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

2008－DPS－134 (24)
2008－CSEC－ 40 (24)
2008／3／6

ACM CCS2007 会議ならびに併設ワークショップ参加報告

堀 良彰† ル・マレコ エルワン‡ 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
‡ 九州大学大学院システム情報科学府情報工学専攻
819-0395 福岡市西区元岡 744 番地
† {hori, sakurai}@csce.kyushu-u.ac.jp
‡ lemalecot@itslab.csce.kyushu-u.ac.jp

あらまし 2007 年 10 月 29 日から 11 月 2 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 14 回 ACM CCS 2007 (Conference on Computer and Communications Security 2007) ならびに、CCS2007 併設ワークショップに関して報告する。

ACM CCS 2007 and workshops report

Yoshiaki Hori† Erwan Le Malécot‡ Kouichi Sakurai†
† Department of Computer Science and Communication Engineering,
Faculty of Information Science and Electrical Engineering,
Kyushu University
‡ Department of Computer Science and Communication Engineering,
Graduate School of Information Science and Electrical Engineering,
Kyushu University
744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan

Abstract This paper reports on the 14th ACM CCS 2007 (Conference on Computer and Communications Security 2007) and CCS2007 workshops, held on October 29 to November 2, 2007, at the Hilton Alexandria Mark Center, Alexandria, VA, U.S.A.

1. はじめに

本稿では、2007 年 10 月 29 日から 11 月 2 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 14 回 ACM CCS 2007 (Conference on Computer and Communications Security 2007) [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 2007 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コミュニケーション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 2007 年の開催で 14 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 3 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 2007 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、投稿数および採択率は大きな変化はなかったが、CCS2007 では投稿数が 300 を超え、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 年からデュアルトラックとなり採択数が大幅に増えることとなった。2007 年の会議では 302 件の論文が投稿され、そのうちの 55 件の論文が採択された。したがって、論文採択率は 18.2%と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 2004～2007 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%

CCS2007 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。前年度の CCS2006 では、初めて CD-ROM 版が配布され、その代わりに冊子版は配布されなかったが、CCS2007 では冊子版が復活することとなった。例年と同様に CCS2007 の会議録は ACM デジタルライブラリ[3]により参照できる。

CCS2007 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ようである。CCS2007 のプログラムは、近年のプログラム編成と同様に研究論文発表のためのリサーチトラックとインダストリアル&ガバメント (I&G) トラックさらにチュートリアルから構成されている。

CCS2007 ではリサーチトラックとして 17 のセッションが設けられ、前述の 55 件の論文発表が行われた。その他に、I&G 招待講演が 4 件とチュートリアルが 4 件企画された。これらのタイトルを次に示す。行頭の記号 I-#は招待講演、T-#はチュートリアルを表す。

I-1. A Path Toward Better Security For Consumer Products (Morris Moore, VP, Security Technology, Motorola Labs, Motorola Inc)

I-2. Why is it so Hard to Transition My Research? (Lee Beausoleli, DTO/ NICIAR Technical SETA)

I-3. Exploiting Online Games (Gary McGraw, Cigital)

I-4. Live Forensics (Frank Adelstein, Senior Principal Scientist, ATC-NY)

T-1. Forensic Techniques for Content Protection (Hongxia Jin, IBM Almaden Research Center)

T-2. Regulatory Compliant Data Management (Radu Sion, Department of Computer Science, Stony Brook University; Marianne Winslett, Department of Computer Science, UIUC)

T-3. Privacy in Location Service: State-of-the-art and Research Directions (Mohamed F. Mokbel, Department of Computer Science and Engineering, University of Minnesota)

T-4. Research Challenges in Securing VoIP (Xinyuan Wang, Department of Information and Software Engineering, George Mason University)

また,基調講演(keynote talk)として,マイクロソフト社の Steve Lipner が "Assurance and Evaluation: What Next?" と題して講演を行った。

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、CCS 2007 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 17 と増えることとなった。したがってセッション名も従来と比較してより狭い範囲を指すようになった。セッション名から新しい研究分野と考えたものを筆者の主観で 3 つ取り上げる。

