AttackTree

Threat Analysis Software

Isograph

AttackTree

脅威分析ソフトウェア

Isograph 社のソフトウェア AttackTree は、強力でユーザが扱いやすい攻撃ツリー分析の環境を提供いたします。グラフ化することにより視覚的に分かりやすく、さまざまな脅威に対する理解を容易にします。セキュリティが要求されるインターネット、銀行システム、防犯設備、個人機密なども AttackTree を用いてその脅威をモデル化することができます。

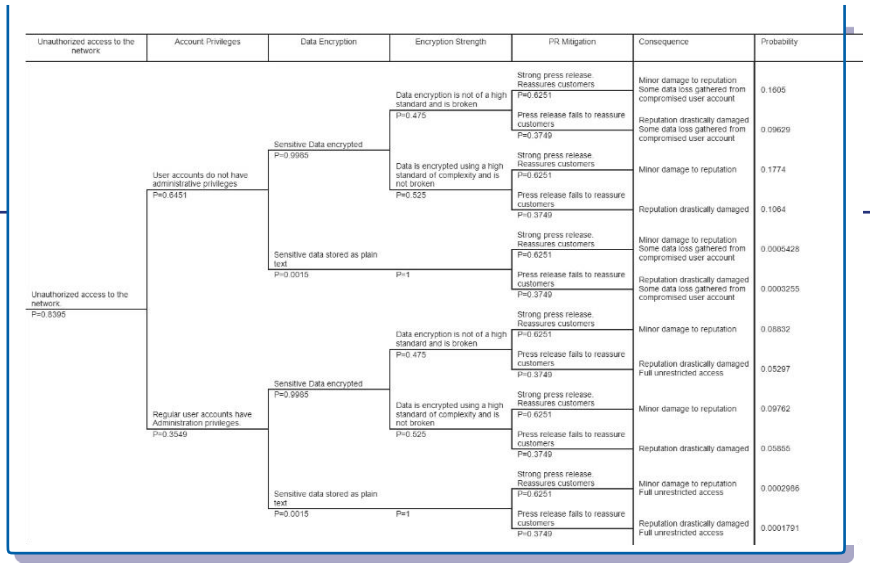
AttackTree は外部からの攻撃が成功してしまった場合に、その攻撃の緩和策を立てるときにも効果を発揮します。その緩和策としては、データの流出を減らすため攻撃を受けたことを知らせ、緊急時の対応に切り替わることが挙げられます。こういった緩和方法も AttackTree 内の緩和ツリー機能を用いて視覚的に表現することが可能です。

システムへの攻撃方法を理解することは、その対抗策や緩和策を策定する上で役立ちます。

自国へのテロリストからの攻撃リスクの増加、コンピュータシステムへのクラッキング、銀行のシステムへの不正利用などを考えると、AttackTree はシステム開発者や保守要員にとって計り知れない価値を持つツールでもあります。

特徴

1. 攻撃ツリーと緩和ツリーの構築、及び分析のための洗練された環境
2. 簡単に質の高い図を作成することができる自動描画機能
3. 攻撃を成功に導く事象を結びつけ、視覚的に表すカットセット分析
4. 攻撃が成功する可能性を評価する確率分析
5. 攻撃の難度、コスト、設備などに応じたモデルをカスタマイズ可能なインジケータ
6. 予想される攻撃効果をモデル化し、分類する結果分類機能
7. 寄与因子と感度因子による重要度分析
8. 攻撃ツリーと緩和ツリーの構造、事象、インジケータ、結果など収納できるライブラリ機能
9. レポートウィザードを有する優れたレポート機能
10. マイクロソフトオフィスとインターフェイスを有するカスタマイズレポート
11. 強力なインポート/エクスポート機能



概要

アタッカーが標的への攻撃を成功させるには様々な障害があります。彼らは個人、もしくはチームで様々なレベルの攻撃を仕掛けてきますが、それらに対する対応策もそれぞれ存在します。

