Vol.2011-CSEC-53 No.15
Vol.2011-IOT-13 No.15
2011/5/13

Network and Distributed System Security Symposium 2011 参加報告

西出隆志[†1,†2]　宮本大輔[†3]
須崎有康[†4]　吉岡克成[†5]

2011 年 2 月 6 日から 9 日にかけてアメリカのカリフォルニア州サンディエゴにて開催された The 18th Annual Network and Distributed System Security Symposium (NDSS2011) に関して報告する．

Report on Network and Distributed System Security Symposium 2011

Takashi Nishide,[†1,†2] Daisuke Miyamoto,[†3]
Kuniyasu Suzaki[†4] and Katsunari Yoshioka[†5]

This paper reports on the The 18th Annual Network and Distributed System Security Symposium (NDSS2011), held on February 6 to February 9, 2011, in San Diego, California, USA.

†1 九州大学
Kyushu University
†2 財団法人九州先端科学技術研究所
Institute of Systems, Information Technologies and Nanotechnologies
†3 情報通信研究機構
National Institute of Information and Communications Technology
†4 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology
†5 横浜国立大学
Yokohama National University

1. はじめに

本稿では，2011 年 2 月 6 日から同月 9 日の間にアメリカ サンディエゴで開催された第 18 回 Network and Distributed System Security Symposium (NDSS2011)[8] に関して報告する．

2. NDSS 概要

NDSS は Internet Society(ISOC)[5] によって主催されている年次シンポジウムであり，1990 年以降は 2 月初旬にアメリカ，カリフォルニア州サンディエゴで開催されている．本シンポジウムは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の研究者や企業研究者らの間での情報交換の促進を目指しており，またネットワークセキュリティ，分散システムセキュリティ，プライバシー保護などの暗号応用技術に関して，理論よりも実際のシステム設計や実装に焦点をあてている．それによってインターネットコミュニティへ貢献可能なセキュリティ技術の推進，普及を目指している．シンポジウムの名前にネットワークという言葉は含まれているが扱われる内容はネットワークに限定されず，コンピュータセキュリティ，システムセキュリティも含まれており，実践的なセキュリティ技術に関することを網羅している．そのため CSEC 研究会参加者にとっても有益な論文が数多く発表されていると考えられる．

3. NDSS2011

3.1 概　　要

NDSS2011 はアメリカ サンディエゴにある The Dana on Mission Bay ホテルで開催された．投稿論文総数は 139 本でありその中から 28 本の論文が採択された．それぞれの論文には 3 人の査読者が割り当てられることになっている．参考として表 1 に過去 8 カ年 (2004 年から 2011 年) の NDSS の投稿論文数，採択論文数，採択率を示す[3]．この表から分かるように採択率は例年 20%以下と低く，狭き門と言える．

本シンポジウムの参加人数は 100 名程であり，その多くはアメリカ，ヨーロッパからの

Vol.2011-CSEC-53 No.15
Vol.2011-IOT-13 No.15
2011/5/13

表 1 NDSS の投稿採択状況

	投稿論文数	採択論文数	採択率
NDSS 2011	139	28	20%
NDSS 2010	156	24	15%
NDSS 2009	171	20	12%
NDSS 2008	118	21	18%
NDSS 2007	125	18	14%
NDSS 2006	127	17	13%
NDSS 2005	124	16	13%
NDSS 2004	98	16	16%

研究者であった．

会場では 1996 年から 2011 年までの全てのプロシーディングズが含まれた CD-ROM が配布された．これらの論文データは NDSS のウェブサイトからも無料でダウンロードが可能となっている．

また今回のシンポジウムでは以下の 3 つの論文が Best Paper として選ばれた．

- “Automated Discovery of Parameter Pollution Vulnerabilities in Web Applications”
- “Location Privacy via Private Proximity Testing”
- “PiOS: Detecting Privacy Leaks in iOS Applications”

3.2 キーノートセッション

初日のキーノートセッションでは “Stuxnet – Getting to the target” というタイトルでシマンテック社の Liam O Murchu 氏による講演が行われた．この講演では Stuxnet と呼ばれるマルウェアが解説された．このマルウェアはイランの特定の組織を狙ったかのように設計されており，特定のハードウェア (Programmable Logic Controller) を対象とし USB ドライブなどを経由して感染することなどが解説された．

3.3 発 表 論 文

次に NDSS 2011 のセッション毎の論文とその概要について説明する．セッションはシングルセッションでの構成となっており，全ての発表を聞くことが可能である．内容としては実装評価まで行ったものが多く，プレゼンの中でデモを行う発表者もいた．また暗号のような理論寄りの内容であってもアプリケーションが具体的かつ実用的というのが特徴的である．

