早稲田大学大学院 基幹理工学研究科

博 士 論 文 概 要

論 文 題 目

Discovering the Hidden Cyber Attacks: Machine Learning Based Approaches

伏在するサイバー攻撃の発見: 機械学習によるアプローチ

申 請 者

Bo	SUN
孫	博

情報理工・情報通信専攻 ネットワークシステム研究

2017 年 10 月

サイバー攻撃の手口は急速に進化している。サイバー攻撃は既存の攻撃検知システムから回避することを意図して開発されるため、検知困難な新たな攻撃が継続的に発生している。攻撃者は検知を回避するために、攻撃に関する情報をインターネットで通常みかけるデータと見分けがつかないように情報を偽装する。したがって、エンドユーザーがそのような攻撃に気が付き、自らを守ることは非常に困難である。たとえば、攻撃者はサービスに関する評判情報（レビュー）を共有するウェブサイトにおいて、偽のレビューを投稿することができる。攻撃者が投稿する偽のレビューは通常のユーザーが投稿するレビューと非常によく似ているため、ユーザーはこの 2 種類のレビューを区別できない。もし攻撃者が書いた偽のレビューが悪性サービスへのアクセスを誘導するものであれば、ユーザーは被害者となるリスクがある。本論文では、検知を回避することを意図して作られた巧妙な攻撃を「伏在するサイバー攻撃」と呼ぶ。伏在するサイバー攻撃は様々なサービスやアプリケーションに遍在し、ユーザーやサービスに大きな被害をもたらし得る。したがって、伏在するサイバー攻撃を早期に検出して防止することは、解決が必要なセキュリティ課題のひとつである。

そこで、本論文では、伏在するサイバー攻撃の検出という研究課題に向け、特に多くのユーザーが使うサービスである Web とモバイルに焦点を当て、これらのサービスにおいて「伏在するサイバー攻撃」を効率的に検出するための具体的な方法の開発と、その有効性を評価した結果を報告する。これらのサービスがいずれも非常に多くのユーザーが利用するため、セキュリティ課題としてのインパクトが高い。その一方で、これらのサービスはきわめて大規模な情報を扱うため、伏在するサイバー攻撃を検知するためには人手によらない、自動化された技術が必要である。そのためのアプローチとして、本研究は機械学習技術を活用する。機械学習技術の効果的な適用により、膨大なデータの中に伏在するサイバー攻撃を自動的に抽出することが期待できる。

第 1 章では、本論文の背景、目的、貢献を示す。

第 2 章では、ウェブ空間に伏在する攻撃を対象とする対策法とその有効性を報告する。ウェブサイトのアドレスを示す識別子として Uniform Resource Locator（URL）が利用されている。一般に URL を見ただけではそのウェブサイトが良性なものであるか、悪性なものであるかを判定することは困難である。すなわち悪性な URL は通常の URL に伏在している。URL が悪性なものであった場合、その URL にアクセスしたユーザーはドライブバイダウンロード攻撃と呼ばれる攻撃の被害に遭う可能性がある。ドライブバイダウンロード攻撃は、悪性の JavaScript コードを利用することでユーザーの Web ブラウザの振る舞いを制御し、マルウェアを自動的にインストールすることを狙いとした攻撃である。そのような攻撃を阻止するアプローチとして、URL のブラックリストを構築するアプローチがある。このアプローチは実用的であり、悪性 URL からユーザーを保護

する手段として広く利用されている。URLブラックリストを構築する上での課題は、一般に悪性なURLの寿命が非常に短いため、常に有効な悪性URLを更新し続けることが必要不可欠である。すなわち、広大なウェブ空間に伏在する悪性URLを効率的に探し当てるための技術が必要である。従って、この問題（伏在する悪性URLの効率的な検索）を最初の研究課題とする。

本論文では、この問題を解決するために、既存の悪性URLをヒントとして新たな悪性URLを自動的かつ効率的に検索・収集する、自動ブラックリスト生成システム（AutoBLG）を提案する。主要なアイディアは任意の悪性URL群と類似した特徴を持つURLを検索することにある。従来手法では、様々な既知の悪性URLと良性URLの特徴を学習した上で、テスト対象となるURLが良性であるか、悪性であるかを判定する技術が提案されてきた。これに対し、本研究は特定の性質を有することがわかっている悪性URLの集合を用意し、その集合に属する確率が高いURLを未知のURL群から検索するアプローチをとる。すなわち単純に悪性・良性の判定を行うのではなく、悪性の中でも特定の固有な性質に着目し、それらの特徴を有する確率が高いURLを抽出することに特徴がある。そのような判定を実現する機械学習技術として、Bayesian Setsを用いている。また、検索の対象となるURLを過去に攻撃に使われたウェブサイトのIPアドレスおよびそれらに紐づけられたDNS情報から導き出すことにより、検索対象の爆発を抑制する工夫をしている。実データを用いた性能評価の結果、同一のExploit kitを用いて作成された悪性URLやフィッシングに用いられる悪性URLを高精度に検索できること、さらに一連の検索が従来的な方法と比較して高速であることを実証した。

