脆弱性情報を利用したセキュリティシステムにおける 脆弱性評価機能および影響範囲算出機能の実装と評価

19G456 楠目 幹 (最所研究室)

脆弱性情報を用いたセキュリティシステムにおける，脆弱性を持つ機器を特定する影響算出部における脆弱性評価機能および影響範囲算出機能の実装と機能の評価について述べる．

1. はじめに

近年，ゼロデイ攻撃による被害が深刻化しており，特定の組織や人物をターゲットとする標的型攻撃を組み合わせた攻撃も行われている[1]．また，大学や企業等では個人で所有する PC やスマートフォン等の機器を持ち込み，組織内のネットワークに接続して利用する BYOD という仕組みが増えている．この事から，組織内の機器だけでなく BYOD 機器もゼロデイ攻撃の被害から守る必要がある．我々の研究室では，インターネット上に公開された脆弱性情報及び組織内のネットワークに接続されている機器の情報を DB 化して一元管理し，それらをもとに脆弱性の存在する機器を特定しアクセス制御を行うことでゼロデイ攻撃による被害の緩和を目的とするセキュリティシステムを開発している[2][3][4]．本稿では，脆弱性の深刻度およびその範囲を評価し脆弱性を持つ機器を特定する影響算出部における，脆弱性評価機能および影響範囲算出機能の実装と評価について述べる．

2. セキュリティシステムの概要

本システムの構成を図 1 に示す．本システムは脆弱性情報収集部，IT 資産管理部，影響算出部，ネットワーク制御部で構成される．

2. 1. 脆弱性情報収集部

脆弱性情報収集部では，インターネット上に公開されている脆弱性情報を収集し，脆弱性の内容や対象となるソフトウェア，ソフトウェアを提供するベンダ，CVSS スコア等を抽出して DB 化する．

2. 2. IT 資産管理部

IT 資産管理部では，組織内のネットワークに接続されている機器のハードウェア情報，インストールされているソフトウェア，機器の重要度，機器で稼働しているサービス等の情報を取得して DB 化する．

2. 3. 影響算出部

影響算出部では，脆弱性情報収集部及び IT 資産管理部の DB をもとに組織内に脆弱性の存在する機器を判定し，脆弱性による影響範囲を算出する．算出した影響範囲をもとに，該当機器の制御手法を判断する．

2. 4. ネットワーク制御部

ネットワーク制御部では該当機器に対して Firewall，L2 スイッチ，VLAN を用いてネットワークからの隔離や復帰といった制御を行う．該当機器に対する制御の例として，外部ネットワークとの遮断や検疫ネットワークへの隔離等がある．

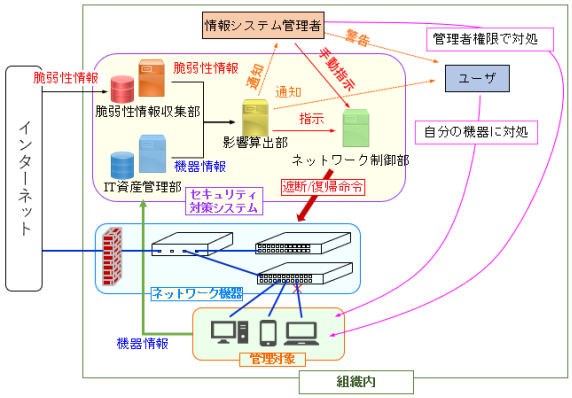

図 1 セキュリティシステムの概要

3. 脆弱性評価機能および影響範囲算出機能

影響算出部では，影響範囲をもとに該当機器に対する制御手法を決定し，それらを管理者に通知する．影響算出部は，脆弱性の存在する可能性のあるソフトウェアおよび機器の特定を行い影響範囲として算出する影響範囲算出機能，脆弱性の深刻度を評価する脆弱性評価機能，影響範囲をもとにネットワーク制御部における制御手法の決定を行う制御手法算出機能の 3 つの機能からなる．本研究では，脆弱性評価機能および影響範囲算出機能の実装を行った．影響範囲の算出を行うまでの流れを述べる．まず影響範囲算出機能が IT 資産管理部から機器の ID やインストールされているソフトウェア，機器で稼働しているサービスの情報を取得し，これらの情報を脆弱性評価機能に渡す．脆弱性評価機能はそれをもとに脆弱性情報 DB から機器にインストールされているソフトウェアに脆弱性が存在しているかどうかを調べ，評価値を算出し影響範囲算出機能に返却する．影響範囲算出機能は機器の ID，ソフトウェア名，脆弱性の評価値のリストを影響範囲として制御手法算出機能に渡す．

脆弱性評価を行う際の指標は CVSS[6]が一般的に用いられる．CVSS では脆弱性そのものの特性を評価する CVSS 基本値，脆弱性の現在の深刻度を評価する CVSS 現状値，製

