IEEE Symposium on Security and Privacy における研究動向調査

田端　利宏†　　櫻井　幸一†

†九州大学　大学院システム情報科学研究院
812-8581　福岡市東区箱崎 6-10-1

{tabata, sakurai}@csce.kyushu-u.ac.jp

あらまし　本稿では，2004 年 5 月 10 日から 12 日にかけてアメリカ合衆国のカリフォルニア州オークランドで開催された 2004（第 25 回）IEEE Symposium on Security and Privacy の参加報告，および同シンポジウムの研究動向の調査結果について述べる．（http://www.ieee-security.org/TC/SP2004/oakland04.html）

A Survey of IEEE Symposium on Security and Privacy

Toshihiro Tabata†　　Kouichi Sakurai†

†Faculty of Information Science and Electrical Engineering, Kyushu University
6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-8581 Japan
{tabata, sakurai}@csce.kyushu-u.ac.jp

Abstract　This paper reports the 2004 (25th) IEEE Symposium on Security and Privacy held on 10-12 May 2004 in Oakland, California, USA. A survey of research trends on this symposium is also presented. (http://www.ieee-security.org/TC/SP2004/oakland04.html)

1　はじめに

本稿では，2004 年 5 月 10 日から 12 日にかけてアメリカ合衆国のカリフォルニア州オークランドで開催された 2004 IEEE Symposium on Security and Privacy の参加報告について述べる．また，近年の同シンポジウムの研究動向の調査を行った結果について述べる．

2　IEEE Symposium on Security and Privacy 概要

IEEE Symposium on Security and Privacy は，1980 年から毎年開催されており，2004 年で 25 回目である．このシンポジウムは，コンピュータセキュリティや電子セキュリティにおける進展を発表し，これらの分野の研究者や参加者を結び付けている会議である．このシンポジウムは，IEEE Technical Committee on Security and Privacy が主催し，International Association for Cryptologic Research の共催で開催されている．このシンポジウムで扱う主なテーマ（2004 年の Call for papers からの抜粋）を以下に示す．

Commercial and Industrial Security,
Mobile Code and Agent Security,
Network Security,

Data Integrity,
Information Flow,
Viruses and Other Malicious Code,
Authentication,
Secure Hardware and Smartcards,
Intrusion Detection,
Language-Based Security,
Security of Mobile Ad-Hoc Networks,
Electronic Privacy,
Distributed Systems Security,
Anonymity and Pseudonymity,
Access Control and Audit,
Security Verification,
Security Protocols,
Biometrics,
Peer-to-Peer Security,
Database Security,
Denial of Service

3 2004 年の参加報告

2004 年 5 月 10 日から 12 日にかけてアメリカ合衆国カリフォルニア州オークランドで開催された IEEE Symposium on Security and Privacy の論文題目とその概要について簡単に述べる.

3.1 参加報告

カリフォルニア州オークランドの Claremont Resort で開催された. 投稿論文 186 件のうち, 採録は 19 件である. 事前参加登録者数は 178 人で, 実際の各セッションの参加人数は 100 人弱〜200 人強であった. なお, 日本からの参加者は確認できただけで 2 名であった.

3.2 発表論文の概要

Session: Attacks and Defenses

Keyboard Acoustic Emanations (Dmitri Asonov et al.)

キーボードを押す音で, どのキーが押されているかを推測する手法とその問題点, および対処法について述べている. 具体的には, キーボードの音を録音し, その特徴を取り出し, ニューラルネットを用いて学習する. 精度を改善した結果, キー 30 個に対し, 80〜95 %の認識率を示した. 対策としては, silent keyboard が有効であると主張している.

Effects of Mobility and Multihoming on Transport-Protocol Security (Tuomas Aura et al.)

トランスポート層のセキュリティに関する論文. IETF で提案されている The Stream Control Transmission Protocol (SCTP) の問題点を指摘し, 具体的な攻撃方法と改善策を示している.

Analysis of an Electronic Voting System (Tadayoshi Kohno et al.)

電子投票システムの分析についての発表. パンチカードによる方法では, 精度に問題があり, 置き換えるべきだというのが発表者の研究動機であった. SMARTCARDS, CRYPTOGRAPHY, SOFTWARE ENGINEERING の観点から, 電子投票システムについて論じている.

