L-028

Attack Tree による脆弱性情報統合手法の提案

Proposal of vulnerability information integration method by Attack Tree

大久保研究室　博士前期課程 2 年　陳 慷
学籍番号 5563103　E-mail mgs163103@iisec.ac.jp
QIAN CHEN

情報セキュリティ大学院大学 情報セキュリティ研究科
Graduate School of Information Security INSTITUTE of INFORMATION SECURITY

要旨

ネットワークの普及に伴い、情報システムの使用は企業や組織の運営に不可欠なものとなっている。システムが脆弱性により、顧客情報の漏洩やサービスの停止などは、会社に悪い影響しか与えない。安全な情報システムを構築する方法が最優先事項となっている。

一般に、情報システムの開発後、脅威分析はめったに行われない。このように、システムの運営時間が長くなると、システムのセキュリティが弱まる。情報システムの脆弱性を利用して、システムがハッキングされるリスクが高くなる。長年運営されてきた情報システムでは、人間に例えると中高年者は年齢とともに抵抗力が減じるように脆弱性に対する抵抗力が劣化すると考えられる。ハッカーは癌細胞のように、常に蔓延している。通常の身体検査と同様に、情報システムの定期検査は非常に重要である。しかし、現在の検査は比較的コストが高く、さまざまなテストの観点が異なるため、問題がどこにあるのかを統一的かつ直観的に伝えることは困難である。

この論文の提案は、ペネトレーションテストを通してシステムの潜在的なリスクを洗い出す。各検査情報や脆弱性テスト結果を Attack Tree を用いて攻撃観点の手法で、整理してまとめ、直観的にシステムに存在する問題点を示す。本提案により情報システムのセキュリティを向上させ、脆弱性診断のコストを削減することが可能になる。

キーワード：Attack Tree、STRIDE、CVSS、ペネトレーションテスト、脆弱性検出ツール、ペネトレーションテストツール

1. 脅威分析手法

1.1 Attack Tree(攻撃木)

Attack Tree とは、脅威を頂点とした木構造で表現され、各ノードに脅威の発生につながる原因を記載される。このようにして脅威と脅威を引き起こす原因を木構造で表現することにより、攻撃の手段と手順を網羅的に整理することができる。[1]

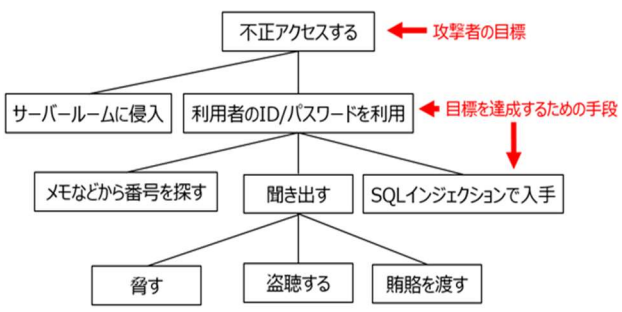

図1：Attack Tree 例[1]

1.2 STRIDE（ストライド）

STRIDE とは脅威を 6 つの特性より導出する。STRIDE という名前は情報セキュリティに関する要素の頭文字になっている。以下はそれぞれの頭文字の基になったセキュリティに関する要素である。

・Spoofing（なりすまし）：第三者を装う。

・Tampering（改ざん）：データを偽造する。

・Repudiation（否認）：ログの消去により証拠隠滅を図る。

・Information Disclosure（情報漏えい）：クレジットカード番号の流出。

・Denial of Service（サービス妨害）：サーバーに多大な負荷をかける。

・Elevation of Privilege（権限昇格）：管理者権限が取得される。[1]

1.3 CVSS

共通脆弱性評価システム CVSS（Common Vulnerability Scoring System）は、情報システムの脆弱性に対する評価手法である。

1.4 ペネトレーションテスト（侵入テスト）

ペネトレーションテストとは、ハッカーの攻撃モードをシミュレートし、ターゲットのセキュリティを確認する手法である。地震訓練、防災訓練、軍事訓練のように、ペネトレーションテストはセキュリティ上の訓練である。

1.5 脆弱性検出ツール

脆弱性検出ツールについては、ホスト脆弱性スキャンツール（Nexpose、Nessus、X-SCAN など）、リモートシステムスキャンツール（Nmap、Zmap）、ネットワークセキュリティ検査ツール（AppScan、WebRavor）、データベースセキュリティ検査ツール（DAS-DBScan）などの様々な種類がある。[2]

1.6 ペネトレーションテストツール

ペネトレーションテストツールについては、SQLmap 、Sqlninja、BeEF、Burp などの様々な種類がある。

2、脅威分析の課題

①脅威分析が人により作成した物、主観が入りやすい、脅威分析の品質を評価することが難しい。

②脆弱性のスキャンのツールが多い、評価基準も統一されてないため、まとめて分析しにくい。

③一般に、情報システムの開発後、脅威分析はめったに行われないため、システムの運営時間が長くなると、システムのセキュリティが弱まる。

3、提案手法

脅威分析の結果とペネトレーションテストの結果を Attack Tree で統括することを提案する。Attack Tree の木構造のため、拡張性が強い。ストライドと融合し、脅威情報がもっと直観的に読める。更に CVSS を利用し、リスク評価するにより、対応の優先順位が分かりやすくなる。

Attack Tree 融合後の階層は下記の通りである。

① 第一階層は情報システム不正アクセス

② 第二階層は STRIDE（ストライド）と結合して、脅威の特徴を示す。

③ 第三階層は脆弱性に対して攻撃種別を記載する。

④ 第四階層は攻撃手法 と セキュリティリスク（点線で表示）を記載する。

・攻撃手法はペネトレーションテストが発見した脆弱性である。

・セキュリティリスクは対応しないと他の攻撃で利用されるリスクある。

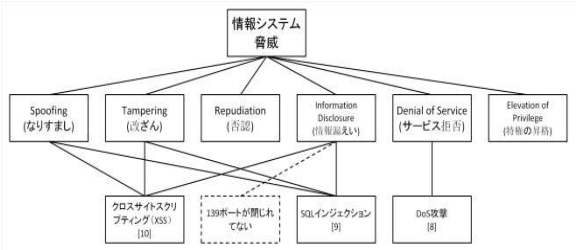

図2：統括した Attack Tree

3.1、提案手法のメリッド

①ペネトレーションテストを利用するより、潜在の脆弱性を発見しやすい。

②統括した Attack Tree で見ると、脆弱性問題を一目でわかる。脆弱性の対応方針を立てやすい。

4、まとめ

本研究では、Attack Tree により脅威分析とペネトレーションテストの結果を統括して、脆弱性診断でしやすくなる。攻撃結果から対応も明確できる。毎年人間ドックを受けるように低いコストで、システムの脆弱性診断することが可能になる。

5、研究課題

Attack Tree の第四階層以後の記載方針については、今後の課題である。

参考文献

[1] Monthly Research「脅威分析の役割と手法の紹介」https://www.ffri.jp/blog/2016/10/2016-10-14.htm（最終閲覧日：2019 年 6 月 8 日）

[2] 夏冰，鄭秋生，李向東，潘恒，「情報システムセキュリティ評価チュートリアル」、2018 年 2 月