IEEE Symposium on Security and Privacy 2014 参加報告

川本 淳平 †§　　須賀 祐治 ‡

† 九州大学
819-0395 福岡県福岡市西区元岡 744
kawamoto@inf.kyushu-u.ac.jp

§ 九州先端科学技術研究所
814-0001 福岡市早良区百道浜 2-1-22

‡ 株式会社インターネットイニシアティブ
102 − 0071 東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
suga@iij.ad.jp

あらまし 本稿では, 2014 年 5 月 18 日から 21 日の 4 日間, サンノゼ THE FAIRMONT にて開催された IEEE Symposium on Security and Privacy 2014 (S&P 2014) に関し, その内容を報告する.

A Report of IEEE Symposium on Security and Privacy 2014

Junpei Kawamoto†§　　Yuji Suga‡

†Kyushu University
744 Motooka, Nishi-ku, Fukuoka 819-0395, JAPAN
kawamoto@inf.kyushu-u.ac.jp

§Institute of Systems, Information Technologies and Nanotechnologies
2-1-22 Momochihama, Sawara-ku, Fukuoka 814-0001, JAPAN
‡Internet Initiative Japan Inc.
Iidabashi Grand Bloom 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, JAPAN
suga@iij.ad.jp

Abstract We report about IEEE Symposium on Security and Privacy 2014 (S&P 2014) which was held in San Jose, CA, USA in May 18-21, 2014.

1　はじめに

IEEE Symposium on Security and Privacy は, IEEE Computer Society's Technical Committee on Security and Privacy の主催により, 毎年 5 月に開催されるトップ会議の一つである. 第 35 回目となる今年は, 5 月 18 日から 21 日の 4 日間, 米国カリフォルニア州サンノゼの The Fairmont Hotel (図 1) にて開催された. 主催者発表によると, 参加者は 482 名で発表はワークショップも含め 82 件であった.

本会議はシングルセッションであり, 広い会場 (図 2) に一同が会し, 落ち着いて発表を聞くことができた. 主なセッションは次の通りであった.

- Attacks
- SSL/TLS
- Automation
- Systems Security
- Privacy and Anonymity
- Android

図 1: 会場となった The Fairmont Hotel.

図 2: 会場の様子.

- E-Cash
- Secure Computation and Storage
- Authentication

Security and Privacy という名を冠してはいるが，セキュリティよりの発表が多かったように思えた.

本会議における各賞は次の通りである.

Best Paper Award University of Warsaw の Marcin Andrychowicz らによる，“Secure Multiparty Computations on Bitcoin”[1]

Best Practical Paper Award University of Texas at Austin の Chad Brubaker らによる，“Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations”[3]

Best Student Paper Award Vrije Universiteit Amsterdam の Erik Bosman らによる，“Framing Signals — A Return to Portable Shellcode”[2] と，Carnegie Mellon University の Shayak Sen らによる，“Bootstrapping Privacy Compliance in Big Data Systems”[4]

また，併設ワークショップは次の 7 つが開催された.

- CREDS: Cyber-security Research Ethics Dialog & Strategy
- DUMA: 4th International Workshop on Data Usage Management
- MoST: Mobile Security Technologies
- IWCC: International Workshop on Cyber Crime
- LangSec: A Workshop on Language Theoretic Security
- WRIT: 2nd Workshop on Research for Insider Threat
- W2SP: Web 2.0 Security and Privacy

2 論文紹介

本節では，いくつかの論文を簡単に紹介する.

Sonoma State University の John P. Sullins による “A Case Study in Malware Research Ethics Education: When Teaching Bad is Good” はマルウェア研究者の倫理について論じたものである．研究目的で記録した情報の取り扱いや研究上の通信占有における倫理問題並びに実証実験のために人工データを利用する場合であっても配慮すべき問題について提起されていた．Birla Institute of Technology and Science-Pilani の Pratik Narang らによる “PeerShark: Detecting Peer-to-Peer Botnets by Tracking Conversations” では，peer-to-peer 型ボットネット通信の検出に関する研究で，ボット間の通信データからボットネットを検出する手法を提案している．具体的には，断続的な通信からボット間のコマンド伝達シーケンスを復元し分類している.

