Vol.2014-CSEC-65 No.29
Vol.2014-IOT-25 No.29
2014/5/23

国際会議 NDSS2014 参加報告

穴田 啓晃[†1]　毛利 公一[†2]　山田 明[†3]

NDSS(Network and Distributed System Security Symposium)は，ネットワーク及び分散システムのセキュリティのトップカンファレンスであり，毎年サンディエゴにて開催される．この度 2014 年 2 月に開催された NDSS2014 に参加した．今回の傾向として，併催ワークショップ SENT(Security of Emerging Networking Technologies)2014 も合わせた全 63 件（各々55 件及び 8 件）の発表中，サイバー攻撃関連が 20 件で 3 割程度，またモバイルセキュリティが 14 件で 2 割程度と多かった．本稿では，サイバー攻撃関連，モバイルセキュリティに加え，興味深く聴講した発表の内容についてその概要を報告する．

A Report on International Conference NDSS2014

Hiroaki ANADA[†1]　Koichi MOURI[†2]　Akira YAMADA[†3]

NDSS (Network and Distributed System Security Symposium) is a top conference on the security of those areas, which is held at San Diego every year. Authors attended NDSS2014 that was held in February 2014.The conference, as well as SENT (Security of Emerging Networking Technologies) workshop, had a tendency that there were about 30 percent (20 presentations) which were related to cyber-attacks and about 20 percent (14 presentations) which were related to mobile security, in 63 presentations in total including 8 in SENT. In this paper, we report abstracts about content of presentations on cyber-attacks and mobile security, and on topics to which we listened with interest.

1. はじめに

NDSS(Network and Distributed System Security Symposium)は，毎年サンディエゴにて開催される，ネットワーク及び分散システムセキュリティのトップカンファレンスである．

サンディエゴは米国カリフォルニア州にある．温暖な気候と聞いていたが，今回 2 月下旬に訪問したところ日中は 20℃を上回るなど，日本の早春とは全く異なる陽気であった（図 1）．海辺に観光客が大勢散策しており，レストランのテラス席で食事を楽しむ光景も見受けられた．時差は 17 時間であり，今回の訪問でも jet lag を強く感じたが，これは致し方ない．なお，ファイタータウンと呼ばれるように，基地の街でもある（1986 年の映画”Top Gun”の舞台）．交通は，今回著者らは成田からサンディエゴへの直行便を利用した（日本航空／アメリカン航空共同運航便:2 月 22 日（土）午前着，27 日（木）正午前発）．サンディエゴ国際空港では有料だがシャトルバンを利用することが出来た（”Super Shuttle”，12 ドル．図 2 参照）．会場のカタマランホテルはリゾートホテルであり，しかし 300 名は収容可能な会議会場やバンケットホールを備えていた．フロントの対応やルームサービスは申し分無く，英語も通じ安かった．周辺にはハンバーガー，ステーキ，フィッシュ，メキシカンと，各種レストランがあり，またコンビニもあったため，会議期間中ホテル以外での食事にも困らなかった．

図 1　サンディエゴの街（会場ホテルの一室から）

図 2　サンディエゴ国際空港（シャトルバン乗車場所）

†1 公益財団法人九州先端科学技術研究所
Institute of Systems, Information Technologies and Nanotechnologies (ISIT)
†2 立命館大学情報理工学部
College of Information Science and Engineering, Ritsumeikan University
†3 KDDI 株式会社
KDDI Corporation

Vol.2014-CSEC-65 No.29
Vol.2014-IOT-25 No.29
2014/5/23

2. NDSS2014 概要

本節では，NDSS2014 及び併催ワークショップの参加者数や発表の傾向など，概要を述べる．

2.1 併催ワークショップ

NDSS2014 に先立ち，2 月 23 日（日）終日に亘りワークショップが併催された．今回は次の二つである．

- Security of Emerging Networking Technologies (SENT)
- Usable Security (USEC 2014)

SENT については著者らが出席した．

2.2 NDSS2014 の運営組織，アクセプト情報，参加者数，Session 構成と発表の傾向

NDSS2014 は 2 月 24 日（月）から 26 日（水）の 3 日間に亘って開催された（図 3）．

2.2.1 運営組織

運営組織の方々を下記に示す

Steering Group

- Thomas Hutton, San Diego Supercomputer Center (Co-Chair)
- Lynn St.Amour, Internet Society (Co-Chair)
- Lujo Bauer, Carnegie Mellon University
- Kevin Craemer, Internet Society
- Deb Frincke, National Security Agency
- Yongdae Kim, Korea Advanced Institute of Science and Technology
- Engin Kirda, Northeastern University
- Tadayoshi (Yoshi) Kohno, University of Washington
- David Molnar, Microsoft Research
- Clifford Neuman, University of Southern California
- Paul Syverson, Naval Research Lab
- Doug Szajda, University of Richmond
- Giovanni Vigna, University of California Santa Barbara
- Helen Wang, Microsoft Research