Panel: Electronic Voting Dan Wallach (Rice), Dana DeBeauvoir (County Clerk, Travis County, TX), Josh Benaloh (Microsoft Research)

電子投票について論点のまとめとパネラーの方の解説.

- Voter anomity
- Auditability for results
- Fast result
- Human facters / accessibility
- 投票形式
- Overvoting
- Digital signature on ballots

Session: Theory of Access Control

Access Control By Tracking Shallow Execution History (Philip W. L. Fong)

実行履歴を基にしたアクセス制御の提案. shadow

access history の後を追うことで，強制可能なセキュリティポリシの特徴を提供できる shadows history automata を導入している．

A Layered Design of Discretionary Access Controls with Decidable Safety Properties (Jon A. Solworth et al.)

Discretionary Access Control (DAC) を三つの Layer に分けた設計に関する論文．layer one: 一般的なアクセス制御モデル．layer two: 特別なアクセス制御を提供するパラメータ．layer three: ユーザとオブジェクトの初期集合．この実装により，安全性の問題を決定可能にしている．

Session: Cryptography

Symmetric encryption in automatic analyses for confidentiality against active adversaries (Peeter Laud)

この論文では，暗号的なプロトコルが秘密メッセージの機密性を保存するかどうかを分析する方法を提案している．この分析は，静的解析のための技術であり，暗号的なプロトコルやセキュリティ定義の理論的な複雑さを修正する．

Automatic Proof of Strong Secrecy for Security Protocols (Bruno Blanchet)

security protocol の strong secrecy の証明の自動化技術の提案．

5-minute work-in-progress talks

work-in-progress のプログラムを以下に示す．

Introduction

Cryptographically Justifying Dolev-Yao Under Active Attacks (Michael Backes)

Static Analyzer for Vicious Executables (SAVE) (A.H. Sung et al.)

Testing Malware Detectors (Mihai Christodorescu et al.)

A Theoretical and Practical Attack Derivation Model (Shai Rubin et al.)

A Semantics-Based Approach to Privacy Languages (Ninghui Li et al.)

Ranking False Positives in Security Checkers Using Probabilistic Static Analysis (Rajeev Gopalakrishna et al.)

Fast Detection of Scanning Worms (Stuart E. Schechter et al.)

Shield: First-Line Worm Defense (Helen Wang)

Privacy in Library RFID : Issues, Practices, and Architectures (David Molnar et al.)

Security Considerations for IEEE 802.15.4 Networks (Naveen Sastry et al.)

Pumped TFTP for UDP Covert Channel Identification, Analysis, and Mitigation (Steven J. Greenwald et al.)

Detecting AAA Vulnerabilities by Mining Execution Profiles (Zhan Xu et al.)

A Method for Detection and Visualization of Anomalous Network Behaviors From IP Traffic Flow (John Zachary et al.)

Views of Privacy: Business Drivers, Strategies, and Directions (Carolyn Brodie et al.)

Isolating Drivers without Tears (Nathanael Paul et al.)

Generating Security Policies for Black-Box Software via Collaborative Execution Monitoring (Hilarie Orman)

Quarantine Region Scheme for Spam Attacks in Wireless Sensor Networks (Serdar Sancak et al.)

Analysis, Design and Real Time Implementation of Electronic Voting Machine (Nachiappan Arunkumar et al.)

Detecting the Misappropriation of Information by Insiders (Matthew Broadhead et al.)

Session: Denial of service

An empirical analysis of target-resident DoS filters (Michael Collins et al.)

四つのフィルタリング方式の分析に焦点を当てた論文．これらのフィルタリング方式を実際のトラフィックレコードを基に分析している．

Large-Scale IP Traceback in High-Speed Internet: Practical Techniques and Theoretical Foundation (Jun Li et al.)

traceback scheme を基にした packet logging の提案．処理や記憶のコストが Snoeren が提案したハッシュベースの方法よりも小さいことが特徴．パケットの 3.3%しか記録しない．

An Endhost Capability Mechanism to Mitigate DDoS Flooding Attacks (Abraham Yaar et al.)

stateless なインターネットフィルタの提案．ルータにより，capability が動的に生成され，それを検証することで，選択的にパケットを落とすことができる．

Session: Access Control and Privacy

Safety in Automated Trust Negotiation (William H. Winsborough et al.)

