Vol.2015-CSEC-71 No.8
2015/12/4

国際会議 S&P2015 参加報告

穴田 啓晃†

概要：国際会議 S&P (IEEE Symposium on Security and Privacy) は，IEEE により毎年米国カリフォルニア州で開催される情報セキュリティのトップカンファレンスである．第 36 回を数える今回も，投稿数 402 件に対し採択数が 55 件と（採択率 13.7%），選りすぐりの研究発表がなされた．S&P2015 本体の他，併催ワークショップも 5 つ開催され，合わせて計 4 日間，聴講者数は全体で 400 名程であった．セッション数は 14 であり，"Protocols and Network Security"や"Malware and Program Analysis"といった定番のセッションテーマの他，"Cryptocurrencies and Cybercrime"や"Android Security"といったここ数年のものもあった．本稿では開催情報及び興味深い研究発表についてのリポートする．

キーワード：国際会議，リポート，情報セキュリティ，プライバシ，S&P.

A Report on International Conference S&P2015

HIROAKI ANADA†

Abstract:. International conference S&P (IEEE Symposium on Security and Privacy) is the top conference of information security held every year in California, U.S.A. by IEEE. At this time to count the 36th, 55 well-selected papers from 402 submissions (13.7% of acceptance rate) were presented. Other than the main body of S&P2015, five co-located workshops were held. They were held for in total four days, and the number of the attendees was approximately 400 altogether. The number of the sessions was 14, and, other than a basic session theme such as "Protocols and Network Security" and "Malware and Program Analysis", there were the things of these past several years such as "Cryptocurrencies and Cybercrime" and "Android Security". This is a report about holding information and interesting presentation of the results of the study.

Keywords: international conference, report, information security, privacy, S&P.

1. はじめに

S&P (IEEE Symposium on Security and Privacy) は，毎年米国カリフォルニア州で開催される，情報セキュリティやプライバシを主題とする国際会議である．S&P は情報セキュリティの分野の四大トップカンファレンスの中でもトップとされており，例えば米国では博士課程の学生やポスドクがこの国際会議での講演実績を一つのステータスシンボルとしているそうである．本リポートでは，著者が参加した 2015 年の S&P （S&P2015）について，研究発表の概要や所感と共に，移動手段や宿泊といった参加付帯情報もお伝えしたい．以下，まず付帯情報から，次いで研究発表について綴る．

S&P2015 は，シリコンバレーの一角であるサンノゼ（San Jose）にあるフェアモントホテルを会場として開催された．最寄りの空港はサンノゼ国際空港（SJC）であった．空港からの移動には米国内チェーンのシャトルバンである“Supershuttle” を利用した．事前予約で往復 98USD で，チップも含めると 120USD であった. 会場までは 20 分程であったから，割高感は否めない．後ほど聞いたところでは，シリコンバレーでは（シャトルバンやタクシーに限らず）高めの料金とのことであった．

会場付近にはバスやトラム（図 1）が走っており，（高級な）会場ホテル（図 2）に宿泊する必要は必ずしもない．著者の場合は, 徒歩で 30 分程の距離の比較的安価なホテルから徒歩で通った．食事処は，日本の飲食店街のように密集している訳ではないが，見つけるのは容易であった．ハンバーガー，中華，肉料理等，選ぶことができる．

図 1　会場付近の交通手段（上：バス／下：トラム）

†公益財団法人九州先端科学技術研究所
Institute of Systems, Information Technologies and Nanotechnologies

図 2　上：会場のフェアモントホテル・サンノゼ．下：会場の入り口付近（第 1 日午前）．

会話はもちろん英語なわけだが，東海岸よりも“下手な英語”に寛容に対応してもらえる気がした．もっともこれは著者の構え方にも要因があるかもしれない．

S&P2015 本体はシングルセッションで進行したため，じっくりと聴講することができた．これは他の情報セキュリティトップカンファレンスと比較すると，Network and Distributed System Security Symposium (NDSS)と似ていて，ACM Conference on Computer and Communications Security (ACM-CCS)のパラレルセッションとは異なる（USENIX は未参加のため不明）．著者の主観に過ぎないが，S&P と NDSS は情報セキュリティの中でも広範囲に影響が及ぶ研究発表が多く，これに対し ACM-CCS は「狭くとも深く」の精神のようである．(なのでシングル／パラレルの使い分けがなされているのではないだろうか．)

