンピュータの使用に基づき認証方法を変更することは有効であり，本システムの仕組みを理解することが容易であると報告した．また，常に PIN を要求することと比較して安全性は低くないと答えた．さらに興味深いことに，セキュリティ・ロックを使用したことがなかった被験者が，CASA を使用したいと報告した．

4.　議論

この研究は，ユーザに最小限の負担でよりよいセキュリティを提供する認証システムの開発において有益である．しかし，Hayashi らの研究はいくつかの制限が存在する．例えば，各 factor において CASA は認証される人が正当でない確率を必要とする．パスワードのようなほとんどの active factor にはこの確率の理論的・経験的推測値が存在する．対照的に，passive factor はこの確率値は存在しない．もう一つの制限は仕事場での処理である．Hayashi らの改良版システムでは，合理的な物理的セキュリティが仕事場に存在すると考えていた．この仮定は，多くの事務員には適切かもしれないが，オフィス等専用スペースを持っていない人には適切でないかもしれない．この問題の解決方法は，合理的な物理的セキュリティを擁している場所を作るようユーザに依頼することである．

将来の研究のひとつの指針として，他の passive factors およびユーザ・モデルを評価することである．本研究はいくつかの passive factor のセキュリティを調査した．しかし，攻撃者が正当なユーザに扮しようとする場合，passive factor のセキュリティは明らかではない．さらに，Hayashi らは単純モデル (3 種類の位置情報，コンピュータの使用をモデル化する 2 つの passive factor) を使用した．Hayashi らのモデルには，実装が簡単で理解しやすいという利点が存在した．passive factor の組み合わせで，よりよい精巧なモデルを作ることは可能である．

5.　結論

この論文では，複数の passive factor を利用して本人かどうかを検証する認証手法を調整する CASA と呼ぶ手法を紹介した．確率的フレームワークにより与えられた passive factors から適切な active factor(認証手法) の選択が可能であることを示し，提案する手法の実現可能性と効果を 3 つの実験を通じて調査した．その結果，個人認証の安全性と利便性に配慮した active factor を選択できることが検証された．被害者実験では，passive factor として，利用者の位置情報を使った場合と位置情報＋身近にある計算機の利用状況をあわせて利用した場合の 2 つの条件で実験を行った．このシステムに対する被験者の印象は，今まで携帯電話の画面ロックを利用していなかった利用者がこのシステムに強い興味を示すなど，好意的であった．

参考文献

[1] Hayashi E., Sauvik D., Shahriyar A., Jason H., Ian O. CASA:Context-Aware Scalable Authentication, In Proc. of the 9th Symp. on Usable Privacy and Security(SOUPS'13), Article No3,(2013)