様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　　元 年　　６ 月 ２６ 日現在

機関番号：３２７２１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１９６

研究課題名（和文）形式手法による攻撃可能性検証の研究

研究課題名（英文）Research on attack probability using formal methods

研究代表者
大久保　隆夫（Okubo, Takao）

情報セキュリティ大学院大学・その他の研究科・教授

研究者番号：８０４１７５１８

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：本研究では、開発中のシステム/ソフトウェアに対するセキュリティリスク評価をするために、対象のシステムを形式的にモデル化し、モデルに対する攻撃可能性を形式手法で検証することで、開発途中におけるリスク評価を行うことができるかの研究を行った。一定の脆弱性モデルを設定することで、SPINやProverif、EVENT-Bなどの形式手法を用いて攻撃可能性の検証を行うことは可能であることが分かった。しかし、具体的脆弱性を扱う場合には脆弱性をある程度明示的に埋めこまないとならないことが分かった。

研究成果の学術的意義や社会的意義
本研究は、攻撃可能性をシステムのセキュリティリスク評価に検討できる可能性を示した。モデル検査を用いた形式手法を用いる場合は、設計仕様などをもとにモデル検査記述言語で対象システムの脆弱性を明示的にモデル化することで、リスク評価が可能になる。その他、未知脆弱性を扱う場合は、脅威分析におけるアタックツリーの妥当性を評価し、再構築すること、あるいは攻撃可能性を機械学習によって示すことで、一定のリスク評価が可能であることを示した。

研究成果の概要（英文）：In this research, in order to evaluate the security risk to the system / software under development, I have modeled the target system formally, and verified the attack possibility using the formal method to evaluate the risk within the development phases. It was found that it is possible to verify the possibility of attack using formal methods such as SPIN, Proverif and EVENT-B by setting a certain vulnerability model. However, when dealing with specific vulnerabilities, it turned out that the vulnerabilities have to be explicitly embedded to the target model.

研究分野：脅威分析、セキュリティバイデザイン

キーワード：形式手法　モデル検査　セキュリティ　リスク評価　攻撃可能性

様　式　Ｃ－１９，Ｆ－１９－１，Ｚ－１９，ＣＫ－１９（共通）

１．研究開始当初の背景

本研究が対象とする形式検証やモデル検査などの**形式手法**技術は 1970 年代から存在し，現在もソフトウェア工学の分野を中心に活発に研究が行われている．また，形式手法をセキュリティ検査への応用した研究も国内外で多くある．特に国内では，暗号プロトコルの安全性の検証に用いる例が多い[1)2)]．しかし，それらの研究は，特定の仕様を満たすかどうかの検証を目的とするものがほとんどであり，対象のシステム仕様に（何の脆弱性か不明な状態で）脆弱性が存在するかを攻撃によって検証するという事例はほとんどない．また，国外では，攻撃元の特定や，脱匿名化などの，攻撃的観点での研究もよく行われているが，国内のセキュリティ分野においては，防御などの対策の研究が行われているのに対し，攻撃そのものの能力について研究されている事例は，暗号などの分野を除き数少ない．従って本研究は，一般的なシステムの任意の攻撃，脆弱性を対象とし，攻撃観点から成功の可否によりリスクを評価する点を主眼に置くことであった．

２．研究の目的

研究期間内においては，次の点を明らかにしたいと考えた．

・対象となるシステムのモデルを，検査者が形式検証等の知識を要せずに生成可能とする技術

・攻撃について，検査者が形式検証等の知識および攻撃，脆弱性に関する知識を要せずに生成可能とする技術

・特定の分野ではなく，任意の分野のシステムに適用可能にする

・未知の攻撃，脆弱性を発見可能にする

３．研究の方法

本研究では，セキュリティのリスク評価に，ソフトウェアの仕様をモデル化した上で形式的手法が使えないかの検討を行った．自動的に検出可能なモデル検査を用い，ソフトウェアの脆弱性を持つモデルがモデル検査によって検出可能かの検討を行った．検討に際し，いくつかの記述能力の異なる言語を検討した．

SPIN/Promela，Proverif，EVENT-B，Alloy などを使い，一定の脆弱性を設定した上で，その発見にモデル検査が利用できることを確認した．

Promela はモデル検査用言語であり，Π計算による記述に対応している．SPIN は Promela の実行環境である．プロセスとチャネルを用いた通信が可能であるため，Web のようなサーバ，クライアントの自然な表現に適する．

