DFDを利用した簡易的な脅威分析手法に関する研究

A Study on a Simplified Threat Analysis Method Using DFD

奥山順子・法制倫理分科会・情報セキュリティ大学院大学

The priority of security-conscious design and implementation for small-scale application (software) development teams or organizations tends to be lower than that of functional implementation and early release. It is difficult to implement sufficient security measures in the target application system due to the lack of the security human resources and/or the budget of security measures. Therefore, I conducted a study on how to develop security-conscious Web applications with a "simplified analysis method". Then I invented the original threat analysis method based on DFD and STRIDE devised a simplified threat analysis method that includes threats specific to the Web applications without conducting the in-depth threat analysis like the attack trees and applies it to the target system.

① 研究の背景と課題克服のための解決策

小規模なアプリ開発現場での課題

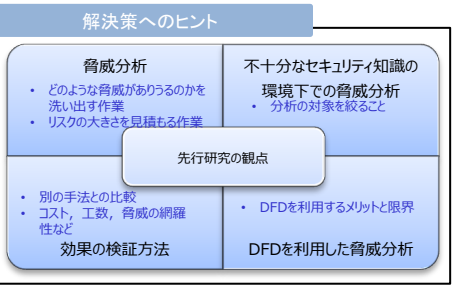
<セキュリティを考慮した開発>
- 専門知識の不足
- 組織内の優先順位の低さ
- 十分な予算が確保できない

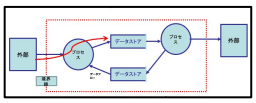
<セキュリティを考慮したい>
- 脆弱性やセキュリティ対策の必要性を認識している
- その情報がどこにあるのかわからない

問題提起

小規模な開発現場には，セキュリティを対象とした分析や設計の専門家でなくても，「簡易な手法」で，セキュリティを考慮したWebアプリケーション開発ができるようにするための方法が必要

解決策へのヒント





DDF(データフロー図)

	S	T	R	I	D	E
プロセス	○	○	○	○	○	○
データストア	-	○	△	○	○	-
データフロー	-	○	-	○	○	-
外部要素	○	-	○	-	-	-

DFDとSTRIDEの着目箇所

要素名	概要	脅威の例
Spoofing	なりすまし	第三者が正規のユーザーを装う
Tampering	改ざん	データを偽造する
Repudiation	否認	ログの消去により証拠隠滅を図る
Information Disclosure	情報漏えい	クレジットカード番号の流出
Denial of Service	サービス妨害	サーバーに多大な負荷をかける
Elevation of Privilege	権限昇格	管理者権限が取得される

STRIDE

簡易的な手法のポイントは2つ

1. DFDとSTRIDEの考え方に基づく脅威分析であること
2. 分析に必要な情報源をWebアプリケーションへの脅威に特化すること

② 提案する「簡易的な」脅威分析手法

脅威の特定のために参照した資料

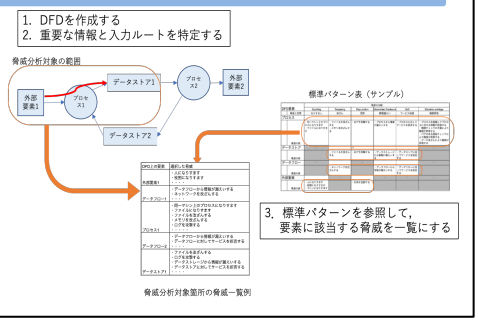
- OWASP Top 10
- 脅威の分類事例 (STRIDE Reference Sheets)
- 攻撃事例（IPA届出，報道）

