SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

脆弱性の概念実証コードに対する網羅的な攻撃パケット生成を用いた侵入検知システムのシグネチャ自動生成

Automatic Signature Generation for Intrusion Detection Systems by Generating Packets Exuhaustively from Proof of Concept Code of Vulnerabilities

小林 雅季 * 鐘本 楊 † 小谷 大祐 * 岡部 寿男 *
Masaki Kobayashi Yo Kanemoto Daisuke Kotani Yasuo Okabe

キーワード ネットワークセキュリティ、HTTP、侵入検知システム、シグネチャ自動生成、PoC コード

あらまし

近年、多種多様なシステムが開発されているが、それに伴い多くの脆弱性が発見されている。これらの脆弱性に対する攻撃を防ぐには、脆弱性情報を日々収集して対策を行う必要があるが、脆弱性の件数自体が膨大であり、この作業を滞りなく実施し続けることは困難である。

ここで、攻撃活発化の一因として、攻撃の実現可能性を示す PoC(Proof Of Concept) コードがパッチ開発促進等のために公開されることが挙げられる。本来、脆弱性への攻撃を行うには、その脆弱性の原理を理解し、ターゲット上で所望の動作を実現するコードの記述が必要であるが、PoC コード公開により、その手間が不要となる。このように、正当な目的で公開されたコードが悪用される可能性があり、公開後は早急な対策が必要となる。

本研究では、そのような攻撃への対策として、侵入検知システム (IDS) のシグネチャを生成し、管理するネットワーク上に設置することで対策を行うことを考える。本来、シグネチャの生成には熟練した専門家による分析が必要であるが、脆弱性の再現や分析に時間がかかり、加えて、前述の通り脆弱性の件数自体が増加しているため、本研究によってその自動化を図る。

関連研究として、シンボリック実行を利用した解析によってシグネチャ生成を行う MetaSymploit[1] があるが、対象の言語やライブラリの拡張が必要で、実装コストが高い。また、IoT の脆弱性に絞った手法としてインターネット上の脆弱性情報の集約によりシグネチャを生成する IoTShield[2] が提案されているが、動的に生成される箇所をシグネチャとして抽出することが出来ない。

本研究では、PoC コードの中でも、Metasploit と呼ばれるツール・Python による、HTTP 通信を行うコードに対し、シンボリック実行を模倣した解析によるシグネチャの自動生成手法を提案する。提案手法は 3 つの段階から成る。1 段階目では、抽象構文木を用いてコードの制御パスを全列挙し、それぞれのパスに従う攻撃コードを生成する。2 段階目では、生成したコードを実行し、攻撃対象に送出されるパケットを採取する。3 段階目では、まず、HTTP リクエストの抽出と、そのクラスタリングを行う。次に、各クラスタ内で極大部分文字列を利用して特徴文字列集合を抽出し、シグネチャとする。

評価実験としては、インターネット上から Metasploit・Python による HTTP 通信を行う PoC コードを収集し、提案手法によって生成されたシグネチャの生成時間と、そのシグネチャによる検知の真陽性・偽陽性の程度について調査した。その後、その結果を踏まえて、本手法の特性・適用できる PoC コードの種別について考察を行う。

参考文献

[1] Ruowen Wang et al.,“MetaSymploit: Day-One Defense against Script-based Attacks with Security-Enhanced Symbolic Analysis” USENIX Security 13，65-80, 2013

[2] Xuan Feng et al.,“Understanding and Securing Device Vulnerabilities through Automated Bug Report Analysis” USENIX Security 19，887-903，2019

* 京都大学, 〒 606-8501 京都府京都市左京区吉田本町, Kyoto University, Yoshidahonmachi, Sakyo Ward, Kyoto, 606-8501
† NTT 社会情報研究所, 〒 180-8585 東京都武蔵野市緑町 3-9-1, NTT Social Informatics Laboratories, 3-9-11 Midori-cho, Musashino-shi, Tokyo 180-8585