不正アクセス対策向け脆弱性情報の自動構築に向けた考察

2H−06

三友 仁史、滝澤 文恵、鳥居 悟、小谷野 修
富士通株式会社

1. はじめに

分散型サービス不能化(DDoS)攻撃等の不正アクセス対策においては、脅威とパッチ、想定被害などをまとめた脆弱性情報を基に、適切な方策を判断し、迅速にそれを実施する必要がある。

しかし、既存の脆弱性情報を取り扱う場合には、以下のような問題が存在している。まず、脆弱性情報の個々の記載内容は充実されてきているが、依然として、本当に知りたい各情報間の相互関連が整理されていない。また、脆弱性情報は、種々の情報源から、一カ月に延べ数百件も発信されているため、そのような関連付けを行うことは非常に高コストとなる。最後に、そのような相互関連を調査／公開する活動として、著名なものにCVE(Common Vulnerabilities and Exposures)[1]があるが、公開に遅延が生じるケースがあり、不正アクセス対策の迅速な実施のために参考とするには不満が残る。

我々はこのような課題を解決するため、複数の情報源から広く情報収集し、それぞれの記載内容の補完・相互関連付けを行い集約することで、情報の精度と網羅性を高めた脆弱性情報 DB を自動構築することを目指している。本発表では、その実現のキーとなる情報集約にフォーカスし、自動化へ向けた検討について述べる。

2. 集約試行実験

我々は、この問題に以前から取り組んできた[2]。このようなDB自動構築のために必要なことは、脆弱性情報の「収集」の自動化と、「集約」の自動化で言い尽くされる。収集の自動化については、スクリプトによって定期的にオリジナル脆弱性情報のコピーを漏れなく取得することによって、ほぼ実現される。

本発表では、残った集約の自動化にフォーカスする。ここで情報の「集約」とは、多くの脆弱性情報に対して、同一の脆弱性について記述した情報同士をそれぞれまとめあげることである。これにより、各情報がお互いの内容を補完し合うことになるため、一つの脆弱性について知りたいユーザが、容易に網羅的な情報を得ることができる。

我々は[2]において、自動構築の鍵を握る「脆弱性情報の集約化」を手作業によって試行した。ここで、集約化作業の軽減化策として、集約化のための情報照合は、専門家による内容の判断をせずに、単純にキーワードを用いた照合によるものとした。このような集約化を行う作業を通じて、有効なキーワードを収集すると共に、照合の判定ルールや記載項目を確立することが出来た。

3. 集約試行から得られた知識

ここでは、集約試行の結果明らかになった知識として、脆弱性情報における固有の特質について紹介する。脆弱性情報を集約する手順を確立するためには、これら知識を最大限に利用する事が不可欠である。また、これら知識は、現状で課題として残っている今後の要検討点を洗い出す際にも有用となる。

3.1. 共通のフィールドが存在

発信元によらない共通のフィールドがいくつか存在する。例えば、SecurityFocus[3]、X-Force[4]、CyberNotes[5]といった著名なサイトが公開する脆弱性情報には、情報のタイトル、発信日、参照先(後述)に対応するフィールドそれぞれが含まれている。

3.2. タイトルの継承

脆弱性情報のタイトルは、どこかで付与されたものがそのまま、或いは小さな変更を加えられて、継承されることが多い。したがって、同一の脆弱性について記述した複数の情報においては、タイトルの相関関係が認められる。

3.3. アドバイザリを参照

アドバイザリ（advisory）は、ベンダ、公的機関などが必要に応じて発行する、脆弱性に関する警戒警報のことであり、一種の脆弱性情報である。アドバイザリは、その性質上、内容に対する信頼性が高く、情報公開時期が早い。このため、一般的な脆弱性情報では、参照先としてこのようなアドバイザリへのリンクを有することが多い。

3.4. 関連ある脆弱性情報の発信日が近似

脆弱性情報の公開には発信元それぞれでタイムラグがある。しかし、同一脆弱性について記述された情報は、異なるサイトにおいても、ほぼ１０日間の間に一斉に公開されることが判明した。

3.5. 特有なスラングを包含

脆弱性情報はアンダーグラウンドに潜むクラッカーが書いた情報が元になっていることも多く、特有のスラングが用いられることがある。例えば、DDoS

Consideration for Automatically Organizing Vulnerability Information
Masashi Mitomo, Fumie Takizawa, Satoru Torii, Osamu Koyano
FUJITSU LTD.

