Vol.2011-CSEC-54 No.34
Vol.2011-SPT-1 No.34
2011/7/13

ACM ASIACCS2011 会議参加報告

溝口 誠一郎[†1]　田 中 哲 士[†1]　南　　和 宏[†2]
須 崎 有 康[†3]　櫻 井 幸 一[†1]

2011 年 3 月 22 日から同月 24 日にかけて香港で開催された，第 6 回 ACM ASIACCS 2011 (6th ACM Symposium on Information, Computer and Communications Security) に関して報告する．

ACM ASIACCS2011 Conference Report

Seiichiro Mizoguchi,[†1] Satoshi Tanaka,[†1]
Kazuhiro Minami,[†2] Kuniyasu Suzaki[†3]
and Kouichi Sakurai [†1]

This paper reports on the 6th ACM ASIACCS 2011 (6th ACM Symposium on Information, Computer and Communications Security) held on March 22th to 24th, 2011, at the HKU SPACE Admiralty Learning Center, Hong Kong.

1. はじめに

本稿では，2011 年 3 月 22 日から同月 24 日の間に，香港の HKU SPACE Admiralty Learning Center で開催された第 6 回 ACM ASIACCS 2011 (6th ACM Symposium on Information, Computer and Communications Security)[1)] に関して報告する．

†1 九州大学
Kyushu University
†2 国立情報学研究所
National Institute of Informatics
†3 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology

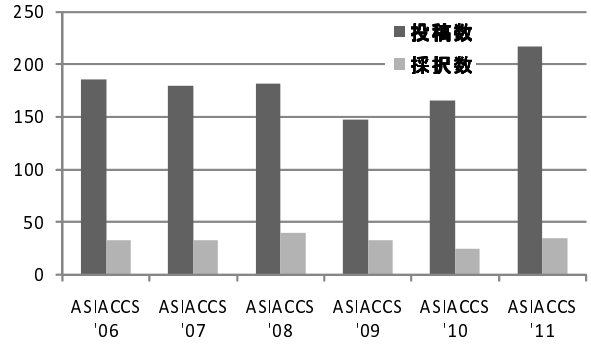

図 1　論文採択状況

2. ACM ASIACCS 2011 会議の概要

ACM Symposium on Information, Computer and Communications Security (以下，ASIACCS とする) は，ACM SIGSAC (ACM Special Interest Group on Security, Audit and Control)[2)] が主催する年次カンファレンスの一つであり，コンピュータおよび通信におけるセキュリティだけでなく，暗号，情報セキュリティに関する話題を取り扱う．2006 年に初めて開催されてから，2011 年の開催で 6 回目を迎える．会議名にある通り，アジア諸国を中心に会議が開催されており，日本では 2008 年に東京で開催されている．

2011 年の開催では，論文投稿締切は 2010 年の 8 月上旬，採択結果は 12 月に通知された．CFP によって募集されたトピックは，2010 年と同じであった．図 1 と表 1 に，過去 6 回の投稿論文数，採択論文数，採択率を示す．2011 年の会議では，217 件の論文が投稿され，そのうち 35 件のフルペーパーと 24 件のショートペーパーが採択された．フルペーパーの採択率は 16.1%である．

ASIACCS2011 の会議録は，会場では冊子版のみが配布された．また，本会議の会議録は，ACM デジタルライブラリ[3)] により参照できる．

ASIACCS2011 のプログラムは，シングルトラックで構成されている．初日と 2 日目の冒頭で，Invited Talk が用意された．表 2 に，今年用意されたセッションを示す．

ASIACCS2011 の参加者は，全体を通して 70 名ほどであった．うち日本人は，10 名弱であった．

Vol.2011-CSEC-54 No.34
Vol.2011-SPT-1 No.34
2011/7/13

表 1　ACM ASIACCS 投稿採択状況

	投稿数	採択数 Full (Short)	採択率
'06	186	33 (15)	18%
'07	180	33 (20)	18%
'08	182	34 (6)	22%
'09	147	33 (7)	22%
'10	166	25 (13)	15%
'11	217	35 (24)	16%
Total	1078	199 (85)	18%

表 2　プログラムテーブル

3/22（1 日目）	3/23	3/24
Invited Talk 1	Invited Talk 2	Security Protocols
Network Security	Access Control	Applied Cryptography II
Malware	Applied Cryptography I	System Security
Software Security	Cryptanalysis and Attacks	Short Papers III
Short Paper I	Short Paper II	Short Papers IV

