平成１５年度　情報工学コース卒業研究報告要旨

石井 (克) 研究室	氏　　名	酒井　健一
卒業研究題目	SELinux を用いた安全なサーバ環境の構築	

背景・目的

近年、我々の生活環境はインターネットの普及と共に大きく変わりつつある。電子決済やチケット予約、通信販売、個人認証など多くのことがネットワーク上で済ませることができるようになった。だがその便利さの反面、個人情報などの機密データの流出や改ざん、システム破壊など、新たな問題も発生している。こうした状況から、セキュリティに関する意識は年々高まり、より強固なシステム構築の必要性が増加している。このため、現在、様々な企業・団体において従来よりも安全性を高めたシステムの開発が進められている。

本研究ではその中でも安全性評価の高い Security-Enhanced Linux（以下 SELinux と呼ぶ）について、従来の Linux と比較して安全性の検証を行った。

SELinux の特徴

従来の Linux は任意アクセス制御（ＤＡＣ）方式を採用している。ＤＡＣとは、リソースのパーミッション（所有者、グループ、その他のユーザ）に基づいて、アクセス制御を行う方式である。所有者が自由にパーミッションを変更でき、”任意 ”にアクセス制御が可能である。このため、侵入者に root 権限が奪われた場合、システム全体を乗っ取られてしまう。

これに対して、SELinux は強制アクセス制御（ＭＡＣ）方式を採用している。ＭＡＣとはセキュリティポリシーに基づいて、プロセスからリソースへのアクセスを制御する方式である。セキュリティポリシーは管理者のみが設定することができ、リソースへの全アクセスは ”強制 ”的に制御される。ＭＡＣは RBAC、ＴＥという二つの機能で実装されている。ＲＢＡＣはユーザに割り振られた役割（role）に基づいて、ユーザによるプロセス起動を制御する機能である。ＴＥはプロセス、リソースに割り振られたドメイン、タイプ・ラベルと、セキュリティポリシーに基づいて、プロセスからリソースへのアクセス、又は他のプロセスの起動を制御する機能である。これらの機能により、ユーザやプロセスの権限を最小限の範囲に限定することができる。このため、たとえ外部から侵入されて、あるプロセスを乗っ取られたとしても、権限の昇格は許されず、それ以上の被害の拡大を防ぐことができる。SELinux 導入の利点は攻撃耐性ではなく、攻撃を受けたときの被害の拡大の防止という点にある。

実験内容・結果

一般的に、ＯＳの安全性の検証は様々な要素を考慮しなければならないため、容易に行えることではない。本研究では、検証内容を重要ファイルへの不正アクセスの可否に限定し、実験を行った。実験方法としては脆弱性の報告されているプログラム（Webmin-0.92）を導入し、セキュリティホール検証用コードを用いて、/etc/passwd、/etc/shadow への不正アクセスを試みた。実験はＭＡＣを有効・無効にした場合の二つの条件について実施した。結果として、従来の Linux の条件（ＭＡＣ=無効）では、両ファイルへの読み込み・書き込みが行えた。SELinux の条件下（ＭＡＣ=有効）では、両ファイルへアクセスすることはできなかった。これはＴＥにより、Webmin への権限が限定されており、ファイルへのアクセス権がなかったからである。たとえセキュリティホールの存在するプログラムであっても、ＭＡＣにより重要ファイルへのアクセスが制限されているということが確認できる。このことから、SELinux は重要ファイルへの不正アクセスを防止するという点では、従来の Linux よりもセキュアな OS であることが検証できた。

今後の展望

SELinux はプロセス単位の緻密なアクセス制御を行える半面、セキュリティポリシーの設定が非常に煩雑である。今回立ち上げた Apache サーバには約 500 行の設定ファイルが必要であった。複雑なポリシー設定は管理者の負担となるだけでなく、設定ミスによる権限の過剰付与も誘発しかねない。今度の課題として、管理者の負担を減らせるようなセキュリティポリシー設定ツールの開発が急務であると思われる。

また、SELinux は攻撃された時の被害の拡大を抑えることはできるが、攻撃そのものに対する耐性があるわけではない。このため、バッファオーバーフロー攻撃やＤｏＳ攻撃には個別に対策を取る必要がある。また、管理者のログイン名とパスワードを盗まれると、セキュリティポリシーを変更され、不正なアクセスを許可される可能性がある。この点に関しては、今後改善の余地がある。