DIMVA 2011 会議参加報告

溝口 誠一郎† 堀 良彰† 櫻井 幸一†

†九州大学大学院 システム情報科学府/財団法人 九州先端科学技術研究所
819-0395 福岡市西区元岡 744 W2-712/814-0001 福岡市早良区百道浜 2-1-22
mizoguchi@itslab.csce.kyushu-u.ac.jp
{hori, sakurai}@inf.kyushu-u.ac.jp

あらまし 本稿では，2011 年 7 月 7 日から同月 8 日まで，オランダ・アムステルダムのアムステルダム自由大学で行われた，第 8 回 不正侵入とマルウェア検知，ならびに脆弱性アセスメント (Detection of Intrusions, Malware and Vulnerability Assessment, DIMVA 2011) 会議に関して報告する．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具体的な攻撃手法，ならびに対策手法が紹介された．

Report of DIMVA 2011 Conference

Seiichiro Mizoguchi† Yoshiaki Hori† Kouichi Sakurai†

†Graduate School of Information Science and Electrical Engineering, Kyushu University/
Institute of Systems, Information Technologies and Nanotechnologies
W2-712, Motooka 744, Nishi-Ku, Fukuoka, 819-0395, JAPAN,
2-1-22 Momochihama, Sawara-ku, Fukuoka 814-0001, JAPAN
mizoguchi@itslab.csce.kyushu-u.ac.jp
{hori|sakurai}@inf.kyushu-u.ac.jp

Abstract This paper reports on the 8th DIMVA 2011 held on July 7th to 8th , 2011, at the VU university, Amsterdam, Netherlands. Several new threats and attack methodologies, and countermeasures are introduced.

1 はじめに

本稿では，2011 年 7 月 7 日から同月 8 日の間に，オランダのアムステルダム自由大学で開催された第 8 回 Detection of Intrusions, Malware and Vulnerability Assessment (DIMVA 2011) に関して報告する．

2 会議の概要

2.1 会議概要ならびに開催状況

SIG SIDAR Conference on Detection of Intrusions, Malware and Vulnerability Assessment (以降 DIMVA) 会議 [1] は German Informatics Society (GI) 内の Special Interest Group of Security - Intrusion Detection and Response (SIDAR)[2] が主催する年次カンファレンスの一つであり，不正侵入検知，マルウェア検知，ならびに脆弱性のアセスメントに関する最新の研究成果が発表される．DIMVA 会議は，IEEE Computer Society Task Force on Information Assurance と共催となっている．

DIMVA 会議は今回で第 8 回目を迎える．第 1 回は 2004 年にドイツのドルトムントで開催された．第 2 回以降，オーストリア，ドイツ，スイス，フランス，イタリア，ドイツ，そして 2011

表 1: 採択率

開催年（回数）	採択/投稿数	採択率
2004 (第 1 回)	情報なし	情報なし
2005 (第 2 回)	15/51	29.4%
2006 (第 3 回)	11/41	26.8%
2007 (第 4 回)	12/51	23.5%
2008 (第 5 回)	13/42	31.0%
2009 (第 6 回)	10/44	22.7%
2010 (第 7 回)	12/34	35.3%
2011 (第 8 回)	11/41	26.8%

年のオランダのように，西ヨーロッパの国々を中心に開催されている．

会議録は，Springer 社の LNCS 6739 として刊行されており，同社のディジタルライブラリに収録されている [3].

2.2 採択率

DIMVA 2011 会議では，41 の投稿があり，うち 11 の Full Paper と 2 の Short Paper が採択されている．これまでの採択率を表 1 に示す．

2.3 プログラムと話題

プログラムはシングルセッションで，7 月 7 日は Keynote Speech, Invited Talk I と Network Security I, Attacks, 8 日は Invited Talk II, Web Security, Network Security II, Host Security で行われた．また併設のワークショップの syssec が 7 月 6 日に行われた．ワークショップでは，Capture the Flag などのイベントが開催され地元の大学生が競技に参加していた．

発表された研究テーマについて，DIMVA 2010 では，新しいタイプの C&C チャネルを持つボットネット対策が主要な話題であったが，DIMVA 2011 では，SNS やオンライン広告等のウェブコンテンツ・アプリケーションを対象としたセキュリティが主要な話題となっている．