- Webアプリケーションにとって見落としてはいけない脅威を網羅するための資料
- 重視するべき脅威に絞り込むために，段階的にパターンを展開

Webアプリケーションに特化した標準パターン

DFD要素	Spoofing なりすまし	Tampering 改ざん	Repudiation 否認	Information Disclosure 情報漏えい	DoS サービス妨害	Elevation privilege 権限昇格
プロセス	1) 不正なファイル，リンクを設置する 2) ファイル名を変更する	1) ファイル・データを改ざんする 2) プログラムを改ざんする 3) メモリ上の機微な情報を改ざんする 4) 他のユーザーのファイル・データを改ざんする 5) Webサイト・Webアプリを改ざんする	1) ログを記録させない	1) 機微のないのに，情報が漏えいする・表示される 2) メモリ上の機微な情報が漏えいする 3) エラーメッセージ，デフォルトの設定値などからシステムの情報が読み取られる	1) システムへのアクセスが拒否される	1) サーバー，ホストの制御を乗っ取られる 2) 意図しないコマンドを実行される 3) 意図しないプログラムを実行される 4) 権限チェックの手順により，権限が昇格する
データストア		1) 個人情報を改ざんする 2) クレジットカード情報を改ざんする 3) 機微な個人情報を改ざんする 4) 機密情報を改ざんする 5) 他のユーザーのデータ，ファイルを改ざんする	1) ログを消去する	1) 機密でないのに情報が漏えいする 2) 個人情報が漏えいする 3) クレジットカード情報が漏えいする 4) 機微な個人情報が漏えいする 5) 他のユーザーのデータ・ファイルが漏えいする	1) データストへのアクセスが拒否される	
データフロー		1) データフローを相手やマシンにリダイレクトする 2) ネットワーク上のデータを修正する		1) 認証情報が漏えいする 2) セッション情報が漏えいする	1) ネットワークリソースを消費させる	
外部要素	1) 脆弱なパスワードを解析して，ユーザーになりすます 2) アクセス制御の不備をついて，特定の役割を持つユーザーになりすます 3) アクセス制御の不備をついて，他のユーザーのアカウントにアクセスする 4) ユーザーのブラウザ上で，不正なコードを実行する		1) 操作をしていないと主張する 2) 他人のアカウント，立ち入り手段を使用する			

標準パターンを適用する，簡易的な脅威分析の手順

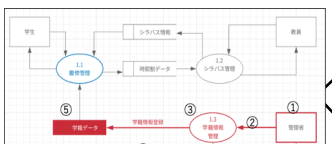


③ 有効性の検証

検証方法

架空のWebアプリケーションをケースとして提案手法と，本格的な脅威分析手法による脅威分析結果を比較する．

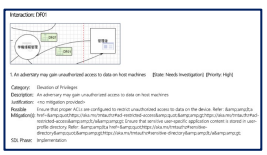
検証用のケース　：学務支援システム（外部から学籍情報へのアクセスルート上にある脅威）
比較対象の手法：TMT (Microsoft Threat Modeling Tool)を利用する脅威分析



比較検証ケース学務支援システムの上位DFD

1.提案手法での分析結果
(標準パターンからの抽出)
①～⑤の要素上に，37件の脅威があった

2.TMT脅威分析機能の結果
提案手法での検証と同じ要素上に，35件の脅威があった



TMTの分析結果出力例

検証結果

- STRIDEごとに分類した脅威の数は，2つの手法で傾向は同様（改ざん，情報漏えいが多い）
- TMTが出力した35の脅威に対して、以下のような同等（類似），差異の件数となった
  - 提案手法と同等の脅威と判断できる：27
  - 提案手法と類似の脅威ならある：6
  - 提案手法にはない脅威：1　（クライアントのブラウザーへの機密情報書き込み）
  - 提案手法であらかじめ除外した脅威：1　（クレジットカード情報に関する脅威）

④まとめ

- 検証を行なった結果，上位レベルDFD上の主要な要素にどのような脅威があるかについては，個別の攻撃を想定した詳細な検討を加えなくても見落としてはならない重視すべき脅威を洗い出せることがわかった．
- しかし現在のアプリ設計者，開発者にとってDFD作図は難しいことが予想される．
- OWASP Top 10 2021の反映は今後の検討する．
- 小規模開発に特化したDFDのパターン，対策とのセットで提示することが課題になる．

参考文献・資料

① • WEBアプリケーションのセキュリティマネジメントについての考察（情報処理学会研究報告 Vol.2017-EIP-75 No.7金根學，原田要之助）
• 情報セキュリティ大学院大学　原田研究室で実施した，ウェブアプリケーション，モバイルアプリ等に関するセキュリティ対策に関して実施した調査
• IPA小規模ウェブサイト運営者の脆弱性対策に関する 調査報告書 (情報処理推進機構，2021年3月)
② • A. Shostack, "Threat Modeling: Designing for Security", Wiley, Feb 2014.
• 中野学，堀部千壽，小林鉄平，松木隆宏．「システムに対する脅威分析におけるコスト及び属人性低減に向けた手法の提案」．（電子情報通信学会 SCIS2018）
• OWASP，「OWSP Top 10 – 2017 日本語版（OWASP 2017年12月）」
• https://www.security-next.com, https://scan.netsecurity.ne.jp
③ • Microsoft，Microsoft Threat Modeling Tool, https://docs.microsoft.com/ja-jp/azure/security/develop/threat-modeling-tool
④ • OWASP Top 10 2021の紹介, https://owasp.org/Top10/ja/