マルチメディア通信と分散処理　111－21
コンピュータセキュリティ　20－21
（２００３．２．２８）

スクリプトによる管理者権限奪取の検出法

岩田　雅士・山本　智一・田中　雅紀・阿部　武彦（金沢工業大学）・木村　春彦（金沢大学）

本研究では侵入手法の一つである、スクリプト言語攻撃による管理者権限の奪取を検出するシステムを構築することを目的とする。スクリプト言語攻撃とはスクリプトを侵入対象のパソコンに送って実行することで、そのパソコンの管理者権限を取得する攻撃手法である。Windowsではユーザ情報はレジストリと呼ばれる階層型データベースに記録されている。そこで、レジストリ以外に正規のユーザ情報を記したユーザ情報データベースを用意し、レジストリのユーザ情報とユーザ情報データベースのユーザ情報とを比較することで、不正なユーザが追加された場合に警告を行う。

The method of detecting the administrator authority capture by a script attack

Masashi Iwata・Tomokazu Yamamoto・Masanori Tanaka・
Takehiko Abe (Kanazawa Institute of Technology)・
Haruhiko Kimura (Kanazawa University)

The purpose of this research is to build an intrusion detection system, which detects the administrator authority capture by a script attack. The script attack is the attack technique which acquires the administrator authority of the personal computer by sending and performing a script in the personal computer for invasion. In Windows, user information is recorded on the class type database called registry. In this paper, we propose a new database named the user information database and use it to record the user information which is the same information recorded on the registry. The system can detect an inaccurate user by comparing the user information on the registry with the user information on the user information database.

1. はじめに

わが日本での高速常時接続回線の普及率の増加に伴い、不正アクセスの数が増加している[2]。これら不正アクセスは、不正アクセス防止法などの法律が施行されてからも増える傾向にある。不正侵入には多くの種類があり、攻撃方法や攻撃ツールをインターネットから入手することも難しいことではない。また、アプリケーションバグなどを利用した侵入もホスト管理者がそのバグ情報を手に入れるまでにそのバグに対する攻撃手法がインターネット上で広まっていることが多いのである。ホストコンピュータへの侵入を防ぐ技術にファイアウォールを用いたアクセス制御技術やワンタイムパスワードなどの認証技術があるが、これらでの防御は完璧ではない[3]。

そこで、侵入を防ぐには不正アクセスを検出し、被害が拡大しないように対策をしなければならない。そのための侵入検出システムの研究が盛んに行われている。各システムが検出の対象としている不正侵入には様々なものがあるが、中でもスクリプト言語攻撃による管理者権

限の奪取[5]は大きな問題とされている。

そこで、本研究ではWindowsNTを対象とし、このスクリプト言語攻撃による管理者権限の奪取を検出する手法を提案する。なおWindowsNTを対象としたのは、小規模オフィスなどに構築されるネットワークには構築しやすいとの理由からNTサーバ系が多いということと、そのようなネットワークには管理者不在の場合が多く、セキュリティ面で大規模ネットワークと比べると不安が残るからである[4]。また、既存のWindows版の代表的な侵入検出システムではスクリプト言語攻撃による管理者権限の奪取を検出できないという問題も存在するためである。

2. 提案手法

2.1 対象とする侵入

本研究ではスクリプト言語攻撃による管理者権限の奪取を検出の対象とする。

スクリプト言語攻撃とは、E-mailなどにより攻撃対象のマシンに悪意のあるスクリプトファイルを送り管理者権限を不正に取得する方法である。

例えば何らかの手段で送り込まれたスクリプトファイルが、管理者権限を持っていたユーザによって実行された場合、新たにユーザを作成し管理者権限を持たせるといった手順で不正が行われる。このスクリプト自体は、システムクラッシュを起こすといった、マシンに大きな変化をもたらすものではない。しかし、不正なユーザが作られることで、そのユーザを利用していつでもマシンにログインすることが可能となってしまうため、後々システムの破壊や、個人情報の漏洩といった脅威にさらされることになる。