General Chair & Local Arrangements Chair

- Thomas Hutton, San Diego Supercomputer Center

Program Chair

- Lujo Bauer, Carnegie Mellon University

Publications Chair & Historian

- David Balenson, SRI International

Publicity Chair & Conference Coordinator

- Kevin Craemer, Internet Society

2.2.2 アクセプト情報

NDSS2014 のアクセプト情報を下記に示す（図 4）．

- 投稿数：295 件
- 採択数：55 件（採択率 19%．例年同様）

2.2.3 参加者数

NDSS2014 及び SENT の会議への参加者数を下記に示す．

- NDSS2014：約 250 名
- SENT　　：約 50 名

なお，日本からの参加者は，NICT，KDDI，富士通研，立命館大学，北陸先端科学技術大学院大学から各々1 名参加されており，本報告者も合わせ 6 名であった．

図 3　会場における NDSS2014 開催案内

2.3 Session 構成と発表の傾向

NDSS2014 の Session 構成を下記に示す．

- Keynote Speech
- Session 1: Network Security
- Session 2: Software and System Security
- Session 3: Security of Mobile Devices I
- Session 4: Web Security
- Session 5: Privacy
- Session 6: Authentication and Identity I
- Session 7: Crypto I
- Session 8: Authentication and Identity II
- Session 9: New Applications, Attacks, and Security Economics
- Session 10: Security of Mobile Devices II
- Session 11: Malware
- Session 12: Crypto II

発表の傾向として，全 63 件の発表中，モバイル端末関連が 14 件であり，20%強と多かった．また Mobile Devices のセッションが 2 つ設けられていた．これはここ数年の，PC からモバイル端末へのシフト（スマートフォン，タブレット端末，等）を反映していると考えられる．また，サイバー関連が 20 件であり，3 割程度であった．14 のセッション（SENT2014 が 2，NDSS2014 が 12）の中には Network Security 及び Malware など，サイバー攻撃に強く関係するセッション設けられていた．

Vol.2014-CSEC-65 No.29
Vol.2014-IOT-25 No.29
2014/5/23

3. Presentation

本節では，著者らが聴講した発表の内から数件を選び，その概要と所感を報告する．

SENT2014

“Cellpot: A Concept for Next Generation Cellular”, R. Borgaonkar, S. Liebergeld, M. Lange
(Telekom Innovation Laboratories & TU Berlin)
ハニーポットは業務妨害攻撃(DoS 攻撃)や不正アクセス等の情報を収集するが，これを携帯電話中継基地局網（Cellular Network）についても開発し評価中との発表であった．通話やデータ通信の品質を落とす Quality-of-Service Attack 等をブロックする対策を検討したとのことである．着想は単純だが重要な研究対象と考える．

図 4　第 1 日のオープニングの光景（査読のステップ）

Keynote

“Hacking the Human: The Science of Human Pentesting Perfected”, C. Hadnagy　(Social-Engineer, Inc.)
ソーシャルエンジニアリングの話題のキーノートスピーチであった．スピーカはソーシャルエンジニアリングに関するセキュリティ診断･評価及び提案で起業した人物である．実際にソーシャルエンジニアリングが脅威であることは周知であるが，これを学術面からのアプローチ（統計評価及び心理学的分析）及び事例検討により改めて脅威を示した，ユニークなプレゼン内容であった．

Session 1: Network Security

“CyberProbe: Towards Internet-Scale Active Detection of Malicious Servers”, A. Nappa[a)b)], Z. Xu[c)], M. Z. Rafique[a)], J. Caballero[a)], G. Gu[c)]
(a): IMDEA Software Institute, b): Universidad Politecnica de Madrid, c): SUCCESS Lab. Texas A&M University)
分散型 DoS 攻撃(DDoS 攻撃)を仕掛ける悪意あるサーバを，攻撃を受ける前に積極的に探し特定する発表であった．“probe”と呼ばれるパケットをブロードキャストし，サーバの反応を見る手法で，C&C サーバ，exploit サーバ，web front-ends, redirect サーバ等を検出出来るとする．