1. Web Applications Security
2. Traffic Analysis and Location Privacy
3. Data Disclosure

CCS2007 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50～100 名程度であった。

3. CCS2007 併設ワークショップ

CCS2007 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。最終日の一部のワークショップはジョージメイスン大で、その他のワークショップは CCS 本会議と同じ会場で開催された。このスタイルは、ここ数カ年同じである。2007 年は、次の 10 の併設ワークショップが開催された。

(1)Workshop on Privacy in Electronic Society (WPES2007)

(2)Workshop on Digital Rights Management (DRM2007)

(3)Workshop on Quality of Protection (QoP2007)

(4)Workshop on Storage Security and Survivability (StorageSS2007)

(5)Workshop on Recurring Malcode (WORM2007)

(6)Workshop on Secure Web Services (SWS2007)

(7) Workshop on Formal Methods in Security Engineering (FMSE2007)

(8)Workshop on Scalable Trusted Computing (STC2007)

(9)Workshop on Digital Identity Management (DIM2007)

(10)Computer Security Architecture Workshop (CSAW2007)

これらの併設ワークショップの会議録は、CCS2007 本会議と同様に ACM デジタルライブラリから参照できる[3]。

3.1. WPES2007

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 6 回目を迎える。WPES2007 は 48 の論文投稿があり、その内の 9 件がロングペーパーとして、7 件がショートペーパとして採択された。会議では次の 3 つのセッション Anonymous Communications, Privacy in Distributed Systems,

Privacy in Distributed Systems およびショートペーパセッションが設けられ研究成果の講演と議論が行われた。

3.2. DRM2007

Workshop on Digital Rights Management (DRM2007)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 7 回目を迎えた。DRM2007 は 28 件の論文投稿があり、その内の 10 件が採択された。会議では、次の 6 つのセッション Architecture and Implementation, Applications of DRM, Legal Aspects, Modeling of DRM System, Software Protection Methods、 Supporting Technology において研究成果の講演と議論が行われた。また、ミネソタ大学の Andrew Odlyzko 教授により、"Digital Rights Management: Desirable、 inevitable、 and almost irrelevant"と題して基調講演が行われた。

3.3. QoP2007

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。2007 年の開催は第 3 回目となる。QoP2007 では 20 件の投稿があり、その中から 7 件がフルペーパとして、4 件がショートペーパとして、1 件がポスターとして採択された。会議では Software Security、 Business Security Metrics, Network Security、 Risk Analysis の 4 つのセッションが設けられ、これらの研究成果について議論された。また、RAND Corporation の Shari Lawrence 博士により、"Measuring Up: How to Keep Security Metrics Useful and Realistic"と題して基調講演が行われた。

3.4. StorageSS2007

Workshop on Storage Security and Survivability (StorageSS) は第 3 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。特に今回はオープンソースのストレージシステムに焦点をあてた。StorageSS2007 では 12 件の投稿があり、7 件が採択された。会議は Confidentiality、Secure Paths、Corruption Is a Fact of Life、Code Archeology 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。

3.5. WORM2007

Workshop on Recurring Malcode (WORM) は、情報セキュリティならびにシステムの可用性に対する脅威であるインターネット規模で感染する悪意あるコードについて取り扱う。本会議は第 5 回目になる。今回は 30 件の投稿があり、10 件が採択された。当会議は、Threats、Worms, Analyzing and Detecting Malware, Mobile Malware の 4 つのセッションから構成された。

3.6. SWS2007

Workshop on Secure Web Services (SWS) は、Web サービスと XML に関するセキュリティを取り扱う。SWS2007 は第 4 回目の開催である。28 件の論文投稿があり、その内の 13 件が採択された。会議では、Web サービス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。

3.7. FMSE2007

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 2007 は第 4 回目となる。当会議では 28 件の論文投稿があり、その内の 8 件が採択された。加えて、招待講演が 2 件あり、Naval Research Laboratory の John McLean 博士が,"Formal Methods in Security Engineering: Where We've Been, Where We Are, Where We Need to Go"というタイトルで、Galois, Inc.の Jeff Lewis 博士が、"Cryptol: Specification, Implementation and Verification of High-grade Cryptographic Applications"というタイトルで招待講演を行った。