2.4 参加者について

DIMVA 会議は，参加者が 100 人未満の比較的小規模な会議である．今回の参加者は約 80 人で，ヨーロッパ並びにアメリカからの参加者がほとんどであり，日本人の参加者はなかった．参加者に関して特筆すべき点は，コンピュータ・ネットワーク・ホストセキュリティの分野で先導的な立場を担っている企業からの参加者が多いことである．今回のキーノートスピーチでも，マイクロソフトリサーチや，トレンドマイクロといった企業で重要な役割を担っている人物が講演を行っており，非常に実践的・実務的な課題に焦点を当てていることが伺える．これは，投稿論文や口頭発表にも現れており，コンピュータシステムにおける脅威の具体的な攻撃シナリオの説明と，実際に攻撃を行い，その結果と対策を述べるという形が多く見受けられた．

3 発表論文の紹介

3.1 招待講演

Keynote Speech

キーノートは，Microsoft Research の Manuel Costa 氏による講演で，タイトルは，“Finding concurrency and memory errors in C++ programs” である．講演内容は，並列プログラミングにおける，共有メモリでの領域侵害への対策手法である．プログラムの対象は C++言語であるが，C++言語はマイクロソフトも含め，最も多くの開発現場で用いられているため，対策を取るべきとしている．領域侵害への対策として，共有領域にアクセスする際，その領域にオーナーシップを持たせることをアイデアとしている．コード規約のような形で，オーナーシップをコード中にアノテーションの形で宣言することで，コンパイル時に領域侵害を事前に発見することができる．また，ランタイム時にもオーナーシップを確認する機構を設けている．この機構では，オーナーシップテーブルと呼ばれるテーブルでメモリ領域のオーナーシップを管理している．さらに，解析を容易にするため，メモリ領域のオーナーシップを色情報を用いて管理することを提案している．例えば，Write 関数やオブジェクトに対して色を付け，コードレビュー時に色付けされるような工夫を行っている．

Invited Talk I

Technische Universitat Darmstadt und Fraunhofer Institute SIT の Ahmad-Reza Sadeghi 氏による講演で，タイトルは，“The Quest for

Trusted Computing: Promises, Expectations, Practice, and Challenges” である．講演では，マルチパーティトラストコンピューティング (Multiparty Trusted Computing, MTC) において，どのように「信頼」を保証するかを解説している．その中で，現実には完全な「トラスト」は存在しないが，そのトラストを数値化し，どこまでなら信頼できるかを閾値として決める必要があると氏は述べている．現在では，TPM などの Trusted Module が信頼の根源となっているが，さらには，Trust of “Root of Trust” が問題になるとしている．これからの分野として，TPM の実装が難しい Mobile Trusted Modules や，Embeded Trusted Computing あるいは Vehicular Network におけるトラストが課題となる．

Invited Talk II

Trend Micro の Max Goncharov 氏による講演で，タイトルは，“Using Traffic Direction Systems to simplify fraud... and complicate investigations!” である．トレンドマイクロ社が調査した，悪性ウェブサイトの動向に関する講演で，最近問題となっている Traffic Direction System (TDS) に関する解説と動向が紹介された．TDS とは，アクセスしてきた人の性質（国籍や趣向など）から，表示させるコンテンツを変化させる（各人に見合ったページへ誘導する）ことを目的とした仕組みで，主にウェブで用いられる．この「性質」は，ウェブのリクエストに含まれる情報から判断しており，これを “fingerprint” という．現在，このフィンガープリントを収集する悪性サイト・マルウェアが急増していることを，トレンドマイクロ社が確認しているが，対策は今のところとられていないという．このようなフィンガープリントの売買が組織的に行われており，新たなアンダーグラウンドビジネスとして注意していく必要があると述べられている．

3.2 論文紹介抜粋

3.2.1 Network Security I

ネットワークセキュリティ最初のセッションでは，DNS に対する攻撃対策，デコイを用いた侵入検知に関する発表等が行われた．

(a) Protecting agains DNS reflection attacks with Bloom filters (Sebastiano Di Paola, Telecom Italia S.p.A, et al.)

