Monthly Research 2016.10

STRIDEの変化形と セキュリティ要件で導き出す脅威分析手法

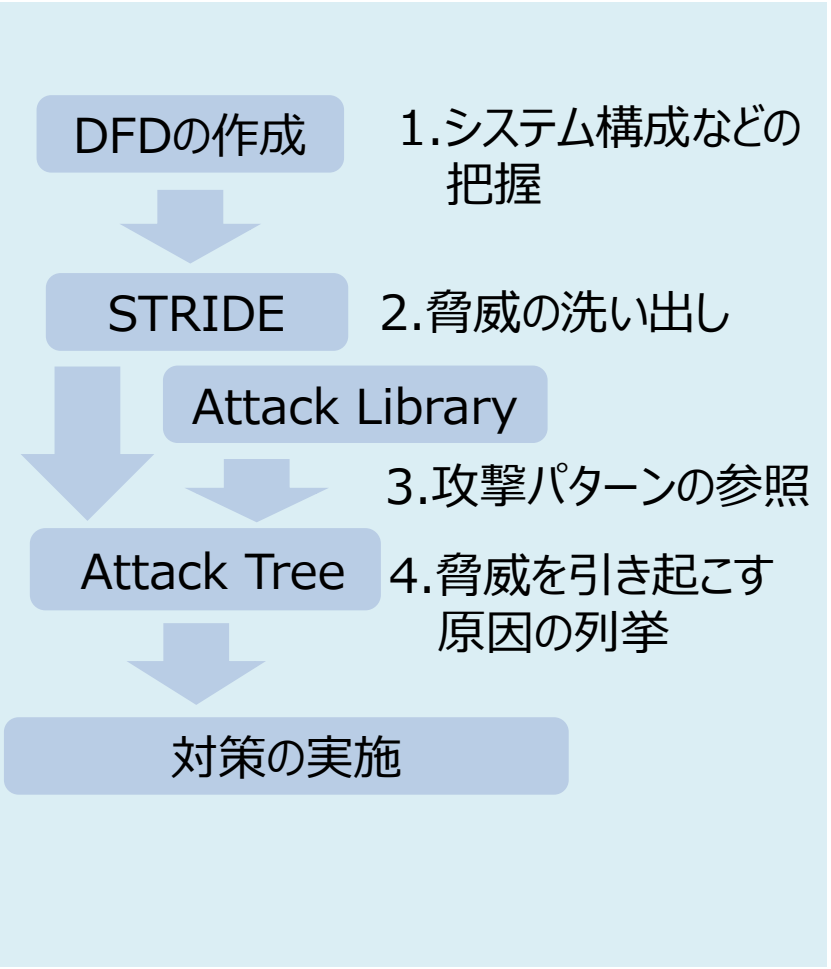
E-Mail: research-feedback[at]ffri.jp
Twitter: @FFRI_Research

ＦＦＲＩ, Inc.
http://www.ffri.jp

目次

- 概要
- STRIDEの変化形
  - STRIDE-per-Element
  - STRIDE-per-Interaction
  - STRIDEの変化形を比較
- セキュリティ要件で導き出す脅威分析手法
- まとめ
- 参考情報

概要



- 今月号は先月号に引き続き脅威分析手法を題材とする
- 『2.脅威の洗い出し』で利用される手法について詳しく紹介
  - STRIDEを具体化し適用しやすくした手法を紹介する
- 設計書などに記載された資産に注目し、セキュリティ要件に基づいて行う脅威分析手法を紹介
  - 選択の幅を広げる

STRIDE-per-Element

- STRIDE-per-Elementとは
  - DFDの要素にSTRIDEを適用し脅威を導出
    - “要素”とはプロセスやデータフローなどの事である
  - 熟練していなくても、機械的に脅威を導出することが可能
  - 同じ脅威を何度も導出してしまう場合もある
- 手順
  - DFDから要素を取り出し、下記の表に当てはめて脅威を導出
  - 下記の表は万能という訳ではないので、利用者が現在の分析対象と項目を検討し、合致していない箇所があれば修正する必要がある

	S	T	R	I	D	E
外部エンティティ	✓		✓			
プロセス	✓	✓	✓	✓	✓	✓
データフロー		✓		✓	✓	
データストア		✓	?(場合による)	✓	✓	

STRIDE-per-Interaction

- STRIDE-per-Interactionとは
  - DFDの中から、Trust Boundary と交差するデータフローを取り出し“origin” , ”destination” , “interaction”に着目して脅威を導出

- Trust Boundary (信頼境界)とは
  - 管理している組織やインターフェイスが変わる境界線
    - 例:ブラウザとWebサーバーの境界線

- Microsoft Threat Modeling Tool
  - Microsoft 社が提供している脅威モデリングツールで、2014年のアップデート以降で類似した手法を採用している
  - ただし Trust Boundary と交差していないデータフローも分析対象としており、ここで説明するSTREIDE-per-Interactionとは違う点もある