AttackTree はそれらの攻撃がどのように成功するかを視覚的に表し、またどの攻撃が最も成功の可能性が高いかを確率分析することが可能です。この方法論は特定の条件下でシステムの脆弱性を明らかにすることも可能です。

例えば、アタッカーにとって最も低コストで成功確率の高い方法は何なのか？ AttackTree は攻撃コスト、攻撃実行の難度、またその他定量化可能な観測量をインジケータとして定義することが可能です。その結果、どのような攻撃が最もリソースが小さいのか？また攻撃を成功させるには特別な設備は必要なのか？などの疑問に AttackTree は答えてくれます。

AttackTree では結果の分類やレベルを攻撃ツリーのノードに割り当てることが可能です。攻撃の成功は財政的、政治的、経営上、安全上重要な結果を引き起こす可能性を持っています。また攻撃が完全ではなく、部分的にでも成功した場合には、また違ったレベルでの影響が出てくる可能性もあります。これらの結果をすべて AttackTree でモデル化できます。

ダイアグラムの構築

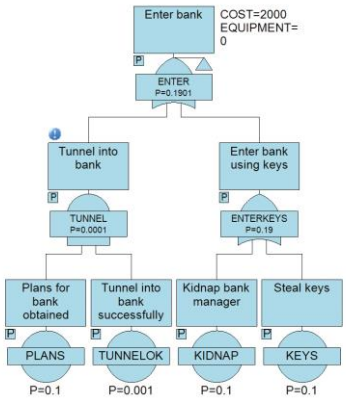
標的となるモデルの構築は、攻撃可能な場所を特定することから始まります。次に達成される可能性のある攻撃方法を特定します。各攻撃の方法は攻撃が成功するために必要な 1 つ以上の条件を満たしています。従って攻撃ツリーの構築における次の段階は、各攻撃を基本条件まで分解することです。これによって、すべて単一で定量化可能な事象で攻撃ツリーを構築することになります。最後に攻撃の影響をどのように緩和できるかを示す緩和ツリーを任意に構築することもできます。攻撃ツリーを構築出来たら、各攻撃の頻度、各事象の発生確率、つまり攻撃が成功する確率を指定してやる必要があります。

AttackTree は攻撃がどのように成功するのかを分析するのに加え、攻撃を実行するのに必要なコストや特別な設備などアタッカーに要求されるものもインジケータを使用して記述できます。そして各インジケータの種類が

各事象に割り当てられます。
最後に、AttackTree でユーザが結果を定義し、それを攻撃ツリーのノードもしくは緩和ツリーのエンドブランチに張り付けることが可能です。このような方法により、攻撃対象となったシステムへの攻撃結果をモデル化することが可能となります。

AttackTree 分析

分析の過程において、AttackTree は各カットセット、ゲート、結果の確率やインジケータの値を計算します。これによって成功確率順にランク付けされた攻撃の成功につながる事象の組み合わせをすべて表示することが可能です。このリストは、インジケータの値(例えばアタッカーにとって低コストの場合など)によってフィルタリングすることが可能です。さらに攻撃ツリーのカットセットの痕跡を追いかけることにより、攻撃が成功した場合の道筋を容易に特定します。
また重要度ランキングの計算により、どのような攻撃がシステムにとって最大のリスクとなるかを、素早く特定することができます。これはシステム内の弱点の発見を支援し、より簡単に有効な対策の実現を可能にします。



外部アプリケーションとの連携

AttackTree には Isograph 社のインポート/エクスポート機能が標準機能として含まれています。この機能では Microsoft Excel、Access、テキストファイルなどをインポート/エクスポートすることが可能です。ウィザード機能を使用すると、このようなデータ転送を簡単に行うことが可能です。

包括的なレポート機能

セキュリティ研究ではプロフェッショナルなレポートを作成することは最重要項目の 1 つです。そのようなレポートを作成できれば、同僚、管理者、顧客、規制当局に明確かつ理解しやすい形で結果を示すことが可能になります。AttackTree Report Designer はプレビュー、フィルター、並べ替え、印刷などの機能を有し、望んだ形式にカスタマイズした高品質なレポートを作成することができるのです。

