Vol.2012-GN-84 No.18
Vol.2012-SPT-3 No.18
2012/5/18

Workshop on Usable Security (USEC12) 参加報告

金岡 晃[1,a)]　高橋 健志[1]

概要：2012 年 3 月 2 日にオランダ領アンティルのボネール島で開催された Workshop on Usable Security (USEC12) の参加報告を行なう。報告は、ワークショップの概要に加え、いくつかの論文に関する紹介も行なう。

キーワード：ユーザビリティ、セキュリティ

Workshop on Usable Security (USEC12) Report

Akira Kanaoka[1,a)]　Takeshi Takahashi[1]

Abstract: Workshop on Usable Security (USEC12) has been hold at Bonaire Island, Netherlands Antilles, on 2nd March. We report this workshop. The report includes workshop outline and introduction for selected papers.

Keywords: Usability, Security

1. はじめに

セキュリティ技術に関する学術的研究や、セキュリティのマネジメントに関する研究はこれまで多くされてきている。高機能なスマートフォンが急激に浸透し、よりユーザがさまざまな脅威にさらされるなか、セキュリティがますます重要とされている。一方で、セキュリティを実現するために利用者のユーザビリティが軽視される部分も存在する。セキュリティは無視できなくなっている現在において、高いユーザビリティを確保しながらセキュリティの確保やプライバシの保護が行なわれることが重要になってくる。ユーザビリティとセキュリティ・プライバシを考慮した研究は、注目が集まりつつある分野であり、それらを対象とした国際会議も開催されてきている。その 1 つの国際ワークショップである Workshop on Usable Security に筆者らは参加をしてきた。本稿では 2010 年 3 月 2 日に開催された Workshop on Usable Security について報告を行なう。

セキュリティ・プライバシにおけるユーザビリティを対象とした国際会議ではSOUPS（Symposium On Usable Privacy and Security）が著名であるが、このような対象を絞った国際会議は他に無く、USEC は SOUPS に続くセキュリティ・プライバシ分野でのユーザビリティに関する国際会議と位置付けることができると思われる。

ユーザビリティの研究は、CHI（Computer Human Interface）の分野としてセキュリティやプライバシの文脈ではなくより広く研究が行なわれてきており、SOUPS や USEC はユーザビリティの研究分野における文化がある。それは技術的なコンピュータセキュリティやネットワークセキュリティ、または暗号理論や暗号技術、セキュリティマネジメントなどの研究分野とは異なる側面であり、論文における表現や提案手法の評価手法、議論される内容などは大きく異なる。本稿ではそれらの側面を示す例として、USEC におけるいくつかの論文も合わせて紹介する。

本論文の構成は以下の通りである。まず第 2 章でワークショップの概要を示す。第 3 章において、発表論文のうちいくつかの論文について概要を紹介する。最後に第 4 章でまとめる。

[1] 情報通信研究機構
〒 184-8795 東京都小金井市貫井北町 4-2-1
[a)] kanaoka@risk.tsukuba.ac.jp

2. ワークショップ概要

USEC は 2012 年 3 月 2 日に、オランダ領アンティルのボネール島の Divi Framingo Beach Resort において開催された [1]。2012 年 2 月 27 日から 3 月 1 日まで開催された Financial Cryptography and Data Security 2012[2] の共催ワークショップの 1 つであり、もう 1 つのワークショップは Workshop on Ethics in Computer Security Research (WECSR 2012) である。

USEC は ISE (Information Security Economics) という団体により主催されているワークショップであり [3]、同団体ではこれまで Workshop on the Economics of Information Security (WEIS) を過去 10 回にわたって開催しており、USEC と題したワークショップは初めての開催であった。

