FRAT & RATTATA

:アタックツリー再利用フレームワークの提案及び実践ツールの開発

Proposal of a framework for reuse of attack trees and development of a practice tool

大矢政基　システム分科会　情報セキュリティ大学院大学

Abstract —We propose a framework to improve the reusability of attack trees (FRAT) to enable organizations, industries, and communities to share and effectively utilize attack trees. FRAT is a framework for generating reusable attack tree parts from the attack pattern database CAPEC, creating attack trees using those parts, and reusing the parts from the created attack trees. We have automated part generation to reduce the cost of updating parts, which can be an issue in industry. In addition, we developed a FRAT implementation tool (RATTATA) and evaluated it with practitioners. The results showed that the average number of reused subtrees from other attack trees significantly increased when creating an attack trees. Future work is to improve the efficiency of FRAT by increasing parts size and improving parts searchability, as well as to identify an evaluation index for part quality.

はじめに

IoTや車両，制御システム等，IT多様化に伴いシステム開発段階でセキュリティを組み込むセキュリティ・バイ・デザインの重要度が増している．アタックツリー* (ATs) は**ITに対する脅威の生起シナリオを分析するのに効果的**な手法であるが、**高度な専門性や実施コストが課題**である。

本研究ではATsの再利用性（他のツリー作成時における再利用しやすさ）を向上させることを目的とし，**CAPEC*を活用し再利用可能なATsを作成する手続きをまとめたフレームワーク「FRAT」の提案**及び**実践するGUIツール「RATTATA」の開発**を行なった．

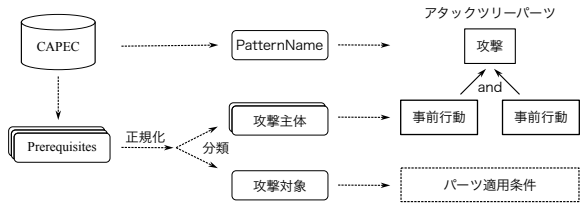
アタックツリー：脅威（攻撃者のゴール）をルートノードとし、親ノードを実現する手段を子ノードとして接続することで，ツリーを展開していく脅威分析手法

CAPEC：公開された攻撃パターンのデータベース。各攻撃パターンには攻撃概要や成立条件、影響等の情報が含まれている

FRAT (Framework for Reuse of Attack Trees)

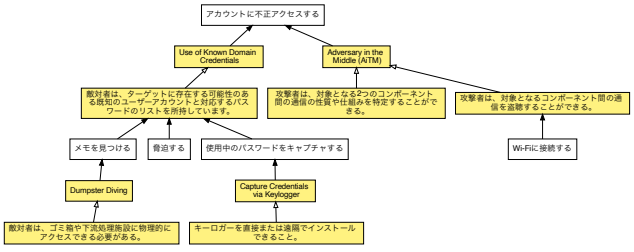
CAPEC から再利用可能なパーツを作成する手続き

攻撃とそれを成立させる事前条件の情報からパーツを作成する．ATsは攻撃主体の行動のみを記述するため，事前条件を攻撃主体のものと攻撃対象のものに分類し，使用する．



CAPEC パーツを組み合わせて再利用可能なアタックツリーを作成する手続き

パーツと分析者が独自に作成したノードを組み合わせてATsを作成する．



RATTATA (Reusable Attack Trees Tool Accessible To All.)

デスクトップ上でATsを作成できるGUIアプリケーションであり，CAPECパーツをインポートする機能や**他のATsで使用されているパーツを検索して再利用する機能**を持つ．

パーツ更新の自動化スクリプト

自然言語処理によりCAPECからパーツを作成する手続きの自動化を実現．精度は71%であるが，高性能なGPU等が不要で一般的なノートPCでも手軽に実行できるのが特徴．大元の**CAPECが更新された際にコストを掛けずにパーツも更新できるため，再利用性を維持することができる**．

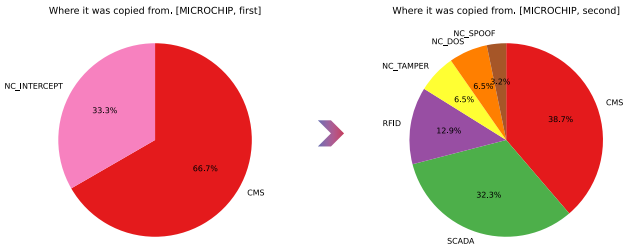
効果の評価

官民のIT部門に所属し，かつセキュリティの専門性を有している10名にFRAT及びRATTATAを使用してもらうことで，その効果を測定した．評価はATs作成において，通常通りとFRATを適用した場合で結果を比較することで行なった．

再利用性が向上

ATs作成時に他のATsからどれだけサブツリーを再利用できたかを比較したところ，**平均再利用回数が1.3 -> 4.9回に有意に増加**していることが確認された．

また，再利用元のバリエーションも増加しており，別種のITで作成されたATsからであっても再利用できていたことが判明した．



効率性は有意な変化が見られなかった

一定時間内に**作成できたシナリオ数及びノード数を比較したが，有意差は無かった．**

今後の課題及びまとめ

パーツの検索性の向上やより大きな単位で再利用できるようにすることで，効率性を向上させる必要がある．依然として課題は多いが，**組織や業界内等においてATsの共有と再利用のサイクル形成を支援**できるよう，研究を進展させていければと考えている．

RATTATA Reusable Attack Trees Tool Accessible To All.
GitHub : https://github.com/RATTATAlab/RATTATA
E-mail : masaki.oya.rattata@gmail.com, mgs214501@iisec.ac.jp