Attack Treeを用いたクリティカルノード検出による効果的対策の提案

Proposal of effective measures by Attack Tree based on detection of critical node.

情報セキュリティ大学院大学・ネットワーク分科会・柴田理洋

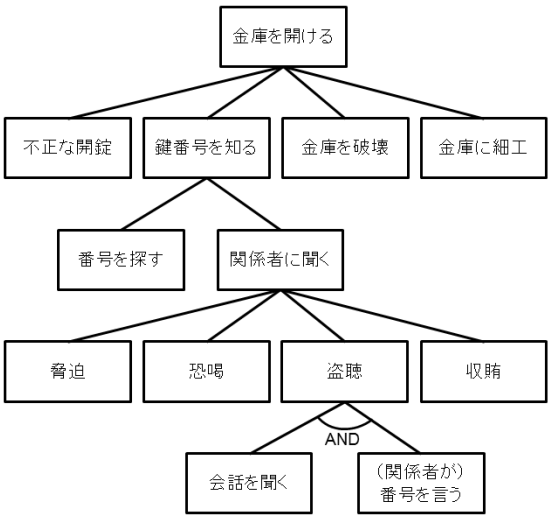
In this research, I propose a new method based on one of the threat analysis method called Attack Tree, for conduct threat analysis more simply and efficiently. It aimed at a method that can simplify the method itself to alleviate the dependency and can easily find the countermeasure. I analyze a threat based on the actual case using the proposed method and show its effectiveness by comparing / examining with the existing Attack Tree. In the comparison, I examine the cost of required security measures extracted by threat analysis and the ease / relevance of the threat analysis itself.

概要

近年その重要性が増している情報セキュリティを実現するにあたって，脅威分析と呼ばれる手法が着目されている．脅威分析とは情報システムの設計段階において，その仕様からセキュリティ上の脅威を抽出する手法である．脅威分析には複数の手法が考案されており，それぞれ何らかの問題点が指摘されているものの，それらの実用性は確かである．本研究ではAttack Treeと呼ばれる手法を改良し，より低コストとなる対策手法選定を行なうことが可能な手法を提案した．

Attack Tree

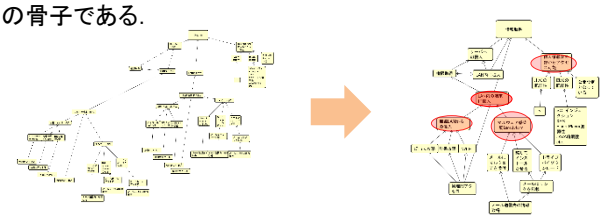
攻撃者視点で，ある攻撃目標を実現するために考えられる手法を抽出する手法である．



表：考案者でるB.Schneier氏のHPより和訳・引用したAttack Treeの一例

提案手法

脅威分析において，異なる攻撃手段の中に同一の手順が含まれることがある．Attack Tree中に出現した同一のノードを統合し，木構造からグラフ構造に変化させることが本提案手法の骨子である．



そしてグラフ構造化したノード群で，最も他ノードからの依存関係が強いノードをクリティカルノードと呼称し，対策を優先的に行なうノードとして導出する．（グラフ中の赤いノード）

	オリジナル	提案手法
対策対象	末端の葉ノード	全てのノード
選定基準	攻撃のしやすさ	防御の完全性
想定相手	スクリプトキディ	標的型攻撃

末端ノードのみで全ての攻撃を防ごうとすると全ての末端ノードを対策しなければならないが，提案手法ではより少数のノードで完全な対策が可能である．

評価

実際のセキュリティインシデントを元に提案手法によるAttack Tree変形グラフを作成し，オリジナルAttack Treeとの比較を行なった．それぞれ導出された必要とされる対策手法にかかるコストを3軸から比較した．

1. 対策を行なうノードの単純な個数．
2. 対策にかかる機能数を比較した．システム設計図より導出される，対策を行なうために影響する情報システムの機能数．
3. 対策にかかる費用を比較した．セキュリティベンダ等の公開カタログ価格をベースに導出される，セキュリティ対策にかかる価格．

結論

評価(1)においては単一ノードであっても複数の対策を必要とする場合があり，有意な比較は得られなかった．しかし評価(2),(3)においては，いずれも本提案湯法によるコスト低減を示すことができた．