“Amplification Hell: Revisiting Network Protocols for DDoS Abuse”, C. Rossow
(VU University Amsterdam, Ruhr University Bochum)
本研究では，RDDoS (Reflective Distributed Denial of Service) に対する脅威について，UDP に基づくプロトコルを網羅的に調査して，潜在的に問題を抱えるプロトコルを提示していた．対象のプロトコルは，通常のサービスに留まらず，P2P サービス・ゲーム・ボットなども含まれていた．特に，少ない通信を増幅して大きな攻撃に変える Amplification 攻撃について評価し，攻撃に悪用される可能性があるプロトコルを 14 種類も発見した．増幅率は，NTP(Network Time Protocol)の 4,670 倍が最大であった．さらに筆者らは，管理サーバへの問い合わせ，およびネットワークの走査および巡回によって，悪用される可能性があるホストの規模を推定していた．本発表の直前にクラウドフレア社が最大 400Gbps の NTP による DDoS 攻撃を観測したと発表していたため，非常に時期を得た発表であった．

Session 2: Software and System Security

“ROPecker: A Generic and Practical Approach For Defending Against ROP Attacks”, Y. Cheng[a)], Z. Zhou[b)], M. Yu[b)], X. Ding[a)] , R. H. Deng[a)]
(a): Singapore Management University, b): Carnegie Mellon University)
Return-Oriented Programming（ROP）と呼ばれる手法は，悪意あるコードを攻撃対象の計算機に送り込むことなく，目的の処理を実現する攻撃方法である．この攻撃を防御すべく，DROP，ROPDefender，ROPGuard などの手法が提案されている．しかし，いずれの方法も対策にソースコードが必要であったり，バイナリ書き換えが必要であったり，オーバヘッドが大きいなどの問題があった．本論文で提案されている ROPecker は, x86 ベースのプロセッサに搭載されている Last Branch Record（LBR）と呼ばれる，分岐を記録する機能を活用し，実行時に実行時フローを記録しつつ，ROP 特有の動作（ガジェットと呼ばれる小さなコード片の実行の連鎖）を検出するものである．Linux にプロトタイプを実装し，その機能性と性能についての評価がなされている．本論文は，ROP 対策が提案されていることはもちろんであるが，LBR の適用例としても興味深い．

Vol.2014-CSEC-65 No.29
Vol.2014-IOT-25 No.29
2014/5/23

Session 5: Privacy

“The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network”, R. Jansen[a], F. Tschorsch[b], A. Johnson[a], B. Scheuermann[b]

(a): U.S. Naval Research Laboratory, Washington, DC,
b): Humboldt University of Berlin)

TCP/IP における接続経路の匿名化を実現するための TOR (The Onion Router) に着眼した，匿名性を損なわせるタイプの DoS 攻撃と，その対策の提案であった．TOR については他の研究会でも攻撃手法が発表されているが，本発表は TOR のプロトコルにおけるメモリの使用方法に目を付けた点が特徴的である．メモリの過剰な使用を招くことでメモリマネージャが TOR プロセスを kill するよう誘導する．結果として通信経路が明らかになる．

Session 7: Crypto I

“Decentralized Anonymous Credentials”, C Garman,
M. Green, I. Miers
(The Johns Hopkins University, Baltimore)

Decentralized な検証の枠組みを有する電子現金システムを想定した暗号学的枠組みを構成した発表であった(図 5)．例として Bitcoin を事例とする．Anonymous Credential は，そもそも 1980 年代半ばに発明されたブラインド署名の応用として発案されたものである.この，暗号の技術領域では traditional な部類に属するプリミティブが，ここ 3，4 年流行りの decentralized 化の技術と融合することで，Bitcoin をより抽象度高く，本質的に取り扱えるようになっているとの感を持った．

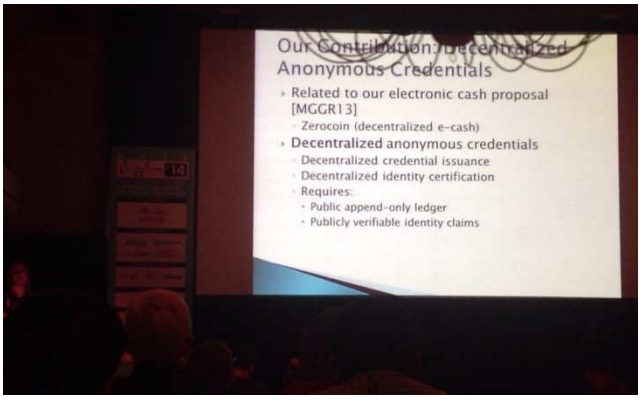

図 5　第 2 日の発表から（Decent. Anonym. Cred.）

Session 8: Authentication and Identity II

“Authentication Using Pulse-Response Biometrics”, K.B. Rasmussen[a], M. Roeschlin[a], I. Martinovic[b], G. Tsudik[a]