3. 各セッションの紹介

ここでは，それぞれのセッションで発表された研究内容をいくつか抜粋して紹介する．ショートペーパーに関しては割愛する．

3.1 Invited Talk 1

Improved Nguyen-Vidick Heuristic Sieve Algorithm for Shortest Vector Problem, Xiaoyun Wang (Tsinghua University)

初日の Invited Talk 1 では，Tsinghua 大学の Xiaoyun Wang 氏が講演を行った．Wang 氏は，暗号研究の分野で活躍されており，ハッシュのコリジョンアタック等の研究をされている．Invited Talk では，ラティスの最小ベクトル問題 (SVP) の高速化に関する取りくみについて紹介がなされた．始めに，SVP と類似する問題について簡単な説明があり，SVP の暗号分野におけるアプリケーションの紹介がなされた．Wang 氏らは，SVP に対する Nguyen-Vidick Heuristic Sieve アルゴリズムを改良し，時間計算量を $2^{0.3836n}$ 回の多項式計算回数に，空間計算量を $2^{0.2557n}$ に落としている．

3.2 Invited Talk 2

Towards Mechanisms for Detection and Prevention of Data Exfiltration by Insiders, Elisa Bertino (Purdue University)

2 日目は，Purdue 大学の Elisa Bertino 氏による講演が行われた．講演の内容は，インサイダーによる情報漏洩の検知・対策手法に関するものである．Bertino 氏は特に，DBMS 層でのデータ漏洩対策手法について検討している．キーアイデアは，データへのアクセスの様子を Profile として表現し，Profile の監視を行うことで異常を検知するというものであり，Profile は SQL のクエリから生成される．検知の場所として DBMS が選ばれているのは，DBMS に対するアクセスは，SQL のような標準化された言語が利用され，Profile 化が容易であることと，生のデータに近い場所ほど監視がしやすいこと，そして，DBMS はアクセス制御機構が既に備わっていることが理由となっている．

3.3 Network Security

Network Scan Detection with LQS: A Lightweight, Quick and Stateful Algorithm, Mansour Alsaleh (Carleton University) et al.

ネットワークスキャンは様々な攻撃につながる初動の攻撃であり，検知する必要がある．しかし，ネットワークの High-Speed 化により，大量のトラフィックからスキャン攻撃を発見することが難しくなっている．さらに，スキャン攻撃自体のステルス化によって，より発見が困難になっている．筆者らは，効果的なスキャン検知アルゴリズム LQS を提案し，High-Speed なネットワーク環境下でのリソースの節約を実現している．LQS はネットワークの特徴 (Key Properties) によって検知手法を変更することができるアルゴリズムである．

Boosting the Scalability of Botnet Detection Using Adaptive Traffic Sampling, Junjie Zhang (Georgia Institute of Technology) et al.

ネットワークベースのボット検知手法において，Deep Packet Inspection (DPI) のみでは検知システムの負荷が大きく，スケールできない．そこで，著者らは計算コストを削減するサンプリングアルゴリズムを提案している．Flow Correlation Algorithm を用いて同期しているホストを割り出した後，初めて DPI を行って，ボットネットであるかを特定する．既存手法の BotMiner と比べ大幅にコストが削減でき，理論上では 2Gbps のネットワークで利用出来ることを示している．

Vol.2011-CSEC-54 No.34
Vol.2011-SPT-1 No.34
2011/7/13

3.4 Malware

WebPatrol: automated collection and replay of web-based malware scenarios, Kevin Zhijie Chen (Peking University and UC Berkeley) et al.

近年，ウェブベースのマルウェアが増加している．従来のマルウェア解析研究は，マルウェアのバイナリコードの解析が中心となっていたが，ウェブベースのマルウェアの場合は，ページの閲覧から感染までのシナリオも解析の対象となる．論文中では，ウェブベースのマルウェア感染シナリオ (Web-based Malware Scenario, WMS) をモデル化し，WMS を自動的に収集するシステムである WebPatrol を実装している．また，WebPatrol は，収集した WMS をリプレイする機能を備えており，ウェブベースのマルウェア解析を動的に行うことができる．評価では，既存のクライアント型ハニーポットである PHoneyC, Capture-HPC と比較を行っており，WebPatrol の WMS 収集能力が，既存のハニーポットに比べ優れていることを示している．

Malware Propagation in Online Social Networks: Nature, Dynamics, and Defense Implications, Guanhua Yan (Los Alamos National Laboratory) et al.

