Vol.2012-CSEC-57 No.7
Vol.2012-IOT17 No.7
2012/5/10

NDSS 2012 会議参加報告

溝口 誠一郎[1,a)]　須崎 有康[2,b)]　吉岡 克成[3,c)]　松浦 幹太[4,d)]

概要：本稿では，2012 年 2 月 5 日から同月 8 日にかけて，米国カリフォルニア州サンディエゴで開催された，第 19 回 Annual Network & Distributed System Security Symposium (NDSS2012) に関して報告する．会議では，コンピュータ・ネットワークシステムにおける最新の脅威と攻撃手法，ならびに対策手法が紹介された．

キーワード：会議参加報告，NDSS，Internet Society

NDSS 2012 Symposium Report

Seiichiro Mizoguchi[1,a)]　Kuniyasu Suzaki[2,b)]　Katsunari Yoshioka[3,c)]　Kanta Matsuura[4,d)]

Abstract: This paper reports on the 19th Annual Network & Distributed System Security Symposium (NDSS2012) held on February 5th to 8th , 2012, at San Diego, CA, USA. Several new threats and attack methodologies, and countermeasures was introduced.

Keywords: Symposium Report, NDSS, Internet Society

1. はじめに

本稿では, 2012 年 2 月 5 日から同月 8 日にかけて, 米国カリフォルニア州サンディエゴで開催された, 第 19 回 Annual Network & Distributed System Security Symposium[1] に関して報告する.

2. NDSS2012 の概要

2.1 開催状況について

The Network and Distributed System Security Symposium (以下 NDSS）会議 [2] は，Internet Society[3] が主催する年次カンファレンスの一つであり，その名の通りネットワークおよび分散システムにおけるセキュリティ技術に関する話題を取り扱う．NDSS 会議は 1993 年に初めて開催されてから 2012 年の開催で 19 回目を数える．会期は毎年 2 月に設定され、第 1 回目から米国カリフォルニア州サンディエゴのミッション・ベイ周辺で開催されている．NDSS2012 は，Hilton San Diego Resort & Spa にて行われた．会期は 2 月 5 日の月曜日から同月 8 日の木曜日までの 4 日間であるが、初日は Welcome セッションの開催であり、本会議は 6 日火曜日から 8 日木曜日の 3 日間で開催された.

2.2 投稿数と採択率について

表 1 に、過去 5 カ年（2008 年から 2012 年）の投稿論文数、採択論文数、採択率を示す．2008 年から 2011 年までは、投稿数は百数十件程度であったが、2012 年は倍近くの 317 件の投稿数となっており、この分野の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、NDSS2011 では

[1] 九州大学, Kyushu University
Nishi, Fukuoka, 819-0395, Japan
[2] 独立行政法人産業技術総合研究所, The National Institute of Advanced Industrial Science and Technology
Tsukuba, Ibaraki, 305-8568, Japan
[3] 横浜国立大学, Yokohama National University
Hodogaya, Yokohama, 240-8501, Japan
[4] 東京大学, The University of Tokyo
Meguro, Tokyo, 153-8902, Japan
[a)] mizoguchi@itslab.inf.kyushu-u.ac.jp
[b)] k.suzaki@aist.go.jp
[c)] yoshioka@ynu.ac.jp
[d)] kanta@iis.u-tokyo.ac.jp

表 1　NDSS2008〜2012 の投稿採択状況

	投稿数	採択数	採択率
NDSS2008	121	20	16.5%
NDSS2009	171	20	11.7%
NDSS2010	156	24	15.4%
NDSS2011	139	28	20.1%
NDSS2012	317	46/258	17.8%

2.5 日間のスケジュールであったが、NDSS2012 からフルタイムで 3 日間のスケジュールへと変更された．NDSS2012 では，317 件の投稿があり，簡単なチェックが行われた後，258 件が査読された．258 件のうち 46 件が採択された．したがって採択率は 17.8%となっており、採択率 20%未満と高い水準となっている．また，プログラム上では，Program Chair の Radu Sion 氏が選んだ 8 件の論文がポスターセッション（通常のポスターショートプレゼンテーション）に招待されている．

