Monthly Research 2016.11

Microsoft Threat Modeling Tool の利用例

F F R I , Inc.
http://www.ffri.jp

E-Mail: research-feedback[at]ffri.jp
Twitter: @FFRI_Research

目次

- 脅威分析を支援するツールについて
- 脅威分析を支援するツールの例
- 分析対象システム
- 分析結果
  - レポートの読み方
  - 洗い出された脅威
- 効果的な使い方
  - テンプレートについて
  - 脅威情報の追加
- 考察
- 参考情報

脅威分析を支援するツールについて

- 脅威分析を支援するツールがいくつか存在する
  - DFD(Data Flow Diagram)作成をサポートするものや DFD に基いて自動で想定される脅威の一覧を出力するものなどが存在する

  - ツール利用により期待できるメリット
    - 脅威の洗い出し、レポート作成の自動化などによる分析時間の短縮
    - 今まで気づいていいなかった脅威を発見できる可能性
    - 入力データが同一であれば結果が同じになることによる属人性の低減

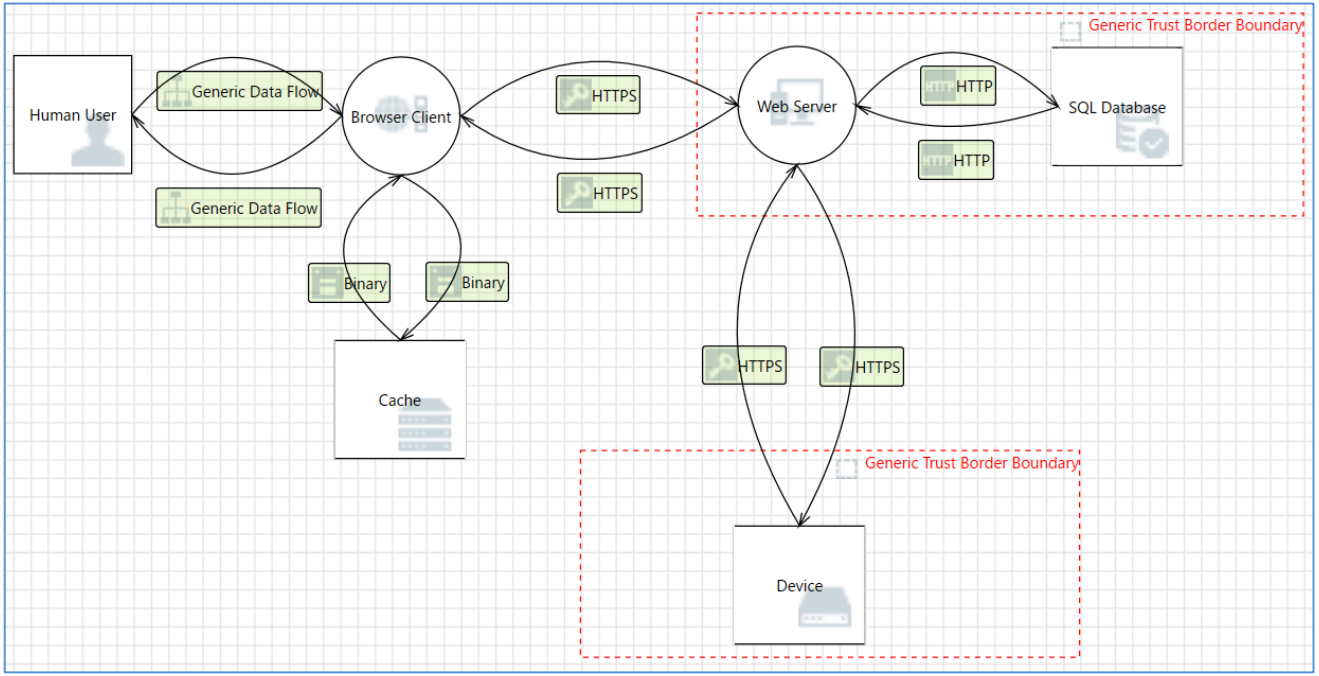
脅威分析を支援するツールの例

- Microsoft Threat Modeling Tool
  - DFD 作成、DFD に基いて自動で脅威を洗い出すツール
- TRIKE
  - DFD 作成、脅威・セキュリティ要件を含めた図の作成ツール
- SeaMonster
  - Attack Tree & ミスユースケース図作成ツール
    - ミスユースケース：意図しない動作のこと
- SecurITree
  - Attack Tree 作成ツール