ソーシャルネットワークサービスは，現在のインターネットユーザ間の重要なコミュニケーションツールとなっている．それに伴い，ソーシャルネットワークを介したマルウェア感染も広まっている．著者らはまず，ソーシャルネットワークにおけるユーザ間の関連や，ユーザの行動モデルを分析している．そして，その結果を基に，ソーシャルネットワークにおけるマルウェア感染の流れをシミュレートしている．その結果，ソーシャルグラフによっては，感染拡大の度合いに差が出ることを示された．また，論文の最後では，ソーシャルネットワークにおけるマルウェア対策手法について，簡単なアイデアが述べられている．

Characterizing kernel malware behavior with kernel data access patterns, Junghwan Rhee (Purdue University) et al.

フロー制御の分析によるマルウェア解析では，静的解析におけるコードの難読化や動的解析における挙動の複雑さ等の問題に直面している．著者らは，カーネルへのデータアクセスパターンを基にカーネルマルウェアの特徴づけを行う手法を提案している．提案手法は，マルウェアコードの分析を必要とせず，フロー制御の分析も必要としないため，生成されたデータアクセスパターン（シグネチャ）を用いて，類似するカーネルマルウェアを検知できるとしている．評価では，良く知られている 3 種類のカーネルルートキットを用いてシグネチャを生成し，正常なカーネルと 16 のルートキットによって攻撃されたカーネルに対して，シグネチャの有効性を検証している．シグネチャは，正常なカーネルではアラートを挙げず，一方で，攻撃されたカーネルを正確に検知することができた．

3.5 Software Security

Automatic Construction of Jump-Oriented Programming Shellcode (on the x86), Ping Chen (Nanjing University) et al.

既存のコードを活用して ShellCode を作成する ROP: Return Oriented Programming は近年脅威になってきているが，ret 命令からの合成のためスタックの監視など，既に幾つかの対処法が現れている．本発表では jmp 命令に着目した JOP: Jump Orient Programming により ROP の対処法でも検出できない ShellCode の作成法を提案した．本手法では合成に使えるコードピース（Gadget と呼ぶ jmp 命令終了するコード）を自動的に集めるアルゴリズムとそれを使った自動合成が可能であるツールが紹介された．更に，このツールを使って既存のマルウェアである milw0rm の一部を合成できたことが報告された．

Jump-Oriented Programming: A New Class of Code-Reuse Attack, Tyler Bletsch(North Carolina State University) et al.

上記の発表に引き続いて Jump Orient Programming による ShellCode の作成法の発表であった．冒頭から上記の発表で JOP が発表されてしまったと始まったが，本手法では Call/ret の Gadget を特殊なケースとして扱うのに対し，jmp のみを対象にして dispatcher Gadget により ShellCode 合成を行う．事例として libc 中に 3 万個以上の Gadget があることが示された．

ROPdefender: A Detection Tool to Defend Against Return-Oriented Programming Attacks, Lucas Davi(Technische Universität Darmstadt) et al.

スタックの中身を解析することで ROP 対処する ROPdefender が発表された．ROPdefender では Shadow Stack を用意し，プログラムが設定したリターンアドレスが実行中に変更されたことを検出する．JIT ベースの Pin により実装されており，OS やアプリケーションを変更することなく適用可能である．事例としては Adobe Reader への ROP を検出することが示された．

3.6 Access Control

Tracer: Enforcing Mandatory Access Control in Commodity OS with the Support of Light-Weight Intrusion Detection and Tracing, Zhiyong Shan (Renmin University) et al.

マルウェアからシステムを守るために，Mandatory Access Control (MAC) と呼ばれる

Vol.2011-CSEC-54 No.34
Vol.2011-SPT-1 No.34
2011/7/13

アクセス制御機構が利用されるが，ビルトインの MAC に関しては様々なソフトウェアとの互換性がなく，管理者が容易に修正できないという課題がある．著者らは，2600 個のマルウェアについて動的解析を行い，挙動を分析し，それに基づく新しい MAC のモデルを作成した．さらに，MAC を利用する Tracer と呼ばれる侵入検知システムを開発した．

3.7 Applied Cryptography

Identity-Based Online/Offline Key Encapsulation and Encryption, Sherman S. M. Chow (University of Waterloo) et al.