Promela を用いてリモートの攻撃(Web であれば，インターネット上からサーバアプリケーションに対する攻撃）をモデル化する場合，正規利用者の用いるクライアントの他に，悪意による攻撃者のプロセスを記述し，正規利用者の用いるクライアントと同様に攻撃を行うふるまいを記述する．

ProVerif は，暗号向けの安全性検証ツールである．reach- ability(到達可能性）や，observational equivalence，non-interference など特性の検証をサポートするが，これらの特性は，攻撃の検証として用いることができると考える．例えば，状態遷移を重ねて攻撃者が目的に到達できるかどうかを，reachability 条件の検証によって行うことができる．また，observational equivalence は，ある操作を正規利用者が行ったのか攻撃者が行ったのか識別ができなければ，攻撃が成功することになるので，なりすましや遠隔操作の検証に用いることができる．

また，Promela 同様Π計算も記述できるため，プロセスとチャネルによるリモート攻撃の記述も可能である．

Event-B は，B メソッドをベースに開発された，要求仕様の形式検証のための言語である．Event-B はソフトウェア開発における検証では，フランスの鉄道システムに導入されているなどの実績がある．Event-B では，初期に定義したモデルを段階的に詳細化するモデルを作成することで，段階的にソフトウェア仕様を詳細化していくたびに，詳細化されたモデル（リファインメントモデル）を作成し，そのモデルが元の要求を満たしているかを検証することができる．元の要求は，詳細化前のモデルに不変条件(invariant）などの形で記述できる．

研究者は，これを元の設計に対し，脅威(攻撃）の可能性によりセキュリティ要求が破られるかどうかをリファインメントモデルにより実現する手法を考案した．

４．研究成果

Promela/SPIN, Proverif, Event-B による攻撃のモデル化は，それぞれ長所と短所がある．

Promela/SPIN を用いた場合,並列処理やプロセス間通信における攻撃のモデル化には適している一方，基本的には定数しか扱えない上に，記述性が高くないため，攻撃はすべて明示的にプロセス定義によって行う必要があった．一方，Proverif によるモデル化では，機密性の記述が容易であったり，プロセス数を任意に増やすことができる点が長所として挙げられる．また，関数が記述できるため，脆弱性のふるまいの記述も Promela よりは容易になる．攻撃の可能性も，reachability や observational equivqlence を用いることでモデルの記述可能性が高い面もある．しかし，完全性や可用性を直接表現できる仕様がなかったり，機密性の仕様も暗号における機密性に特化しているため，それ以外の特性の記述には工夫が必要となる．

Event-B は，リファインメントを用いることによって，セキュリティ要件や攻撃，対策を対象のリファインメントとして記述することにより，それぞれを分離して扱うことができる．また，状況に応じて攻撃そのものもリファインメントで詳細化できるため，攻撃によるリスク評価にも用いることができ，脅威分析(attack tree の下位ノードの発見など）の自動化の助けになることが期待できる．

SPIN/Promela，ProVerif，EVENT-B，Alloy どの言語においても，モデルに脆弱性を明示的に組み込む必要があることが分かった．これは，本研究において目標としていた，未知の脆弱性を含むモデルについて，その攻撃可能性評価を評価することが困難であることを示す．形式手法あるいはモデル検査そのものをモデルとしたリスク評価が困難ということが判明したため,本研究では方針を調整し次の 2 つの方向でリスク評価を検討することとした．

(1)攻撃の要因分析に用いる attack tree を用い，リスク評価の精度を高める手法．

この手法では，グラフ化した attack tree の中で，最もボトルネックとなっている個所を検出し，リスクの重要性順序付けに用いる手法である．特にコストの問題に着目し，現場レベルの実用的な低コストでの脅威分析を実現するための手法を提案した．コストとトレードオフの関係となる網羅性・完全性については多少失うことを許容するものとする．具体的な手法としては，まずはアタックツリー分析をベースとして，ある情報システムにおける脅威を分析する．その結果として得られるツリー構造において，ボトルネックとなっているノードを抽出し，当該中間ノードの対策の優先順位を高く設定する．これにより全末端ノードの対策を行なうよりも低コストで最終目標を達成することが可能であるという仮定を立てた．

