プライバシー保護を実現するオペレーティングシステム

コンパイラと OS の連携によるデータフロー間伝播解析

研究技術の背景

近年、社会問題化している情報漏洩の多くは、管理ミス、誤操作、盗難・紛失といった正当なアクセス権限を持つユーザーの人為的ミスが要因となっています。これらの情報漏洩は、暗号化や認証などの外部からの攻撃を防ぐことを目的としたセキュリティ技術で防ぐことは難しく、また、Windows や SE Linux 等に実装されるアクセス制御機構では、操作主体プロセスから操作対象（データ）に対するアクセス自体を制限するため、情報漏洩防止の目的からすると、データの機密性を意識されておらず、制限が厳しくなりすぎ利便性が損なわれます。本技術は、「データの読み込みは許可するが、それを外部に出力することは禁止する」といった、従来実現できなかったアクセス制御を実現するものです。

研究技術の実用化への開発 OS（*DF-Salvia*）

情報漏洩の防止を目的としたアクセス制御機構を備えるセキュア OS の *DF-Salvia* では保護対象ファイル（以下、保護ファイル）ごとに、データ所有者の意図する保護方針をデータ保護ポリシ（以下、ポリシ）として設定できます。ポリシでは、ユーザー ID、時刻、計算機の位置、送信先計算機の IP アドレスなどのプロセスや計算機の状況を示すコンテキストを使用することで、「保護データへのアクセスは許可するが、USB メモリへのコピーは禁止する」、「ネットワーク上への送信は禁止する」といった設定を可能としています。そして、OS が、プロセスの動作を監視し、保護データの格納元である保護ファイルに設定されたポリシに従って、プロセスによる保護データの外部への書き出しを制御します。

アクセス制御手順

DF-Salvia では、以下の手順によりアクセス制御を行います。

1. プロセス実行前にコンパイラによって静的に解析し、データフロー情報を生成。
2. *read* システムコールが発行された時、読み込み対象が保護ファイルなら、どのデータフローへデータが読み込まれるか判定し、保護ファイルのポリシを適用。
3. *write* システムコールが発行された時、書き出されるデータが属するデータフローに対して、適用されたポリシの有無を確認。
4. ポリシが適用されている場合は、そのポリシに従ってシステムコールの実行の可否を判断。

上記の処理を行うためには、手順２、３において、システムコールが発行された時点で使用されているデータが属するデータフローを OS が特定できなければなりません。

毛利研究室グループ研究紹介から

・情報漏洩事件　―発生件数 :1,551 件
　　―個人情報 :628 万人
・情報漏洩を起こしてしまうと
　　―社会的信用の失墜
　　―損害賠償責任
・一般的なセキュリティ対策が必要に
　　―セキュリティ教育の強化
　　―暗号化、認証などのセキュリティ技術の導入
・情報漏洩の要因ベスト 3
　　―1 位 : 誤操作
　　―2 位 : 管理ミス
　　―3 位 : 紛失・置き忘れ
・情報漏洩への対策も必要に
　セキュリティ教育による対策
　　―気を付けても人為的ミスの発生
　セキュリティ技術の導入による対策
　　―外部からの攻撃や不正アクセスに効果的
　　―認証後や復号後は、自由に操作が可能となって人為的ミスには効果があります。

研究者

立命館大学
情報理工学部 情報システム学科

准教授　毛利　公一

研究テーマ

・Multi-core/Virtualization Technology を用いた適応型 OS/Hypervisor
・リアルタイム OS のための毛利仮想計算機モニタ
・プライバシー保護を実現するオペレーティングシステム
・仮想化技術を用いたマルウェア解析
・適応型ワイヤレス指向オペレーティングシステム

問い合せ先　立命館大学リサーチオフィス(BKC)
〒525-8577 滋賀県草津市野路東1-1-1
TEL:077-561-2802　FAX:077-561-2811　Email:liaisonb@st.ritsumei.ac.jp