様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月 ２１ 日現在

機関番号：６２６１５
研究種目：基盤研究(B)（一般）
研究期間：2011～2015
課題番号：２３３０００２５

研究課題名（和文）未知のサイバー攻撃を検知追跡するセンサーシステムの構築

研究課題名（英文）Development of Sensor Systems to Trace and Detect Unknown Cyber Attacks

研究代表者
高倉　弘喜（Hiroki, Takakura）

国立情報学研究所・アーキテクチャ科学研究系・教授

研究者番号：７０２８１１４４

交付決定額（研究期間全体）：（直接経費）　　14,800,000円

研究成果の概要（和文）：本研究では、まず、IoT装置も含めた様々な装置に対するサイバー攻撃を観測するIPv6ベースのハニーポットを開発した。また、 疑わしいトラフィックを識別するSVMベースのアルゴリズムを提案した。さらに、それらのトラフィック中で、マルウェアによって引き起こされる通信を検出する、ファジーハッシュベースのアルゴリズムも開発した。一方で、正常なデータと悪意ある通信に完全に分離された教師データを準備することは不可能であるため、これらのアルゴリズムは、教師データなしで利用できるように開発した。
これらの技術を、実環境または実ネットワークから得られたベンチマークデータで評価し、それらの有効性を確認した。

研究成果の概要（英文）：This research has developed IPv6 based honeypots by which the attacks various types of devices including IoT ones were observed. SVM based algorithm has been proposed to identify suspicious traffics. For detecting communication caused by malwares among the suspicious traffic, Fuzzy hashing based algorithm has also been developed. Because it is impossible to prepare clean teacher data for machine learning algorithms in advance, i.e., sets of completely clean sessions and those of completely malicious sessions, these algorithms can be utilized without teacher data.
These techniques were evaluated by real environment or benchmark data obtained from the real networks. As results, their feasibility was confirmed.

研究分野：サイバーセキュリティ

キーワード：サイバーセキュリティ　攻撃検知　未知攻撃　機械学習　Fuzzy hashing　SVM　ハニーポット　マルウェア検知

１．研究開始当初の背景

サイバー攻撃に用いられる手法は高度化を続ける一方で、その対策技術はどこかで攻撃を観測した後でなければ有効な検知パターンが生成できないという後追いを強いられてきた。この状況に対し、様々な種類のセンサー(ハニーポット)を構築し、そこで収集したトラフィックデータを解析することにより、未知のサイバー攻撃の存在を察知する技術が必須のものとなった。

２．研究の目的

近年、様々なサイバー攻撃が頻繁に発生するようになり、その手法も徐々に高度化しつつある。これら新たな攻撃に共通する特長として、目的とするコンピュータに到達するまでは、目立たぬように正常な通信を装いつつ感染を繰り返すだけで、システム破壊や盗聴といった攻撃を控えるなど、その存在を認識し難くなっている点が挙げられる。

しかし、感染活動と正常な通信には僅かであるが差異が存在し、これを観測するなどにより、その存在を察知できる。また、攻撃を受けたコンピュータが発する異常パケットにより、第三者が攻撃元および被害先を推定できる。そこで、本研究では、感染や攻撃による被害拡大を最小限に留めるため、これらの不自然な通信を追跡し、その存在を特定する手法を開発する。

３．研究の方法

本研究では、まず、新種のサイバー攻撃を検知するセンサーシステムを開発する。当該システムは、攻撃を受けマルウェアに感染するが、第 3 者への攻撃機能を無効化する機能を搭載する。本システムと、既設の IDS やハニーポットにより不自然な状況の発生を追跡し、何れかでこれを察知するとインターネット空間に分散設置したセンサー間での情報交換を支援するためのデータベースシステムシステムも開発する。また、新種のサイバー攻撃に関連すると推定される通信を抽出するアルゴリズム、未使用 IP アドレスに対する攻撃、並びに、使用 IP アドレスに関する急激な状況変化を追跡し、盗聴情報を収集していると推定されるサイトを特定するアルゴリズムを開発する。

４．研究成果

(1) ハニーポットシステムの開発

未知のサイバー攻撃を受けるためのセンサーとして、平成 23 年度当時普及が想定された IPv6 空間における IoT 機器を模倣するハニーポットの開発を行った。

IPv6 では、Stateless Address Auto Configuration (SLAAC)により、機器の MAC アドレスから自動的に生成される IPv6 アドレスを使用することが一般的になる。MAC アドレスは上位 24 ビットが製造元であるベンダーコード、下位 24 ビットがシリアル番号に相当する。そこで、スキャンなどの偵察活動を観測すれば、どのメーカのどの機種を探索しているかの推測が可能であると考えた。

