毛利研究室輪講資料　令和 4 年度 第 10 回　令和 4 年 12 月 16 日（金）

Expected Exploitability: Predicting the Development of Functional Vulnerability Exploits

山下 恭平

概要：本稿は 31st USENIX Security Symposium にて掲載された論文「Expected Exploitability: Predicting the Development of Functional Vulnerability Exploits」[1] の内容についてまとめたものである. 既存の脆弱性評価基準の分析を通じて得られる結果は, その脆弱性が悪用されることを予測するのには不十分であるため, ソフトウェア脆弱性の公開時の悪用可能性を評価することは困難である. さらに,「悪用できない」という評価は不確実性が高く, 悪用可能性の評価にはバイアスがかかっていることが問題として挙げられる. これらの問題を解決するために, 機能的なエクスプロイトが開発される可能性を経時的に反映する,Expected Exploitability（EE）と呼ばれる新しい指標を提案する.

1. はじめに

エクスプロイトがセキュリティに深刻な影響を与えた事例として,2017 年に世界中で大流行した WannaCry と NotPetya がある. これらが悪名高い成功を納めた原因として, 武器化されたエクスプロイトの使用が挙げられる. しかし, 武器となり得る脆弱性を利用するプログラムを開発する難易度が上がっていることから, 既知の脆弱性のうち 5%のみを悪用することに注力するようになっている. そういった中で, 着目すべき脆弱性の優先順位をつけることで業界の人々に対して最適な意思決定をもたらし, 悪用防止に向けた研究機会の深い理解のために, 各脆弱性の悪用可能性を評価する必要がある. しかし, 悪用可能性の評価は, どの脆弱性が, どのように利用されるかが不明なため, 困難である. 具体的には,WannaCry や NotPetya によって悪用された脆弱性である CVE-2017-0144 は, 当時の専門家が推奨するパッチから省かれたいた. このことから, エクスプロイトの開発によってエクスプロイト可能性を証明することはできるが, 非エクスプロイト可能性を証明することは困難である. この結果,「悪用不可能」という評価にはバイアスが発生し, 不確実性を持つことが分かる.
この問題を解決するために,Expected Exploitability (EE) と呼ばれる新しい指標を提案する.

2. おわりに

参考文献

[1] Octavian Suciu , Connor Nelson , Zhuoer Lyu , Tiffany Bao , and Tudor Dumitras. Expected Exploitability: Predicting the Development of Functional Vulnerability Exploits. In 31th USENIX Security Symposium (USENIX Security 22), pages 377-394, 2022

[2] InnoDB deadlock detection is CPU intensive with many locks on a single row. `https://bugs.mysql.com/bug.php?id=49047` . (11/25/2022)