USEC がターゲットとしている分野は, セキュリティの文脈におけるユーザビリティと人間の要素のあらゆる側面の研究であるとされている。

投稿は LNCS フォーマットで 12 ページを上限とされている通常投稿と、上限が 6 ページであるショートペーパーの 2 種類が可能であった。投稿は開催のおよそ 3 ヶ月半前の 2011 年 11 月 21 日に締め切られ、採録通知は 12 月 16 日、カメラレディの投稿が 2012 年の 1 月 16 日というスケジュールであった。

発表された論文は 8 本で、そのうち 1 本が Short Paper であった。

セッションとそれぞれのセッションでの発表数は以下の通りである。

(1) Passwords (発表数 3)
(2) End User Management (発表数 3)
(3) Methods (発表数 2)

参加者およそ 30 名程度であり、大規模とは言えないが各発表に対する質疑応答は活発であった。

3. 発表論文概要

3.1 Linguistic Properties of Multi-word Passphrases

University of Cambridge の Joseph Bonneau らによる論文である [4]。

複数のパスフレーズを認証情報として利用するシステムでの利用されるパスフレーズの特徴を解析し、出現確率の偏りを示したものである。

Amazon 社の PayPhrase では、ログインに際しユーザ ID などは必要とせず複数のパスフレーズを入力することによりユーザ認証を行なう。PayPhrase ではすでに利用されたパスフレーズの組は新規登録時のログイン情報として利用できないことに加え、新規登録におけるログイン情報の試行の上限回数が定められていなかったため、著者らはさまざまなパスフレーズを合わせて 100000 用意し、それらの組合わせをチェックし、その偏りを示した。

論文の狙いは、大量のデータからパスフレーズを複数使うことによる統計的な偏りを示すことで、その強度を測る部分にあった。PayPhrase はそのログイン方法や上限回数の無さに問題があるシステムであったがそれを利用することで統計情報を得ている。ユーザが選ぶ情報に関する偏りを示す、という研究もユーザビリティに関する研究として受け入れられるということを示した論文でもあろう。

3.2 My Privacy Policy: Exploring End-User Specification of Freeform Location Access Rules

Indiana University の Sameer Patil を筆頭著者として、University of Pittsburgh の共著者 2 人を含む 4 名での論文である [5]。

スマートフォンの増加に伴い、位置情報を利用した Web 上のサービスが増えていることを踏まえ、それらの位置情報に対するアクセス制御はユーザにとってどう捕らえられているかをフリーフォームのアンケートを取ることで解析したものである。

質問は以下の 7 つの項目について、それらの情報が保護されるべきかについて 1-5 までで点数付けしてもらい、その理由を記載するものである。

(1) だれが位置情報を取得するか
(2) 情報へのアクセス理由
(3) 1 日のうち何時にアクセスしているか
(4) 何曜日にアクセスしているか
(5) ユーザの現在位置
(6) 開示された位置情報の特徴
(7) 一定期間でのアクセス数

項目 1、2 はいずれも高い点数を付ける傾向にあり、それらは予想できるものであった。一方、項目 3、4 に関しては点数が分散する傾向にあり、ユーザ間で重要性の認識に違いがあることが伺える。また、ユーザの現在位置と一定期間でのアクセス数は高い点数にあることがしめされた。

ユーザにアンケートを取ることでそのユーザビリティを調査する研究は多く、本論文もその 1 つである。調査の方法やその分析については、セキュリティのユーザビリティとしてではなく、CHI (Computer Human Interface) 分野などで多く研究されており確立されているものと見える。

3.3 A Conundrum of Permissions: Installing Applications on an Android Smartphone

Carnegie Mellon University の Patrick Kelley を筆頭著者とした計 6 名の著者による論文である。他の著者の所属として University of Washington, Microsoft がある [6]。

スマートフォンのアプリケーションがインストールされるときに表示されるさまざまな権限設定などの情報について、利用者がどのようにそれらの情報を捕らえていて、どうアプリケーションに対する信頼を確率しているかの調査を行なったものである。