2. 開催概要

本節では，編集委員，投稿状況・査読プロセス，参加状況，セッション構成について触れる．

2.1 組織委員

編集委員は下記の 18 種から成るものであった．

1) General Chair
Sean Peisert, UC Davis/Lawrence Berkeley National Lab.
2) Program Chairs
Lujo Bauer, Carnegie Mellon University
Vitaly Shmatikov, University of Texas, Austin
3) Vice Chair / Registration
Michael Locasto, University of Calgary
4) Treasurer
Mark Gondree, Naval Postgraduate School
5) Donations Chair
Jason Li, Intelligent Automation, Inc.
6) Publications Chair
Kevin Butler, University of Florida
7) Site Chair
Cara Candler, Executivevents, Inc.
8) Registration Manager
Yvonne Lopez, Executivevents, Inc.
9) Publicity Chair
Anuja Sonalker, TowerSec
10) Student Travel Committee Chair
Alvaro Cárdenas, UT Dallas
11) Co-Student Travel Committee Chair
Cliff Wang, US Army Research Office
12) Poster Chair & Co-Publications Chair
Sophie Engle, University of San Francisco
13) Web Chair
Sean Whalen, UC San Francisco
14) Workshops Chair
Cynthia Irvine, Naval Postgraduate School
15) Co-Publicity Chair / Workshops Vice Chair
Zachary Peterson, Cal Poly
16) Co-Treasurer & Workshops Treasurer
Gabriela Ciocarlie, SRI International
17) Co-Publications Chair / Workshops Publications Chair
Ashley Podhradsky, Dakota State University
18) General Chair Emeritus
Greg Shannon, Carnegie Mellon University

2.2 投稿状況・査読プロセス

投稿と査読プロセスについて program chair から説明があったので（図 3），以下にまとめる．

投稿数：**402 件**
Round 0：-
：**386 件**
Round 1：2 reviewers/paper, identify top 50%
：**195 件**
Round 2：1-3 additional reviewers / Author responses
：**216 件**
Round 3：+10 days online discussion (including 21 papers that did not receive Round 2 reviews / In-person 1.5 day PC meeting (94 papers discussed)
採択数：**55 件**
採択率：**55/402=13.7%**
Reviews: 1216 / Comments: 1929

今回は昨年と比較して，投稿数が 333 件から 20%増，採択数が 44 件から 25%とのことで，多かったそうである．

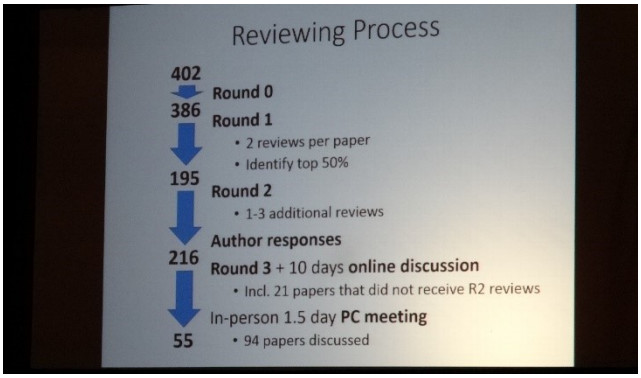

図 3　投稿状況と査読プロセス．Program chair より説明された．

2.3 参加状況

参加者数は目測で 400 人ほどであった（図 4）．オープニング時はほぼ満席であり，本トップカンファレンスの人気の高さを感じさせた．確かにプレゼンは聴いていて引き込まれるものが多く，一言で申して，スライドを見ないでも力点が分かる気がするのが特徴と言える．

図 4　会場の様子．シングルセッションでじっくり聴講．

2.4 セッション構成

S&P2015 のセッション構成を表 1 に，併催ワークショップを表 2 に示す．

S&P2015 では“Cryptocurrencies and Cybercrime”が新セッションであった．また，パネルディスカッションは豪華メンバーが集まり，研究予算の投じられる『重点領域』に関する貴重な意見を聴くことができた（後述）．

表 1　S&P2015 セッション構成．

Date	No.	Session
May 18	1	Hardware-Aided Security
	2	Cryptocurrencies and Cybercrime
	3	Protocols and Network Security
	4	Cryptographic Protocols
	-	Poster Reception
May 19	5	ORAM and Secure Multi-Party Computation
	6	Security du Jour
	7	Protocols
	8	Side Channels
	9	Short Talks
May 20	10	Malware and Program Analysis
	11	Memory Integrity
	12	Security du Jour II
	13	Android Security
	14	NITRD Panel: 2015 Federal Cybersecurity R&D Strategic Plan