最初の発表は，DNS のリフレクション攻撃に対する対策である．DNS リフレクション攻撃は，攻撃者がソースアドレスを偽って DNS サーバにリクエストを大量に発行する攻撃である．被害者 PC の IP アドレスをソースアドレスにして DNS クエリを発行することで，それに対するレスポンスが被害者 PC へと送信され，被害者 PC あるいはそれが所属するネットワークのリソースを消耗させる．また，DNS サーバのリソースも消費される．この攻撃は，一般的な DOS 攻撃と類似しており，本発表では，パケットフィルタリングによって攻撃回避を試みている．フィルタリングのルールは，観測された DNS レスポンスが，以前発行されたリクエストの内容と一致しているかを確認する，というものである．この手法自体は簡単であるが，これを実装する場合のパフォーマンスが問題となる．発表者らは，ブルームフィルタを用いて，レスポンスが過去のリクエストによるものかを確認している．発表者らは，80 万パケット/秒のパフォーマンスを目標とし，Juniper Networks 社のルータに実装し，正規の通信を含む 600Mbps のトラフィックで，99.9%の攻撃パケットをブロックできたと述べている．質問では，フィルタをリセットする際にどのように行うかが質問としてあげられた．メモリが小さいときは，短期間でフラッシュし，メモリが大きいときはずっと残しておけるとしている．

(b) Decoy Document Deployment for Effective Masquerade Attack Detection (Malek Ben Salem, Columbia University, et al.)

マスカレードアタックと呼ばれる攻撃を前提としている．既存の手法として，正常な挙動をモデル化し，それと逸脱した挙動を検知する手法を挙げ，誤検知の問題について示している．発表者は，ホストベースでの侵入検知を行う際，デコイのファイルを配置して，それへのアクセスから検知を行う手法を提案している．攻撃者は，ファイル名やそれらが配置されている場所

の名前から，有益な情報を取得するとして，あたかもそれらしいファイルをそれらしい場所に配置し，そのファイルや場所へのアクセスを監視することで，いち早く不正な活動を検知することを提案している．デコイに HMAC を入れておき，ファイルが読み込まれたときに HMAC を調べてデコイかどうかをチェックしている．どのような場所・名前にするべきかを，実際に学生に攻撃させて，考察している．正規のユーザが操作した場合にどれくらいの誤検知が発生するかを調べている．

3.2.2 Network Security II

二つ目のネットワークセキュリティのセッションでは，一般ユーザのネットワークにおけるセキュリティアセスメント，不正アフィリエイトボット等の研究が発表された．

An Assessment of Overt Malicious Activity Manifest in Residential Network (Gregor Maier, International Computer Science Institute, et al.)

発表者らは,「一般ユーザはセキュリティ対策をとっていないのでマルウェアに感染しやすい」という一般論に着目し，それが正しいかどうかを確認する調査を行っている．3 つの一般ネットワークにおいてモニタリングを行い，ポートスキャンなどの Malicious Activity と，ユーザがセキュリティ対策をとっているかどうかを示す Security Hygiene 並びに，悪性 URL にアクセスする等の Risky Behavior の関連性を調査している．その結果，3 つのネットワークにおいて，Security Hygiene はきちんと行われているが，それと Malicious Activity との関連は無いこと，一方，Risky Behavior に対して Malicious Activity は 2 倍の発生率となると述べている．

What's Clicking What? Techniques and Innovations of Today's Clickbots (Brad Miller, University of California Berkeley, et al.)

近年，ウェブページ上の広告をクリックして不正にアフィリエイトを得る，Affiliate Fraud あるいは，Click Fraud が増加している．発表者らは，Click Fraud を行うボット，Click Bot について調査を行っている．よく知られているクリックボットの “Fiesta” と “7cy” について，その挙動と，ボットネットの構造について分析を行っている．

3.2.3 Attacks

Attack セッションでは，インターネットにおける新しい脅威について提言し，実際に攻撃を行い，その結果と対策について考えるセッションである．1 件目は，近年急速に広がりつつある SNS におけるソーシャルエンジニアリングについて，2 件目はスクリーン上のテンキーによって入力される 4 桁の PIN コードを推測する攻撃について言及している．

Reverse Social Engineering Attacks in Online Social Networks (Danesh Irani, et al.)

