様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　２６　日現在

機関番号：　３２６９２
研究種目：　若手研究(B)
研究期間：　2014～2017
課題番号：　２６８７０６６０

研究課題名（和文）人間の心理特性と振る舞いを利用した弱者のための携帯端末向けセキュリティ技術の研究

研究課題名（英文）Researches of information security on mobile phones for non-technical people using psychology and behavior

研究代表者

宇田　隆哉（UDA, Ryuya）

東京工科大学・コンピュータサイエンス学部・講師

研究者番号：５０３５０５０９

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：本プロジェクトは、リテラシーの低いスマートフォン利用者にセキュリティ技術を提供する研究を行うものである。成果の一つとして、スマートフォンのフリック入力時に本人の特徴を抽出することで、追加の特殊デバイスやセキュリティを向上させるためだけの特殊な操作をユーザに強いることなしに、パスワードによる本人確認を強化できる手法を提案した。また、仮想OSを利用したファイルのアクセス制御技術、脆弱と推測されるWebサイトを見分ける技術、歩きスマホの抑止技術の研究も行った。仮想OS上の実装は困難であったが、深層学習はWebサイトの自動判別に有効であること、抑止は防止よりも歩きスマホ対策に有効であることがわかった。

研究成果の概要（英文）：The aim of this project is to provide new technological secure methods for smartphone users who are not unfamiliar with information literacy. The most significant output is a method for enhancing security of inputting password on smartphones. Password identification on smartphones is enhanced by personal characteristics on flick inputs. The method requires no additional special device or special training for security. In addition, there are some more outputs which are a file access control method on virtual OS, a method for finding vulnerable web sites and a deterrence method of walking while on the phone. As a result, we found that deep learning was effective for the automatic classification of web site and deterrence was more effective than prevention for stopping walking while on the phone, while implementation on virtual OS was difficult.

研究分野：　情報セキュリティ、デジタルフォレンジック、本人確認

キーワード：　専門的知識を有しない利用者へのセキュリティ技術　スマートフォンのセキュリティ

１．研究開始当初の背景

スマートフォン上で動作するアプリケーションソフトウェア（以下、アプリ）には、電話帳の情報や全地球測位網（以下、ＧＰＳ）の機能、通信機能を利用するものもあり、これらはインストール時にユーザが許諾を与える仕組みになってはいるが、ゲームやソーシャルネットワーキングサービスやそれらに関連、類似するアプリに必須の機能でもあり、情報リテラシー教育だけで利用者に危険なアプリを使用させないようにすることはもはや不可能といえる。さらに、知人からの勧めにより特定のウェブサイトに接続したりアプリを導入したりすることも頻繁に行われているが、不特定多数を結びつけるソーシャルネットワーキングサービスが発展した現在、何を以って誰が信用のおける知人か判断するのは従来の社会的基準では困難になってきている。

もちろん、これらの問題には対策も行われている。現在、スマートフォンに導入されているウイルス対策ソフトウェアにはクラウド対応のものがある。導入されるソフトウェアが悪意あるもの（マルウェア）であるかどうか調べるにあたり、スマートフォン上でジェネリック手法やダイナミックヒューリスティック手法などを用いて念入りに調べると、バッテリーや計算資源を多く消費してしまい、スマートフォンの性能が著しく低下してしまう。そのため、クラウドサーバの仮想ＯＳ上でソフトウェアの検査を行い、スマートフォンと連携している。しかし、仮想ＯＳと実ＯＳの差をマルウェアが判断可能という研究発表があり、仮想ＯＳ上で従来の手法を用いても、振る舞いを変えて検知を回避するマルウェアが広まる可能性が高い。悪意のあるウェブサイトをフィルタにより排除する技術も一般的ではあるが、これらは短期間で場所を変えたり、正規のウェブサイトを乗っ取ったりするため、対策としては不十分である。さらに、ソーシャルネットワーキングサービスを介した問題発言や差別、誹謗中傷などは、アプリやサービスの問題ではなく、利用者の利用方法によるものであるため、全利用者に普遍的な一律の対策は困難である。