このスクリプト言語攻撃の対象となるマシンは、主にクライアントである。サーバーに対しては、管理者が管理をしていたり、厳重なセキュリティ対策が施されていたりするが、クライアントにはそのような対策はあまり施されていないのが現状である、また、不特定多数の人間が使用することが予想されるが、その不特定多数の人間の中にはパソコンに対して無知な人も含まれる。管理者や知識のある人であれば開かないであろう危険なスクリプトでも、無知な人間にはそのファイルが危険であることがわからない為、それを開いてしまう可能性がある。そういったことから、本手法はクライアント側の立場で構築していく。

2.2 提案手法概要

WindowsNT系のOSではユーザ情報はレジストリ[6]と呼ばれる階層型データベースによって管理されている。

通常、スクリプト言語攻撃でユーザの不正な追加を行うと、このレジストリにユーザの情報が書き加えられることになる。そこで、このレジストリ以外にユーザ情報を管理するDBを用意することで、たとえ不正にレジストリの内容が書き換えられても、本来の正規の情報を持つそのDBとレジストリのユーザ情報を比較することで不正なユーザを検出するシステムを構築する。

2.3 開発環境

提案システムは以下の表1のような環境で開発を行った。

表1　開発環境

CPU	Intel PentiumIII Processor 1GHz
OS	Microsoft Windows2000 Professional Service Pack 2
開発言語	Microsoft Visual Basic 6.0 Service Pack 3

2.4 システム構成

提案システムは以下のコンポーネントから構成される(図1参照)。

・ ログインプログラム
　ユーザのログインの際にレジストリよ

りユーザ情報を調査する。

・ 比較プログラム
レジストリのユーザ情報とユーザ情報DB とを比較して正規のユーザかどうかを判定する。

・ ユーザ情報 DB
正規のユーザ情報を DB 化したもの。

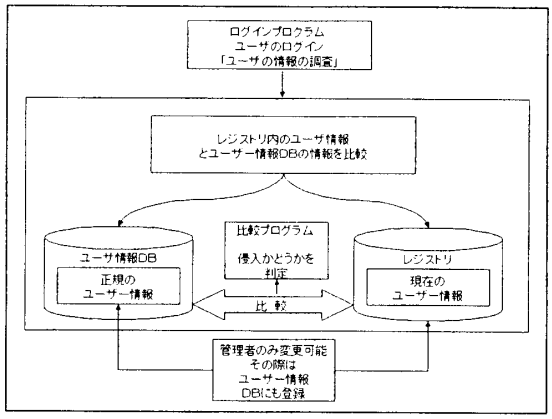

図 1. システム構成

2.5 提案システムの流れ

提案システムによる侵入検出の流れを以下に記述する（図 2 参照）。

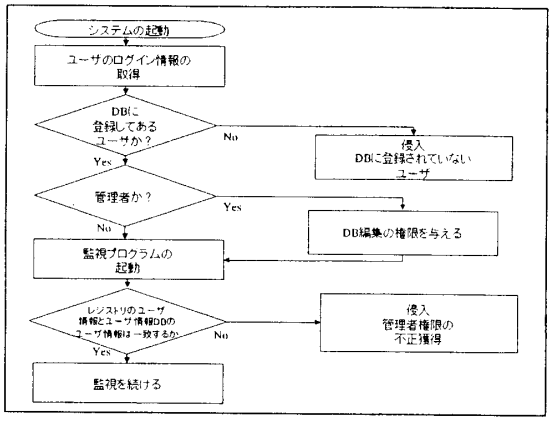

図 2. 提案システムの流れ

(1) ユーザがログインした際に、そのユーザの情報を調査して、ユーザ情報 DB のユーザ情報と比較して、正規のユーザでなければ警告する。
(2) ログインしたユーザが管理者かどうかを判断し、管理者であれば DB 編集の権限を与える。
(3) 監視プログラムを起動してリアルタイムの監視を開始する。
(4) レジストリのユーザ情報とユーザ情報 DB を比較し、一致しないユーザが存在する場合に警告し、不正なユーザを表示する。