第3章では、モバイルアプリストアにおけるプロモーション攻撃の対策法とその評価結果を示す。スマートフォン等の端末ではアプリをインストール際にモバイルアプリストアを利用する。例えばGoogle PlayはAndroid端末が用いる公式のモバイルアプリストアである。一般にモバイルアプリストアは、アプリに関する情報として、アプリのレーティング、レビュー、インストール数、カテゴリ等の情報を提供している。ユーザーはモバイルアプリストアでアプリを検索し、アプリのレーティング、レビュー、およびその他の情報を参考として、そのアプリをインストールするかしないかを決定する。したがって、レビュー情報等を意図的に操作することにより、ユーザーの意思決定に影響を与えることができる可能性がある。より具体的には攻撃者は、偽のレーティングやレビューを多数投稿することにより、ユーザーに悪性アプリをインストールするよう誘導するプロモーション攻撃（PA）を行う可能性がある。一方、攻撃者は巧妙にレビュー情報を投稿するため、一般のレビュー情報と見分けをつけることが困難である。つまりそのような悪性レビューは通常のレビューに伏在する状況である。本論文では、モバイルアプリストアにおける伏在するプロモーション攻撃を第二の研究課題と

する。

本論文では、上記の研究課題に取り組み、プロモーション攻撃を行う可能性のある悪性ユーザーを検出する PADetective というシステムを開発した。主要なアイディアは、マルウェアに対してのみレビューコメントを投稿していた悪性ユーザーを抽出し、それらの悪性ユーザーに特徴的なレビューコメントの特徴を機械学習によって学習することにある。はじめに 1723 個のラベル付きレビューコメントのデータセットを作成し、そのデータを用いて PADetective システムの性能評価を行ったところ、真陽性率が 90%、偽陽性率が 5.8%を達成し、実用的な精度を達成可能なことを検証した。つぎに 100 万個のアプリに対して 2,000 万人のユーザーが評価した 5,700 万のレビューデータセットに対して PADetective システムを適用することによって、脅威の特徴を明らかにした。その結果、289 の潜在的な PA 攻撃アカウントを検出した。これらの潜在的な PA 攻撃者は、21,000 の悪性アプリを含む 136,000 のアプリに対してレビューを投稿していた。また、潜在的な PA 攻撃者がコメントを投稿したアプリの中にはアンチウィルスチェッカーによって検出されなかった伏在する悪性アプリも含まれていた。

第 4 章では、この論文の課題と今後の研究方向について論じる。伏在する攻撃が存在する対象はウェブやモバイルの他にも多岐にわたるため、今後は本研究で培った知見を他の領域、例えば Internet of Things (IoT)における検討に研究を拡張することができる。また、攻撃者が新しい脆弱性などを悪用することにより、本研究の提案システムからの検知を回避する可能性がある。そのような検知回避を未然に防ぐため、常に最新の特徴で検知モデルを更新する技術の開発は今後の有望な研究方向性のひとつである。さらに、データ収集・分析のオンライン化と動的なデータ収集システムの構築などが今後の研究発展として考えられる。

第 5 章では、伏在するサイバー攻撃に対して本研究が提示した 2 つの解決策の内容と、有効性を検証した結果をまとめる。

本論文では、2 つの異なるタイプの伏在するセキュリティ脅威に対する共通の対策として、機械学習のアプローチを効果的に活用した方法を提案し、実データを元にしてその有効性を明らかにした。このようなアプローチにより、セキュリティオペレータやマルウェア解析者にとって有効な支援ツールの提供が可能となる。本論文が提案したアイディアや手法は、他の伏在するサイバー攻撃への対策にも有効であり、この研究領域のさらなる発展が期待できる。