2.3 会議録について

NDSS2012 の会議録は、会場では USB メモリに保存された形で参加者に配布された．また、各発表の論文と発表資料が、各年の NDSS 会議ホームページ上で公開されている[*1]．

2.4 プログラムについて

NDSS2012 では、ネットワークならびに分散システムのセキュリティに関する理論的な研究と実用的な研究の双方の論文が採択されている．しかしながら、NDSS では実際のネットワーク・分散システムの設計や実装に則した実用的なセキュリティ技術について議論することが会議の方針となっており、実用面での関連性を重要視している．

NDSS2012 のプログラムは、3 日間ともシングルトラックで構成された．3 日間で 14 のセッションが設けられ、前述の 54 件の論文発表が行われた．その他に、3 件の基調講演ならびに 2 件の招待講演が設けられた．招待講演は、スポンサー企業による企業説明等が行われた．これらの講演タイトルを次に示す．

基調講演 1　“Moving the Network Security Needle Forward,” John N. Stewart (Vice President and Chief Security Officer, Cisco Systems, Inc.)

基調講演 2　“Sipping from a fire hose: the future of human information processing and security,” David Brin (Scientist and New York Times Best Selling, award-winning science-fiction author)

基調講演 3　“Authentication at Scale,” Eric Grosse (Vice President of Security Engineering, Google)

招待講演 1　“Security experimentation opportunities on the GENI platform,” Vicraj Thomas (BBN Technologies, Inc.)

招待講演 2　“Internet2’s Researcher Support Service and R&E Network Research Liaison Program,” Steve Wolff (Internet2)

続いて，NDSS2012 に設けられた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．Posters セッションでは，プログラムチェアによって選ばれた 8 件の論文発表が行われた．

- Networking(2)
- Social Networks and User Behavior(2)
- Mobile Networks
- Clouds/Crypto
- Applied Crypto
- Smartphones
- Privacy and Anonymity
- Host Security
- Web
- Distributed Systems
- Software
- Posters

NDSS2011 では，Social Networks と Smartphones が一つのセッションとなっていたが，NDSS2012 ではそれぞれが独立したセッションとなっている．さらに，Social Networks については 2 つのセッションに増えており，これらの分野の関心度が伺える．また，Wireless Attacks のセッションが，Mobile Networks のセッションへと変わっており，OS Security は Host Security となっている．NDSS2011 では，バイオメトリクスがセッション名に含まれているが，NDSS2012 ではなくなっている．また，Privacy に加え，Anonymity が新たなキーワードとして加えられた．

2.5 参加者ならびに会場の様子

NDSS2012 の参加者は 200 人程であった．日本からの参加者は 5 名であった．図 1 は，会場の様子を写した写真である．特徴的な点は，2 つの通路上にマイクが立てられており，質問がある人は随時マイクの前に並ぶスタイルをとっている点である．この形式は，Internet Society が主催する IETF 会議でも見られるスタイルである．

3. 基調講演の概要

3.1 Keynote I

基調講演 1 では，CISCO Systems の副社長であり，セキュリティ最高責任者でもある John N. Stewart 氏による講演が行われた．講演のタイトルは，“Moving the Network Security Needle Forward” である．講演の内容は，情報技術の過去，現在，そして未来を見据え，世界がどのように変化してきたかを把握し，我々が今後どのようなことをし

[*1] NDSS2012 の会議ホームページは http://www.isoc.org/isoc/conferences/ndss/12/

図 1 会場の様子

図 2 発表者と聴講者の質疑の様子

ていけばよいかを考える，というものであった．社会的あるいは技術的な変化について確認するところから始まり，現状を理解するという流れで講演が進められた．我々は「混沌であることがプロフェッショナルであると勘違いしている」と Stewart 氏は述べ，基本に立ち返り，問題をシンプルに捉え，解決のための戦略もシンプルに考えることが，我々にとって重要なことであると主張している．質疑では，未来で重要となってくる技術は何か，という質問にた対し，Stewart 氏は，仮想化と分散コンピューティングであると述べた．