これらの問題を鑑み、本プロジェクトでは、スマートフォンに対するセキュリティ技術の研究に焦点を当てた。従来対策の情報漏洩防止技術や利用者教育も重要であるが、情報漏洩後に個人情報を守る技術や、IT 教育と縁遠い利用者にもセキュリティ技術を提供しようと考えたのが申請時の動機である。さらに、サイバー空間では物理空間に比べて攻撃側のリスクが低いという背景にも注目し、攻撃者のリスクを向上させることが犯罪の抑止に繋がるという動機から、電子的な証拠を蓄積するデジタルフォレンジック技術も取り入れることにした。

２．研究の目的

スマートフォンを利用したソーシャルネットワークサービスやネットワークゲームが未成年にも普及する一方で、情報リテラシー教育の欠落が、個人情報の漏洩やプライバシの侵害を引き起こしている。新規サービスの登場に教育が追いついておらず、これらは教育で対応可能な限界を超えている。そこで、本プロジェクトでは、リテラシーの低いスマートフォンの利用者にも、高いセキュリティを提供できる技術の研究を行う。具体的には、情報漏洩時に個人情報が特定できない技術の研究や、問題行動を推測して抑止、防止する技術の研究を行う。さらに、攻撃者に対して、電子的な証拠を秘密裏に蓄積するデジタルフォレンジック技術の研究も行う。

３．研究の方法

(1) リテラシーの低いスマートフォンの利用者にも高いセキュリティを提供する技術の研究のひとつとして、スマートフォンで標準的な文字入力方法として使用されているフリック入力において、個人の特徴を抽出する研究を行った。具体的には、フリック入力時に加速度、角速度、移動距離、時間などをスマートフォンから取得し、個人識別を行うものである。なお、単独での精度は低いため、パスワードそのものと組み合わせ、覗き見耐性を向上させた。

(2) 従来の PC とは異なり、スマートフォンのデータはクラウドサーバ上で管理されることが一般的となってきたため、サーバのファイルシステムにおいて、アプリケーションソフトウェアプログラムごとにファイルアクセス制御を可能とする研究を行った。具体的には仮想 OS が仮想マシンモニタ(VMM)を通してアクセス可能なファイルを制限するものであるが、VMM の仕組みの制約上、提案通りの実装は行えなかった。

(3) 個人情報が適切に管理されていないと推測される Web サイトを、リテラシーの低い利用者にも判別できるよう、機械学習を用いて自動的に区別するという研究を行った。具体的には、深層学習により、HTML のコードの構造だけで Web サイトを分類した。ただし、サンプルを大量に集める都合上、実際に行ったのは別の方法で機械的に分類された Web サイトを深層学習で再度分類できるか確認したに留まっており、本当に可能かどうか確かめるには、リテラシーの高い利用者が手動で分類した Web サイトを深層学習で再度分類して評価しなければならない。

(4) 人間の心理を利用して、歩きスマホを行いづらくする研究を行った。これは従来の防止技術とは異なり、周囲の人の視線が集まることで、心理的に歩きスマホをしづらくさせる抑止技術である。具体的には、スマートフ

ォンの振動機能を利用し、歩きスマホを検知するとスマートフォンが振動するというものである。従来の防止技術とは異なり、振動してもスマートフォンは引き続き利用可能であるため、どうしても利用せざるを得ない場合には利用可能であるが、振動音により周囲からの視線が集まるため、非常時以外は心理的に利用しづらくなる。10 名の被験者で実験を行ったところ、9 名が歩きスマホの頻度が下がるという結果が得られた。