- 本レポートでは Microsoft が無償で提供している Threat Modeling Tool 2016 を利用した脅威分析の一例を紹介する

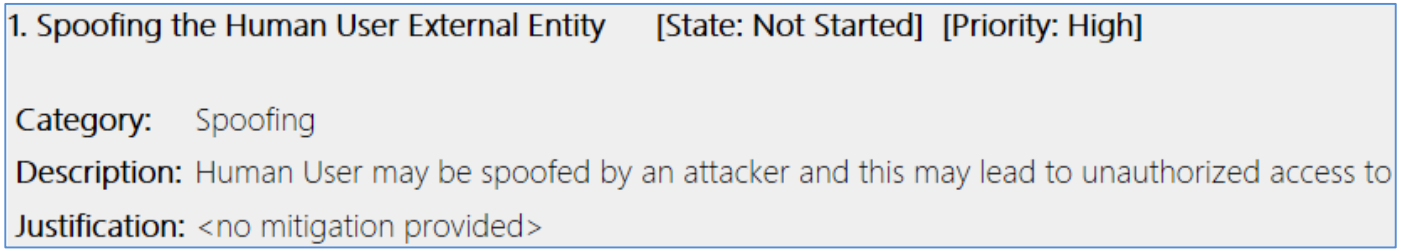
分析対象システム

- 一般的なネットワークカメラシステムを分析対象とする
- 下記が Threat Modeling Tool で作成した DFD である
  - システム構成要素であるサーバーやデータベース、ブラウザ、利用者を画面上に配置し、データフローを追加して作成



分析結果 – レポートの読み方

- DFD 作成後、Analysis View を表示すると洗い出された脅威を確認できる
  - STRIDE に基づいた脅威のカテゴリ(Category)と説明 (Description)が出力される
    - 脅威は機械的に洗い出されるため、実際のシステムでは発生する可能性のない脅威が誤検出されることがある。脅威の実現可能性について利用者による分析が必要
      - 出力例: Webサーバーは、信頼できない入力をサニタイズしないため、クロスサイトスクリプティング攻撃の対象となる可能性がある。
        - » 入力を処理する機能のないWebページの場合、上記の脅威は存在しない
  - 脅威ごとに優先度(Priority)や対策内容(Justification)を入力できる
    - 優先度はデフォルトでは全てHighになる
      - 脅威の性質や存在箇所に応じて利用者が個々に優先度をつける必要がある
    - 状態(State)や対策内容を追記できるのでチームで分析を行う際にも使える



分析結果 -洗い出された脅威

- 合計 47 件の脅威が洗い出された
  - なりすまし(Spoofing) 10件
  - 改ざん(Tampering) 8件
  - 否認(Repudiation) 4件
  - 情報漏えい(Information Disclosure) 3件
  - サービス妨害(Denial of Service) 12件
  - 権限昇格(Elevation of Privilege) 10件