[Session 1: Secure Emerging Applications: Social Networks and Smartphones]

- “Soundminer: A Stealthy and Context-Aware Sound Trojan for Smartphones” (Roman Schlegel et al. from City University of Hong Kong)
  概要: Smartphone 上での銀行との「電話の」やり取りを録音し，解析してクレジットカード番号などの情報を盗み取る技法の研究と対策．従来の攻撃手法との違いは，(1) マルウェアで録音，録音されたデータを解析して，攻撃者に送信，　(2) マルウェアに持たせる権限を少なくする，(3) 情報解析の精度を高めるという試みがなされている．
- “A Security API for Distributed Social Networks”(Michael Backes et al. from Saarland University)
  概要: Facebook や twitter のような SNS での漏れうるプライバシー情報を守るための暗号 API の提案．例えば ACL からはユーザ間の関係が漏洩しうる．提案方式は仮名 (pseudonym) を用いたゼロ知識証明 (Schnorr 証明) から構成されており安全性は ProVerif によって自動検証されている．
- “Location Privacy via Private Proximity Testing”(Arvind Narayanan et al. from Stanford University)
  概要: 友人同士がお互い近い距離にいるときのみ通知され，そうでないときはお互いどこにいるかは秘密に保たれるサービスの提案．ロケーションプライバシーを強化するためのロケーションタグというものが導入されている．Alice と Bob がお互い近くにいるか確認するためにサーバを介してプロトコルを実行する．Android での実装評価もされている．Best paper の一つ．

[Session 2: Wireless Attacks!]

- “Relay Attacks on Passive Keyless Entry and Start Systems in Modern

Vol.2011-CSEC-53 No.15
Vol.2011-IOT-13 No.15
2011/5/13

Cars”(Aurelien Francillon et al. from ETH Zurich)
概要: 非接触の車のキー (無線を使うもの) に対し，電波漏れを Relay することにより，車の持ち主が車から離れている場合でも鍵を開ける攻撃が可能であることが示されている．攻撃を検知することは難しく，対策は車から降りた後は鍵を電波シールドするか，鍵の電源を外すなどが必要と述べられている．

- “Using Classification to Protect the Integrity of Spectrum Measurements in White Space Networks”(Omid Fatemieh et al. from University of Illinois at Urbana-Champaign)
  概要: 電波の空き周波数帯を動的に判別し利用するネットワークにおいて空いている周波数帯を占有されている報告したり，使用中の周波数帯を空いていると報告する攻撃がありうる．このような攻撃を検知する手法として，自然なシグナル送信パターンを機械学習によって記憶しておき，不自然なシグナル送信パターンを検知するという提案.
- “Good Neighbor: Ad hoc Pairing of Nearby Wireless Devices by Multiple Antennas” (Liang Cai et al. from University of California, Davis)
  概要: 2 本のアンテナを使い，Relay Attack を防止しつつ，2 つのワイアレスデバイスを安全にペアリングにする方法の提案．プレゼンでは 2 つのアンテナを持つノート PC ととデバイスがペアリングするデモが行われた．実際に動くアプリケーションとして iPhone の上で動くものも作っているとのこと．

[**Session 3: OS Security**]

- “Practical Protection of Kernel Integrity for Commodity OS from Untrusted Extensions”(Xi Xiong et al. from The Pennsylvania State University)
  概要: 悪意あるカーネル extension を想定した，カーネル内での不正改造などの識別方法の提案．ページ毎に kernel-code, kernel-data, extension-code などのラベル付けを行い，また保護領域毎に複数のページテーブルを用意し，ハードウェア支援ページングを仮定している．ハイパーバイザーで監視する防御システムで Xen で実装されている．
- “Efficient Monitoring of Untrusted Kernel-Mode Execution”(Abhinav Srivastava et al. from Georgia Institute of Technology)
  概要: 上記論文では対象がカーネル extension だったのに対し，こちらの論文は悪意あるドライバを対象としている．同様にハイパーバイザーを使って監視する．違いはドライバの行う挙動を全て監視し，またカーネル空間への jump などを監視する．
- “SigGraph: Brute Force Scanning of Kernel Data Structure Instances Using Graph-based Signatures”(Zhiqiang Lin et al. from Purdue University)
  概要: カーネルの空間のメモリをブルートフォース的に全てスキャンし，含まれているオブジェクトの型推測を行う手法の提案．メモリ走査時にグラフを構築し，シグネチャ生成を行う．フォレンジクスやルートキットの検知などに適用可能とのこと．

[**Session 4: Network Malware**]