STRIDE-per-Interaction

- 脅威を連想する手順
  1. 予め要素と相関作用によって発生しうる脅威をまとめた一覧表を作成
  2. 分析対象のシステムのDFDを作成、Trust Boundaryも記述
  3. Trust Boundary と交差しているデータフローを抽出
  4. データフローの両端の要素のどちらか(origin, destination)と相関作用をもとに、1の一覧表と比較、脅威を見つけ出す
  5. 見つけ出した脅威を表にまとめる

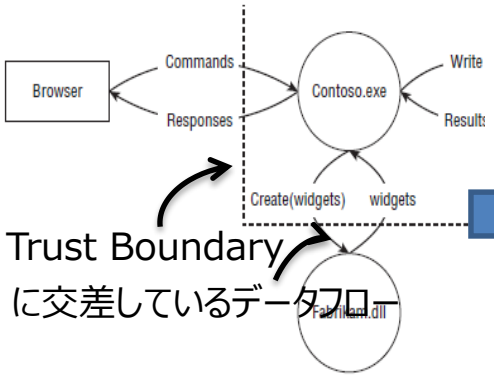


Figure 3-1: The system referenced in Table 3-10

Table 3-10: STRIDE-per-Interaction: Threat Applicability

#	ELEMENT	INTERACTION	S	T	R
1	Process (Contoso)	Process has outbound data flow to data store.	x		
2		Process sends output to another process.	x		x
3		Process sends output to external interactor (code).	x		x
4		Process sends output to external interactor (human).			x

Table 3-11: STRIDE-per-Interaction (Example)

	ELEMENT	INTERACTION	S	T	R
1	Process (Contoso)	Process has outbound data flow to data store.	"Database" is spoofed, and Contoso writes to the wrong place.		
		Process sends output to other process.	Fabrikam is spoofed, and Contoso writes to the wrong place.		Fab cla hav cal Co
3		Process sends output to exter-	Contoso is confused about the identity of the		Bro dis

http://threatmodelingbook.com/index.html

STRIDEの変化形を比較

- スウェーデンのチャルマース工科大学で2つの脅威分析手法を同じシステムに対し実施、それぞれの長所・短所について下記の通りまとめている
  - AUTOSARのSecOCモジュールに脅威分析を実施
    - ECU間の安全な通信を行うための仕組みを提供するもの
  - 正脅威率とは
    - 導出された脅威の内、研究者が確認し実際に脅威であると判断した比率
  - 各手法に対応したMicrosoft 社(以下MS)の脅威分析ツールを利用、利便性を評価

	所要時間	脅威発見数	正脅威率	長所	短所
STRIDE-per-Element	26.0H	99	54.55%	• 短時間 • 比較的正確な情報が入手できる	• 属人的 • 対応ツールは使いづらい
STRIDE-per-Interaction	32.5H	114	26.32%	• 脅威を理解しやすい • 対応ツールは使いやすい	• 長時間 • 巨大なシステムでは作業が複雑化 • “誤発見”が多い

セキュリティ要件で導き出す脅威分析手法

- 概要
  - ソニーデジタルネットワークアプリケーションズ株式会社の松並勝氏が(ISC)2 Japan chapter発足記念イベントなどで紹介
  - 仕様書・設計書からセキュリティ要件を導出し、仕様・設計でセキュリティ要件が満たされているか分析する手法
- 利用実績
  - ソニー株式会社の電子お薬手帳サービス「harmo」のセキュリティ設計分析に利用された
- 脅威を発見する手順
  - 対象のシステムの設計資料から【資産】と【人】を洗い出す
  - 【資産】に【人】が【読み取り・書き込み・実行】が【できる・できない】で、脅威事象を抽出
    - 脅威事象例:【個人情報】が【悪意ある第三者】に【読み取り】【できる】
    - 必要に応じて【場所】も洗い出す
  - 脅威事象を基にセキュリティ要件を決定
    - セキュリティ要件例:【個人情報】が【悪意ある第三者】に【読み取り】【できない】
  - セキュリティ要件を基にセキュリティ分析グラフを作成、設計の問題点を分析・修正する

セキュリティ要件で導き出す脅威分析手法

- セキュリティ分析グラフとは
  - 木構造の頂点にセキュリティ要件を配置、これを木構造の”命題”とする
  - 命題を達成させるために必要な条件をノードとして記述
  - 葉ノードのすべての条件が対応済みであるかを確認する