3.8. STC2007

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。STC2007 は第 2 回の開催であり、30 件の論文投稿があり、4 件のフルペーパと 6 件のショートペーパが採択された。会議は Mobile and Embedded Trusted Computing, Trusted Platform, Channel, and Storage, Property-Based Attestation, Applications の各セッションと 2 件の招待講演から構成された。AMD の Leendert van Doorn 博士は、"Trusted Computing Challenges"というタイトルで、ジョン・ホプキンス大の Yair Amir 教授は、"The Insider Threat in Scalable Distributed Systems: Algorithms, Metrics and Gaps" というタイトルで招待講演を行った。

3.9. DIM2007

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 Digital Identity のユーザビリティについて焦点をあてている。DIM2007 は、第 3 回目の開催であり、26 件の論文投稿があり、その内の 10 件が採択された。会議は、次の 4 つのセッション Usability and Authentication, Identity Assurance and Linkability、 Network-Based Approach, Reputation and Trust から構成された。

3.10. CSAW2007

Computer Security Architectures Workshop (CSAW) は今回が第 1 回の開催であった。30 件の投稿があり、9 件が採択された。会議は 3 つのセッション Hardware Environments, Authorization and Authentication, Cryptography and Storage およびイリノイ大学シカゴ校の Daniel J. Bernstein 教授による"Some Thoughts on Security After Ten Years of qmail 1.0"と題した招待講演が行われた。

4. CCS2007 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、CCS2007 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 2007 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) Stealthy Malware Detection Through VMM-Based Out-of-the-Box" Semantic View Reconstruction (X. Jiang (George Mason University) et al.

著者らは、マルウェア検出のために、VMM

(Virtual Machine Monitor)を用いて、VMの状態を収集し、それを VM 現在どのような処理を実行しているかという情報を再構成するためのシステム VMwatcher を提案し実装している。VMwatcher は VM 外にありながらも、VM 上のメモリやディスクの状態を再構成し、それを比較参照することで、マルウェア検出を可能にしている。

b) Panorama: Capturing System-wide Information Flow for Malware Detection and Analysis (Heng Yin (CMU) et al.)

著者らは、マルウェア検出のために、システムに入力された情報に対する汚染検出グラフを構築し、当該情報に OS 上のどのようなプロセス、モジュールあるいは資源が関与したかをグラフ化し、それを評価するシステム Panorama を提案し構築している。本システムにより、キーロガー、パスワードスニファ、パケットスニファ、隠しバックドア、スパイウェア、ルートキット等のマルウェアを検出できるとしている。

c) An Analysis of Browser Domain-Isolation Bugs and a Light-Weight Transparent Defense Mechanism (Shuo Chen (Microsoft Research) et al.)

著者らは、ブラウザに内臓されている sender origin policy (SOP)がうまく機能しない場合があるということを示し、それへの攻撃に対抗するために、script accenting と呼ばれる手法を提案している。script accenting はそれぞれのドメイン毎にランダムに生成したキーを用意し、それを用いてスクリプトおよび URL を変化させることである。これにより、Windows Shell Address Parser を介した場合の不具合を解決できるとしている。

5. CCS2008 について

本年秋に開催される CCS2008[4]は、前年と同じ米国バージニア州アレクサンドリアでの開催が予定されている。会期は、2008 年 10 月 27 日（月）から 10 月 31 日（金）の 5 日間である。会議場も CCS2005 以来のヒルトン・アレクサンドリア・マークセンターとアナウンスされている。リサーチトラックで講演を行うための論文の投稿締切は 2008 年 4 月 14 日とアナウンスされている。

6. おわりに

本稿では、2007 年 10 月 29 日から 11 月 2 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 14 回 ACM CCS 2007 (Conference on Computer and Communications Security 2007)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 2007 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。ここに謝意を示す。

参考文献

[1] The 14th ACM Conference on Computer and Communications Security (ACM CCS 2007). http://www. sigsac.org/ccs/CCS2007/.

[2] CCS2007 Workshops. http://www.sigsac.org /ccs/CCS2007/workshop.html.

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

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