この仮定を元に、IPv6 アドレス空間に対する探索活動を監視するセンサー網、および、その監視結果から狙われている IPv6 機器を推定するアルゴリズム、当該機器の動作を模倣するハニーポットの開発を行った。

ただし、開発当時は IPv6 の普及が進んでおらず、実験環境において、上記の仕組みが正しく動作することを確認するまでであった。

なお、当該技術を元に、IPv4/v6 アドレス空間における、偽ネットッワーク情報の流布、IP アドレスの乗っ取り、IPv6 アドレス使用の妨害などの活動を検知する手法を開発し、名古屋大学のキャンパスネットワーク NICE4 において実証実験を行った。その後、当該ネットワークで、サイバー攻撃等のインシデント発生時の機器特定として実運用に用いている。

(2) 未知攻撃検知手法の開発

まず、未知のサイバー攻撃を検出するため、グリッド分割に基づいたクラスタリングによるトラフィック分類手法を開発した。その際、多次元空間を均等に分割するのではなく、トラフィックデータが疎に存在する領域は大雑把に、密に存在する領域はきめ細かく分類することで、クラスタ数が爆発的に増大することを抑えた。

次に、機械学習によるサイバー攻撃検出手法の開発を行った。次元数の高い多次元データであるトラフィックデータを一括して k-means 法で学習させることは計算機資源の制約上困難であることから、複数の小型の識別器を用いて、多数決によって正常な通信からの乖離度を計測する手法を開発した。さらに、k-means 法に変えて、SVM による分類手法についても開発を行った。

次に、サイバー攻撃に関与していると推定される通信について、この通信を生じさせているマルウェアが既知のものか未知のものかを判定する手法を開発した。

まずは、トラフィックフローをパケット単位にクラスタ化し、それをシーケス列として特徴化する手法を開発した。、そこで得られたシーケンス列と既知のマルウェアによって生成されたトラフィックフローのシーケンス列をアライメントアルゴリズムである Smith-Waterman 法と Needleman-Wunsch 法の統合アルゴリズムにより比較し、その類似性から既知/未知の判定を行った。

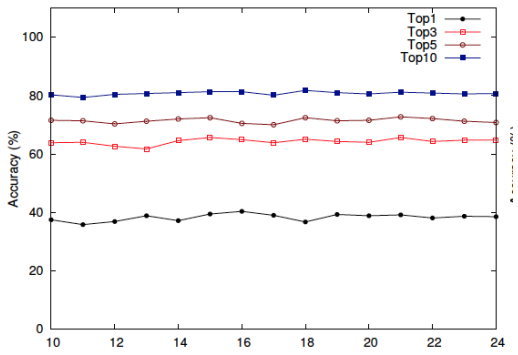

図 1：分類精度

その結果、図 1 に示す通り、上位 10 までに類似するマルウェアがない場合、80%の精度で未知のものと判定できるようになった。

さらに、類似するシーケンス列であれば類似したハッシュ列が得られる Fuzzy Hashing を用いて判定を行う手法も開発した。

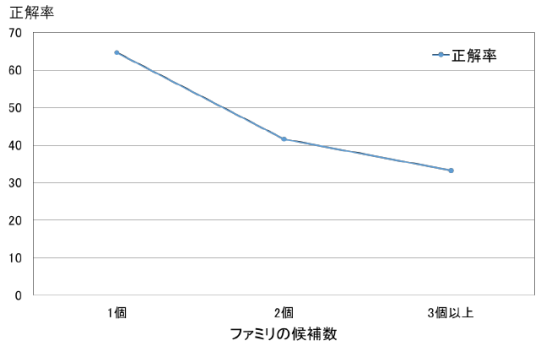

図 2：候補数の違いによる正解率

その結果、図 2 にある通りに、類似性から候補が一つに絞れるマルウェアの場合 65%、二つの場合 40%、三つ以上の場合 35%という正解率が得られた。未知のマルウェアは複数のマルウェアから関数等の機能を複製して作られる得ることが多いため、候補数が増えるほど、未知のマルウェアである可能性が高いことを意味している。

なお、平成 28 年度現在、専用 ASIC を用いた不正アクセス検知システムの処理性能は 20Gbps に留まっている。これに対し、開発したアルゴリズムのうちの一部を軽量化することでハードウェアアルゴリズムとして実装し、汎用の FPGA を用いても、10Gbps の通信をワイヤレートで識別できることを確認した。

なお、本手法を元に、spam メールを識別し、受信拒否を行う手法を開発した。本手法を実際の大学のサブドメインを用いて実証実験を行った結果、90%の spam メールに対して受信拒否が行えることを確認した。