Facebook 等の SNS が普及したことによって，Reverse Social Engineering という新しい脅威が広がりつつある．これまでのソーシャルエンジニアリングは，攻撃者が被害者に対して接触を試みていたのに対し，リバースソーシャルエンジニアリングは，被害者側から攻撃者に接触するように誘導するのが特徴である．そこで発表者は，Facebook 上に，攻撃者になりすましたアカウントを複数作成し，どれくらいの人がアクセスしてくるかを調査している．それぞれのアカウントは異なるプロファイルを持ち，どのようなプロファイルが被害者を誘導するのに効果的かを分析している．誘導の仕方について，Recommendation-based, Demographic-Based, Visitor Tracking-Based など，様々な手法を施行している．特に，推薦ベースの手法が効果的であるとしている．また対策としては，ユーザ間のリンクの強さに基づいてアクセス制限する，あるいは，推薦する際に CAPTCHA を適用するという対策を挙げている．

Timing attacks on VoIP PIN input (Short Paper) (Ge Zhang, et al.)

画面上のテンキーをクリックして入力を行うタイプの PIN コードについて，パケット観測から「ボタンをクリックする」というイベントの発生を特定し，そのイベントの遅延時間からク

リックされたPINコードを推測する攻撃について述べられている．すべてのPINコードの組み合わせで時間を測定し，遅延時間のガウス分布を描くことでパスワードの推測を行う．例えば，PINコードが「4466」の場合は遅延時間が短いが,「1391」の場合は遅くなる，という実験結果を得ている．

3.2.4 Web Security

1件目は，近年，マッシュアップ等で利用されるようになったクライアントサイドのFlashプロキシに関する研究である．2件目はオートコンプリートなどのフォームの履歴情報をスパムメッセージで埋めてしまうスパム攻撃を扱っている．3件目は，クライアント型ハニーポットの悪性サイト検知を回避しつつ，Drive-by-Downloadを成功させる攻撃について扱った研究である．

Biting the hand that serves you: A closer look at client-side Flash proxies for cross-domain requests (Martin Johns, et al.)

クライアントサイドのFlashプロキシは，JavaScriptコードが，Flashプログラムをインターフェースとして，ウェブサーバにコンテンツを要求する手法である．ユーザのブラウザ上で実行されるため，Flashプロキシから送信されたリクエストは，あたかもクライアントのブラウザがリクエストを出したかのように見える．これを利用し，直接にはアクセスが許可されていないサイト間で，Flashプロキシを用いて間接的にアクセスすることが可能となる．また，これを応用することで，情報漏えいやセッションハイジャックなどの脅威が発生する可能性がある．

Mitigating Cross-Site Form History Spamming Attacks with Domain-based Ranking (Chuan Yue, et al.)

ブラウザのオートコンプリートを利用した新たなスパムが紹介されている．これは，ユーザが悪意のあるサイトでフォームへの入力を行った際，フォームの履歴に大量のスパムメッセージを挿入する攻撃である．攻撃を受けた後，正規のサイトでオートコンプリートを有効にすると，挿入されたスパムメッセージが表示され，ユーザビリティの低下や不快感を得ることになる．このような攻撃に対し，発表者らはドメインベースのランキング手法を用いて，ユーザが閲覧中のサイトのドメイン内で入力されたフォームのデータを，候補の先頭に表示する機能を，既存のブラウザ上に実装している．

Escape from Monkey Island: Evading High-Interaction Honeyclients (Alexandros Kapravelos, et al.)

クライアント型ハニーポットは，悪性ウェブサイトを発見･分析するのに有効なツールであるが，これらのツールは，悪性サイトを踏むことによるサイドエフェクトだけを観測しており，悪性ウェブサイトがどのような攻撃を行っているかは観測していない．発表者らは，既存のクライアント型ハニーポットについて，その異常検知機能を回避しつつ，Drive-by-Download攻撃等を成功させる手法を示している．その中で，クライアント型ハニーポットの存在を検知する三つの手法 (JavaScript-based honeyclient detection, in-memory execution, whitelist-based attacks) を紹介している．

3.2.5 Host Security

ホストベースのプログラムの不正挙動検知手法が2件発表されている．両者とも，既存の手法では対応できない，Return-Oriented Programming手法を挙げており，その攻撃に対する対策手法を提案している．また，1件目では，たとえコードインジェクションが成功したとしても，目的のコードが実行されないようにするというアプローチとなっている．

Code Pointer Masking: Hardening Applications against Code Injection Attacks (Pieter Philippaerts, et al.)