3.2 Keynote II

基調講演 2 では, 科学者であり, 発明家であり, ニューヨーク・タイムズのベストセラー SF 作家でもある David Brin 氏による講演が行われた．講演のタイトルは，“Sipping from a fire hose: the future of human information processing and security” である．これからの世界に必要なことは何かという大テーマのもと，セキュリティ技術で重要なことは何かについて考えるという内容の講演であった．講演で挙げられた重要なものとして，“Reputation” “Identity” さらにこれからは，“Psudominity” と “Accountability” がオンラインの世界で重要になると Brin 氏は語る．相手をどのように認識（認証）していけばよいかについて考える，哲学的な内容の講演であった．

3.3 Keynote III

基調講演 3 は，Google の Eric Grosse 氏による講演で，タイトルは “Authentication at Scale” である．講演のテーマは Google の認証に関する取り組みで，Google アカウントの二段階認証サービスに関する背景が述べられていた．Google では，日々 10000 ものアカウントハイジャックが行われ，さらにパスワードの強度が攻撃の成功率に関係しなくなってきたと Grosse 氏は述べる．また，Google が提供するサービスでは，HTTPS を使用せず，クッキーのやり取りだけでユーザ認証を行う仕組みも存在し，そのような技術が開発された背景が述べられていた．会場からの質問では，アカウントの二段階認証に対するユーザの反響について問われる場面が多くあり，実際のユーザは二段階認証を面倒に思っていると Grosse 氏が語り，笑いに包まれる場面も見られた．

また，Google ではプライバシーを非常に慎重に扱っているが，「プライバシーを強調するグループは User Profile is eveil と言うが，profile があなたを守っているのだ.」という発言があり，プライバシー情報が個人のセキュリティに貢献しいているのを無視できない現実を確認できた．

4. 各セッションの紹介

ここでは，各セッションで発表された論文について，いくつかセッションを抜粋して紹介を行う．

4.1 Networking I, II (Session 1, 12)

Networking I では，既存のプロトコル（DTLS, OSPF）に対する攻撃，コンテンツベースのネットワークにおけるプライバシー侵害の 3 件が発表された．Networking II では，DNS に任意のドメインを生存させ続ける攻撃，ネットワークの障害発生箇所特定手法，正規表現の高速化，TLS サーバ証明書のプリフェッチなど，様々なテーマの研究発表が行われた．コンテンツベースのルーティングは，これまでの IP ベースのルーティングに変わる手法として登場している．正規表現の高速化に関する研究は，内容は純粋な数学であり，ACM CCS では Reject されたがタイトルに “Network Intrusion Detection and Prevention Systems” を加えたことで NDSS2012 では採択された，という経緯がある．

ANDaNA: Anonymous Named Data Networking Application (Steven Dibenedetto, et al., Colorado State University 他)

コンテンツベースのネットワークでは，ユーザが “Inter-

est" を発行すると，Interest がコンテンツ提供者に届きコンテンツが配送される．その際，コンテンツがノード上にコピーされるため，Interest とコンテンツが紐付けられると，ユーザのプライバシーを侵害することとなる．ANDaNA では，オニオンルーティングの考え方を用い，ユーザから最初のオニオンルータまでは Interest がわからないようにすることで，ユーザのプライバシーを保護する．会場では，Tor との違いや，実現方法について質問が挙がった．

Persistent OSPF Attacks (Gabi Nakibly, et al., National EW Research & Simulation Center, Israel 他)

OSPF では，ルーティングテーブルを作成するために，OSPF ルータが LSA (Link-State Advertisement) をやり取りする．発表者らは，攻撃者が LSA を偽装し，OSPF ルータが持つ self-defense メカニズムである fight-back を回避することによって攻撃を成功させている．発表では，どのように LSA を偽装するかが説明されており，今のところ対策は取られていないとしている．

4.2 Social Networks and User Behavior I, II (Session 2, 8)

このセッションでは，Online Social Networks におけるセキュリティが 2 件，P2P ネットワークにおける Sybil Attack 対策が 2 件，人間のセキュリティ意識に関する研究が 1 件，XSS ワーム対策が 1 件発表された．

You are what you like! Information leakage through users' Interests (Abdelberi Chaabane, et al., INRIA France)

OSN における好きなアーティストといった情報は，多くのオンラインソーシャルネットワークにおいて収集することができるが，ユーザの「興味」に関する情報が，ユーザの年齢などのプライバシー情報を推測するのに利用できる．また，同じ興味を持つ他のユーザとの相関を取ることによって，より正確にターゲットとなるユーザの個人情報を推定することができる．実験では，Facebook で収集された 10 万のプロファイルと実験に協力してくれた 2000 人分のプロファイルを用いて評価を行なっている．