本論文では，効率的な ID-based online / offline encryption scheme を提案している．提案されたスキームには SK-IBE スキームのランダムオラクルモデルに対するセキュリティ仮定に基づいた CPA に耐性のある効率的なバージョンと，ID-based online / offline KEM の一方向性に基づいた CCA に耐性のあるバージョンの 2 つのバージョンが存在する．これらのスキームは従来のものよりも計算コストや空間コストが低い為，スマートカードやワイヤレスセンサー上で利用するのに適している．

Compact Identity-Based Encryption without Strong Symmetric Cipher, Joonsang Baek (Institute for Infocomm Research) et al.

本論文では，KEM / DEM framework 等の前提条件に依存しない，ciphertext expansion が最小となるような 2 つの ID ベース暗号スキームを提案している．提案されたスキームは GBDH(Gap Bilinear Diffie- Hellman) 問題，q-GBDH 問題といった既に知られている数学問題の仮定に基づき，CCA に対して耐性を持つ．また，これらのスキームはセンサー等の速度の遅いデバイス上で実装するのに適している．

Strongly Secure Certificateless Key Exchange without Pairing, Guomin Yang (National University of Singapore) et al.

著者らは，認証を必要としない鍵交換方式である CLKE について研究を行っている．従来の TYPE-I，TYPE-II と呼ばれる認証鍵交換方式に対する攻撃手法に耐性のある認証鍵交換方式は，発信したデータから全てのユーザのデータが漏れない “Forward Secrecy” の概念に適さないと考えられる．そこで，認証鍵交換における新たなセキュリティモデルとペアリングを用いずに強い耐性を持つ認証鍵交換プロトコルを提案している．

Examining Indistinguishability-Based Security Models for Key Exchange Protocols: The case of CK, CK-HMQV, and eCK, Cas Cremers (TH Zurich) et al.

鍵交換方式におけるセキュリティ概念である CK，CK-HMQV，eCK は形式的にだけではなく実際にも比較することができない．著者らは，Key derivation function とマッチングセッション間の関係性の解析により，従来の Okamoto プロトコルや CMQV プロトコルの証明に微妙な誤りがあることを示している．不完全なセッションマッチングにおける問題を示しその問題を回避するための特別化したセッションマッチング構成を行うための手順を示している．

3.8 Cryptanalysis and Attacks

Extended Cubes: Enhancing the Cube Attack by Extracting Low-Degree Non-Linear Equations, Shekh Faisal Abdul-Latip (University of Wollongong) et al.

2009 年に Dinur と Shamir が提案した Cube Attack の改良．オリジナルの Cube Attack が不得意としていた低次の方程式充足を解決させるため，二次の項が一つであるようなシンプルな低次元の方程式を除く効率的な手法を提案．提案した Cube Attack は PRESENT 暗号に対して PRESENT-80 を時間計算量 2^{16} かつデータ量 2^{13} の選択平文攻撃に成功した。これは Yang らが行ったアタック 2^{32} の時間計算量、データ量 2^{15} よりも良くなっている。また、PRESENT-128 で時間計算量 2^{64} かつデータ量 2^{13} の選択平文が必要となっている。

Attack on the GridCode One-Time Password, Ian Molloy (IBM T. J. Watson Research Center) et al.

SyferLock が提供している GridCode と呼ばれるワンタイムパスワード認証システムに対して，攻撃を行った際の耐性について検討している．どのようにパラメータ選択をすれば脆弱性が発生するかを描いている．シンプルな Malkov 連鎖とパスワード候補の確率的文法を利用することで，10.4〜14.06%のパスワードが復元可能であり，リプレイ攻撃により 13.88〜16.75%のケースで認証に成功した．また，囮となるビットを使用することでブルートフォース攻撃が促進される誘因となりえることを示した．GridCode は擬似乱数において元の像を容易に発見可能であることが問題となっている．よりセキュアに認証システムを使用するのであれば Hopper-Blum プロトコルが条件に適している．

Rethinking about Guessing Attacks, Zhiwei Li (UNC Charlotte) et al.