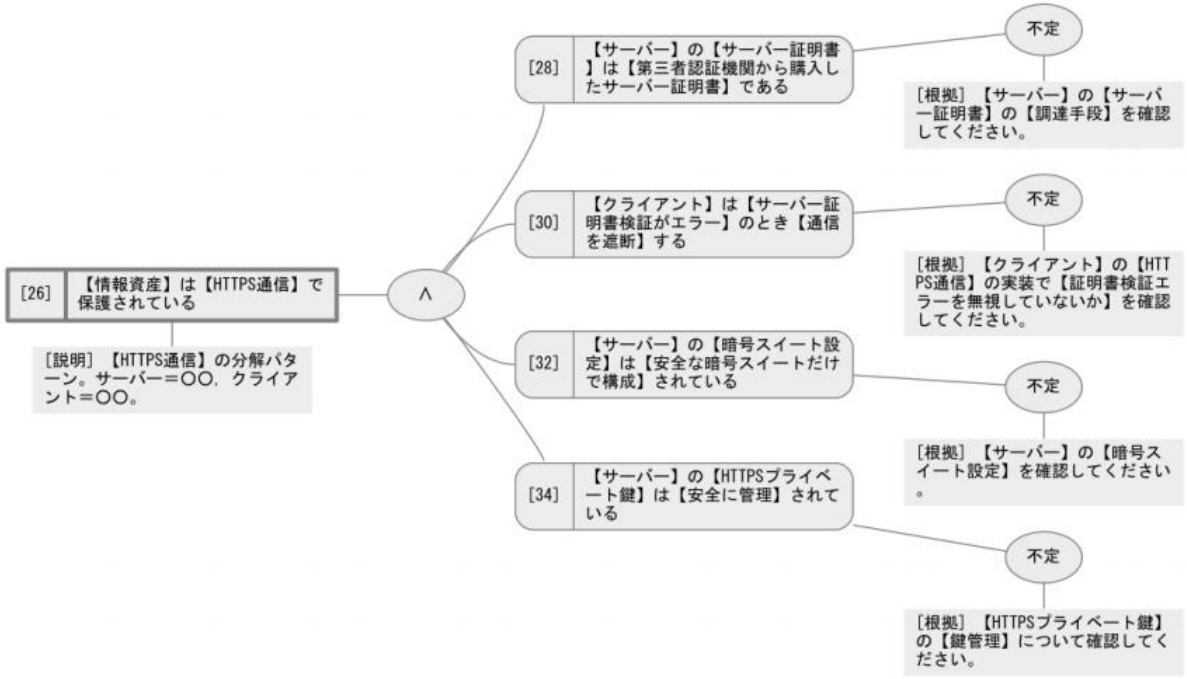


図 15-A-9-15 【HTTPS 通信】分解テンプレート https://www.ipa.go.jp/files/000049366.pdf

セキュリティ要件で導き出す脅威分析手法

- 利点
  - 要件定義・設計の初期段階から脅威分析が実施可能
    - システム構成を詳細に表したDFDは必須ではない
    - セキュリティ分析グラフの分解パターンを知識DB化することでセキュリティの専門家でなくても脅威分析ができるようになる

- 問題点
  - セキュリティ分析グラフの分解パターンを多く持っていない場合時間がかかる

まとめ

- STRIDE変化系手法は下記のような特徴を持つ
  - STRIDE-per-Element
    - 比較的短時間で情報が手に入るが、ツールなどが使いづらい手法
    - 専門家など知識・経験のある人材による脅威分析には向いていると考えられる
  - STRIDE-per-Interaction
    - 比較的利活用しやすいが、時間がかかってしまい精度も低い
    - 人材の知識・経験は不定だがリソース数は豊富という場合に有効と考えられる
- 仕様・設計からセキュリティ要件を導出して行う脅威分析手法もある
- 脅威分析には様々な手法やフローがある為、求めている情報の精度やかけられる時間を考え、要求に適した方法を選ぶ必要がある

参考情報

- Threat Modeling
  - http://threatmodelingbook.com/index.html
- Chapter 6 Privacy Tools
  - https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6NDRhNmE5N2JhYjQ0ZTkwOA
- Vehicle Control Unit Security using Open Source AUTOSAR
  - http://publications.lib.chalmers.se/records/fulltext/219822/219822.pdf
- 脅威分析 （仕様と設計のセキュリティ分析）
  - https://www.asteriskresearch.com/wp-content/uploads/2016/01/ThreatModeling_requirements_and_design20160204.pdf
- Chapter 3 STRIDE
  - https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzaWdzdGF3ZWJ8Z3g6MmY4ZTgxNmY5ODFhZWY5MA
- ねぇねぇやってる？ 仕様・設計のセキュリティ分析♪ 面白いよぉー
  - http://isc2chapter.jp/wp-content/uploads/2014/03/%E4%BB%95%E6%A7%98_%E8%A8%AD%E8%A8%88%E3%81%AE%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E5%88%86%E6%9E%90.pdf
- ソニーの電子お薬手帳システム「harmo」に適用した セキュリティ設計分析手法
  - https://www.ipa.go.jp/files/000049366.pdf
- FFRI Monthly Research 2016.9
  - http://www.ffri.jp/assets/files/monthly_research/MR201609_Introduction_of_Threat_Analysis_Methods_JPN.pdf