Automated Trust Negotiation(ATN) に formal framework を導入し，ATN における正確で使いやすく直感的にわかる enforcement の定義を与える．

Securing OLAP Data Cubes Against Privacy Breaches (Lingyu Wang et al.)

この論文では，許可されていないアクセスや悪意のある妨害から，OLAP data cube の重要なデータを保護する解決法を提案している．

Panel: Grand Challenges in Computer Security Research

Virgil Gligor (U. Maryland), Mike Reiter (Carnegie Mellon), Dan Simon (Microsoft Research), Gene Tsudik (U.C. Irvine)

Session: Static Analysis

Run-time Principals in Information-flow Type Systems (Stephen Tse et al.)

既存の方式は，principal を実行時に決めて強制する．この論文では，言語レベルで実行時の principal をサポートする方式を提案する．

Formalizing Sensitivity in Static Analysis for Intrusion Detection (Henry Hanping Feng et al.)

Push Down Automata (PDA) には，スタックの動きが non-determinism であるため，操作が非効率的である．この論文では，PDA モデルのフレームワークを形式的な解析を提供し，determinism と stack-determinism の概念を導入する．この方法は効率的で，少ないメモリしか必要としないことも示している．

Session: Network Security

Fast Portscan Detection Using Sequential Hypothesis Testing (Jaeyeon Jung et al.)

ポートスキャンを効率よく検知できる手法の提案．TRW (Threshold Random Walk) と名付けたアルゴリズムを利用する．実験結果から，検出の効率と正確さを合わせ持つ手法であることを示していた．

On-the-Fly Verification of Rateless Erasure Codes for Efficient Content Distribution (Maxwell N. Krohn et al.)

マルチキャストでの効率のよいファイル配布についての論文．配送されたブロック単位での内容チェックを実現している．

Multicast Authentication in Fully Adversarial Networks (Anna Lysyanskaya et al.)

マルチキャストにおける認証の問題を示し，この問題を解決する手法を提案している．

Session: Security Against Physical Attacks

An Interleaved Hop-by-Hop Authentication Scheme for Filtering False Data Injection in Sensor Networks (Sencun Zhu

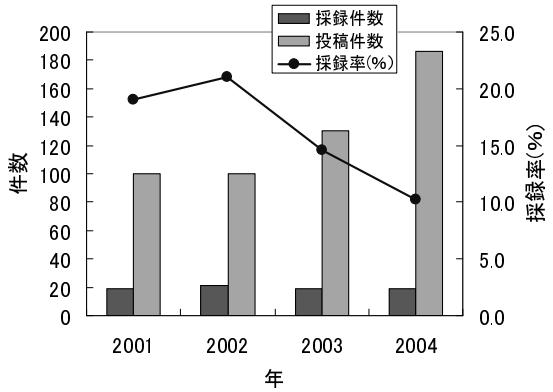

図 1: 論文投稿の傾向

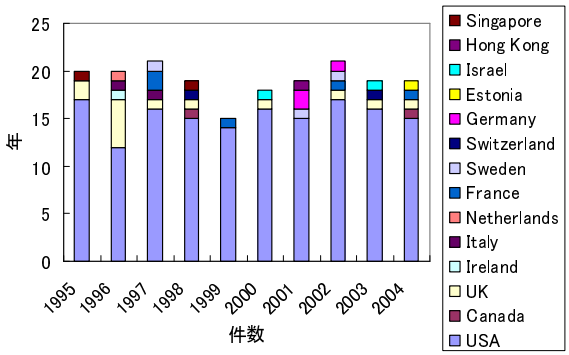

図 2: 第一著者の国別の分類

et al.)

センサネットワークにおけるセキュリティの問題を解決する手法の提案.（Interleaved hop-by-hop authentication scheme）この手法により，送り込まれた偽のデータを検出することができる.

SWAtt: Software-based Attestation for Embedded Devices (Arvind Seshadri et al.)

組み込み装置のソフトウェアの検証する手法.組み込みソフトウェアに自分のハッシュ値を返す関数を組み込んでおく．攻撃者が不正なコードを組み込み，そのことを隠蔽するため正しいハッシュ値を返すようにそのソフトウェアを改版しても，応答時間を見ることで異常を検出できることを示している.

4 IEEE Symposium on Security and Privacy 研究動向

4.1 投稿件数と採録率

オープニングで，2004 年は論文の投稿件数が増加していることが報告された．最近 4 年の論文投稿件数は，2001 年は約 100 件，2002 年は約 100 件，2003 年は約 130 件であった．今年は 186 件の投稿があり，論文の投稿件数の増加から，セキュリティ分野への関心が高まっていることがわかる.