(3) 攻撃対策支援システム

(2)で開発した手法によりサイバー攻撃が

存在する可能性を察知したとしても、有効な対策が採れなければ、攻撃が本当に存在するかの確認ができないだけでなく、本当の攻撃の場合、被害を免れることはできない。

そこで、サイバー攻撃の可能性が疑われる場合、組織内のネットワークを部分的に隔離したり、臨時のアクセス制限を施すことで、攻撃存在の確認、攻撃による被害範囲の推定、被害による業務への影響度算出を行う手法を開発した。

さらに、それらの結果から、効果が期待される対策案を提示するネットワーク管理支援システムの開発を行った。

当該システムを実際にネットワーク管理にあたっている管理者に利用してもらった結果、表 1 に示す通り、通信遮断や制限といったアクセス制御の設計に要する時間が大幅に短縮できることを確認した。

表 1：アクセス制御設計の所要時間

	システム非利用時	システム利用時
被験者 1	35 min	5 min
被験者 2	48 min	14 min
被験者 3	26 min	11 min
被験者 4	27 min	16 min
被験者 5	22 min	16 min

(4) 人材育成への応用

これらの成果を元に、次世代のネットワーク管理者およびセキュリティ技術者に求められる技能について検討を行った。これまでに開発した技術が実用化された場合、学部教育においては、マルウェア解析などの高度な技術よりも、基礎学力およびネットワーク全体を俯瞰する能力などの育成が重要であるとの結論になった。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 5 件）

1. 長谷川皓一, 山口由紀子, 嶋田創, 高倉弘喜, 標的型攻撃に対するインシデント対応支援システム, 情報処理学会論文誌, Vol. 57, No. 3, pp.836-848, 2016 年 3 月（査読有り）.
2. 北川直哉, 高倉弘喜, 鈴木常彦, 通信挙動の特異性を利用した spam 送信ホスト検出システムの開発, 電子情報通信学会論文誌, Vol. J97-D, No.5, pp.987-1000, 2014 年 5 月（査読有り）.
3. 大平健司, 山口由紀子, 八槇博史, 高倉弘喜, 星野寛, 中野博樹, インシデント対応を考慮した IPv6 ノード情報収集システムの設計と試作, 電子情報通信学会論文誌 D(インターネット技術とその応用論文特集), Vol.J96-D, No.6, pp.1483-1492, 2013 年 6 月（査読有り）.
4. Jungsuk Song, Hiroki Takakura, Yasuo Okabe, Koji Nakao, “Toward a More Practical Unsupervised Anomaly Detection System,” Information Sciences, Vol.231, doi 10.1016/j.ins.2011.08.011, pp.4-14, 10 May 2013（査読有り）.
5. 北川直哉, 高倉弘喜, 鈴木常彦, 再送動作のリアルタイム検出による spam 判別手法の実装と評価, 電子情報通信学会論文誌 D, Vol.J96-D, No.3, pp.552-561, 2013 年 3 月（査読有り）.

〔学会発表〕（計 17 件）

1. Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura, “An Automated ACL Generation System for Secure Internal Network,” The 6th Workshop on Network Technologies for Security, Administration and Protection (NETSAP 2016), Atlanta (USA), June 2016.
2. Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura, “An Incident Response Support System Based on Seriousness of Infection,” The 30th International Conference on Information Networking (ICOIN 2016), pp. 69-74, Kota Kinabaru (Malaysia), Jan. 2016
3. Satoshi Fuchigami, Hajime Shimada, Yukiko Yamaguchi, Hiroki Takakura,

"FPGA Base TCP Session Features Extraction Utilizing Off-Chip Memories," The 7th International Conference on Evolving Internet, pp.38-42, St. Julians (Malta), Oct. 2015.