表 2　併催ワークショップ．

Date	No.	Session
May 21	1	IWPE: First International Workshop on Privacy Engineering
	2	GenoPri: Second International Workshop on Genome Privacy and Security
	3	LangSec: Second Workshop on Language Theoretic Security
	4	MoST: Mobile Security Technology
	5	W2SP: Web 2.0 Security and Privacy

3. 聴講した研究発表の概要，所感

本節では，聴講した研究発表の中から興味深く感じたものについてその概要を述べ，所感を記す．

3.1 S&P2015 本セッション

Cryptocurrencies and Cybercrime

“Research Perspectives and Challenges for Bitcoin and Cryptocurrencies”

Joseph Bonneau (Princeton University), Andrew Miller (University of Maryland), Jeremy Clark (Concordia University), Arvind Narayanan (Princeton University), Joshua A. Kroll (Princeton University), Edward W. Felten (Princeton University)

本発表は，2009 年の運用開始以来，劇的に普及した暗号通貨 Bitcoin の，技術的な本質まとめたものであった（サーベイ論文）．その本質とは次の三要素から成るとする：取引とその記述様式（transactions & script），合意形成とマイニング（consensus & mining），P2P 通信ネットワーク（peer-to-peer communication network）．これら三要素の簡潔な紹介の後，著者らはセキュリティとプライバシに対する攻撃手法の既存研究をまとめている．最新技術の現況を知るのに有用な参考文献となると思われた．

“The Miner's Dilemma”

Ittay Eyal (Cornell University)

本研究発表は“Block withholding attack”の新たな解析について論じていた．ユーザ間で次々と行われる取引きの履歴を一定時間幅毎に区切った個々の集合がブロックであるが，これを故意に更新せずに，という攻撃である．論文ではその成功確率について論じている．

Protocols and Network Security

“Temporal Lensing and its Application in Pulsing Denial-of-Service Attacks”

Ryan Rasti (UC Berkeley, ICSI), Mukul Murthy (UC Berkeley), Nicholas Weaver (UC Berkeley, ICSI), Vern Paxson (UC Berkeley, ICSI).

本研究発表は分散型リフレクション攻撃の強力な一手法を提案したものであった．提案攻撃手法は，低い帯域幅の信号を高い帯域幅の信号に集中化する（“lensing”）ことを可能にするため，近年見られる「100Gbps 超 DDoS 攻撃」の一手法となりうる．提案攻撃手法の要点はルーティングパスの時間評価であり（“Estimating Attack Path Latencies”）確率評価に基づきリフレクションをスケジューリングすることを可能にする．分散型リフレクション攻撃の対策を研究する方々には一読の必要があると思われた．

図 5　意見交換で賑わっていたブレイクタイムの様子．

Cryptographic Protocols

“Geppetto: Versatile Verifiable Computation”

Craig Costello (Microsoft Research), Cédric Fournet (Microsoft Research), Jon Howell (Microsoft Research), Markulf Kohlweiss (Microsoft Research), Benjamin Kreuter (Google), Michael Naehrig (Microsoft Research), Bryan Parno (Microsoft Research), Samee Zahur (University of Virginia)

本研究発表は，検証可能移譲計算の効率的な手法を提案したものであった．スマートフォン等で必要な計算結果に対し，計算はクラウド上の豊かな計算資源に委譲し結果のみ送信してもらう研究はここ 10 年ほど盛んである．提案方式の Geppetto は Quadratic Arithmetic Program (QAD) のマルチ版（multi-QAD）に基づくもので，これまでの研究の流れを汲みつつ推し進めた結果とのことである．

“Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs”

Eli Ben-Sasson (Technion), Alessandro Chiesa (ETH Zurich), Matthew Green (Johns Hopkins University), Eran Tromer (Tel Aviv University), Madars Virza (MIT)

本研究発表は，common reference string (crs)を証明者と検証者が共有するのにマルチパーティ計算(MPC)を使うアプローチを取り，これを succinct ゼロ知識証明に利用する提案であった．後述のように，crs を共用する新しいアプローチには MPC を使うものの他に proof-of-work を使うものもあるのではないだろうか．

Poster Reception

S&P2015 ではバンケットが無く，ポスターレセプション（軽食を摂れる）があった．40 程度の数のポスターが展示された会場では，説明員と閲覧者が意見を交わす光景が多数見受けられ，賑わっていた．