エンタープライズシステム

AttackTree には Isograph 社エンタープライズシステムが組み込まれており、大規模な組織内でのコラボレーションや、バージョン管理が可能となっています。エンタープライズシステムを使用すると、プロジェクトは中央データベースに保存され、ネットワークを経由し安全に情報をやり取りすることができます。またユーザが、システム管理者の情報の読み取り、書き込み、また権限の変更権などを決定できます。

詳しい情報は Wavefront までお問合せください。

Isograph 社の関連製品

Isograph 社の Reliability Workbench は Parts Libraries、Reliability Growth、FMECA、 Reliability Block Diagram、System Safety Assessment、Fault Tree、Event Tree、 Markov analysis を含む統合ソフトで、コンポーネントの故障率の算出を支援します。

Isograph 社

Isograph 社は 1986 年に設立され、信頼性、可用性、保全性、安全性に関するソフトウェアの開発と提供において世界有数の企業の一つです。現在は、イギリスとアメリカに拠点を構えています。

Isograph 社のソフトウェアのご利用ユーザーは世界で約 10000 サイト以上に上ります。また、すべてのソフトが専門知識を有するグループによって完全に維持管理されています。ソフトウェアの強化は、安全性、信頼性を研究するユーザーコミュニティ、コンサルタント、大学との連携により、大きく推進されています。

適用事例

2015 年 8 月に、Charlie Miller 氏と Chris Valasek 氏はワイヤレステクノロジーによって、車内のオンボードシステムに攻撃する方法を説明する論文を発表しています。[1] この方法を使用するとドアロックやヘッドライト、ステアリング、ブレーキなど重要なシステムにアクセスすることが可能となります。また同じく 2015 年 8 月に Foster 氏と Koscher 氏はドングルを搭載した車両に通常どのような攻撃が行われるかを実証した論文を発表しています。[2]

AttackTree はこのような攻撃についての脅威を理解し、モデル化するための有効な手段であることが実証されています。[3] この分析手法によってリスクを評価しシステムの設計または再設計を促し、より安全な設計を可能にします。

AttackTree 及び Isograph 社製品のお問合せは、下記までお願いします。

株式会社ウェーブフロント

sales@wavefront.co.jp

045-682-7070

動作環境

対応 OS	Windows XP SP3 (all versions except media center and Home) Windows Vista (all versions) Windows 7 (all versions) Windows 8 and 8.1 (all versions except RT) Windows 10 (all versions) Windows Server 2003 Windows Server 2008 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 ※すべて64bit版(32bit版はありません) ※※NET Framework version 4.0 (Full) とWindows Installer 3.1 がインストールされていない場合はそれらのインストールを要求されます。インストール前にOSの最新サービスパックへの更新をお勧めしております。
最低動作環境	CPU1.4GHz(x64 processor)、メモリ 1GB、空き容量 5GB
推奨動作環境	CPU2GHz 以上、メモリ 2GB、空き容量 5GB 以上

補足

この要件に加えてハードディスクは、プロジェクトの作成、テンプレートの報告、およびオペレーティングシステムの機能の修正に使用できる必要があります。上記のディスク容量要件では、プロジェクトやレポートを格納するために必要なディスク容量は考慮されていません（一般的な大規模な AttackTree プロジェクトは 50MB のディスク容量を占有し、20 ページのグラフレポートは 3.5MB を占有します)。

参考文献

[1] Miller, C. & Valasek, C. 2015 Remote Exploitation of an unaltered passenger vehicle. In *Black Hat USA 2015; Proc. Intern symp., Las Vegas, 1-6 August 2015.*

[2] Foster, I. & Koscher, K. 2015 Exploring controller area networks. In *24th Usenix Security Symposium; Proc. intern. symp., Washington, D.C., 12-14 August 2015.*

[3] Wiseman,D.R reliability and safety: innovating theory and practice, In Attack tree analysis,pp1023-1027,CRC Press, September 2016