偽装PC環境によるアクティブ・プロテクト方式

上村, 宗嗣 / KAMIMURA, Munetsugu

(出版者 / Publisher)
法政大学大学院理工学・工学研究科
(雑誌名 / Journal or Publication Title)
法政大学大学院紀要. 理工学・工学研究科編 / 法政大学大学院紀要. 理工学・工学研究科編
(巻 / Volume)
55
(開始ページ / Start Page)
1
(終了ページ / End Page)
6
(発行年 / Year)
2014-03-24
(URL)
https://doi.org/10.15002/00010472

偽装 PC 環境によるアクティブ・プロテクト方式

Active Protect Architecture to collect profiling information of malicious person.

上村宗嗣
Munetsugu Kamimura
指導教員　金井敦

This paper describe about an Active Protect Architecture to collect profiling information of malicious person. To protect PC, password is commonly used. And previous work proposes security level management method. This method protects PC by restricting the behavior of malicious person. However, those ways are not able to collect malicious person profile. In this paper, the architecture of active protect is proposed. The prototype is developed and feasibility is evaluated.

***key words** : Computer Security, VM*

１．はじめに

ある情報を攻撃者から守ることを考える時, セキュリティレベルを高いものにすると, その情報の安全性は高いものになるが, それに比例してその情報の利便性は低下してしまう. なので, セキュリティレベルを高いものにしたとしても, その情報を標的としている攻撃者が存在しなければ, セキュリティレベルを高めることは単に利便性を損ねるだけの結果となる. ここで, 防御対象の周囲の環境を判断して動的に防御対象のセキュリティレベルを変化させることで安全性を保持したままセキュリティの可用性を高めることが期待できる. 先行研究では, 防御対象と攻撃者距離, 攻撃者の種類という２種類の動的変化要素を判断して攻撃者への対応策を変化させる手法を提案している[1]. この方法での攻撃者への対応は, 攻撃者が危険な人物である, 攻撃者と防御対象の PC の距離が近いなどの危険性が高い状況では攻撃者に防御対象 PC の操作をさせないという対応になっている. このようにリスクの低減を目的として攻撃者の行動を制限する防御方式を本稿ではパッシブ・プロテクト方式と呼称する. パッシブ・プロテクトにおいて攻撃者に PC を操作させない事は安全な対抗策であるが, 攻撃者が PC に対してどのような目的でどのような操作を行いたかったのかを把握することは出来なくなるため攻撃者の情報を収集する機会を失うという見方にもなる. よって攻撃者の特定を考える場合, 攻撃者の行動を制限せずに攻撃者の情報収集を行う積極的なセキュリティが求められる. 本稿ではこれをアクティブ・プロテクト方式と呼称する. 本研究ではアクティブ・プロテクト方式の概念とそれを実現する方式を提案する.

２．攻撃者・環境の想定と基本コンセプト

アクティブ・プロテクトは攻撃者の不正操作から PC を保護すると同時に, 不正操作している人物の特徴や操作目的を把握するための情報収集を行う. 収集する情報は攻撃者の行動や PC 上での操作履歴, PC に付属するカメラでの撮影が可能だと考えられる. 操作や行動から情報を収集することを考えると攻撃者の行動は制限するべきではない. 今回提案するアクティブ・プロテクトは攻撃者に対して PC を操作可能な状態であると認識させ, 攻撃者に操作させることで情報を収集するものであるため, 意図的に攻撃者が攻撃を行いやすい状況を作るという点でネットワークでの情報収集に用いられるハニーポットとの類似性が考えられる[2].