Towards Online Spam Filtering in Social Networks (Hongyu Gao, et al., Northwestern University)

OSN におけるスパムは，これまでの E-mail ベースのスパムに比べてメッセージサイズの分布が異なるなどの違いがあるため，既存のコンテンツ解析によるスパム判定が難しくなっている．発表者らは，個々のメッセージ解析ではなく，スパム「活動」に着目した判定手法を提案している．スパムの活動を表す特徴量として，送信者の OSN における友達関係の深さや，他のユーザとのインタラクション履歴等を用いて，スパム判定を行なっている．

Insights into User Behavior in Dealing with Internet Attacks, (Kaan Onarlioglu, et al, Northeastern University 他)

発表者らは，ユーザのセキュリティに関する知識と実際の行動にどのような関係があるかを明らかにしようとしている．164 人の被験者に対し，3 つのセキュリティシナリオを体験させ，知識と行動の関連を調べている．

4.3 Mobile Networks (Session 3)

Mobile Networks のセッションでは，端末の位置情報に関する攻撃が 3 件，フェムトセルに対する攻撃が 1 件発表された．移動端末の位置情報の保護技術は年々増えてきているように見受けられる．

Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunications (Nico Golde, et al., Berlin Institute of Technology)

携帯ネットワークのオフロードの手法として，フェムトセルを使ったネットワーク構築手法が提案されている．発表者は，現在手に入れる事のできるフェムトセルについて，モバイルネットワークで重要な多くのセキュリティ対策が取られていないことを指摘している．考えうる攻撃は数多く，例えば，フェムトセルの場所をリストアップして地図上にマッピングすることも可能になると発表者は主張している．

4.4 Applied Crypto (Session 6)

暗号や認証あるいは匿名化を用いるシステムの実装に必要な要素技術を分析評価する論文を中心に，4 件の発表があった．中でも，セキュアチャネルに頼らずパスワード漏洩対策を施した個人認証システム（LRPS: Leakage-Resilient Password System）の限界を論じた Yan らの論文 [4] は，優秀論文賞を受賞して注目を集めた．

On Limitations of Designing Leakage-Resilient Password Systems: Attacks, Principles and Usability (Qiang Yan, et al., Singapore Management University)

Yan らは，チャレンジ・レスポンスを観測できる強い受動攻撃者まで想定し，代表的な LRPS の類型がいずれも脆弱であることを定量的に示した．また，さらなる対策は利便性と安全性のトレードオフの観点から非現実的であることを，認知科学的負荷と記憶負荷に着目した評価の枠組みに基づいて体系的に論じた．以上の結果から，セキュアチャネルに頼らず利便性と安全性を両立するためには信頼できるデバイスが必要，という主張がなされた．

なお，セッション直後のオフライン討論で「デバイス起動時にパスワードが必要ならば，結局パスワード漏洩対策になっていない」「デバイスをパスワード無しで起動できるならば，所有しているだけで本人と見なしていることに

なり，LRPS に頼らない暗号学的認証方式の方が優位」という指摘がなされ，発表者も認めていた．

4.5 Smartphones (Session 7)

スマートフォンのアプリケーションや OS に関する脆弱性ならびに攻撃をテーマとして研究発表が行われた．アプリケーションに対する攻撃が 1 件，アンドロイドマーケット上のマルウェア対策が 1 件，モバイル端末におけるコントロールフロー攻撃対策が 1 件，アンドロイド OS の特権違反に関する発表が 2 件行われた．

Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications (Sebastian Schrittwieser, et al., SBA Research)

本発表では，WhatsApp に代表されるスマートフォンのメッセージングアプリケーションについて，その認証機構に対する攻撃を試みた結果を述べている．9 種類のメッセージングアプリケーションに対して，アカウントハイジャックや盗聴などの攻撃を成功させている．発表者らは，この結果をアプリケーションの開発者に報告し，いくつかのアプリケーションでは対策がなされたと述べている．

MoCFI: A Framework to Mitigate Control-Flow Attacks on Smartphones (Lucas Davi, et al., Technische Universitat Darmstadt)