3. 実験

3.1 検出実験

3.1.1 実験方法と結果

以上のような機能を持つシステムを試作し、この試作システムの侵入に対する検出能力の評価を行うために検出実験を行った。実験環境は表 1 の開発環境と同様である。実験はインターネット上で入手したスクリプトを使用して行った。このスクリプトは、管理者権限を持つアカウントでログインしている状態で実行されるとユーザ権限情報の不正追加と、新規ユーザの不正追加を行うものである。

スクリプトを実行した結果、不正ユーザを追加し、そのユーザでログインした際には不正なユーザであることを検出することはできたが、追加された瞬間を検出することは不可能であった。権限情報の変更についても同様に、不正変更されたユーザでログインした際には検出が可能であったが、変更された瞬間を検出することは不可能であった。

3.1.2 非検出に対する考察

試作システムの非検出の理由について検証を行った。レジストリに記載されている権限情報がどのように変更されるのかを調べるために、正規にユーザ権限の変更を行った。

まず、実験用マシンの管理者権限を所持しているユーザを使用し Guest ユーザのユーザ権限を変更した結果、この時点では変更した情報はレジストリに反映されていないことがわか

った。そこで、管理者権限を所持しているユーザをログアウトして再度同じユーザでログインしてみたが結果は同じだった。

次に、このユーザをログアウトさせ Guest ユーザ（権限情報の変更を行ったユーザ）でログインしたところ、この時点で変更した情報がレジストリに反映された。つまり、変更された情報がこの試作システムで使用したレジストリの情報取得部分に反映されるのは、変更されたユーザのログイン時である。そのため、常にこの箇所を監視していても、リアルタイムで検出できないことが判明した。そこで、リアルタイムに検出が行えるように試作システムを改良することにした。

3.1.3 再実験と結果

リアルタイムに監視を進めるにはレジストリの変更がいつ行われているか、また、どの箇所が変更されているかを調べる必要がある。そこで、レジストリをリアルタイムで監視するソフト「Regmon」[7]を使用し、変更されている部分を調査した。その結果、レジストリの SECURITY¥SAM 部が変更されていることがわかった。この箇所では Windows2000 のセキュリティ情報が含まれており、通常はユーザが変更することはできない部分である。そこで、SECURITY¥SAM 部のユーザ情報をチェックするようにし、監視プログラムに組み込んだ。

改善したシステムで、新規ユーザの不正追加をリアルタイムで検出できるかどうか再実験を行った。なお、実験に使用した侵入用スクリプト、実験環境は前実験と同じものである（表 1 参照）。再実験の結果、新ユーザの不正な追加をリアルタイムで検出することができた。

3.2 誤検出検証実験

3.2.1 実験方法と結果

提案システムに誤検出の恐れがないかどうかの検証を行った。検証方法は、監視プログラムを動作させている状態で、正規にユーザの追加・削除を行い検出されないことを確認する。しかし、ユーザを追加し、その後すぐに、ユーザ情報 DB の変更も行ったが、正規の方法でユーザの追加を行った直後、レジストリのユーザ情報の変更を検出してしまうため誤検出となってしまった。

ユーザの削除の実験においても、同様に誤検出となってしまった。

3.2.2 再実験と結果

この誤検出の原因は、正規に追加・削除されたユーザの情報がレジストリに反映されてから、ユーザ情報 DB を編集するまでのタイムラグによるものと考えられる。

対策としては以下の方法が考えられる。

(1) 監視プログラムを停止させた状態でユーザの追加・削除を行う。
(2) 正規のユーザ追加・削除と同時にユーザ情報 DB にも変更を加える。

(1)の方法では、監視プログラムの停止中に不正なユーザが追加された際には発見が遅れるため、(2)のような機能を持つプログラムを作成して提案システムに付加することにした（図 3 参照）。