- “Losing Control of the Internet: Using the Data Plane to Attack the Control Plane”(Max Schuchard et al. from University of Minnesota)
  概要: BGP セッションを行っているリンクの上をねらって攻撃することで，インターネットを全体をコントロール不能に追い込むことが可能であることを示している論文．攻撃の対象リンクを選別し，その上にバーストトラフィックを発生させる方法としてボットネットによる BGP ルータ同士の近傍性を評価方法などを提案.
- “EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis”(Leyla Bilge et al. from Institute Eurecom)
  概要: DNS トラフィックを観測してマルウェアに使用されているドメインをリアルタイムに発見する試み．2.5 ヶ月分の DNS データを解析し，Time, TTL, DNS Answer List, Domain Name Queried などを分析することでトレーニングデータを取得．このデータを基に提案システムを ISP に配置し，未知の不正ドメインを 3117 個発見できたと報告されている．論文の中では不正ドメインを特定するための 15 個の行動特徴を定義している．提案システムは Passive に DNS トラフィックを解析するため攻撃者が発見されることを回避するのは困難と述べられている．

Vol.2011-CSEC-53 No.15
Vol.2011-IOT-13 No.15
2011/5/13

[Session 5: Software Security / Code Analysis]

- “Howard: A Dynamic Excavator for Reverse Engineering Data Structures”(Asia Slowinska et al. from Vrije Universiteit Amsterdam)
  概要: シンボルテーブルがない C バイナリからデータ構造を抽出する方法の提案．フォレンジクスやリバースエンジニアリングに有効な技術．基本アイディアはバイナリを実行し，メモリへのアクセスパターンを QEMU を使って観測することでデータ構造を決定していく．プレゼンの中ではデモも行われた．
- “No Loitering: Exploiting Lingering Vulnerabilities in Default COM Objects”(David Dewey et al. from IBM)
  概要: COM オブジェクトを使った攻撃と対策に関する論文．プログラムから COM オブジェクトをロードすることで攻撃が発生しうる．この攻撃に対し，まだ攻撃が発生していない clean system を対象とし，全ての COM の installation API をフックし，CLSID を調べそれが pre-defined な blacklist にあれば，停止する，という手法を提案．
- “TIE: Principled Reverse Engineering of Types in Binary Programs”(JongHyup Lee et al. from Carnegie Mellon University)
  概要: バイナリプログラムからデータ構造をリバースエンジニアリングによって抽出する試み．プログラムの実行処理に基づいた型推論を行う．例えば符号ビットのチェック処理があれば符号付き整数と判定するなど．既存の REWARDS[6] などと比較してより正確な型推論が行えるとしている．
- “DTA++: Dynamic Taint Analysis with Targeted Control-Flow Propagation”(Min Gyung Kang et al. from UC Berkeley)
  概要: 動的テイント (汚染) 解析において，汚染とマークされるべきデータかマークされない Under-tainting という問題がある．この論文では Under-tainting が起こりうる制御フローを特定する DTA++を提案．
- “AEG: Automatic Exploit Generation”(Thanassis Avgerinos et al. from Carnegie Mellon University)
  概要: ソースコードを与えられ，Buggy であればその脆弱性を突くエクスプロイトコードを自動生成するシステム AEG の提案．14 のオープンソースプロジェクトを解析し，16 の制御フローハイジャックエクスプロイトの生成に成功したと報告されている (そのうちの 2 つは今まで知られていなかった脆弱性を突くもの)．またプレゼン中にデモでは strcpy の src に argv を使っている例ばかりが示された．youtube でデモを見ることができる[1]．

[Session 6: Web Security]

- “Automated Discovery of Parameter Pollution Vulnerabilities in Web Applications”(Marco Balduzzi et al. from Institute Eurecom)
  概要: HTTP Parameter Pollution (HPP) と呼ばれる攻撃がある．HTTP のクエリのパラメータにエンコードされた区切り文字を不正にインジェクトすることで問題を引き起こす攻撃である．この攻撃に対する脆弱性の有無を自動検出する PAPAS (PArameter Pollution Analysis System) と呼ばれるシステムが提案されている．1499 個の脆弱なアプリケーションのうち 46.8% がこの種の方法で検知できたと述べられている．Best paper の一つ．
- “WebShield: Enabling Various Web Defense Techniques without Client Side Modifications”(Zhichun Li et al. from NEC Laboratories America)
  概要: WebShield と呼ばれる MiddleBox(Proxy) アプローチの提案．HTML, JavaScript の処理はプロキシで行われ，その出力のみがクライアント側で trusted JavaScript rendering agent によって処理されることでクライアントを保護する．この提案方式ではインタラクティブなウェブアプリケーションも対応可能，また未知の脆弱性も発見することが可能とされている．
- “HTTPOS: Sealing Information Leaks with Browser-side Obfuscation of Encrypted Flows”(Xiapu Luo et al. from The Hong Kong Polytechnic University)
  概要: ウェブトラフィックは暗号化されていてもトラフィック解析によりパケットサイズなどから情報漏洩する可能性があると指摘されている[2]．本論文では HTTPOS と呼ばれるクライアントサイドのみの修正による対策が提案されている．HTTPOS はユー