(a): University of California, Irvine, b): University of Oxford)

本研究では，新たな生体認証方式として，人体の皮膚に矩形電気信号を加えたときの反応を利用する方式を提案していた．3 つの論文賞の内の一つである．この方式は，PIN コードによる認証の付加的に利用することや，高い安全性が求められるシステムのキーボードの入力時に連続的に認証することを想定していた．電気信号の応答による生体認証では，人体に対して微弱な矩形電気信号(1V，0.1mA，100nsec)を加えたとき，個人に固有の反応を示すことを応用している．論文中の実験では，静的なデータセットに対して 100%の精度を示しており，数週間後の再試験において 88%の精度を達成している．所感としては，従来にない新しい生体認証を提案している点と，PIN・パスワードのような他の既存認証方式を強化するために利用できる点を評価されたと考えられる．ただし，数週間後の再試験において精度が下がっていることや，気温・湿度・皮膚の状態といった環境変化に対する頑強性が課題となりそうである．

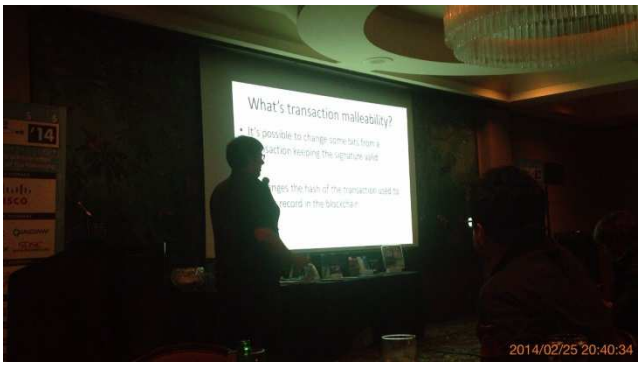

図 6　第 2 日のナイトセッションから（Bitcoin 関連）

Session 10: Security of Mobile Devices II

“AppSealer: Automatic Generation of Vulnerability -Specific Patches for Preventing Component Hijacking Attacks in Android Applications”, Mu Zhang
(Syracuse University)

Android アプリケーションには，Component Hijacking と呼ばれる脆弱性が広く発見されている．これらが攻撃者に利用されると，電話帳や位置情報などのセンシティブデータの漏洩や改ざんにつながることが知られている．このような脆弱性はもちろん修正されるべきであるが，個々の脆弱性を確認しパッチを作成するのは時間がかかる．また，開発者が脆弱性への対応に慣れているとは限らないため，開発者だけに頼るのは現実的ではない．さらに，既存研究では，静的解析によって脆弱性の可能性を解析していたため，可能性を広く見積もることが多く誤検出が多い．このような背景から，静的解析と動的解析を組み合わせて，自動で修正パッチ生成をするシステム AppSealer を提案している．AppSealer は，ソースコードのない Android アプリケーションに対してもパッチを生成することが可能で，パッチのサイズを小さく抑え，パッチによるオーバヘッド増加も抑えているといった特徴を有している．実装としては，AppSealer は Java で 16,000 行程度で実現されている．評価では，16 の実在の脆弱性に対応可能であることを示してい

る．パッチのサイズはアプリケーションのソースコードの15.9%程度に抑えられている．オーバヘッドも2%程度になっている．Android アプリケーションにおいて，パッチ自動生成を試みている点で面白い．

Session 11: Malware

“Nazca: Detecting Malware Distribution in Large-Scale Networks”, L. Invernizzi[a)], S. Miskovic[b)], R. Torres[b)], S. Saha[b)], S.-J. Lee[b)], M. Mellia[c)], Giovanni Vigna[a)], C. Kruegel[a)]
(a): UC Santa Barbara, b): Narus, Inc. c): Politecnico di Torino)
DDoS 攻撃において, マルウェアが PC にダウンロードされるフェーズに着目し，その通信状況を解析し検出する方法の発表であった．インターネットサービスプロバイダのような大規模な観測が出来る事業者に効果的な手法で, DDoS 攻撃を予測出来るようになる．

