社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2009－ＤＰＳ－138 (4)
2009－CSEC－ 44 (4)
2009／3／5

ACM CCS2008 会議ならびに併設ワークショップ参加報告

堀 良彰† ‡　　櫻井 幸一† ‡
† 九州大学大学院システム情報科学研究院情報工学部門
〒819-0395 福岡市西区元岡 744 番地
‡ 財団法人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
福岡 SRP センタービル 7 階
† {hori, sakurai}@csce.kyushu-u.ac.jp

あらまし 2008 年 10 月 27 日から同月 31 日の間、米国バージニア州アレクサンドリアで開催された第15回ACM CCS 2008 (2008 Conference on Computer and Communications Security) ならびに、CCS2008 併設ワークショップに関して報告する。

ACM CCS 2008 and workshops report

Yoshiaki Hori† ‡　　Kouichi Sakurai† ‡
† Department of Computer Science and Communication Engineering,
Faculty of Information Science and Electrical Engineering,
Kyushu University
744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan
‡ Institute of Systems, Information Technologies and Nanotechnologies (ISIT)
Fukuoka SRP Center Building 7F
2-1-22 Momochihama, Sawara-ku, Fukuoka City 814-0001, Japan

Abstract This paper reports on the 15th ACM CCS 2008 (Conference on Computer and Communications Security 2008) and CCS2008 workshops, held on October 27th to 31th, 2007, at the Hilton Alexandria Mark Center, Alexandria, VA, U.S.A.

1. はじめに

本稿では、2008 年 10 月 27 日から同月 31 日の間に米国バージニア州アレクサンドリアで開催された第 15 回 ACM CCS 2008 (Conference on Computer and Communications Security 2008) [1] とその併設ワークショップ[2] に関して報告する。

2. ACM CCS 2008 の概要

ACM Conference on Computer and Communications Security（以下、CCS とする）は ACM SIGSAC (Special Interest Group on Security, Audit and Control)が主催する年次コンファレンスのひとつであり、その名の通りコンピュータおよび通信におけるセキュリティに関する話題を取扱う。1993 年に初めて開催されてから 2008 年の開催で 15 回目を数える 2002 年以降の会議はワシントン DC かその郊外に位置するアレクサンドリア市にて開

催されている。特に、2005年以降の4カ年はバージニア州アレクサンドリア市のヒルトン・アレクサンドリア・マークセンターホテルで開催されている。会期は月曜日から金曜日までの5日間であるが、初日と最終日は併設ワークショップの開催であり、本会議は火曜日から木曜日の3日間の開催である。

表1に、過去5カ年(2004年から2008年)の投稿論文数、採択論文数、採択率を示す。2004から2006年までは、投稿数は250件程度であったが、2007年および2008年は302件および280件であり、この分野における関心の高さを伺わせる。これはプログラム編成にも影響を与え、2006年までは、いわゆる学術論文発表の講演はシングルトラックであったが、2007年以降デュアルトラックとなり採択数が増えることとなった。2008年の会議では280件の論文が投稿され、そのうちの51件の論文が採択された。したがって、論文採択率は18.2%と前年と同じで、過去数箇年と比較すると若干上昇することとなったが、20%未満と低い採択率であるには変わらない。

表1 ACM CCS 2004〜2008の投稿採択状況

	投稿数	採択数	採択率
CCS2004	251	34	13.5%
CCS2005	250	38	15.2%
CCS2006	256	38	14.8%
CCS2007	302	55	18.2%
CCS2008	280	51	18.2%

CCS2008本会議の会議録は、会場では冊子版とCD-ROM版の両方が配布された。一方で、CCS2008併設ワークショップではCD-ROM版のみ配布された。例年と同様にCCS2008本会議ならびに併設ワークショップの会議録はACMデジタルライブラリにより参照[1]できる。

[1] ACM Digital Library, http://portal.acm. org/dl.cfm

CCS2008では、コンピュータセキュリティに関する理論的な研究と実用的な研究(事例研究や実施経験を含む)の双方の論文が採択されている。しかし、CCSでは理論的な研究論文であっても、説得力のあるアプリケーションを例示し、実用的な面での重要性に関する議論を行うことを求めている。すなわち、CCSでは実用面での関連性を重要視している。