ザレベルのプロセスで，パケットサイズや送信タイミングの変更により，暗号化されたウェブトラフィックを難読化し，トラフィック解析を無効にする．．これらを実現するために Maximal Segment Size (MSS) negotiation や HTTP Range などを使用する．

[Session 7: Network Security]

- “Accurate and Provably Secure Latency Estimation with Treeple”(Eric Chan-Tin et al. from University of Minnesota)
  概要: ノード間のネットワークレイテンシを安全に測定するためのプロトコル Treeple の提案．データの近傍性に応じてクライアントに応答するサーバを選択することなどに利用できる．形式的に安全性モデルを定義し，それに基づき提案方式の安全性を証明している．攻撃者はノードのみを乗っ取り可能で，ルータを乗っ取ることはできないと仮定されている．そして攻撃者が存在しても honest なノード間のレイテンシは正確に計算できることが保証されている．
- “On Measuring the Similarity of Network Hosts: Pitfalls, New Metrics, and Empirical Analyses”(Scott Coull et al. from RedJack, LLC)
  概要: ネットワークデータ分析のための統一的なメトリクスの提案．複数のネットワーク活動の類似性判定の自動化に利用できる．ホストの振る舞いを空間的，時間的な特性から捉え多次元空間の点として扱い，点の時系列によって表現する手法を与えている．
- “SWIRL: A Scalable Watermark to Detect Correlated Network Flows”(Amir Houmansadr et al. from University of Illinois at Urbana-Champaign)
  概要: 踏み台に使われるホスト (Stepping Stone) の検知手法として Watermark Detection がある．そのうち，パケット同士の large delay をみる packet-based watermark 方式，2 つの traffic flow の delay をみる interval-based watermarks がある．この両方にも問題があるが，本論文では 2009 年に発表された RAINBOW 方式 (packet-based)[4] をさらにスケーラブルであるように拡張した SWIRL(interval-based) を提案している．

[Session 8: Real-World Security: Cloud Computing, Biometrics, and Humans]

- “SPARE: Replicas on Hold”(Tobias Distler et al. from Friedrich-Alexander University Erlangen-Nuremberg)
  概要: Web サービス用のビザンチン障害耐性のあるシステム SPARE の提案．通常 f 個のビザンチン障害に対応するには $3f+1$ 個のレプリカが必要となる．Trusted subsystem を仮定することで $2f+1$ 個のレプリカで対応可能な方式も提案されている[9]．本提案では動かしていない VM Server を必要に応じて on/off することにより必要なレプリカを $f+1$ 台にするという試み (f 台で 2 VM あげるというアイディア)．
- “Efficient Privacy-Preserving Biometric Identification”(Yan Huang et al. from University of Virginia)
  概要: サーバが持つ暗号化された複数の生体情報のどれかにクライアントの生体情報がマッチするか (充分に近いか) 安全に計算する方式の提案．Semi-honest な攻撃者を想定したモデル．生体情報はベクトルで表現されており，(1) クライアントの生体情報と各生体情報のユークリッド距離の計算，(2) 最小のユークリッド距離の特定，(3) 最小ユークリッド距離が閾値より小さいか確認，といったことを行う．暗号要素技術としては (1)Homomorphic Encryption, (2)Oblivious Transfer, (3)Garbled circuits を使用している．ソフトウェアはプロジェクトのウェブサイト[10] で公開されている．
- “Usability Testing a Malware-Resistant Input Mechanism”(Alana Libonati et al. from University of North Carolina)
  概要: 2009 年の NDSS で発表された Bumpy[7] と呼ばれるシステムに対し，被験者を使ってユーザビリティをテストする試み．Bumpy は，(1)PC は TPM を持っている，(2) キーボードマウスと PC の間を暗号化，(3)Web Server からの転送は Trusted Monitor で監視，といった特徴を持っており，ユーザの入力値をマルウェアから保護するためのシステム．オリジナルの Bumpy に更なる改良を加えた実装により，(1)Trusted Monitor は必須，(2) グラフィカルなデザインはそれほど効果を得られなかった，などの知見が得られたと報告されている．