コードインジェクション攻撃に対する対策を提案している．これらの攻撃に対しては，Stack Canaryや Address Space Layout Randomizationなどの対策手法が提案されているが，RiC (return-into-libc/return-oriented programming) や HS (Heap Spraying) などの手法によって回避されてしまう．そこで発表者らは，コードポ

インタマスキング (CPM) という手法を提案している．コードポインタは，従来のファンクションポインタやリターンアドレスと置き換えられて用いられるポインタのようなものである．実行時に，ポインタの種類によって決められたビット列でマスキングされ，マスキングされた後のアドレスが実行される仕組みとなっている．そのため，攻撃者がメモリ上のアドレスを変更しても，マスキングされた後のアドレスが実行されるため，間違った場所が実行される可能性はあるが，少なくとも攻撃者の意図したコードが実行されることは無いとしている．実装はGCCの上で行われ，複数のプログラムをコンパイルし評価を行い，数%程度のオーバーヘッドで実行できたと述べられている．

Operating System Interface Obfuscation and the Revealing of Hidden Operations (Abhinav Srivastava, et al.)

システムコールを監視するセキュリティツールを回避するため，システムコールを隠蔽するルートキットが現れている．既存の対策手法は，割り込み処理やシステムコールの処理を改変して，目的のコードを実行することを前提としており，Interrupt Descriptor Table (IDT) や System Service Descriptor Table (SSDT) 等による対策が提案されているが，システムコールを隠蔽するマルウェアの登場により，状況が変化している．これらは，カーネルやドライバが利用する正規のライブラリを実行することで，目的のシステムコールを実行する，ROP の手法を用いている．発表者らは，このような攻撃を Illusion Attack と命名し，その具体的手法を論文中で紹介している．そして，Illusion 攻撃を検知するためのシステム Sherlock を提案している．これは，カーネルコードの中に watchpoint と呼ばれるコードを埋め込み，カーネルコード実行時に watchpoint も実行されるようにし，ある実行中のプログラムが，本来どのシステムコールを実行したかったかを推測するものである．システムコールと実行中のプログラムのルーチンに齟齬が発生した場合，Illusion 攻撃と判断する．Sherlock は XEN ハイパーバイザベースの監視システムで，パフォーマンス評価では，Disk-bound なアプリケーションで10%程，Network-bound なアプリケーションで1〜3%のオーバーヘッドがかかるとしている．

4 DIMVA 2012 について

来年の DIMVA 2012 会議は 2012 年 7 月にギリシャのクレタ島で開催される．会期，会議場，並びに CFP と投稿スケジュールは後日発表される予定である（2011 年 8 月末日現在）．

5 おわりに

本稿では，2011 年 7 月 7 日から 8 日にかけて，オランダ，アムステルダムのアムステルダム自由大学で開催された，第 8 回 Detection of Intrusions, Malware and Vulnerability Assessment (DIMVA 2011) 会議ならびに発表論文に関する紹介を行った．会議では，ネットワークセキュリティ・攻撃・ウェブセキュリティ・ホストセキュリティの四つのセッションが設けられ，SNS におけるリバースエンジニアリング，DNS リフレクション攻撃，ROP などの最新の脅威が紹介され，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の予知技術の研究開発 (総務省) の支援を受けたものである．また，本稿をまとめるにあたり貴重な示唆をいただいた Hua Jingyu 氏に感謝します．

参考文献

[1] Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA) 2011. http://www.cs.vu.nl/dimva2011/index.shtml.

[2] Special interest group on security - intrusion detection and response. http://www1.gi-ev.de/fachbereiche/sicherheit/fg/sidar/.

[3] Proceedings of dimva 2011, springer,. http://www.springer.com/computer/communication+networks/book/978-3-642-22423-2.