４．研究成果

(1) スマートフォンで一般的に使用されているフリック入力において、個人の特徴を抽出する研究を行った。しかしながら、フリック入力から得られる個人の特徴は、プロジェクトの研究目的である個人情報保護やデジタルフォレンジックには不十分な精度であった。そこで、従来のスマートフォンのロックに使用されている一般的なパスワードと組み合わせ、攻撃者にパスワードが部分的に知られた場合でも、簡単にはスマートフォンのロックを不正に解除できない仕組みに応用することにした。本研究の技術を用いれば、難解なセキュリティ技術を学ぶことなく、スマートフォンのセキュリティ機能を向上できる。スマートフォンは公共の場でも使用するため、端末をパスワードで保護していても、背後からパスワードを盗み見られる可能性が高い。一方、背後からパスワードを盗み見る攻撃者にしても、パスワード入力画面を凝視することは不自然であるため、パスワードを部分的またはおおよそしか把握できないことが多い。狙った端末に攻撃者がキーロガーやバックドアなどの不正ソフトウェアを仕込むには、利用者の隙をつき、短時間の内に端末を操作する必要がある。本技術を用いれば、フリック入力時の特徴とパスワードの両方が一致しなければスマートフォンのロックが解除されないように設定できるため、パスワードがはっきり分からない攻撃者にはロック解除にかかる時間を引き延ばせる。一方、本来の利用者には特別な操作を何も強要しないため、本技術の導入は容易である。研究実績としては、識別率向上のためのアルゴリズムの改善、電車内などでの利用時に床の揺れを吸収するアルゴリズムの提案を行った。成果は、査読付きの国際会議にて 4 回発表を行い、国際会議論文が IEEE から 2 件、ACM から 2 件発行されている。この仕組みは全世界のスマートフォンに適用可能である。特許も出願中である。しかし、研究を開始した当初には予期していなかった、一般的に人工知能と呼ばれている深層学習が短期間に台頭してきた。そのため、学術論文誌（ジャーナル）に論文を掲載するためには、これらを用いて比較を行う必要が生じた。従来の研究に深層学習を適用したという研究が目覚ましい成果を上げており、本研究にも取り入れるべきという知見が得られた。

(2) 近年流行しているクラウドコンピューティング技術により、スマートフォンのデータがサーバで管理されることも一般的になってきた。しかし、従来のファイルシステムにおいては、データのアクセス制御が利用者単位で行われており、端末が不正に利用されると利用者の全てのデータにアクセスされてしまうおそれがあった。そこで、サーバのファイルシステムにおいて、アプリケーションソフトウェアプログラムごとにファイルアクセス制御を可能とする研究を行った。成果は、査読付きの国際会議にて１回発表を行い、国際会議論文が IEEE から 1 件発行されている。また、国内の研究会においても１回発表を行い、研究報告論文が電子情報通信学会から１件発行されている。この仕組みはスマートフォンのデータに限らず、全世界のクラウドコンピューティング環境に適用可能である。

(3) 個人情報が適切に管理されていないと推測される Web サイトを見分けて利用者に通知する研究を行った。Web サイトにおいて、氏名、住所、電話番号などの個人情報を入力する場合がある一方、システムやサイトの構造上、情報が適切に管理されず、情報漏洩の危険性が高いと思われるものがある。そこで、リテラシーの低い利用者にも判別できるよう、これらの Web サイトを機械学習を用いて自動的に区別するという研究を行った。これにより、高い精度で Web サイトの判別が行えるという知見が得られた。成果は、査読付きの国際会議にて１回発表を行い、国際会議論文が ACM から１件発行されることが決定している。なお、今回の研究に用いたサンプルは、Web のしくみに詳しい技術者が手動で分類したものではなく、分類可能であるという事例を示したものに留まっているため、厳密には手動で分類したサンプルで再評価する必要がある。

(4) 人間の心理を利用して、歩きスマホを行いづらくする研究を行った。従来の防止技術では、歩きスマホをさせないことを前提にしており、画面に警告を表示したりしている。しかし、これではどうしてもスマートフォンを使用する必要がある場合に使用できなくなることから、普及が進んでいない。そこで、周囲に振動音が聞こえるバイブレーション機能を用いて、歩きスマホを行いづらくするように工夫した。これは従来の防止技術とは異なり、周囲の人の視線が集まることで、心理的に歩きスマホをしづらくさせる抑止技術である。研究を行った結果、本大学の学生には一定の抑止効果があるという知見が得られた。成果は、査読付きの国際会議にて 1 回発表を行い、国際会議論文が ACM から１件発行されることが決定している。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 8 件）

[1] Xueyan Liu and Ryuya Uda, Classification of Web Site by Naive-Bayes and Convolutional Neural Networks, In Proceedings of the 12th International Conference on Ubiquitous Information Management and Communication (IMCOM'18), ACM, 査読有, 掲載確定

[2] Hiroya Kato and Ryuya Uda, Texting while Walking Deterrence System by Vibration of Smartphone, In Proceedings of the 12th International Conference on Ubiquitous Information Management and Communication (IMCOM'18), ACM, 査読有, 掲載確定

[3] 市川実, 宇田隆哉, 共通鍵暗号とプログラムのハッシュ値によるファイルアクセス制御を用いた機密情報保護, 電子情報通信学会技術報告, 査読無, Vol.116, No. 501, EMM2016-104, pp.103-108, 2017 年 3 月.