Vol.2011-CSEC-53 No.15
Vol.2011-IOT-13 No.15
2011/5/13

[**Session 9: Privacy**]

- “Tracker: Security and Privacy for RFID-based Supply Chains”(Erik-Oliver Blass et al. from Institute Eurecom)

  概要: RFID によるサプライチェーン管理における偽の商品情報混入攻撃への対策 Tracker の提案．Tracker では商品の辿ってきた経路情報の正当性を安全に確認することができ，攻撃者による偽造ができない仕組みを提供する．またサプライチェーンの管理者以外は商品の経路情報を得ることができず，プライバシー保護を実現している．技術的には準同型暗号を用い，多項式により経路情報を表現する．

- “PiOS: Detecting Privacy Leaks in iOS Applications”(Manuel Egele et al. from Vienna University of Technology)

  概要: iPhone には 10 billion アプリケーションがあり，一応審査 (Vetting) が行われているが，iPhone では Android のような情報漏洩が起こりえるのか，それを検証するツール PiOS の提案．PiOS は Objective-C からコンパイルされたバイナリを解析し，制御フローグラフを生成する．そして，プライバシー情報にアクセスし，それを外部へ送信する制御フローが存在するかをチェックする．1400 のアプリケーションをチェックし，多くのものがデバイス ID をリークするがパーソナル ID 情報はリークされないことを確認したと報告されている．Best paper の一つ．

- “Privacy-Preserving Aggregation of Time-Series Data”(Elaine Shi et al. from PARC/UC Berkeley)

  概要: データアグリゲータに対し個々のデータは秘匿しながらもデータの総和は計算可能である暗号方式の提案．Trusted setup によってアグリゲータと n 人の各参加者 P_i は秘密鍵 sk_i をそれぞれ持つ，ここで $0 = \sum_{i=0}^{n} sk_i$ であり，アグリゲータは sk_0 を保持し，P_i は sk_i を保持する．アグリゲーションはある一定のタイムインターバル毎に行われると仮定され，時刻 t で各参加者はデータ v_i の暗号文 $c_i = g^{v_i} H(t)^{sk_i} \bmod p$ をアグリゲータに送る．ここで H はハッシュ関数であり，g, p は公開パラメータである．アグリゲータは $g^{\sum_{i=1}^{n} v_i} = H(t)^{sk_0} \prod_{i=1}^{n} c_i$ を計算し，離散対数を解くことで総和 $\sum_{i=1}^{n} v_i$ を取得する．ここで $\sum_{i=1}^{n} v_i$ は離散対数が解ける程度の範囲であると仮定されている．

4. おわりに

以上，The 18th Annual Network and Distributed System Security Symposium (NDSS2011) の概要の報告，および発表論文の概要について報告を行った．NDSS2011 の論文は現在 (2011 年 4 月) ウェブサイト[8] からまだ参照できないが，近いうちに参照できるようになると思われる．

参考文献

1) AEG Demo.
available from ⟨http://www.youtube.com/watch?v=M_nuEDT-xaw⟩
available from ⟨http://www.youtube.com/watch?v=VPe1W7SIdBE⟩
2) S. Chen, R. Wang, X. Wang, and K. Zhang, “Side-channel leaks in web applications: a reality today, a challenge tomorrow,” In Proc. IEEE Symp. Security and Privacy, 2010.
3) Conference Acceptance Rate,
available from ⟨http://faculty.cs.tamu.edu/guofei/sec_conf_stat.htm⟩
4) A. Houmansadr, N. Kiyavash, and N. Borisov, “RAINBOW:A robust and invisible non-blind watermark for network flows,” In Proceedings of the Network and Distributed System Security Symposium, 2009.
5) Internet Society,
available from ⟨http://www.isoc.org/⟩
6) Z. Lin, X. Zhang, and D. Xu, “Automatic reverse engineering of data structures from binary execution,” In Proceedings of the Network and Distributed System Security Symposium, 2010.
7) J. M. McCune, A. Perrig, and M. K. Reiter, “Safe passage for passwords and other sensitive data,” In Proceedings of the Network and Distributed System Security Symposium, 2009.
8) NDSS2011 web site,
available from ⟨http://www.isoc.org/isoc/conferences/ndss/11/⟩
9) H. P. Reiser and R. Kapitza, “Hypervisor-based efficient proactive recovery,” In Proceedings of the 26th IEEE Symposium on Reliable Distributed Systems, pp.83–92, 2007.
10) Secure Biometrics,
available from ⟨http://www.mightbeevil.org/secure-biometrics/⟩