特徴づけと検知推測攻撃は推測攻撃の定義と同じ観念を持たない．その為，推測攻撃に対するセキュリティプロトコルの resilience の評価を困難としている．この問題を解決するために攻撃者の推測性能を完全に特徴づける新しい定義の提案を行い，セキュリティプロトコルにおける推測攻撃とどのように関係するかを示す．また推測に対する一般的なフレームワークを提供している．

Vol.2011-CSEC-54 No.34
Vol.2011-SPT-1 No.34
2011/7/13

3.9 System Security

A software-based root-of-trust primitive on multicore platforms, Qiang Yan (Singapore Management University) et al.

信頼チェーンは，あるアプリケーションが信頼できることを，他の信頼できるアプリケーションによって保証する考え方であり，この場合，Root-of-Trust が重要となってくる．従来，Root-of-Trust として，TPM 等のハードウェアベースのモジュール等が用いられてきたが，実装と変更に多大なコストがかかるため，近年はソフトウェアベースの Root-of-Trust が注目されてきた．しかし，これまでのソフトウェアベースの Root-of-Trust は，シングルコアのシステムを前提としており，マルチコアシステムにおける Root-of-Trust を実現する仕組みについては考慮されていなかった．著者らは，マルチコアな環境下において，既存の手法に対する二つの攻撃手法の存在を示している．そして，マルチコア環境下でそのような攻撃に耐えうる Root-of-Trust を実現する MT-SRoT を提案し，Intel のデュアルコアとクアッドコア CPU 上に実装を行った．

3.10 Security Protocols

Efficient Audit-based Compliance for Relational Data Retention, Ragib Hasan (University of Illinois) et al.

US ではエンロン等数々の不正経理の事件の後，WORM ファイルシステムがビジネス情報の信憑性の確保のために幅広く用いられてきたが，この論文ではさらにデータベースのレコード単位でのデータの信頼性を保証する仕組みを提案している．効率的にオーディットを行うために，WORK にはデータベースのレコードのハッシュ値を格納し，ハッシュ関数は加算演算に対する準同型を利用してデータ更新の信憑性を検証可能にしている．論文ではシステム性能の評価実験も行っており，WORM への定期的なデータ書き出し等のオーバーヘッドは最大１１％とそれほど高くないことを示している．論文は今回の仕組みの安全性を証明しているが，システムモデルが複雑なために，データベースのクラッシュ等，多くの場合を列挙しており，全ての場合の網羅性の保証することは困難な作業と思われる．

Mind How You Answer Me!, Mauro Conti (Vrije Universiteit Amsterdam) et al.

現状のスマートフォンによるユーザ認証では，PIN 番号の入力などユーザのアクションを要求するものか，認識精度がユーザの物理環境に影響を受ける画像処理の技術を必要とするものが主流であった．この論文では，電話を受けるときの動作がユーザによって異なることに着目して，加速度センサーと方向センサーを用いた新しいユーザ認証の方法を提案している．認証のアルゴリズムはトレーニング用データと実際のユーザの動きの相似具合をしきい値と比べるものであるが，複数の相似の指標を定量的に組み合わせることで精度の改善に成功している．但し，１０人のテストユーザによるプロトタイプによる評価実験では，ユーザを誤認するフォールス・ネガティブ（false negative）が最善の場合でも２％程度存在することなので，適用するアプリケーションが限定される点が今後の課題となり得ると感じた．

4. 次回の会議について

次回の ACM ASIACCS 2012 会議は，2011 年 5 月 1 日から 5 月 3 日にかけて，韓国のソウル市内，The Seoul Olympic Parktel Hotel にて開催される[4]．

5. おわりに

本稿では，2011 年 3 月 22 日から同月 24 日の間に，香港の HKU SPACE Admiralty Learning Center で開催された第 6 回 ACM ASIACCS 2011 (6th ACM Symposium on Information, Computer and Communications Security)[4] に関して，その概要を紹介した．さらに，ASIACCS 2011 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　本研究は科研費（23300027）の助成を受けたものである．

参考文献

1) ACM ASIACCS 2011 (ACM Symposium on Information, Computer and Communications Security), http://www.cs.hku.hk/asiaccs2011/
2) ACM Special Interest Group on Security, Audit and Control, http://www.sigsac.org/
3) ACM ASIACCS 2011 Online Proceedings on ACM DIGITAL LIBRARY, http://portal.acm.org/citation.cfm?id=1966913&picked=prox&CFID=19680273&CFTOKEN=10948424
4) ACM ASIACCS 2012 (ACM Symposium on Information, Computer and Communications Security), http://elec.sch.ac.kr/asiaccs/