論文の投稿件数と採録率をグラフにしたものを図 1 に示す．このグラフから，2004 年の採録率は 10 %にまで下がっており，競争率がかなり高くなっていることがわかる.

4.2 採録論文の地域別分類

1997 年から 2004 年の採録論文について，第一著者を国別に分類した結果を図 2 に示す．アメリカからの論文が多くの割合を占めることがわかる．また，過去 10 年間でアジアからの論文は 3 件であった.

4.3 論文の特徴

実装よりも理論面に重きを置いた論文が多い．ほとんどの論文では，理論的な考察を裏付けるために証明がなされている．実装と評価が重視される NDSS[1][2] や USENIX Security Symposium[3] とは，論文の傾向が大きく異なる.

4.4 研究動向

過去 10 年間（1995 年から 2004 年まで）について，発表動向を調査を行った．特に，発表動向に変化のある分野を取り上げ，調査結果を報告する.

4.4.1 IDS (Intrusion Detection System)

1997 年から 2003 年までセッションが組まれている．特に 2001 年から 2002 年は 2 セッショ

ンが組まれている．しかし，2004 年は関連する論文は 1 件しかなく，セッションは組まれていない．以前に比べて論文件数が減少している．

4.4.2 Operating System

Operating System (OS) のセッションは，1995 年と 2003 年に組まれている．1997 年と 1999 年のパネルでも，OS に関する発表がある．1995 年の主なトピックは，Domain and Type Enforcement や Multilevel filesystem などのアクセス制御やデータ保護に関する内容である．1997 年のパネルでは，これまでの研究事例として Exokernel Project, Fluke Project, Fox Project, Scout Project, SPIN Project について紹介している．一方，2003 年の OS セッションでは，Denial of Service (DoS) 攻撃への対策について述べられており，OS に関する研究内容が変化していることがわかる．

4.4.3 Access Control

1995 年から 1998 年にかけては，Multi level Security，BLP モデル，Mandatory Access Control などに関する研究が多い．この時期には，新しいモデルの提案などが多く行われている．一方で，1999 年以降はこれらに関する研究は，非常に少なくなっており，その代わりに認証 (PKI, Java など) や完全性に関するアクセス制御の研究が行われている．

4.4.4 Cryptography, Protocols

このシンポジウムでは，暗号に関する発表が多いが，暗号理論そのものを扱う発表はなく，暗号をどのようにしてシステムに適用し，セキュリティを確保するのかという議論が多い．また，鍵交換に関する論文も多い．

Protocol に関するセッションは，1995 年と 1996 年に組まれている．その後は，セッションとしては組まれていないが，プロトコルに関係する論文は発表されている．

4.4.5 Network

ネットワークに関する研究としては，ファイヤウォール，侵入検知がある．2004 年には，IP Traceback や Portscan Detection など，このシンポジウムでは取り上げられなかった研究が採録されている．

4.4.6 新しいトピック

ここ 2，3 年で目に付いた新しいトピックとして，電子投票システム，センサネットワーク，DoS がある．電子投票システムは，実際の投票に利用される事例があり，2004 年のパネルでもトピックとして取り上げられていた．センサネットワークは，2003 年と 2004 年に論文が採録されている．また，DoS も 2004 年に初めてセッションが組まれている．

5 おわりに

本稿では，2004 年の IEEE Symposium on Security and Privacy 参加報告と最近の動向について述べた．最近の会議の情報や 2005 年の Call for Papers の情報は，以下の URL から参照できる．http://www.ieee-security.org/TC/SP-Index.html

謝辞 本研究の一部は，財団法人セコム科学技術振興財団 平成 15 年度研究助成「インターネット妨害障害に対する暗号論的対策技術の研究」の支援を受けている．

参考文献

[1] 小手川 祐樹，田端 利宏，堀 良彰，櫻井 幸一: ”Network and Distributed System Security Symposium における研究動向の調査，” 情報処理学会 コンピュータセキュリティ (CSEC) 研究会，(5, 2004).

[2] NDSS2004: http://www.isoc.org/isoc/conferences/ndss/04/

[3] USENIX Security Symposium 2004: http://www.usenix.org/events/sec04/