ハニーポットと異なる点として次の要素が挙げられる．

A)　**正規利用と防衛利用を１つの PC で両立させる**．

ハニーポットとして稼働する PC は情報の収集というタスクに専念するが，今回のモデルでは正規のユーザが PC を利用する場合と攻撃者が PC を不正操作する場合で利用の形態を異なるものにしなければならない．

B)　収集する情報の違い

ハニーポットが収集する情報は新たなマルウェアや新規の攻撃手法といった研究的利用が期待出来る情報であるが，今回のモデルでは攻撃者の特定が期待出来る情報を収集する．

C)　攻撃者の環境の違い

ネットワークを通して遠隔的に不正操作が行われるハニーポットと異なり，今回は攻撃者が PC を直接操作する状態を想定している．そのため攻撃者が PC を操作する以前に PC 付近で行う行動も収集の対象とすることが出来る．また，遠隔的な環境とは異なり，攻撃者が視覚や操作感から得られる情報もあるため，防衛利用稼働の際は攻撃者に察知されない工夫が必要となる．

また，モデルが満たすべき条件を決定するため攻撃者及びモデルの適応環境を以下のように想定する．

A)　環境の想定

モデルが導入されるのは企業のオフィスのように１つの室内に１つから複数台の PC が配置されている環境とする．攻撃者の範囲を設定するために，システムが導入される部屋は他の部屋よりもセキュリティレベルが高いものであるとする．

B)　攻撃者の想定

上で述べたようにシステムが導入されるオフィスは他のオフィスよりもセキュリティレベルを高いものとするため，システムが導入されている PC の正規ユーザは攻撃者として考慮しない．システムが導入されている PC に対して情報の窃盗，情報の改ざん，ネットワークに繋がっている他の PC へのアクセスを試みるものとする．また，攻撃者は単独で行動を行うものとする．

ここまでの要素から，本セキュリティモデルに求められる機能を以下に示す．

A)　オフィス内の PC 及びネットワーク上で繋がる PC が保護される

B)　攻撃者を特定するための情報収集が可能

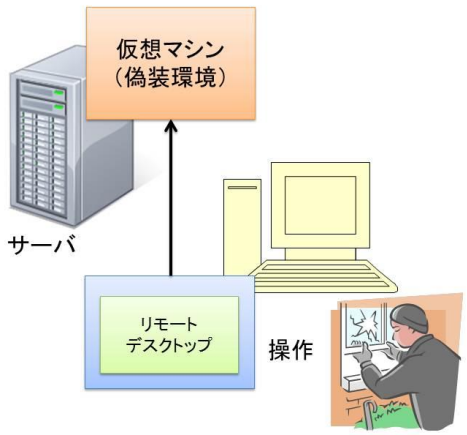
C)　正規利用と防衛利用の両立

D)　攻撃者の行動や操作からの情報収集

E)　情報収集の際の看破防止

以上より，本論文では正規ユーザが実際に操作する環境に似せた偽装環境を用意し，PC 上で稼働する偽装環境と各 PC に設置する近接センサを用いて攻撃者からの PC 保護と攻撃者特定のための情報収集を行うシステムを提案する．図１に提案するシステムの方式を示す．図 1(a)のように，PC を操作する人物が正規のユーザである際は PC の実環境が操作されるが，図 1(b)のように攻撃者が操作する際はサーバ上に立ち上がっている偽装環境を操作することになる．また，攻撃者が実空間を移動する際の行動を記録するためにシステムが導入される全ての PC に近接センサを付加し，室内での人物の行動を記録する．

(a)　正規ユーザが操作する場合



(b)　攻撃者が操作する場合

図１　提案するセキュリティシステムの基本方式

３．アクティブ・プロテクトの機能

本章では，偽装環境の構築，収集する情報と収集手法について述べる．

(1) 偽装環境

攻撃者が偽装環境である事を看破する可能性は，攻撃者の「攻撃対象 PC でどのような作業が行われているか」という知識に依存する．看破を防止するためには，攻撃者に操作させる偽装環境を実環境と似せた環境にすべきである．今回の方式では実環境の情報の一部を偽装環境で利用することで偽装性を向上させる．今回偽装環境で利用する情報は以下の通りである．

A) 盗まれても害のないファイル

B) 漏洩が許されないファイルのファイル名

C) 上記のファイルが存在するフォルダ

攻撃者が窃盗などを目的としている場合には重要なファイルを開く可能性が考えられるが，攻撃者の情報を収集するのは重要ファイルを開くまでとし，それ以降は攻撃者に偽装環境であることを看破されることは許容し，看破される際は PC をシャットダウンし攻撃者の操作を遮断する．