“Persistent Data-only Malware: Function Hooks without Code”, S. Vogl, J. Pfoh, T. Kittel, C. Eckert
(Technische Universität München)
従来のマルウェアからコンピュータを守る保護機能としては, tripwire, セキュアブート, カナリア等のスタック保護, ヒープ保護，W⊕X，アドレス空間のランダム化などがある．一方で，攻撃も洗練され，スタック上の shell code 実行のためにプログラムカウンタを操作する手法や，Return-Oriented Program(ROP)のような複雑なヒープ exploit もある．ROP は，プログラムコードを送り込まずに制御フローを操作するため data-only exploit とも言われ, 比較的新しい上述の保護機能を回避してしまう．しかし，data-only exploit は実行コードを持たないので，永続的に攻撃し続けることは難しい．永続的な攻撃の方法としては，関数をフックするのがシンプルな方法であるが，どのようにすれば良いだろうか．本論文では，永続的な data-only マルウェアが，rootkit の形で実現できる証拠を示している．このような，手法が存在することを示せている点で有益である．また，今後の攻撃対策にも有用である．

“Neural Signatures of User-Centered Security: An fMRI Study of Phishing, and Malware Warnings”, A. Neupane, N. Saxena, K. Kuruvilla, M. Georgescu, R. Kana
(University of Alabama at Birmingham)
本研究では，ユーザ中心セキュリティの基礎研究として，セキュリティに関わる意思決定と脳活動の関係を fMRI(functional Magnetic Resonance Imaging)
装置を利用して調査していた．3 つの論文賞受賞研究の一つである．被験者に対して，fMRI 装置の中で，フィッシングサイトを見分けることとセキュリティ警告から情報を読み取るという 2 つの課題を実施させていた．そして，それぞれの課題における脳の活動を測定することによって，実際の行動と脳の活動の関係を調査した．調査の結果，セキュリティに関する課題の際には，意思決定・警告・言語全般に関わる脳の活動が観測できた．所感としては，研究として未熟な部分が多いものの，医療分野において利用されている fMRI をセキュリティの研究に適用している点が評価できる．今後，ユーザ中心のセキュリティの研究において，さらに社会心理学・医学分野における研究が取り入れられると思われる．

図 7　コーヒーブレイクの様子

Session 12: Crypto II

“Efficient Private File Retrieval by Combining ORAM and PIR”, T. Mayberry, E.-O. Blass, A.H. Chan
(Northeastern University, Boston)
本研究では，プライバシーを考慮した情報取得において，木構造による Shi らによる ORAM(Oblivious RAM)と従来の PIR(Privacy Information Retrieval)を組み合わせることによって, 効率を改善する Path-PIR という方式を提案していた．論文賞に選ばれた 3 つの研究の内の 1 つである. ORAM は，サーバ側に要求される計算費用が小さいが，クライアントが定期的にデータベース全体をダウンロードして再攪拌する必要があった．一方，PIR は，純同型暗号によって実装されるため，クエリごとにサーバ上でデータベース全体に対して演算を行う必要があった．Path-PIR は，PIR がデータベースの要素数が比較的小さい場合に効率的なことと，木構造による ORAM が要素数を制限できることを利用して効率的な構成を実現していた．プライバシーを考慮した情報獲得は，演算能力を外部委託するクラウド環境が発展する現在において非常に重要な研究テーマであり，従来法に比べて高い計算効率 O(l・log^2 (N))を実現していることが評価できる．

Vol.2014-CSEC-65 No.29
Vol.2014-IOT-25 No.29
2014/5/23

図 8　第 3 日のエンディングの光景（次回アナウンス）

4. 補遺，むすび

NDSS はネットワーク及び分散システムセキュリティについて最先端のトピックや動向を収集するのに好適な国際会議である．また，参加者の多様さ（米国，欧州，アジア全般）から，交流・コネクション作りにも有用である．今回の NDSS2014 で，ナイトセッション（図 6）は 150 名程の参加で盛り上がり，またコーヒーブレイクでは非英語圏人の英語力を補ってもらえるだけの温かさを感じることができた（図 7）．結果，サイバー攻撃やスマートフォン，暗号といったトピックについて意見交換・交流をすることが出来た．

なお，次回の開催日程は 2015 年 2 月 8 日から 11 日であることが最終日にアナウンスされた（図 8）．場所は同じサンディエゴである（図 9）．

図 9　会場付近の風景

5. 謝辞

第一著者は本シンポジウムへの参加に関し，次の研究費に部分的に支援を受けております．ここに深謝申し上げます．

■ 総務省委託研究　国際連携によるサイバー攻撃の予知技術の研究開発「PRACTICE」

参考文献

NDSS2014Web サイト：
http://www.internetsociety.org/events/ndss-symposium-2014