ランタイムならびにコントロールフローに対する攻撃は，スマートフォン上のアプリケーションにも広まりつつある．本発表は，iOS やアンドロイドといった ARM 上で動作する OS 上で上でコントロールフロー監視を実現する MoCFI を提案している．MoCFI のコアとなるライブラリは，NDSS2011 でも発表されている．

Towards Taming Privilege-Escalation Attacks on Android (Sven Bugiel, et al., Fraunhofer Institute for Secure InformationTechnology)

Priviledge Escalation は，2 つの異なる権限を持つアンドロイドアプリケーションがプロセス間通信を行うことにより，互いの権限を補い合う手法である．例えば，端末情報にアクセスできるアプリケーションが，インターネットと通信できる権限を持つアプリケーションとデータをやり取りし，端末情報をインターネットに送信することが可能となる．本発表では，2 つのアプリケーション間通信を，ミドルウェアレベルならびにカーネルレベルで監視を行い，Priviledge Escalation 攻撃を防ぐ手法を提案している．

4.6 Host Security (Session 10)

SecureSwitch： BIOS-Assisted Isolation and Switch between Trusted and Untrusted Commodity OSes (K. Sun，et al., George Mason University)

Trusted OS と UnTrsuted OS の 2 つの実行環境を BIOS の機能を使って切り分ける SecureSwitch を提案している．SecureSwith では CPU の実行を BIOS 機能である ACPI S4 mode による Sleep/Wakeup や SMM(System Management Mode) を使って切り替える．また，物理メモリは BIOS の DIMM スロット設定機能を使って Trusted OS と UnTrsuted OS の領域を切り分ける．現在の実装はオープンソース CoreBoot+SeaBIOS を使って実装している．今までも Trusted OS と UnTrsuted OS を切り替える研究はあったが，多くは仮想マシンモニタを使うため，負荷がかかる問題があった．しかし，SecureSwitch は BIOS 機能による軽量な切り替えを実現している．

SMART: Secure and Minimal Architecture for (Establishing a Dynamic) Root of Trust (K.E. Defrawy，et al., UC Irvine 他)

Trusted Computing で信頼の元 (Root of Trust) になるセキュアチップ TPM(Trusted Platform Modlue) のない組み込み環境で Root of Trust と実現する " SMART " を提案している．SMAET では組み込みの Micro Controller units (MCU) をハードウェアアシストとしてソフトウェアとの CoDesign で実現している．SMART は組み込み環境を想定しているが、仮想マシンモニタにも同様の技術を流用することが可能であると思えた．

4.7 Web (Session 11)

セキュアブラウザに関する研究が 1 件，悪性 URL 検出が 1 件，ブラウザのフィンガープリンティングに関する攻撃対策が 1 件発表された．

WarningBird: Detecting Suspicious URLs in Twitter Stream (Sangho Lee, et al., Pohang University of Science and Technology)

Twitter における悪性 URL 対策について取り組んでいる研究である．アクセスするブラウザによってリダイレクトされるページが変わるという特徴を用い，リダイレクトページの URL のチェーンと IP アドレスを収集し，同じ IP アドレスを持っているドメイン名を特定する．本提案では，悪性 URL の学習を行う際に，tweet の意味的特徴も利用しているところが新しい．しかしながら，共通のリダイレクトページを使わない手法も容易に考えうるため，今後の改善が必要だと感じた．

Using replicated execution for a more secure and reliable web browser (Hui Xue, et al., University of Illinois)

近年の悪性ウェブサイトは，特定のブラウザを狙った攻撃を行う傾向にある．そこで発表者らは，攻撃が特定のプラットフォームに依存していることを逆手に取り，ウェブサーバからのレスポンスをレプリケートして複数のブラウザで実行させ，挙動の違いを比較するシステム "Cocktail" を提案している．このシステムの肝は，プロキシを介して

データをレプリケートすること，ならびに安全なブラウザを “Voting (投票)” によって選ぶところである．

4.8 Posters (Session 5)

Posters セッションでは，一人持ち時間 10 分で計 8 件の発表が行われた．発表のテーマは様々で，通常のセッションと同様に，まんべんなく選ばれているように見える．いくつかの発表を簡単に紹介する．