CCS2008のプログラムは、2つの研究発表講演トラックと1つのチュートリアルトラックから構成された。前年度まであったインダストリアル&ガバメント(I&G)トラック今年は設定されなかった。

CCS2008ではリサーチトラックとして18のセッションが設けられ、前述の51件の論文発表が行われた。その他に、チュートリアルが3件企画された。これらのタイトルを次に示す。行頭の記号K-#は基調講演、T-#はチュートリアルを表す。

K-1. The Good, The Bad, and The Provable (Martin Abadi, Univ. of California, Santa Cruz and Microsoft Research)

T-1. Trusted Hardware (Radu Sion, Stony Brook University)

T-2. RFID Security and Privacy (Kevin Fu, University of Massachusetts Amherst)

T-3. Understanding Android's Security Framework (William Enck and Patrick McDaniel, Pennsylvania State University)

リサーチトラックにおけるCCS2006以前のセッション数はシングルトラック×3日間の開催であったため11前後であったが、CCS2007以降では前述のようにリサーチトラックがデュアルトラックとなったためにセッション数が18と増えることとなった。次にセッション名を挙げる。セッション名の後の"(2)"は2

つのセッションから構成されていたことを示す。

- Software Security(2)
- Network Security
- System Security(2)
- Browser Security
- Device Security
- Attacks(2)
- Formal Methods(2)
- Privacy(2)
- Access Control
- Anonymity
- Identity-Based Encryption
- Applied Cryptography(2)

CCS2008 の参加者は 400 名程であった。しかし、2 つのリサーチトラックにおける聴講者は各々50～150 名程度であった。日本からの参加者は 10 名程度であった。

3. CCS2008 併設ワークショップ

CCS2008 では前述の通り、会期の初日（月曜日）と最終日（金曜日）に併設ワークショップが開催された。初日のワークショップは本会議と同じ会場で、最終日のワークショップはジョージメイスン大で開催された。このスタイルは、ここ数カ年同じである。2008 年は、次の 12 の併設ワークショップが開催された。

(1)Workshop on Formal Methods in Security Engineering (FMSE)
(2)Workshop on Quality of Protection (QoP)
(3)Workshop on Privacy in the Electronic Society (WPES)
(4)Workshop on Digital Rights Management (DRM)
(5)Workshop on AISec
(6)Workshop on Digital Identity Management (DIM)
(7)Workshop on Secure Web Services (SWS)
(8)Workshop on Computer Security Architectures (CSAW)
(9)Workshop on Scalable Trusted Computing (STC)
(10)Workshop on Network Data Anonymization (NDA)
(11)Workshop on Storage Security and Survivability (StorageSS)
(12)Workshop on Virtual Machine Security (VMSEC)

ほとんどの併設ワークショップは、前年に引き続き開催されているが、2007 年に開催されたもののうち Workshop on Recurring Malcode (WORM)が開催されず、AISec・NDA・VMSEC は 2008 年に新たに開催されたものである。

3.1. FMSE 2008

Workshop on Formal Methods in Security Engineering (FMSE) はセキュリティ技術における形式的手法による検証手法について議論するためのワークショップであり、FMSE 2008 は第 6 回目となる。当会議への投稿論文数は不明だが、採択率 1/3 未満で 7 件の論文が採択された。加えて、招待講演が 1 件あり、A Cryptographic Compiler for Information-Flow Security と題して Cedric Fournet (Microsoft Research, UK, and MSR-INRIA, France)氏が講演を行った。

3.2. QoP 2008

Workshop on Quality of Protection (QoP) は、セキュリティサービス等に量的な評価を与えるための研究開発について取り扱うワークショップである。今年は第 4 回目の開催である。19 件の投稿があり、その中から 5 件がフルペーパとして、5 件がショートペーパとして採択

された。また、招待講演として、Gunnar Peterson (Arctec Group)氏が、"The Economics of Finding and Fixing Vulnerabilities in Distributed Systems" と題して講演を行った。Security Measurement, Software Security, Risk と 4 つのセッションにおいて、それぞれの観点からセキュリティのための数値化に関する講演が行われた。