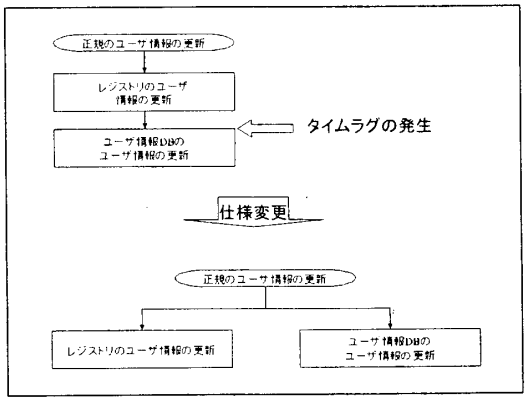

図 3. ユーザ情報変更方法

システム構成に以下のプログラムを付加する（図 4 参照）。

・ ユーザ追加・削除プログラム

ユーザ追加・削除のプログラムである。このプログラムを使用してユーザを追加・削除すると、その情報はレジストリとユーザ情報 DB の両方に反映される。

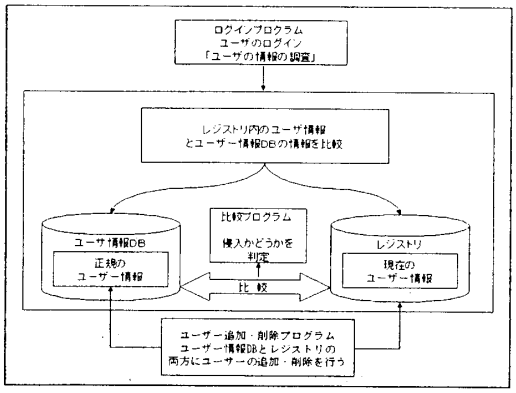

図 4. システム構成 ver. 2

前回の誤検出の検証実験と同様に監視プログラムを動作させ、新たに作成したプログラムを用いてユーザの追加・削除を行った結果、誤検出されることなく監視を続行することができた。

3.2.3 パフォーマンス実験と結果

提案システムの検出プログラムが起動した際と、検出を行うために OS に常駐させているときの CPU 使用率とメモリ使用量を調査した。実験環境は CPU が IntelMMXPentium233MHz、メモリが 64M のパソコンである。

その結果、CPU 使用率に関しては約 3%以下でほとんど変化が見られなかった。また、表 1 の開発環境においても同様に CPU 使用率を測定したところ、ほぼ 0%のままであった。

4. 考察

4.1 実験結果に対する考察

今回、一度非検出という結果に終わってしまったシステムを再度見直し、検出できるように改良できた。これは、プログラムにレジストリの SECURITY¥SAM 部という、通常は管理者でも操作することのできない部分を監視させることで、より正確なユーザ情報をリアルタイムに得ることができたからである。

また、誤検出に対する検証実験も行った。一度は、誤検出を起こしてしまったが、これは正規のユーザ追加の際に、レジストリとユーザ情報データベースに発生する、ユーザ情報の更新のタイムラグによるものであった。そこで、ユーザを追加する際に、レジストリとユーザ情報データベースに同時にユーザを追加する機能を提案システムに付加することで、タイムラグをなくし、誤検出をなくすことができた。

最後にパフォーマンス実験の結果より、提案システムはインストールしたマシンに対しての負荷がほとんどないことがわかった。

4.2 提案手法の有効性・実用性

本システムはスクリプト言語攻撃による管理者権限の奪取を検出することを念頭において設計した。管理者権限は通常は使用せずに、システムに対する変更等を行うときに使用するものである。しかし、実際にはそのような管理の煩わしさから、すべてのユーザが管理者権限でログインを行い、パソコンを使用するといった例も多く見られる。そのような状態でスクリプトを送り込まれた場合、簡単に管理者権限を奪われ、侵入を許してしまう為、危険な状態であると言える。現状ではこのような危険な例が多く見られる。スクリプト言語攻撃により、管理者権限を奪われてしまえば、システムに対するどのような変更も可能であるため、これを検出することができれば、早期対策の実現につながる。

