第5回 IFIP WG 11.2情報セキュリティ理論と実践ワークショップ (WISTP 2011)参加報告

華　景煜 †*† 伊豆 哲也 ‡ 櫻井 幸一 †

† 九州大学大学院　システム情報科学府
〒 819-0395 福岡市西区元岡 744
{huajingyu, sakurai}@itslab.csce.kyushu-u.ac.jp

‡ 富士通研究所
〒 211-8588 川崎市中原区上小田中 4-1-1
izu@labs.fujitsu.com

あらまし 本稿では、2011 年 6 月 1 日から 6 月 3 日まで、ギリシャ・ヘラクリオン市で開催された第 5 回 WISTP (The Fifth IFIP WG 11.2 International Workshop on Information Security Theory and Practice) に関して報告する。 会議の目標、歴史および主催者などを含む基本情報を紹介し、基調講演と採択された論文を概説する。

Report on the Fifth IFIP WG 11.2 International Workshop on Information Security Theory and Practice (WISTP 2011)

Jingyu Hua† Tetsuya Izu‡ Kouichi Sakurai†

†Graduate School of Information Science and Electrical Engineering, Kyushu University
744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan
{huajingyu, sakurai}@itslab.csce.kyushu-u.ac.jp

‡FUJITSU LABORATORIES Ltd.,
4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki, 211-8588, Japan
izu@labs.fujitsu.com

Abstract This paper reports on The Fifth IFIP WG 11.2 International Workshop on Information Security Theory and Practice (WISTP 2011) held during June 1-3, 2011, in Heraklion, Greece. We introduce the basic information of this workshop including its purpose, history, organizers, etc. We also introduce the Keynote speeches and several accepted papers.

1 はじめに

本稿では、2011 年 6 月 1 日から同月 3 日の間にギリシャ・ヘラクリオン市で開催された第 5 回 WISTP 2011 (The Fifth IFIP WG 11.2 International Workshop on Information Security Theory and Practice) [1] に関して報告する。

*NEC C&C財団国際会議論文発表者助成を受けたものである。
†中国国家留学基金管理委員会（Chinese Scholarship Council）の奨学金を受けている。

表 1: WISTP 2007〜2011 の概要

	開催地	開催期間	採択率	会議録
WISTP 2011	Heraklion, Greece	June 1-3	23% (19/83)	LNCS 6633 [2]
WISTP 2010	PASSAU, German	Apr.12-14	28% (20/69)	LNCS 6033
WISTP 2009	Brussels, Belgium	Sep. 1-4.	44% (12/27)	LNCS 5746
WISTP 2008	Sevilla, Spain	May. 13-16	34% (10/29)	LNCS 5019
WISTP 2007	Heraklion, Greece	May. 8-11	29% (20/68)	LNCS 4462

2 WISTP 2011 の概要

WISTP は IFIP の WG 11.2 (Security and Provacy of Mobile Devices in Wireless Communications) が主催する国際会議である。2007 年に初めて開催され、2011 年の開催で 5 回目である。今年度はギリシャ・ヘラクリオン市の Adelmar Royal Mare Village ホテルにて開催された。本会議はモバイル通信におけるセキュリティに関する話題を取扱い、モバイルデバイスのプライバシー保護の研究を目的としている。

表 1 に、今年度を含む過去 5 カ年（2007 年から 2011 年）の会議概要を示す。2007 から 2011 年の 5 カ年だけであるが、毎年５０件前後の投稿があり、20１１年は８３件 (WISTP の過去最高) で、この分野における関心の高さが伺われる。また、WISTP は、毎年特別なテーマを持っている。過去５カ年のテーマ を以下に示す。

- 2011: Security and Privacy of Mobile Devices in Wireless Communication
- 2010: Security and Privacy of Pervasive Systems and Smart Devices
- 2009: Smart Devices, Pervasive Systems, and Ubiquitous Networks
- 2008: Smart Devices, Convergence and Next Generation Networks
- 2007: Smart Cards, Mobile and Ubiquitous Computing Systems

2011 年の会議では、欧米及びアジア各国からの８３件の論文の投稿のうち（WISTP の記録）、２７件の論文が採択された。内、１９件が full paper、８件が short paper としての採択である。full paper 採択率は２２%で、過去５年と比較しても下がる傾向にあり、低い採択率であると言える。例年と同様に、WISTP2011 の会議録は Springer から LNCS として出版された。