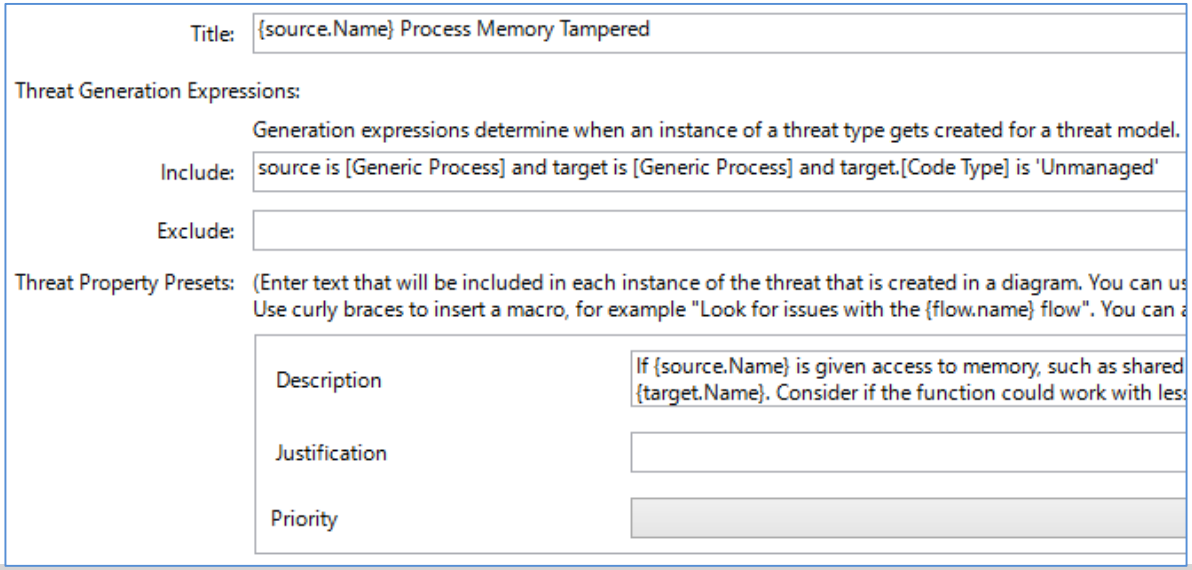
- Web サーバーに関係する部分に多くの脅威が洗い出された
  - 洗い出された脅威のカテゴリに偏りはなかった

- 各要素で起こり得る脅威が STRIDE に基づいて漏れなく洗い出されている
  - 脅威の説明は一般的な条件や環境を想定したものであった
    - より具体的あるいは対象システム固有の説明が必要な場合は利用者が追記することができる

効果的な使い方 – テンプレートについて

- テンプレートの追加によってできること
  - DFD の要素のテンプレートで任意の画像を設定することで見やすい DFD が作成できる
  - 脅威情報のテンプレートの追加により、分析可能な脅威の幅を広げられる

- 下記は脅威情報テンプレート作成時の入力画面である



効果的な使い方 – 脅威情報テンプレートの追加

- テンプレートを活用することによって分析の効率化が期待できる
  - 脅威情報を追加できるため、新しい脅威の分析にも対応できる
    - 追加する脅威情報テンプレートの例
      - Title: デフォルトパスワード利用による不正アクセス
      - Include: target is [Web Service]
      - Description: デフォルトパスワードを変更せずに利用を続けると第三者に不正アクセスされる可能性があります。
  - デフォルトで用意されている脅威情報の説明文は英語だが、テンプレートの書き換えによって日本語化も可能である

考察

- メリット
  - 作成した DFD に基いて自動的に脅威を洗い出すことができるため、脅威分析の経験が少ない人でも手軽に利用できる
  - システム設計の際に本ツールを利用し、脅威について対策を行いつつ設計を進めることで、効率的に脅威対策ができる
  - 洗い出された各脅威に対して対策や優先度を記載できるため、複数人で脅威対策を検討する際に利用しやすい

- デメリット
  - 自動で脅威が洗い出されるが、システムの仕様上実現する可能性のない脅威が誤検出される場合がある。そのため、脅威の実現性について人による分析を行った上で脅威への対策を検討する必要がある

参考情報

- Threat Modeling
  - http://threatmodelingbook.com/index.html
- SDL Threat Modeling Tool
  - https://www.microsoft.com/en-us/download/details.aspx?id=49168
- Microsofts New Threat Modeling Tool
  - https://blog.secodis.com/2016/07/06/microsofts-new-threat-modeling-tool/
- TRIKE
  - http://octotrike.org/
- SeaMonster
  - https://sourceforge.net/projects/seamonster/?source=navbar
- SecuriTree
  - http://www.amenaza.com/