3.3. WPES2008

Workshop on Privacy in Electronic Society (WPES) は現在のコンピュータネットワークに潜在しているプライバシの問題とその解決方法について議論するためのワークショップである。WPES は今回で 7 回目を迎える。42 件の論文投稿があり、その内の 9 件がフルペーパとして、6 件がショートペーパとして採択された。会議では社会ネットワーキングにおけるプライバシ関連課題、ロケーションベースサービス、プライバシポリシとメトリック、認証、出版・購読システム、データアウトソーシング、プライベート・コンピューティングに関する講演が実施された。

3.4. DRM2008

Workshop on Digital Rights Management (DRM)は、インターネット上のデジタルコンテンツに関する知的所有権保護方式やコピープロテクション、デジタルコンテンツ保護のためのアクセス制御について議論するためのワークショップである。DRM は今回で 8 回目を迎えた。4 つのセッション Traitor Tracing, Models for Rights and Interoperability, Applications, Implementation and Legislation において研究成果の講演と議論が行われた。また、基調講演として Robert Kahn 氏により "The role of identifiers in information access" と題してた講演が、Yacov Yacobi (Microsoft Research)氏により "Content identification" と題して基調講演が行われた。

3.5. AISec2008

Workshop on AISec は今回が初めての開催でありセキュリティ研究コミュニティと AI 研究コミュニティの共同研究を刺激しようと企画された。20 件の投稿があり、うち 7 件の研究論文と 2 件のポジション論文が採択された。基調講演として、Chris Clifton (Purdue University)氏が "Opportunities for Private and Secure Machine Learning" と題して、Carl Landwehr (IARPA and University of Maryland)氏が "Cyber Security and Artificial Intelligence: From Fixing the Plumbing to Smart Water" と題して講演を行った。

3.6. DIM2008

Workshop on Digital Identity Management (DIM) は Digital Identity 管理について扱うワークショップである。本年度は特にサービスにおける ID 管理に焦点をあてている。本年は、第 4 回目の開催であり、20 件の論文投稿があり、その内の 12 件が採択された。会議は、次の 4 つの発表講演セッション Privacy in Services, Novel Services, Federation for Services, Discovery and Negotiation、そして、Services and Identity による議論のためのセッションから構成された。本ワークショップに関しては発表講演スライドがウェブで公開されている[2]。

3.7. SWS2008

Workshop on Secure Web Services (SWS) は、サービス指向アーキテクチャと XML に関するセキュリティを取り扱う。第 5 回目の開催である。17 件の論文投稿があり、その内の 11 件が採択された。会議では、Web サービス

---

[2] http://www2.pflab.ecl.ntt.co.jp/dim2008/preliminary-program.html

やサービス指向アーキテクチャ(SOA: Service Oriented Architecture)におけるアクセス制御、XACML ポリシ等について議論が行われた。また、アウトソース時におけるセキュリティに関する議論があった。

3.8. CSAW2008

Computer Security Architectures Workshop (CSAW) は今回が第2回の開催であった。会議は 3 つのセッション Architecture for Application Requirements, Host Security Architecture, Network Security Architecture において計8件の発表講演が実施された。本年は特に大規模システムにおいてどのようにトスおよび個々の利用者のアクセス制御を行うかという議論が多く見られた。

3.9. STC2008

Workshop on Scalable Trusted Computing (STC) は Trusted Computing を大規模なシステムに適用したときに発生するスケーラビリティやそのときにセキュリティ上の問題について議論するためのワークショップである。STC2008 は第3回の開催であり、34 件の論文投稿があり、9 件の論文が採択された。会議は Attestation and Scalability Issues, Trusted Computing Building Blocks, Special Trusted Platform Enhancements, Applications of Trusted Computing の各セッションから構成された。

3.10. NDA 2008

Workshop on Network Data Anonymization (NDA 2008) は初めての開催である。本会議ではインターネットトラヒックの計測関係研究において必要となるネットワークデータの匿名化について取り扱うものである。ネットワークアプリケーションのデータの匿名化は特に新しいトピックではないが、近年特に実データを研究対象にしようという動きがることや、セキュリティ保全の目的をもってトラヒックデータの共有に対する要求が高まっている。本会議のプログラムは、1 件の招待講演、2 件のパネル、および 5 件の発表講演から構成された。基調講演として、Richard Bejtlich 氏により "OpenPacket.org: The Challenge of a Free, Public Packet Capture Repository" と題した講演が行われた。