攻撃において負荷を生成するホストの呼称には、(DDoSの)踏み台、エージェント、ゾンビ、等がある。

4. 集約試行結果の集計

ここでは、集約試行の結果について、簡潔に評価する。集約試行の結果は、CVE と比較することにより、相対的に評価を行うこととした。この結果、現状の集約結果の正解率(全情報に対して CVE と整合性が取れている情報の割合)は、56.7%である。

なお、CVE と整合性が取れない場合が発生した支配的要因は「集約の粒度の粗さ」にあった。すなわち、CVE においては形の上で同一の脆弱性をプラットフォーム毎に分けて集約するのに対し、我々はそうでなかったからであると類推される。これは、方針の違いであり、どちらが正解ということはない。なお、もし集約の粒度の粗さによって集約が失敗したと見られるエントリをすべて正解に導けば、正解率は飛躍的に向上し89.7%となる。このことは、専門家を介した情報集約結果の大部分は、簡便な手法で機械的に行うことによっても得られることを示している。したがって、我々の集約手法は妥当である。

5. 集約の自動化に向けた考察

ここでは、集約化を自動化する際に障害となりうる問題点を洗い出し、自動集約化ツール構築への手がかりを得ることを目指した検討を行う。

5.1. 課題

情報集約を自動化するためには、情報の照合を自動化すれば良い。以下では、照合技術として、簡易なキーワード照合を採用することとする。これは、２つの情報それぞれからいくつかの対応する「(照合のための) キーワード」を抽出し、それらを互いに照合することによって、情報の照合を行おうとするものである。この手法のポイントは、以下である。

① キーワードの選択
② キーワードの照合
③ キーワード照合結果の情報照合結果への反映

以下では、これら３課題について順に説明する。

5.2. キーワードの選択

キーワードとしては、タイトル、参照先(アドバイザリ)、発信日が有効である。その理由を以下に示す。

キーワードの要件として以下の２点が挙げられる。

1） 脆弱性情報からの抽出が容易
3.1節にある通り、これら３つは特定のフィールドを割り当てられており、抽出が容易に行える。

2） 関連情報同士を結びつける効果が大
3.2〜3.3節にある通り、タイトル、及び参照先は、同一の脆弱性に関する複数の脆弱性情報に対して、非常に類似している。また、3.4節にある通り、発信日についても強い相関関係が認められる。

したがって、上記３つはキーワードとして適切であることが導かれる。

なお、脆弱性のプラットフォームもキーワードとして採用し、CVEと同じ方針(4章参照)で集約を行うことも考えられるが、シンプルさを重視し、これまで通りの方針を踏襲することにする。

5.3. キーワードの照合

異なる２情報におけるキーワード同士を照合する際には、キーワードを包含するフィールドに対し、それらをマッチングが図れるような統一的な記述に変換を施す必要がある。

しかし、ここには以下の問題ある。3.5節の通り、脆弱性情報にはスラングが用いられていることも多く、その使用傾向は情報作成者によってまちまちである。また、このような文書の照合には常に付きまとう問題であるが、表記の揺れを解決する必要もある。これらの問題については、自然言語処理に一般に用いられている手法の適用によって解決が可能であると思われる。

5.4. キーワード照合結果の情報照合結果への反映

キーワード照合はあくまでも情報照合のための道具である。すなわち、キーワード同士を照合した結果を、情報照合と関連付けなければならない。ここにはいくつかのギャップが存在し、それらは明確に解決されねばならない。

「キーワードの照合結果」を「情報の照合」に結びつけるためには、「異なる情報の符合条件」を定める必要がある。これは、具体的には、それぞれの「キーワードの照合結果」に重み付けを行うことである。また、この重み付けは、照合する２情報の発信サイトによって変化することも必要である。詳細の検討については、今後の課題とする。

6. まとめ

脆弱性情報 DB の自動生成のキーとなる情報集約に関して、脆弱性情報における固有な特質、及び脆弱性情報 DB を自動構築するための基礎となる知見を得ることが出来た。

今後は、今回得た知見を元に、脆弱性情報の自動集約化の実現に向けた研究に取り組む予定である。

謝辞

本研究は、通信・放送機構の委託研究テーマ「サービス不能化 (DDoS) 攻撃に対する防御技術に関する研究開発」の一環として行われているものである。

参考文献

[1] http://www.cve.mitre.org/
[2] 滝澤 他, “不正アクセス対策DBの自動構築に向けた考察”, 情報処理学会第 62 回全国大会, Mar. 2001
[3] http://www.securityfocus.com/cgi-bin/vulns.pl
[4] http://xforce.iss.net/static/
[5] http://www.nipc.gov/cybernotes/cybernotes.htm