Best Paper Award を受賞した “Secure Multiparty Computations on Bitcoin”[1] は，セキュアマルチパーティ計算に BitCoin プロトコルを応用する研究である．BitCoin には，ある時間内に秘密情報を計算できなければ罰を負うという，‘timed commitments’ のアイデアがある．彼らは，このアイデアを応用したセキュアマルチパーティ計算における公平性の保証について議論している．また，著者らによれば，通常のセキュアマルチパーティ計算では信頼できる第三者のシミュレーションするプロトコルを用いており，正しい入力に対して期待する結果が得られているか否かは定義外であるという．一方，BitCoin におけるトランザクション処理を応用することで，入出力の正当性を保証する定義について議論している．

Best Practical Paper Award を受賞した “Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations” は，SSL/TLS プロトコルにおける検証における大規模な adversarial testing を提案している．提案手法の特徴の一つは，frankencerts と呼ばれランダムに突然変異させた人工的な証明書を用いてテストを行う．この frankencerts を用いることで，普段使われないコンディションや稀な値に対するテストが行えるという．二つ目の特徴は，differential testing と呼ばれ，ある SSL/TLS 実装が受け付けた証明書が他の実装では拒絶された場合，どちらかは間違っているという事実を用いる．この食い違いを，個別の実装における欠陥を発見する為のオラクルとして用いている．

Best Student Paper Award を受賞した “Framing Signals — A Return to Portable Shellcode” は，Unix システムにおけるシグナル処理に関する研究である．シグナル処理は Unix システムの中心的な機能であり，バックドア攻撃の突破口となり得る．著者らは，新しい攻撃手法である Sigreturn Oriented Programming (SROP) を導入している．Return-oriented programming (ROP) 同様に，SROP でも攻撃者が挙動を変更できる weird machine を作成する．そしてシグナルフレームを作成しカーネルの知らないシグナルに対する返答を準備しこの weird machine をコントロールし攻撃に用いるという．また，“Bootstrapping Privacy Compliance in Big Data Systems” は，ビッグデータ，クラウドコンピューティングにおけるプライバシ問題に取り組んでいる．通常，クラウドサービスにおけるプライバシはプライバシポリシという形で述べられていることが多い，しかし，これらのポリシが満足されているのか否かの検査は人手によるレビューや監査などが主流であり十分保証されているとは言えない．著者らは，大規模な検索エンジンにおけるプライバシポリシの管理方法に付いて述べている．彼らは，プライバシポリシの記述言語である LEGALEASE と Map-Reduce に似たデータ処理システムを用いて，人々のデータを処理しているとのことである．なお，本システムは実際に一年以上にわたって運用されているとのことであった．

3 おわりに

2014 年の IEEE Symposium on Security and Privacy (S & P 2014) の模様を報告した．今年の S & P では，日本からの発表はポスター発表 1 件のみであり，参加者は我々も含め 5 名程度であった．2015 年は，5 月 18 日から 20 日にかけて，今年と同様に米国カリフォルニア州サンノゼにある The Fairmont Hotel にて開催される．

謝辞

本報告の一部は，総務省による「国際連携によるサイバー攻撃の予知技術の研究開発 (PRACTICE)」の支援を受けている．

参考文献

[1] Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek. Secure multiparty computations on bitcoin. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*,

SP '14, pages 443–458, Washington, DC, USA, 2014. IEEE Computer Society.

[2] Erik Bosman and Herbert Bos. Framing signals - a return to portable shellcode. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, SP '14, pages 243–258, Washington, DC, USA, 2014. IEEE Computer Society.

[3] Chad Brubaker, Suman Jana, Baishakhi Ray, Sarfraz Khurshid, and Vitaly Shmatikov. Using frankencerts for automated adversarial testing of certificate validation in ssl/tls implementations. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, SP '14, pages 114–129, Washington, DC, USA, 2014. IEEE Computer Society.

[4] Shayak Sen, Saikat Guha, Anupam Datta, Sriram K. Rajamani, Janice Tsai, and Jeannette M. Wing. Bootstrapping privacy compliance in big data systems. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, SP '14, pages 327–342, Washington, DC, USA, 2014. IEEE Computer Society.