(2) 攻撃者特定のための情報収集・解析

システムが導入されている PC が存在する室内に攻撃者が侵入してから偽装環境の看破に至るまでの過程で攻撃者特定のために収集する情報は以下の通りである．

A) 攻撃者の歩行経路と PC 操作開始までの所要時間

二章で述べた様に，今回のシステムを導入する PC には近接センサが付加される．近接センサでは PC の周囲約 4m に物体が存在するかを判別し，これを連続的に行うことで攻撃者の PC 付近の移動速度を収集する．複数の PC が室内の通路に面して密に並ぶ環境では複数の近接センサの情報を統合して攻撃者のオフィス内での移動経路を収集する．

B) PC 操作時のフォルダ遷移履歴と最終的な操作対象

偽装環境稼働中は操作者のフォルダ遷移や操作するファイルを記録する．実環境における重要なファイルは偽装環境では内容が意味のないものになっており，攻撃者が内容を見た際に偽装環境であることを看破される可能性が高いため，情報の収集はそれらのファイルの内容が見られるまでの物を解析に用いる．

C) 外部記憶媒体内情報取得及び PC 間とのファイル移動

攻撃者が外部記憶媒体を PC に接続した場合，外部記憶媒体にファイルがある場合は偽装環境にそれらを全て偽装環境内に移動させる．また，PC との間で外部記憶媒体からファイルが移動された場合は移動先・移動元フォルダとファイル名を記録する．

D) カメラでの攻撃者撮影

攻撃者は操作対象 PC に向き合うため，PC にカメラを付加することで攻撃者を正面から撮影した画像を取得することが可能である．

(C)の外部記憶媒体内の情報取得と(D)のカメラでの攻撃者撮影は直接的に攻撃者の情報を取得することを目的としている．(B)における最終的な操作対象及び(C)における PC と外部記憶媒体でのファイル移動操作の記録は攻撃者の攻撃意図を収集する目的がある．(A)と(B)は攻撃者の持つ知識を推測するための情報である．収集した情報を元に推測可能な攻撃者の持つ知識は以下のものが考えられる．

A) システム導入室内についての知識

攻撃者の室内での移動速度，攻撃対象 PC までの移動経路がスムーズであるほど攻撃者が持つ室内についての知識が高いものであると推測できる．精度を向上させるためには室内の設置 PC を多くする必要がある．

B) 企業，個人についての知識

攻撃者がファイルの集取，改ざんや特定フォルダの集取を行う場合，フォルダを遷移して対象物を探す必要がある．その際にフォルダの選択ミスによる手戻りやフォルダの選択時間から操作のスムーズ度から，PC の正規ユーザやシステムを導入している団体についての知識が得られると考えられる．収集した情報から最終的な攻撃者の目標物を特定し，そこに至るまでの過程で目標物のファイル名・フォルダ名と同分類の過程フォルダ名をいかにスムーズに遷移したかを解析することで実現する．

偽装環境を利用して攻撃者の操作を元に収集した情報は偽装環境内に保存し，それ以外の情報は仮想マシンが動作するサーバ内に保存する．攻撃者の操作が終了した後に偽装環境内に保存されている収集情報をサーバ上に移し解析を行う．

(3) システムの方式

本章ではシステムの動作方式について述べる．本モデルでは正規ユーザが利用する正規利用と攻撃者の情報を収集する防衛利用を１つの PC で行うため，実環境と偽装環

境を切り替えるための条件を設定する必要がある. 今回は, PC の置かれる状態を３つに分類し，状態の遷移によって PC の稼働形態を切り替える．以下に分類した状態の内容と，その時の稼働形態について記す.

A) **セーフティ状態**

正規ユーザが PC の前にいる状態である．この時 PC で操作可能なのは実環境である．セーフティ状態では偽装環境の更新を定期的に行う.

B) **スタンバイ状態**

正規ユーザが席を離れ, 攻撃者が PC の操作を行なっていない状態である．スタンバイ状態に遷移した時, 近接センサを用いた室内の情報収集を開始する．この時 PC では偽装環境が動作するが, 偽装環境を用いた情報収集動作は開始しない.