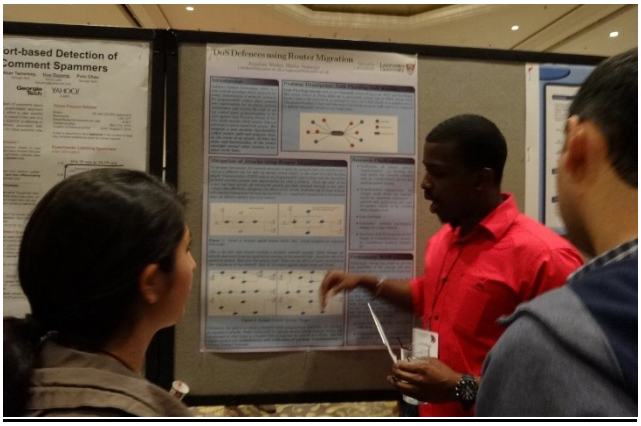

図 6　ポスターセッション．写真は DoS 攻撃の緩和手法を提案したもの．

Protocols

“Post-quantum key exchange for the TLS protocol from the ring learning with errors problem”

Joppe W. Bos (NXP Semiconductors), Craig Costello (Microsoft Research), Michael Naehrig (Microsoft Research), Douglas Stebila (Queensland University of Technology)

本研究発表は，耐量子鍵交換プロトコルを提案したものであった．耐量子では主流方式といえる Ring LWE の技術によるアプローチを取り，性能評価を行い，TLS プロトコルへの適用可能性まで論じていた点は注目に値する．ただし，暗号化とデジタル署名については提案しておらず，この領域の研究がまだ発展途上であることを伺わせた．

Short Talks

10 件ほどプレゼンテーションがあった. 特に Tamassia 教授らのゼロ知識証明の適用等，道具として有用なものは何でも使うという姿勢が感じられ, 引き込まれるものがあった.

NITRD Panel: 2015 Federal Cybersecurity R&D Strategic Plan

本セッションはパネルディスカッションであった．パネリストは次の四つの機関から招かれていた.

1) Homeland Security Advanced Research Projects Agency
2) NIST
3) DOD Cyber Security & Technology
4) National Science Foundation

パネリストによって意見の相違はあったものの，今後米国において研究資金が投入されるべき（情報セキュリティの）重要領域は下記のキーワードによるとのことであった.

- Cyber-Physical Systems
- Smart Grid
- Authentication -National Strategy for Trusted Identities in Cyberspace-
- Privacy Engineering
- Security Automation & Continuous Monitoring
- Data Analysis
- Cloud
- Risk Management
- Supply Chain Risk Management
- Education / Workforce – National Initiative for Cybersecurity Education

図 7　パネルディスカッション.「何の新しい話題が（重点領域に）含められるべき？」.

3.2 併催ワークショップ

IWPE: First International Workshop on Privacy Engineering

“Decentralizing Privacy: Using Blockchain to Protect Personal Data”

Guy Zyskind, Oz Nathan and Alex ’sandy' Pentland

信頼できる第三者機関を, peer-to-peer ネットワークと block chain の組み合わせでシミュレートするアイデアについての研究発表であった．先に述べたように，例えば common reference string (crs) の共用を，マルチパーティ計算 (MPC) でなくこちらのアプローチで行う方法もありそうである.

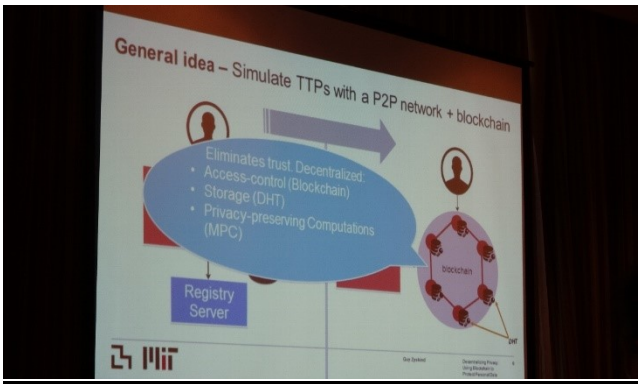

図 8　Trusted third party に取って替わる分散型管理.

4. むすび

S&P2015 では研究領域へのインパクトのみならず，社会への影響も考えられる重要な研究発表があったように思う. プレゼンテーションは，トップカンファレンスらしい質であった．日本人の参加者は会議中 2 名様のみ見掛けた（コンタクトできた）が，もっと多くの方が参加なさってもよいのではないだろうか.

謝辞　著者は本コンピュータセキュリティ研究会への参加に関し下記の支援を受けております.
日本学術振興会 科研費／研究課題番号：15K00029／研究課題名：「対話型証明と秘密分散に基づく認証方式・署名方式の設計及び安全性評価」

参考文献

1) 36th IEEE Symposium on Security and Privacy (S&P20215) http://www.ieee-security.org/TC/SP2015/index.html