Hubble: Transparent and Extensible Malware Analysis by Combining Hardware Virtualization and Software Emulation, Lok Yan, Syracuse University 他

ソフトウェアエミュレーションを認識するマルウェアを解析するために，ハードウェアによる仮想化環境で実行トレースを取り，そのトレースをエミュレーションで再現することで解析を容易にする Hubble の提案．

FreeMarket: Shopping for free in Android applications, Daniel Reynaud, UC Berkeley

アンドロイドマーケットにおける “in-app billing” という仕組みを悪用し，アプリケーションを無料でダウンロードする．試したアプリケーションの 50%がダウンロードできた．

Throttling Tor Bandwidth Parasites, Rob Jansen, Naval Research Laboratory

Tor ネットワークにおける，特定のアプリケーションが帯域を占有する “Bandwidth Parasites” への対策．Tor Guard Relays において，経路を Multiplexing することで帯域の Throttling を行う．

Taking Routers Off Their Meds: Why Assumptions Of Router Stability Are Dangerous, Maxfield Schuchard, University of Minnesota

特定の BGP ルータを対象に，リソースを浪費させてサービスを不能にできることを示している．CISCO のルータに対して攻撃が可能であることを確認し，現在 CISCO に問い合わせている．

Charm: A Framework for Rapidly Prototyping Cryptosystems, Joseph A. Akinyele, Johns Hopkins University

2000 年以前は，RSA や DSA といった暗号の実装を容易にするツール（OpenSSL 等）が存在したが，2000 年以降に登場した Advanced Crypto に対するツールはあまり存在しない．そこで，Advanced Crypto の実装を容易にするフレームワークを提案している．ツールは Web[5] から取得することができる．

5. 前回との比較

前回の会議と今回の会議の明らかなプログラム上の差は，Poster セッションが導入され，採録されなかったものの，評価が高かった論文を Invite していたことが挙げられる．これらの Poster は，速報的な意味合いのもので，ここで発表したとしても他の学会へ同様の内容を投稿することを妨げないようになっており，実際に Poster として投稿されていた論文のいくつかは別の会議でアクセプトされている．

また，Usenix Security 等の会議でも見られる傾向であるが，ますます脆弱性指摘，攻撃の発表が増えているように見える．実際に使われているシステムの問題点を明らかにするということはインパクトもあり，その結果採録されやすいのではないかと予想できる．システムを守る側の研究は全ての攻撃を想定しなければいけないのに対して，攻撃側の論文は穴を一つ見つければよいため，扱い易いのではないかと考えられる．

さらに，モバイル系，スマートフォン系，ソーシャルネットワーク系の発表が増加している．この傾向も NDSS 会議に限ったことではなく，セキュリティ関係の会議で全般的に言えることである．

最後に，NDSS の会議の特徴として，ネットワーク系の論文とホストセキュリティ (OS，プログラム解析) の論文がバランスよく採録されるという特徴が見受けられる．しかしながら，今年は，少しプログラム解析関係の発表件数が少なかったように見受けられた．

6. おわりに

本稿では，2012 年 2 月 5 日から 8 日にかけて，米国カリフォルニア州サンディエゴで開催された，第 19 回 Annual Network & Distributed System Security Symposium に関して報告した．会議では，身近なネットワーク・分散システムに対する最新の攻撃手法ならびに対策手法が紹介され，今後もこの分野における研究が期待されている．

謝辞 本研究の一部は，国際連携によるサイバー攻撃予知技術の研究開発（総務省）の支援を受けている．

参考文献

[1] NDSS 2012 Symposium, San Diego, CA, USA, 2012, http://www.internetsociety.org/events/ndss-symposium-2012
[2] The Network and Distributed System Security Symposium, http://www.internetsociety.org/events/ndss-symposium
[3] Internet Society, http://www.internetsociety.org/
[4] Qiang Yan, Jin Han, Yingjiu Li, and Robert H. Deng: “On Limitations of Designing Leakage-Resilient Password Systems: Attacks, Principles and Usability”, 19th Annual Network & Distributed System Security Symposium (NDSS2012), February 2012.
[5] Charm: A tool for rapid cryptographic prototyping, http://www.charm-crypto.com/Main.html