C) **アラート状態**

攻撃者が PC の操作を行う状態である. アラート状態で操作可能であるのは偽装環境であり，アラート状態となった PC は偽装環境による情報収集動作を行う.

３つの状態は図２の状態遷移図に従って, その状態が移行する．状態遷移が発生する時の動作について以下に記す.

A) 正規ユーザが PC の前から離れる．この時 PC 上では偽装環境が起動する.

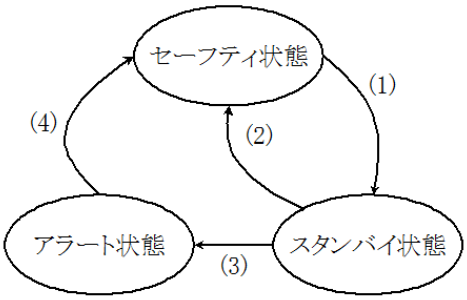
B) 正規ユーザが席を離れている間に攻撃者が現れず, 正規ユーザが再び PC の前に戻るとき，PC 上の偽装環境が終了する.

C) 正規ユーザが席を離れている間に攻撃者が PC の操作を行うとする. この時攻撃者が操作可能であるのは偽装環境である．PC は偽装環境を用いた情報収集を開始する.

D) 攻撃者が攻撃を完了し，席を離れている時，正規ユーザは偽装環境の状態を保存し，PC をセーフティ状態に戻す.

４．実装

今回, システムは保護対象となる PC を１台として実装した. 本システムは図３の様に全ての構成機器をネットワークで接続する形で構築される. サーバ上の偽装環境用仮想マシンと保護対象 PC には, それぞれ常駐ソフトウェアが稼働しており，セーフティ，スタンバイ，アラートの各状態において連携して動作することで提案する手法を実現している.



(1) 正規ユーザがPCから離れる
(2) 正規ユーザがPCに戻る
(3) 攻撃者が攻撃者を開始する
(4) 正規ユーザの手動による遷移

図２　システムの状態遷移

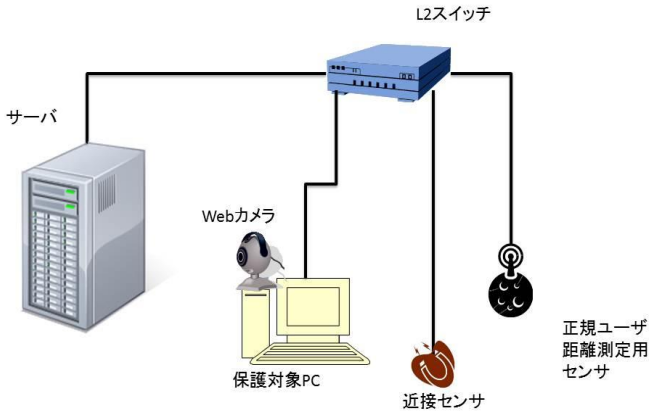


図３　実装の構成図

５．評価

本章では４章で述べた実装を評価する. 評価はシステムの可用性の指針と鳴るセーフティ状態とスタンバイ状態感での切り替え速度, 最も攻撃が行われる可能性が高いと考えられる外部記憶媒体を用いた情報窃盗に対して偽装環境看破可能性の指針となる偽装環境と外部記憶媒体間でのデータ転送速度の２点をもって評価する.

表１に２状態の切り替え速度を記す. 表１の上がユーザが離席してから状態の遷移が完了するまでの時間, 下がユーザが席に戻る際の状態遷移完了までの時間である. 今回の実装では閾値を約４m として離席と在席を区別している. 今回測定した秒数を一般的に離席時に使用するスリープモードの遷移時間と比較すると, スリープ状態への遷移が 11 秒，スリープ状態からの復帰が６秒という結果になり，提案手法は実用の範囲内であると評価できる.