WISTP ２０１１のプログラムは、３件の基調講演、２７件の講演形式での研究発表から構成された。２７件の講演形式の研究発表は、次に挙げる特定のテーマにより 8 セッションとしてまとめられた。行頭の記号 S-# はセッションを表す。

- S-1. Hardware Implementation
- S-2. Algorithms
- S-3. Security and Trust
- S-4. Security Attacks
- S-5. Lightweight Authentication
- S-6. Security and Cryptography
- S-7. Security Attacks and Measures (Short Papers)
- S-8. Mobile Authentication and Access Control & Mobile Application Security and Privacy

本会議には、約１０カ国から、４０名ほどの参加者があった。そのうち、アジアからの出席者は１０名であった（日本３名、中国１名、シンガポール３名、マレーシア３名）。

本節では以下に、基調講演およびプレナリ講演について紹介する。次節において、各セッション毎の研究発表について紹介する

3 基調講演

WISTP2011 ではキーノートセッションとして 3 つ のセッションが設けられた。これらのタイトル及び概要を次に示す。行頭の記号 K-# は基調講演を表す。

3.1 K-1. Polymorphic code as a solution against power attacks (Navid Naccache, Professor in Ecole Normale Superieure, France)

Naccache 教授らの研究紹介、サイドチャネルアタックに対する防衛手法として自己書き換えプログラムの利用が紹介された。現在の暗号プログラムを含むほとんどのソフトウェアは単一的なソフトウェアである。現在のソフトウェアは同じソースコードから同じコンパイラによって生成され，同じ OS の制御下にある同じプロセッサファミリによって実行される。このような単一性はアタックを容易にする。これらのメンバーのいずれか一つに対する攻撃はグループ全てのメンバーに対する攻撃として適用できる。Naccache 教授らの目的はソフトウェアの方向性を単一性から多様化に向ける事である。

3.2 New Developments in Hardware Intrinsic Security (Pim Tuyls, CEO of Intrinsic-ID)

PimTuyls 博士は、半導体 IP とハードウェア固有のセキュリティに基づく組み込みソフトウェア製品を販売する Intrinsic-ID[3] の CEO である。Intrinsic-ID はセキュリティソリューションの世界的なリーダーとして認識されている。彼は主にキーストレージデバイスの新製品の紹介を行った。現在のキーストレージ機器は生成した鍵をセキュリティ操作を行うデバイスに保存する。オフチップの秘密鍵ストレージには外部メモリとチップ間のバスを盗聴し論理解析器を利用する有能な攻撃者に対して脆弱性を持つ。彼らの製品は深いサブミクロン製造プロセスの多様性から生まれるデバイス固有の指紋から鍵を展開する。展開された鍵はデバイスの電源が入っていない時には存在しない。更に、鍵はチップの指紋 (PUF, Phisically Unclonable Function) から生成される為、与えられたデバイスに一意的に結び付けられ、鍵を別のデバイスで再現したり、正確な鍵を持つデバイスを製造したりすることはできない。

3.3 eID and eSignature with mobile devices - a contribution to the Digital Agenda (Reinhard Posch, Professor in The Institute for Applied Information Processing and Communications)

Posch 教授はオーストリアの行政機関と電子政府における ICT (Information and Communication Technologies) の調整機関のプラットフォーム“ Digital Austria ”の先頭に立つ。彼は初めに「Secure idenTity acrOss boRders linKed」(STORK) プロジェクト [4] を紹介した。STORK プロジェクトは、企業や市民、政府の公務員が欧州連合のいずれの国でも国家電子識別子 (eID) を利用出来るようにすることを目的とした 3 年間の取り組みである。そのようなシステムは，EU の国境を超えた公的サービスに安全にオンラインで接続する手段を提供することで行政手続を簡単化する。次に，彼は我々が eID をクラウドに適用する上で直面する挑戦課題として、non-natural person への対応、モバイル機器への対応、クラウド基盤との対応、が紹介された。

4 WISTP ２０１１ 本会議における発表

WISTP201 1 発表された full paper を以下に示す。行頭の記号 F-# は full paper を表す。(発表順)

F1. A Cryptographic Processor for Low-Resource Devices: Canning ECDSA and AES like Sardines Michael Hutter (Institute for Applied Information Processing and Communications) et al.