3.11. StorageSS 2008

Workshop on Storage Security and Survivability (StorageSS) は第4回目の開催である。本ワークショップではディスク上あるいはネットワーク越しのストレージについて、またその回復・修復技術について取り扱った。今回は 13 件の投稿があり、8 件が採択された。会議は Encryption, Practice, Data Security, Untrusted Storage の 4 つのセッションにおいて各研究成果について議論された。

3.12. VMSec2008

Workshop on Virtual Machine Security (VMSec)は、仮想化技術とセキュリティに関して最新の研究成果を持ち寄り議論する場として企画された。会議は初の開催である。今回は 20 件の投稿があり、7 件が採択された。当会議は、Portability & Recovery および Hardware & Monitoring の2つのセッションと基調講演1件から構成された。基調講演は、Brandon Baker (Hyper-V 社) 氏および William Arbaugh(Microsoft Research)氏から、Building Virtualization Security と題して講演が行われた。

4. CCS2008 本会議におけるコンピュータシステム関係発表

以上のように、CCS2008 本会議および併設ワークショップにおいて取り扱われるトピックは多岐にわたることから、ここでは CCS 2008 本会議において研究発表が行われた論文

から、コンピュータシステムおよびそのアーキテクチャにかかわる最近のトピックについて紹介する。

a) Code Injection Attacks on Harvard-Architecture Devices (Aurélien Francillon (INRIA Rhône-Alpes) et al.)

組込みシステムで広く用いられているハーバードアーキテクチャにおけるコード挿入攻撃に関する研究であり、当該アーキテクチャを使用したセンサーネットワークデバイス(e.g. Micaz)に対してワームを設計し、その対策について議論した。

b) Efficient and Extensible Security Enforcement Using Dynamic Data Flow Analysis (Walter Chang, The Univ. of Texas at Austin, et al)

著者らは、ソフトウェアが取り扱うデータが信頼できるかどうかを、ソースコードを再コンパイルすることで、解析用のコードを挿入しプロセスが取り扱うデータの信頼性を評価する動的なデータフロー評価解析システムを考案している。

c) Increased DNS Forgery Resistance Through 0x20-Bit Encoding (David Dagon, Georgia Institute of Technology, et al.)

DNS は大文字と小文字を区別しないことを利用し、ドメイン名の大文字小文字の組合せを利用してドメイン名の表現自体に情報を挿入することでDNSの偽造パケットを回避する手法を提案している。

d) Towards Automatic Reverse Engineering of Software Security Configurations (Rui Wang, Indiana University, et al)

アプリケーションプログラムにおけるセキュリティ設定に対するリバースエンジニアリングを自動で行うツール ConfigRE を開発している。ConfigRE 仕様記述言語を出力するので、それを利用してアプリケーションのセキュリティ設定の妥当性を評価することを可能にしている。

5. CCS2009 について

本年秋に開催される CCS2009[3]は、ここ数年とは異なり米国イリノイ州シカゴでの開催が予定されている。会期は、従来より 2 週間ほど遅い 2009 年 11 月 9 日（月）から同月 13 日（金）の 5 日間である。会議場は、ハイアット・リージェンシー・シカゴとアナウンスされている。研究発表講演を行うための論文の投稿締切は 2009 年 4 月 20 日とアナウンスされている。

6. おわりに

本稿では、2008 年 10 月 27 日から同月 31 日の間に米国バージニア州アレクサンドリアで開催された第 15 回 ACM CCS 2008 (Conference on Computer and Communications Security 2008)とその併設ワークショップに関して、その概要を紹介した。さらに、CCS 2008 本会議で発表されたコンピュータシステム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。

謝辞

本調査研究の一部は、総務省戦略的情報通信研究開発制度（SCOPE）の支援を受けている。また、本研究の一部は、独立行政法人情報通信研究機構が実施するインシデント分析の広域化・高速化技術に関する研究開発の支援を受けている。ここに謝意を示す。

参考文献

[1] The 15th ACM Conference on Computer and Communications Security (ACM CCS 2008). http://www. sigsac.org/ccs/CCS2008/.

[2] ACM CCS 2008 Workshops. http://www. sigsac.org /ccs/CCS2008/workshop.html.

[3] The 16th ACM Conference on Computer and Communications Security (ACM CCS 2009). http://www.sigsac.org/ccs/CCS2009/.