安全保障技術研究推進制度　令和２年度採択大規模研究課題　中間評価結果

1.　評価対象研究課題

（１）研究課題名：強化学習を用いた環境適応型ファジングシステムの提案

（２）研究代表者：株式会社リチェルカセキュリティ　木村　廉

（３）研究期間　：令和２年度～令和６年度（予定）

2.　中間評価の実施概要

日時　　：令和４年１０月２１日

場所　　：ビジョンセンター浜松町

評価委員：未来工学研究所　理事長、上席研究員／東京大学　名誉教授
　平澤　泠（委員長）
東京工業大学　環境・社会理工大学院　特任教授
　岩野　和生
理化学研究所 革新知能統合研究センター　副センター長
　上田　修功
情報セキュリティ大学院大学 情報セキュリティ研究科長 教授
　大久保　隆夫
玉川大学　名誉教授
　大森　隆司
NTT コミュニケーション科学基礎研究所　NTT フェロー
　柏野　牧夫
東京工業大学　名誉教授
　佐藤　誠
兵庫県立大学大学院　情報科学研究科　教授
　田中　俊昭

（委員長以外は五十音順・敬称略）

3.　研究の進捗状況

研究の概要

本研究では、「対象プログラムの特性に応じて、そのクラッシュを効率的に誘発するファジング※アルゴリズムは異なる」という洞察のもと、アプリケーションから IoT 機器に至るまで、多種多様な対象プログラムごとに最適なファジングアルゴリズムを選択する手法の実現に向けて、（１）ファジングシステムの実装、（２）強化学習エンジンの実現・検証、（３）アクセラレータの実現・検証を実施し、従来手法よりも効率的に脆弱性を発見する手法を確立する。

※ ファジング：プログラムへの入力に変異を施し、クラッシュを誘発する入力を繰り返し生成することで、その脆弱性を自動的に発見する技術

進捗状況

主な実施項目に対する進捗は以下の通り。（●：主題的成果、○：副次的成果）

（1）ファジングシステムの実装

●多腕バンディット問題※の強化学習に適した新規フレームワーク（SLOPT）を作成した。

●中間目標5 件を上回る7 件の既存のファジングシステムのSLOPT への移植に成功した。

●未知脆弱性4 件を発見し、効率的に脆弱性を発見するという本研究の主旨を体現した。

○ファジングシステム単体に留まらず、ファジングシステムに内包される複数種のアルゴリズムを効率的に組み替えることが可能な独自言語（HiearFlow）を考案し、開発効率を向上させた。

○再現・実装した既存のファジングシステムをオープンソースとして公開し、共同研究に繋げた。

（2）強化学習エンジンの実現・検証

●強化学習を用いてアルゴリズムの組み合わせを最適化してファジングを効率化するコンセプトの実現可能性を示し、当該手法の論文が国際会議 ACSAC に採択された。

●ファジングシステムと本強化学習エンジンに関する特許を出願済。

○未知脆弱性 3 件を発見。これらは既存のシステムでは発見不能なもので、強化学習を用いたファジング効率化の独自性・有用性を裏付けた。

（3）アクセラレータの実現・検証

●ARM 環境※※向けアクセラレータを実装し、ソースコードのない条件下において既存手法の 1.6 倍の時間効率を達成。

○任意の環境に適用できるアクセラレータの実現にはブラックボックスでのアプローチの重要性を明らかにし、当該課題にアプローチする過程で、未知脆弱性6 件を発見。

※ 多腕バンディット問題：限られた資源を複数の候補に割り当てる際、最大の期待利得を得るための配分を探る問題

※※ ARM 環境：ARM アーキテクチャーを採用したCPU のこと。サイズが小さく消費電力が少ないため、モバイル機器などで広く普及している。

4. 中間評価の評点

A　研究計画を超えた成果を挙げており、さらなる発展を期待する。

5. 総合コメント

プログラムの脆弱性は大きな被害につながる可能性があり、悪意のあるハッカーよりも早く網羅的に見つけて対策に繋げることには大きな意味があります。本分野において企業として事業を発展させている実用面と、難易度の高い国際会議で採択

されるなど研究面の両面で、順調に進捗していると高く評価できます。今後はクラッシュ原因の推定や脅威度の解析といった研究によりトップ国際会議への採択を期待します。
ただし、本手法が偶発的発見に留まるのか/体系的な知見になりうるのかを評価する指標を示し、手法の重要性、優位性、および限界を整理した説明を検討するとともに、脆弱性の迅速発見等の本手法の優位性が最も生きる適用先（発電所の制御など社会的な影響力の大きい分野）を見つけ、汎用システム開発に向けた適切な目標を設定してください。

6. 主な個別コメント

- 目標より高い成果を上げている
- 新たな脆弱性の発見、国際会議での採択など突出した成果が出ており、今後も新たなファジングシステムを開発して最終的な目標達成が期待できる。サブ課題としてクラッシュ原因の推定や脅威度評価などが目指されており、評価できる。
- 順調に研究進捗している一方で、汎用システム実現のための、技術課題の整理と体系化も行い、より挑戦的な研究開発を目指していただきたい。
- もし人手でなら見つかるがこのツールでは見つけらないものがあるとしたら、その理由はなぜなのか、今後どうしていくべきか。この方式で限界があるのか、外形的な技術強化をやろうとしている技術レベルがどこまでなのかということを整理することに意味がある。
- 当初の目標を達成することに加えて、今回のアプローチの優位性やファジングシステムの限界などを体系的に分析・整理するとともに、有用なビジネス領域など社会実装を踏まえた検討を期待する。
- ファジングシステムがセキュリティ分野に影響をもたらす方策を是非考えてほしい。また新たに発見された脆弱性の重要度や共通性などの分析もほしい。
- 環境適応型のファジングシステムを実現するために、強化学習の汎用性について議論する必要がある。IoT 機器向け汎用アクセラレータの開発が重要。
- 研究内容のクオリティは高いので、研究の重要性に関する説明力を高めることが更に求められる。
- ファジングシステムが内包する優位性と課題について、今までの実績や経験から考察を深め、今後の方針の見直しやステップアップの方向性に関し一段と努力を払われることを期待する。
- バックオフィス要員の雇用、進捗管理ツールの更新など適切なマネジメントが行われている。