また本システムは簡易的なものであるが、スクリプト言語攻撃による管理者権限の奪取の検出という高い効果を発揮できるものであるうえ、システムに対する負荷もほとんどない。

したがって、本手法の有効性・実用性は非常に高いといえる。

4.3 既存の侵入検出システムとの比較

既存の Windows 対応の代表的な侵入検出システムに、株式会社東陽テクニカの『Black ICE Defender』[8]、AirG 開発の『AirG_PC 監視』[9]といったものが挙げられる。

しかしこの二つとも本システムで検出が可能であった、スクリプト言語攻撃による管理者権限の奪取を検出することはできなかった。

また、侵入検出ソフトではないが、(株) シマンテックの『Norton Anti Virus 2002』というウイルス対策ソフトの機能の一つとして、スクリプトの遮断というものが存在する。これは、"アイ・ラブ・ユー"ウイルスや"アンナ・クルニコワ"ウイルスなどのスクリプトベースの脅威をウイルス定義による対応前の段階でも検出するという機能だが、本システムの評価実験に使用したスクリプトの実行を検出することは不可能であった。

つまり、既存システムでは検出・対処できなかったスクリプト言語攻撃による管理者権限の奪取を、本システムでは検出することができた。

5. まとめ

本検出システムはスクリプト言語攻撃による管理者権限の奪取を防ぐことを目的として構築されたものである。本研究ではクライアントを対象としたが、それはスクリプト言語攻撃によってねらわれるパソコンは、サーバー機よりも、一般に使われるクライアントであるためである。一般的に管理者はサーバーに対しての防御や不正アクセスの対策は施すものの、クライアントに対してまでは対策が行き届かず対策が手薄になりセキュリティが脆弱なままであることが多い。サーバーに対してどれだけセキュリティ対策を施しても、そのサーバーに対してのアクセス権限を保有しているクライアントの管理者権限が奪われてしまえば、サーバーに対しての脅威にもなりかねない。

そのため本研究では既存の Windows の侵入検出システムでは検出できなかったスクリプト言語攻撃による管理者権限の奪取を検出できるシステムを提案し、実験により有効性と効果を確認した。

しかし問題点として、既存のユーザの権限情報を操作された場合にはリアルタイムでの検出が不可能であることが挙げられる。今後の課題として、レジストリや Windows の権限情報の今まで以上の調査を行う必要があると考える。

参考文献

[1] 岩田雅士・山本智一・田中雅紀・阿部武彦・木村春彦:レジストリとユーザ情報データベースを用いた侵入検出システムの構築, 平成 14 年度電気関係学会北陸支部連合大会・講演論文集 F-5、p. 290

[2] "U. S. DOE-CIAC (Computer Incident Advisory Capability) Website", http://www.ciac.org/ciac/

[3] 村松英和:図解入門　よくわかるインターネットセキュリティと「安号」の仕組みがわかる本, pp. 118 - 119(2000)

[4] 片瀬和子, 中堅・中小企業の情報ネットワーク化の展望と課題, 電子情報通信学会 OFS 研究会(2000)

[5] "Port139", http://www.port139.co.jp/ntsec_script.htm

[6] Microsoft Corporation : Microsoft Windows 2000 Professional リソースキット　下, p. 878(2000)

[7] "Sysinternals Freeware - Information for Windows NT and Windows 2000 - Regmon", http://www.sysinternals.com/ntw2k/source/regmon.shtml

[8] "ネットワークセキュリティ (東陽テクニカ)", http://www.toyo.co.jp/security/

[9] "AirG 開発", http://www.blue.b-city.net/~gg99486/

[10] "シマンテック・ワールド・ワイド・ホームページ", http://www.symantec.com/region/jp/products/nav/index.html