表１　セーフティ状態とスタンバイ状態間での状態遷移速度

セーフティから スタンバイへの遷移	11 秒
スタンバイから セーフティへの遷移	8 秒

表２　実環境と偽装環境のデータ転送速度の比較

	実環境での動作時間	偽装環境での動作時間
ファイルの転送時間 (236KB)	USB→PC　1 秒未満 PC→USB　1 秒未満	USB→PC　1 秒未満 PC→USB　3 秒
ファイルの転送時間 (48.1MB)	USB→PC　2 秒 PC→USB　4 秒	USB→PC　23 秒 PC→USB　37 秒
ファイルの転送時間 (1.27GB)	USB→PC　7 分 30 秒 PC→USB　7 分 45 秒	USB→PC　25 分 3 秒 PC→USB　27 分 30 秒

表２に外部記憶媒体を用いた実環境と偽装環境のデータ転送速度の比較を記す．外部記憶媒体には USB メモリを用い, 比較のために大きさの異なる３つのファイルを用いた．表のように，ファイルサイズが大きくなると実環境よりも偽装環境の転送速度が大きく遅れる結果となった．これは仮想マシンのデータ書き込み速度が低速である事に起因する．今回の実装の場合，一般的な文書ファイル程度なら速度低下は発生せず看破可能性は低いという結果になった．

６．考察

(1) アクティブ・プロテクト方式の検証

提案する手法は実環境を保護したまま攻撃者の室内行動や操作履歴というパッシブ･プロテクトでは収集不可能な情報を収集する事が可能である. 今回収集した情報を解析して得られる攻撃者の知識情報や攻撃目的は単体で攻撃者の特定に至るものとなるのは難しいため, 現時点では視覚的情報などの直接的に特定が期待できる情報の補助として用いる事となる. 現状よりも更に攻撃者の特定に近づく情報収集や解析が必要である.

(2) システム導入の利点

図 12 に示す通り，提案したアクティブ・プロテクト方式はネットワークを利用して PC，サーバ，周辺機器を接続して構築するものである. ここで大きな利点として挙げられるのは，室内に特別な工事が必要ない点である．監視カメラや扉開閉用センサの場合, オフィスの転移が発生すると新たに工事を伴うセキュリティシステムを構築する必要があり，時間とコストが発生する．一方でアクティブ・プロテクト方式の場合，必要機材とネットワークさえ存在すれば構築することが可能であるため, コストと構築時間面では優れていると評価できる.

(3)実装についての考察

今回のシステム構成はリモートデスクトップによる偽装環境接続の方式を取った. そのためサーバやネットワークが事前に攻撃者に攻撃される場合やネットワーク障害が発生した場合システムが無効化される. リモートデスクトップ方式以外にも, 保護対象 PC 上に仮想マシンとして偽装環境を立ち上げるスタンドアローンの手法が提案されている[3]．この手法はネットワーク障害の影響は受けないが, 表１の評価を行った場合提案手法よりもそれぞれ 52 秒，16 秒提案手法のほうが高速であった．可用性を考えた場合, スタンドアローンの手法では動作速度が実用上厳しく，提案手法の方が優れていると言える.

７．終わりに

本研究では偽装環境を用いて攻撃者の情報を収集することによって特定を行うための手法を提案した. 本研究では攻撃者の特定を行うために攻撃者の目的, 知識量を解析するための情報収集を行う方式を取った. 本研究は情報収集に重点を置いたため，解析については考察に留まった. そのため, より詳しい解析の手法は今後の課題となっている.

謝辞

指導教授の金井先生をはじめ, 本研究にご協力頂きました全ての皆様に感謝いたします.

参考文献

[1]榎本真也，金井敦，谷本茂明，佐藤周行，”ダイナミックに制御する情報量英対策システムの検討”，情報科学技術フォーラム FIT 2012 講演論文集

[2]小泉芳，小池英樹，安村通晃，“行動制限型ハニーポットの改良方法の提案・実装・運用”，情報処理学会研究報告， 2004 vol.129，pp.57-pp.62

[3]上村宗嗣，金井敦，谷本茂明，佐藤周行，”偽装環境による PC 保護と不正操作者情報収集技術の提案”，コンピュータセキュリティシンポジウム 2012 論文集, 2012