4. Sohei Hiruta, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura, "Evaluation on Malware Classification by Combining Traffic Analysis and Fuzzy Hashing of Malware Binary," the 2015 International Conference on Security and Management (SAM'15), pp. 89-95, Las Vegas (USA), July 2015.
5. Yang ZHONG, Hiroshi ASAKURA, Hiroki TAKAKURA, Yoshihito OSHIMA, "Detecting Malicious Inputs of Web Application Parameters using Character Class Sequences," The 39th Annual International Computers, Software and Applications Conference (COMPSAC2015), pp.525-532, doi 10.1109/COMPSAC.2015.73, Taichung (Taiwan), July 2015.
6. Hyoyoung Lim, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura, "Malware Classification Method Based on Sequence of Traffic Flow," 1st International Conference on Informaiton Systems Security and Privacy, Angers (France), Feb. 2015.
7. Shun Yanase, Hajime Shimada, Yukiko Yamaguchi, Hiroki Takakura, Network Access Control by FPGA-Based Network Switch using HW/SW Cooperated IDS, IEICE Tech. Rep., vol. 114, no. 286, IA2014-52, pp. 91-96, Chiang Mai (Thailand), Nov. 2014
8. Shohei Araki, Yukiko Yamaguchi, Hajime Shimada and Hiroki Takakura, "Unknown Attack Detection by Multistage One-Class SVM Focusing on Communication Interval," The 2014 Cybersecurity Data Mining Competition and Workshop, Neural Information Processing Lecture Notes in Computer Science, Vol.8836, pp.325-332, doi 10.1007/978-3-319-12643-2_40, Kuala Lumpur (Malsysia), Oct. 2014.
9. Soshi Hirono, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura, "Development of a Secure Traffic Analysis System to Trace Malicious Activities on Internal Networks," The 38th Annual International Computers, Software and Applications Conference (COMPSAC2014), pp.305-310, 10.1109/COMPSAC.2014.41, Vasteras (Switzerland), July 2014 (short paper).
10. Hirokazu Hasegawa, Yukiko Yamaguchi, Hajime Shimada, Hiroki Takakura, "A Countermeasure Recommendation System against Targeted Attacks with Preserving Continuity of Internal Networks," The 38th Annual International Computers, Software and Applications Conference (COMPSAC2014), pp.400-405, 10.1109/COMPSAC.2014.63, Vasteras (Switzerland), July 2014 (short paper).
11. Hiroki Takakura, "New Detection

Technologies to Mitigate Damage of Targeted Attacks," The 6th International Workshop on Data Mining and Cybersercurity, Invited Talk, Daegu (Korea), 2 Nov. 2013.

12. Yang Zhong, Hirofumi Yamaki, Yukiko Yamaguchi, Hiroki Takakura, "ARIGUMA Code Analyzer: Efficient Variant Detection by Identifying Common Instruction Sequences in Malware Families," The 37th Annual International Computers, Software and Applications Conference (COMPSAC2013) , pp.11-20, DOI: 10.1109/COMPSAC.2013., Kyoto (Japan), July 2013..
13. Kazuya Kishimoto, Kenji Ohira, Yukiko Yamaguchi, Hirofumi Yamaki, Hiroki Takakura, "An adaptive honeypot system to capture IPv6 address scans," 2012 ASE International Conference on Cyber Security, doi 10.1109/CyberSecurity.2012.28, pp.165-172, Washington D.C. (USA), Dec. 2012.
14. Naoya Kitagawa, Hiroki Takakura, Tsunehiko Suzuki, "An Anti-spam Method Via Real-time Retransmission Detection," The 18th IEEE International Conference on Networks (ICON2012), 10.1109/ICON.2012.6506588, pp.382-388, Taipei (Taiwan), Dec. 2012.
15. Masaaki Sato, Hirofumi Yamaki and Hiroki Takakura, "Unknown Attacks Detection Using Feature Extraction from Anomaly-based IDS Alerts," The Third Workshop on Network Technologies for Security, Administration and Protection (NETSAP 2012), pp.273-277, DOI: 10.1109/SAINT.2012.51, Izmir (Turkey), July 2012.
16. Yang Zhong, Hirofumi Yamaki and Hiroki Takakura, "A Malware Classification Method based on Similarity of Function Structure," The Third Workshop on Network Technologies for Security, Administration and Protection (NETSAP 2012), pp.256-261, DOI: 10.1109/SAINT.2012.48, Izmir (Turkey), July 2012.
17. Zhong Yang, Hirofumi Yamaki and Hiroki Takakura, "A Grid-Based Clustering for Low-Overhead Anomaly Intrusion Detection," The Fifth International Conference on Network and System Security (NSS 2011), pp.17-24, Milan (Italy), Sep. 2011.

ホームページ等
http://www.takakura.com/hiroki

６．研究組織

(1)研究代表者
高倉弘喜（TAKAKURA Hiroki）
国立情報学研究所・アーキテクチャ科学研究系・教授
研究者番号：70281144

(2)研究協力者
荒木翔平（ARAKI Shohei）
淵上智史（FUCHIGAMI Satoshi）
福島達也（FUKUSHIMA Tatsuya）
長谷川皓一（HASEGAWA Hirokazu）
廣野壮志（HIRONO Soshi）
蛭田将平（HIRUTA Sohei）
Jungsuk Song
岸本和也（KISHIMOTO Kazuya）
北川直哉（KITAGAWA Naoya）
孫英敬（LIM Hyoyoung）
佐藤正明（SATO Masaaki）
柳瀬駿（YANASE Shun）
鐘揚（ZHONG Yang）