品利用者の利用環境を含めた最終的な脆弱性の深刻度を評価する CVSS 環境値の 3 種類の基準値から脆弱性評価を行う．CVSS 現状値および CVSS 環境値は算出する際の技術的な要求が高く，算出が難しい．JVN iPedia[5]では，脆弱性対策詳細情報の中に CVSS 基本値のみが記載されており，CVSS 現状値および CVSS 環境値は記載されていない．CVSS 基本値のみでは脆弱性固有の評価しか行うことが出来ず，対象システムを加味した脆弱性評価を行うには不十分であることが多い．そこで本システムでは，脆弱性評価を行う際に CVSS 基本値だけでなく脆弱性の種類を示す CWE 識別子(CWE-ID)を併せて用いる．CWE[7]とはソフトウェアにおける脆弱性の種類を分類する仕組みであり，分類された脆弱性ごとに CWE 識別子を付与して階層構造で体系化している．機器で稼働しているサービスに関連する脆弱性の種類に対して CWE-ID スコアを設定し，CVSS 基本値との合計値を用いて脆弱性評価を行う．これにより，CVSS 基本値のみでの場合に比べてより対象システムを加味した脆弱性評価を行うことができる．

4. 評価実験

脆弱性評価および影響範囲算出の評価実験および製品のバージョン情報の抽出実験について述べる．

4. 1. 脆弱性評価および影響範囲算出

Web サービスが稼働しているマシンと， NW サービスが稼働しているマシンの 2 種類のマシンに対する CVSS 基本値のみを用いて脆弱性評価を行った場合と，CWE-ID スコアを併せて用いて脆弱性評価を行った場合の影響範囲算出結果の比較を行った(図 2)．実験の結果，CWE-ID を併せて用いた場合に機器で稼働しているサービスに関連するソフトウェアの脆弱性の評価値が上昇していることを確認した．またサービスに関連しないソフトウェアであっても CWE-ID が一致する場合は評価値が増加し，ソフトウェアに付随するライブラリに関しては脆弱性情報がほとんど存在しないことも判明した．よって今後脆弱性評価手法のさらなる改善および脆弱性情報の情報源の拡大が課題である．

Webサービス想定マシン		NWサービス想定マシン	
[1, 'python', 9.8]	[1, 'python', 12.8]	[2, 'wget', 8.8]	[2, 'wget', 11.8]
[1, 'rake', 8.1]	[1, 'rake', 11.1]	[2, 'iptables', 5.5]	[2, 'iptables', 8.5]
[1, 'php', 6.1]	[1, 'php', 9.1]	[2, 'ftp', 3.3]	[2, 'ftp', 6.3]
[1, 'apt', 7.8]	[1, 'apt', 10.8]	[2, 'systemd', 6.7]	[2, 'systemd', 9.7]
CVSS基本値のみ	CWE-IDスコア併用	CVSS基本値のみ	CWE-IDスコア併用

図 2 影響範囲算出結果の比較(一部抜粋)

4. 2. バージョン名の抽出

制御手法算出機能において，ネットワーク制御の実施の有無を決定するためにソフトウェアのバージョンの比較を行う．バージョンの比較を行うためには脆弱性の対象となるバージョンの範囲を情報として保持しておく必要があるため，脆弱性情報 DB からバージョン範囲の抽出実験を行い，日本語表現によるバージョン範囲の表現への対応を行った(図 3)．実験の結果，26208 件のバージョン範囲を抽出し，そのうちの約 9 割の 23808 件の DB 化に成功した(図 3)．同一の脆弱性情報，製品名，バージョンの範囲が抽出された場合に DB 化が失敗していたため，今後は DB 化に失敗した場合への対応およびバージョン範囲の表現方法への対応の拡大を目指す．

形式	例
○○ から △△	1.0.1 から 1.2.1
○○ およびそれ以前	2.2.4 およびそれ以前
○○ まで	1.2.2 まで
○○ までの △△	2.0.9.1 までの 2.0.0
○○ 未満	1.1.2 未満
○○ 未満の △△	2.3.5 未満の 2.3
○○ 以上 △△ 未満	2.2 以上 2.2.10 未満
○○ より前のバージョン	6.5 より前のバージョン

図 3 日本語表現によるバージョン範囲の表現形式

5. おわりに

脆弱性情報を利用したセキュリティシステムにおける脆弱性評価機能および影響範囲算出機能を実装し，その評価を行った．また，日本語によるバージョン範囲の表現への対応を行った．今後の課題は，脆弱性評価機能の改良，バージョン範囲の表現への対応の拡大，各機能を統合し 1 つのシステムとして運用することである．また，BYOD 機器に対する本システムの適用も課題である．

6. 参考文献

[1] 修正プログラム提供前の脆弱性を悪用したゼロデイ攻撃について，
https://www.ipa.go.jp/security/virus/zda.html (2021/02/16 参照)

[2] 楠目幹，喜田弘司，最所圭三，“脆弱性情報を利用したゼロデイ攻撃対策システムにおける構成情報収集機能の実装および脆弱性評価機能の設計”，電子情報通信学会技術研究報告，Vol.119, No.140, pp1-6,2019

[3] 西岡大助, "BYOD に対応した IT 資産管理システムの開発", 学士論文, 香川大学, 2020

[4] 竹原一駿, "脆弱性情報を用いたセキュリティシステムにおけるネットワーク制御機構に関する研究", 学士論文, 香川大学, 2020

[5] JVN iPedia, https://jvndb.jvn.jp/ (2021/02/16 参照)

[6] 共通脆弱性評価システム CVSS 概説,
https://www.ipa.go.jp/security/vuln/CVSS.html (2021/02/16 参照)

[7] 共通脆弱性タイプ一覧 CWE 概説,
https://www.ipa.go.jp/security/vuln/CWE.html (2021/02/16 参照)