調査の結論として、以下の 3 点が挙げられている。

- 権限設定情報などがあることはユーザはしっており、読むこともしているが理解はしていない
- 信頼は、口づてや他のユーザによるレーティング、アンドロイドマーケット上のレビューコメントなどにより確立されている
- 利用者はマーケット上にマルウェアが存在することを知らされていない

スマートフォンにおけるユーザビリティとセキュリティ、そしてプライバシの問題は本分野では非常に盛んに取り上げられている分野であり、2011 年の SOUPS でもいくつかの論文がスマートフォンに対するセキュリティとプライバシを対象としていた。

3.4 Understanding the Weaknesses of Human-Protocol Interaction

Royal Holloway University of London の Marcelo Carlos を筆頭著者とした論文である [7]。

Computer と Human の相互作用が発生するシステムでは、その攻撃の多くは暗号学的な要素に対して行なわれているのではなく、人間との相互作用部分に対して行なわれているという点に注目し、人間系の相互作用における弱点（Weakness）について、分類を行ない、また分類された情報から、それぞれに対して対策として設計はどうあるべきかの指針をマッピングしている。

人間との相互作用部分はまさにユーザビリティが関係する部分であり、それらを整理し分類することは非常に重要だと考えられる。聴講者からも活発な質問があったことなどから、重要なポイントを押さえていた発表であったことがわかる。

4. まとめ

セキュリティ・プライバシにおけるユーザビリティに焦点を当てた国際ワークショップ Workshop on Usable Security の報告を行なった。報告ではワークショップが対象としている分野や、採録された論文、またセッション名などからそのワークショップの特性を示すことを狙った。

ユーザビリティの分野は、スマートフォンを初めとする高機能デバイスが人の身近なところに多く存在するようになった現代においてより重要な分野となってきている。セキュリティ・プライバシの視点をもったユーザビリティの研究は、ますます重要となって行き、これらの分野の発展が十分に予想される。一方で、技術的なセキュリティやマネジメントの分野とは異なる評価軸や文化があり、それらに注意して投稿や発表を行なう必要があるであろう。

3 章で紹介をした論文では、いずれも人間系を強く捕らえた評価が論文内で行なわれており、本分野の特徴がよく現れたものであると言える。

USEC は決してレベルの高い国際会議とは言えないが、ユーザビリティの分野でのセキュリティ・プライバシの扱われ方やこれからの発展を見定めるには良い場所であった。今後、USEC を始めとするセキュリティ・プライバシのユーザビリティに関する研究分野はより活発となっていくことであろう。そのときに、研究における提案手法に人間系を考慮にいれた評価を行なうことや、人間の特徴そのものを調査することなどが行なわれると同時に、セキュリティ・プライバシの視点でのユーザビリティの研究はどのような評価がされるべきかという側面の研究や議論も行なわれてくるであろう。

参考文献

[1] Workshop on Usable Security (USEC12), http://infosecon.net/usec12/index.php
[2] Financial Cryptography and Data Security 2012 (FC12), http://fc12.ifca.ai/index.html
[3] Information Security Economics (ISC), http://infosecon.net/
[4] Joseph Bonneau, Ekaterina Shutova, "Linguistic Properties of Multi-word Passphrases", Workshop on Usable Security (USEC12), 2012
[5] Sameer Patil, Yann Le Gall, Adam Lee, Apu Kapadia, "My Privacy Policy: Exploring End-User Specification of Freeform Location Access Rules", Workshop on Usable Security (USEC12), 2012
[6] Patrick Kelley, Sunny Consolvo, Lorrie Cranor, Jaeyeon Jung, Norman Sadeh, David Wetherall, "A Conundrum of Permissions: Installing Applications on an Android Smartphone", Workshop on Usable Security (USEC12), 2012
[7] Marcelo Carlos, Geraint Price, "Understanding the Weaknesses of Human-Protocol Interaction", Workshop on Usable Security (USEC12), 2012