F2. An Evaluation of Hash Functions on a Power Analysis Resistant Processor Architecture Simon Hoerder (University of Bristol) et al.

F3. A Comparison of Post-Processing Techniques for Biased Random Number Generators Siew-Hwee Kwok (DSO National Laboratories) et al.

F4. Formal Framework for the Evaluation of Waveform Resynchronization Algorithms Sylvain GUILLEY (TELECOM-ParisTech) et al.

F5. Solving DLP with Auxiliary Input over an Elliptic Curve Used in TinyTate Library Yumi Sakemi (Okayama University) et al.

F6. Information Leakage Discovery Techniques to Enhance Secure Chip Design Alessandro Barenghi (The Dipartimento di Elettronica e Informazione) et al.

F7. Formal Analysis of Security Metrics and Risk Leanid Krautsevich (University of Pisa) et al.

F8. STORM - Collaborative Security Management Environment Theodoros Ntouskas (University of Piraeus) et al.

F9. Trust Agreement in Wireless Mesh Networks Andreas Noack (Ruhr University Bochum) et al.

F10. A SMS-Based Mobile Botnet Using Flooding Algorithm Jingyu Hua (Kyushu University) et al.

F11. FIRE: Fault Injection for Reverse Engineering Manuel San Pedro (Institut TELECOM) et al.

F12. Hardware Trojan Side-Channels Based on Physical Unclonable Functions Marc X. Makkes (Eindhoven University of Technology) et al.

F13. SSL/TLS Session-Aware User Authentication Using a GAA Bootstrapped Key Chunhua Chen (South China University of Technology) et al.

F14. An Almost-Optimal Forward-Private RFID Mutual Authentication Protocol with Tag Control Paolo D ’Arco (Dipartimento di Informatica)

F15. Affiliation-Hiding Authentication with Minimal Bandwidth Consumption Bertram Poettering (Technische Universitat Darmstadt) et al.

F16. AES Variants Secure Against Related-Key Differential and Boomerang Attacks Jiali Choy (DSO National Laboratories) et al.

F17. Leakage Squeezing Countermeasure Against High-Order Attacks Houssem Maghrebi (TELECOM ParisTech) et al.

F18. Mobile Electronic Identity: Securing Payment on Mobile Phones A.W. Roscoe (Oxford University) et al.

F19. Role-based Secure Inter-operation and Resource Usage Management in Mobile Grid Systems Antonios Gouglidis (, University of Macedonia) et al.

採択率２３％で選ばれた各論文は、いずれも興味深い内容であった。 本稿では、無線ネットワーク運用におけるセキュリティの実現に関し、実用性と有効性の観点から筆者が興味を持った４つの論文を紹介する。

1. 最優秀論文賞： 高次攻撃に対しての漏洩削減対策 [Leakage Squeezing Countermeasure Against High-Order Attacks, by Houssem Maghrebi, researcher in TELECOM-ParisTech]

近年、サイドチャネルアタックが広く研究されている。特に、差分電力解析（DPA）攻撃に対する効率的な防止策の開発が行われている。マスキングは防止策の中のメジャーなアプローチの一つである。しかしながら、マスキングの実装はより高次命令の DPA 攻撃によって破られる。そこで著者は「leakage　squeezing」と呼ばれる新しい高次命令の DPA 攻撃に対する防衛を行う手法を提案する。彼らは漏洩分布が処理されたデータからほとんど独立となるような特別に構成した全単射となるマスクパスのインスタンスにより内部クラスの分散を削減する。

2. 学生論文賞：　帯域幅最小使用量の所属隠ぺい認証　[Affiliation-Hiding Authentication with Minimal Bandwidth Consumption, by Bertram Poettering, Ph.D. student in Technische Universitat Darmstadt]