早稲田大学　博士（工学）　学位申請　研究業績書

氏名　孫　博　　印

（2017年11月　現在）

種類別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
○論文	Bo Sun, Xiapu Luo, Mitsuaki Akiyama, Takuya Watanabe, and Tatsuya Mori, “PADetective: A Systematic Approach to Automate Detection of Promotional Attackers in Mobile App Store,” Journal of Information Processing. (掲載決定)
○論文	Bo Sun, Mitsuaki Akiyama, Takeshi Yagi, Mitsuhiro Hatada, and Tatsuya Mori, “Automating URL Blacklist Generation with Similarity Search Approach,” IEICE Transactions on Information and Systems, Vol.E99-D, No.4, pp. 873-882, April 2016.
○国際会議	Bo Sun, Mitsuaki Akiyama, Takeshi Yagi, Mitsuhiro Hatada, and Tatsuya Mori, “Characterizing Promotional Attacks in Mobile App Store,” Proceedings of the 8th International Conference on Applications and Techniques in Information Security (ATIS 2017), pp. 113-127, July 2017 (BEST PAPER AWARD).
○国際会議	Bo Sun, Mitsuaki Akiyama, Takeshi Yagi, Mitsuhiro Hatada, and Tatsuya Mori, “AutoBLG: Automatic URL Blacklist Generator Using Search Space Expansion and Filters,” Proceedings of the Twentieth IEEE Symposium on Computers and Communication (ISCC 2015), pp. 205-211, July 2015.
国際会議（招待講演）	Bo Sun, Xiapu Luo, Mitsuaki Akiyama, Takuya Watanabe, and Tatsuya Mori, “Understanding Promotional Attacks in Mobile Software Distribution Platform,” The 44nd APAN Meeting, Network Security Workshop, August 2017
国際会議（招待講演）	Bo Sun, Mitsuaki Akiyama, Takeshi Yagi, Mitsuhiro Hatada, and Tatsuya Mori, “Automatic Generation of URL Blacklist,” The 42nd APAN Meeting, Network Security Workshop, August 2016
国際会議（ポスター）	Bo Sun, Aakinori Fujino, Tatsuya Mori, “Toward Automating the Generation of Malware Analysis Reports Using the Sandbox Logs,” Proceedings of 23rd ACM Conference on Computer and Communications Security 2016 (ACM CCS 2016), October 2016.
国際会議（ポスター）	Bo Sun, Takuya Watanabe, Mitsuaki Akiyama, Tatsuya Mori, “Seeing is Believing? The analysis of unusual ratings and reviews on Android app store,” Proceedings of 18th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2015), November 2015.
講演	孫博, 秋山満昭, 森達哉, “Towards Automatically Detecting Promotional Attacks in Mobile App Store,” コンピュータセキュリティシンポジウム 2016 論文 集, vol. 2016, No. 2, pp. 1040-1047, 2016 年 10 月 (MWS 優秀論文賞)
講演	Bo Sun, Mitsuaki Akiyama, Takeshi Yagi, Mitsuhiro Hatada, and Tatsuya Mori, “Building statistical URL blacklist generation system for web security,”

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
	Hanyang-Waseda IT workshop 2015, November 2015.
講演	Bo Sun, Takuya Watanabe, Mitsuaki Akiyama, Tatsuya Mori, “The analysis of unusual ratings and reviews on Android app store,” Android Security Mini Workshop, November 2015.
講演	孫博, 渡邉卓弥, 秋山満昭, 森達哉, “Android アプリストアにおける不自然な レーティング・レビューの解析,” コンピュータセキュリティシンポジウム 2015 論文集, vol. 2015, No. 3, pp. 655-662 , 2015 年 10 月.
講演	孫博, 秋山満昭, 八木毅, 森達哉, “広大な web 空間を対象とした悪性 URL 検索技術,” 信学技報, vol. 114, no. 340, ICSS2014-61, pp. 61-66, 2014 年 11 月.
講演	孫博, 秋山満昭, 八木毅, 森達哉, “既知の悪性 URL 群と類似した特徴を持つ URL の検索,” コンピュータセキュリティシンポジウム 2014 論文集, vol. 2014, No. 2, pp. 1-8, 2014 年 10 月.
その他（国際会議）	Yuta Ishii, Takuya Watanabe, Fumihiro Kanei, Yuta Takata, Eitaro Shioji, Mitsuaki Akiyama, Takeshi Yagi, Bo Sun and Tatsuya Mori, “Understanding the Security Management of Global Third-Party Android Marketplaces,” Proceedings of the 2nd International Workshop on App Market Analytics (WAMA 2017), September 2017.
その他（国際会議）	Takuya Watanabe, Mitsuaki Akiyama, Fumihiro Kanei, Eitaro Shioji, Yuta Takata, Bo Sun, Yuta Ishii, Toshiki Shibahara, Takeshi Yagi and Tatsuya Mori, “Understanding the Origins of Mobile App Vulnerabilities: A Large-scale Measurement Study of Free and Paid Apps,” Proceedings of IEEE/ACM 14th International Conference on Mining Software Repositories (MSR 2017), May 2017.
その他（講演）	守屋潤一, 孫博, 森達哉, 後藤滋樹, “標的型攻撃の被害者となる人を予測することは可能か?” 暗号と情報セキュリティシンポジウム (SCIS 2017), 2017 年 1 月.
その他（講演）	竹越健斗, 孫博, 森達哉, “Twitter におけるフォロワーマーケットの実態調査 とフェイクアカウントの抽出方法”, 暗号と情報セキュリティシンポジウム (SCIS 2016), 2016 年 1 月.