Attack Tree の作成手順を以下に示す．

1.脅威分析を行なう情報システムにおいて想定されるセキュリティリスクから，攻撃者が目標にすると推測されるリスクを抽出する．

例：情報の取得，システムの停止，web ページの改竄，など．

2.手順 1 で抽出された要素をルートノードとして，それぞれに通常の Attack Tree 分析を行なう．

3.共通ノードを正規化し，ツリー構造からグラフ構造に変化させる．

4.ルート・末端を含む全ノードにおいて，当該ノードに指向するノード数および当該ノードから指向するノード数を計算する．

5.上記計算式で得られた数値において，数字が大きいノードがボトルネックであり，優先して対策を行なうべきノードである．

この手法を 2016 年に起きた日本年金機構での情報漏えい事故に適用し,クリティカルとなる脅威を抽出することに成功した．

(2)アタックツリーの冗長性や関係性の欠如の有無の評価と最適化

アタックツリーは複数のレベルを持ち，ルートノード，サブノード，およびリーフノードを含むさまざまなノードで構成されている．これらのノードは，それらの関係を議論するときに親ノードと子ノードに分けることができる．子ノードは，直接の親ノードを真にするために満たさなければならない条件として定義することにより，アタックツリーとの間の垂直関係を表現することができる，しかし，設計されたアタックツリーが不適切なため，ノードが不正確になる可能性がある．これらの問題を解決するために，記述したアタックツリーを Interpretive Structural Modeling (ISM）を用いて新しいツリーに再構築するための新しい方法を提示する．

提案手法は，並列関係を除去することによって，親ノードと子ノードとの間の関係を容易に修復することができる．提案手法は，より正確なシステムの脅威分析とより良い防御策のための明確なアタックツリーを導き出した．

(3)既存のプログラムについて,脆弱性評価を行うテストを機械学習により自動生成する手法の研究

Web アプリケーションの脆弱性である SQL インジェクションとクロスサイトスクリプティングに着目し，Web サーバーに対する「チャレンジクエリ」を送信し，Web アプリケーション側の処理後に生成されたレスポンス情報から正常構文の特徴を抽出した．

次に，正常構文の特徴と攻撃コードの可変長シーケンスのペアを学習済みモデル「Seq2Seq」に渡すことで，レスポンス情報の特徴から攻撃コードを予測する手法を提案した．

また，評価対象には，様々な既知の脆弱性が意図的に埋め込まれている Web アプリケーションの「OWASP BWA」を用いて，提案手法の有効性について確認を行った．

提案手法については，Mysql を用いた「bWAPP」などの本手法が SQL インジェクションとクロスサイトスクリプティング検知に一定の効果があると考えられる．

５．主な発表論文等

〔雑誌論文〕（計 1 件）

H. Shimamoto, N. Yanai, S. Okamura, J. P. Cruz, S. Ou and T. Okubo, "Towards Further Formal Foundation of Web Security: Expression of Temporal Logic in Alloy and Its Application to a Security Model With Cache," in IEEE Access, vol. 7, pp. 74941-74960, 2019.

〔学会発表〕（計 6 件）

Tadahiro Shibata, Takao Okubo, Proposal of effective measures by Attack Tree based on detection of critical nodes, The 1st International Workshop for Models and Modelling on Security and Privacy, 2016.

Cai Hua, Hironori Washizaki, Yoshiaki Fukazawa, Takao Okubo, Kaiya Haruhiko and Yoshioka Nobukazu Yoshioka. Restructuring Attack Trees to Identify Incorrect or Missing Relationships between Nodes, WESPr-18: The International Workshop on Evidence-based Security and Privacy in the Wild 2018.

大久保隆夫，矢内直人，vent-B を用いた攻撃，脆弱性の検証のための脅威モデル化の検討，暗号と情報セキュリティシンポジウム，2017.

矢内直人，大久保隆夫，非干渉性の再考と応用，暗号と情報セキュリティシンポジウム，2017.

柴田理洋，大久保隆夫，Attack Tree を用いたクリティカルパス検出による効果的対策の提案，コンピュータセキュリティシンポジウム，2016.

大久保隆夫，セキュリティ，セーフティのリスク評価手法に関する調査，暗号と情報セキュリティシンポジウム，2018.

陳含悦，大久保隆夫，機械学習による Web アプリ脆弱性の検出技術に関する研究，第 81 回情報処理学会全国大会，2019.

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）
○取得状況（計 0 件）

〔その他〕
ホームページ等は無し

６．研究組織

(1)研究代表者
大久保 隆夫(0kubo，Takao)
情報セキュリティ大学院大学・その他の研究科・教授
研究者番号:80417518