所属隠ぺい認証 (AHA) プロトコルはユーザが所属をグループの外部に明らかにすることなく、互いにグループのメンバーであると認証できる矛盾した性能を有する。ユーザ毎に複数のグループを管理するようなグループ発見の分散においては特に興味深いものである。解の一致は近年導入され始めたにすぎず、更にユーザと所属毎に数キロビットもの高い帯域幅の消費と、現実的なアプリケーションのシナリオ内はそこそこの性能しか持たないという二つの欠点を持つ。この研究の貢献は新しく高効率的な接続可能グループ発見型 AHA/KE プロトコルの構築である。このプロトコルは以下の点において既存のプロトコルよりも優れている。第一に、このプロトコルは実際に $O(nlogn)$ の解決時間を持つ初のプロトコルである。第二にプロトコルの帯域幅は目覚ましく小さい。これらのプロトコルは携帯電話のような限定的なデバイス上に配置可能なプライバシー保護技術を与える。

3. 筆者からの発表 (1): Solving DLP with Auxiliary Input over an Elliptic Curve Used in TinyTate Library, by Tetsuya Izu, researcher in FUJITSU LABORATORIES Ltd

近年、ペアリングと呼ばれる関数を利用したさまざまな暗号プロトコルが提案されている。しかし、これら暗号の安全性は新しく導入された数学的問題に根拠を置いているため、これら問題の詳細な解析は必須である。本論文では、TinyTate という組み込み機器向けペアリング暗号ライブラリが使用するパラメータにおいて、補助入力付き離散対数問題と呼ばれる数学的問題が実際に解けたことを報告するとともに、いくつかの暗号プロトコルの安全性に与える影響を指摘する。

4. 筆者からの発表 (2): フラッディングアルゴリズムを用いたショートメッセージサービスに基づく移動ボットネット [A SMS-Based Mobile Botnet Using Flooding Algorithm, by Jingyu Hua]

携帯電話の役割が重要になってくるにつれて、それは攻撃者にとっても格好の標的となってきた。実際、ここ数年間で携帯電話を標的とした多くのマルウェアがすでに見つかっている。この時、それらのマルウェアに感染した携帯電話がボットネットに利用されるかどうかという問題が重要になる。そこで本研究では、指揮統制に SMS を利用したボットネットの構築に取り組みその評価を行った。設計したボットネットは SMS を通じてコマンドを伝播する際に，より簡単な flooding アルゴリズムを用いるので、コマンドの伝播速度とステルス性が遥かに向上している。シミュレーションでは、SMS ボットネットはとても効率的に命令を伝達することが可能で、1 つの命令を 20 分間でボットネット全体の 90 %に伝達することが可能であった。さらに，命令伝達プロセスにおいて，各携帯電話は最大でも四つの SMS を伝播するだけでボットネットが機能することが確認できた。本研究ではその SMS ボットネットの対策手法についても取り組んだ。

5　本人の知見

WISTP は比較的小規模な学会であり、参加者は 40 人ほどあった。発表された内容は、ほと

んどがモバイルデバイスのセキュリティ、特にハードウェア暗号に関するものであった。参加者のほとんどは、この分野において先導的な立場を担っているヨーロッパの研究所の人々であった。彼らの研究の焦点は，従来のパーソナルコンピュータから、モバイルデバイスへとシフトしている。彼らによると,「Internet of Things」というコンセプトは，最近ヨーロッパでも非常にホットな話題であり、政府もこの分野における研究と産業の発展を後押ししている。会議では、参加者同士で非常に活発な議論が行われた。また、会議が行われたヘラクリオン島は非常に美しい場所だった。

6 WISTP 2012 について

来年の WISTP は、イギリスで開催予定であるとアナウンスされた。会期、会議場及び研究発表講演を行うための論文の投稿〆切等の募集要項の詳細については、未だ公表されていない((201 1 年6 月末日現在)。

7 おわりに

本稿では、201 1 年6 月1 日から同月3 日の間に、ギリシャ. ギリシアヘラクリオンで開催された第 5 回 WISTP 2011 (The 5th Workshop in Information Security Theory and Practice) に関して、その概要を紹介した。さらに、WISTP 2010 本会議で発表されたモバイルデバイスのセキュリティに関するいくつかの研究について概要を示した。

参考文献

[1] The 5th Workshop in Information Security Theory and Practice (WISTP 2011), http://www.wistp.org/

[2] Information Security Theory and Practice: Security and Privacy of Mobile Devices in Wireless Communication. Springer LNCS, Vol. 6633. 2011, http://www.springer.com/computer/communication+networks/book/978-3-642-21039-6

[3] Intrinsic-ID Company, http://www.intrinsic-id.com/

[4] STORK project, https://www.eid-stork.eu/