[4] Minoru Ichikawa and Ryuya Uda, "Protection of Secrets by File Access Control with Common Key Cipher and Message Digests of Program Files", In Proceedings of the 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA 2016), IEEE, 査読有, pp.226-231, 2016. DOI: 10.1109/WAINA.2016.25

[5] Takumi Nohara and Ryuya Uda, "Personal Identification by Flick Input Using Self-Organizing Maps with Acceleration Sensor and Gyroscope", In Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication (IMCOM'16), ACM, 査読有, Article No. 58, 2016.

[6] Nozomi Takeuchi and Ryuya Uda, "Password Security Enhancement Method by Flick Input with Considering the Floor Shake", In Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication (IMCOM'15), 査読有, Article No. 5, 2015. DOI 10.1145/2701126.2701176

[7] Nozomi Takeuchi and Ryuya Uda, "Password Security Enhancement by Characteristics of Flick Input with Double Stage C.V. Filtering", In Proceedings of World Congress on Sustainable Technologies (WCST), IEEE, 査読有, pp.58-65, 2014. DOI 10.1109/WCST.2014.7030098

[8] Nozomi Takeuchi, Shuhei Kobata and Ryuya Uda, "Improvement of Personal Identification by Flick Input with Acceleration Sensor", In Proceedings of IEEE the 38th International Computer Software and Applications Conference Workshops (COMPSACW), 査読有, pp.276-281, 2014. DOI 10.1109/COMPSACW.2014.49

〔学会発表〕（計 8 件）

[1] Xueyan Liu and Ryuya Uda, Classification of Web Site by Naive-Bayes and Convolutional Neural Networks, The 12th International Conference on Ubiquitous Information Management and Communication (IMCOM'18), ACM, Jan 5 -7, 2018, Langkawi, Malaysia.

[2] Hiroya Kato and Ryuya Uda, Texting while Walking Deterrence System by Vibration of Smartphone, The 12th International Conference on Ubiquitous Information Management and Communication (IMCOM'18), ACM, Jan 5 -7, 2018, Langkawi, Malaysia.

[3] 市川実, 宇田隆哉, 共通鍵暗号とプログラムのハッシュ値によるファイルアクセス制御を用いた機密情報保護, 電子情報通信学会, マルチメディア情報ハイディング・エンリッチメント研究会, 2017 年 3 月 6 ～7 日, 宮古島マリンターミナル 大研修室.

[4] Minoru Ichikawa and Ryuya Uda, "Protection of Secrets by File Access Control with Common Key Cipher and Message Digests of Program Files", The 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA 2016), IEEE, Mar 23 - 25, 2016, Crans-Montana, Switzerland.

[5] Takumi Nohara and Ryuya Uda, "Personal Identification by Flick Input Using Self-Organizing Maps with Acceleration Sensor and Gyroscope", The 10th International Conference on Ubiquitous Information Management and Communication (IMCOM'16), ACM, Jan 04 - 06, 2016, Danang, Viet Nam.

[6] Nozomi Takeuchi and Ryuya Uda, "Password Security Enhancement Method by Flick Input with Considering the Floor Shake", The 9th International Conference on Ubiquitous Information Management and Communication (IMCOM'15), Jan 8 - 10, 2015, Bali, Indonesia.

[7] Nozomi Takeuchi and Ryuya Uda, "Password Security Enhancement by Characteristics of Flick Input with Double Stage C.V. Filtering", World Congress on Sustainable Technologies (WCST), IEEE, Dec 8 - 10, 2014, London, UK.

[8] Nozomi Takeuchi, Shuhei Kobata and Ryuya Uda, "Improvement of Personal Identification by Flick Input with Acceleration Sensor", IEEE the 38th International Computer Software and

Applications Conference Workshops (COMPSACW), Jul 21 - 25, 2014, Vasteras, Sweden.

〔産業財産権〕

○出願状況（計 1 件）

名称：フリック入力時の特徴を機械学習させて個人を識別する方法
発明者：宇田隆哉，野原拓実
権利者：宇田隆哉，野原拓実
種類：特許
番号：特願 2016-141855
出願年月日：2016 年 7 月 26 日提出
国内外の別：国内

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

６．研究組織
(1)研究代表者
宇田 隆哉（UDA, Ryuya）
東京工科大学・コンピュータサイエンス学部・講師
研究者番号：50350509