Activity Report 04

Project Theme　暮らしを支える安全・安心のインビジブル・セキュア・プラットフォーム

情報漏洩を防ぐ強力・柔軟なオペレーティング　システム

ソフトウェアのライフサイクル全体で一貫したセキュリティのプラットフォームの形成を目指しています。

一見してコンピュータが活用されているとわかるところから、私たちの目には見えない（インビジブル）部分まで、現代社会はあらゆるところに情報技術が浸透し、世界中がネットワークでつながっています。この現実は非常に便利な一方で、情報漏洩やウィルス・ワームの感染などによって、暮らしや種々の活動が脅かされる危険をはらんでいます。こうした脅威を払拭し、ネットワーク社会で安全・安心に暮らすためにソフトウェアの安全性の向上を目指すのが、私たちのプロジェクトです。

本プロジェクトでは、ソフトウェアのライフサイクル全体を横断的に捉え、ソフトウェアの開発から生成、実行まですべての段階において確固としたセキュリティを持つ一貫したプラットフォーム（基盤）を形成しようとしています。そのために個別に扱われることの多いオペレーティングシステム（OS）、コンパイラ、ソフトウェア各々を連携・協調させることは、他にはない新しい試みです。

「誰が」ではなく、「何を」に着目してデータ漏洩を防ぐOSを開発しました。

すでに私たちは、情報漏洩の発生を動的に検出するための仕組みを考え、Linuxをベースとして開発したOS（Salviaと命名）でこの仕組みを実現することに成功しています。

近年頻発している情報流出事件の原因の多くは、実は外部からの侵入ではなく、誤操作や管理ミス、紛失といった正当なアクセス権限を持つユーザによるものなのです。こうしたデータの漏洩を暗号化や認証といったセキュリティ技術で防ぐことは困難です。そこで私たちは、「誰が」ではなく、プロセスが「何をしようとしているか」という点に着目してデータ漏洩を防ぐSalviaを開発しました。

Salviaでは、まずデータ提供者があらかじめ保護方針をデータ保護ポリシ（ポリシ）として定義し、それを保護対象のファイル（保護ファイル）と組にして管理します。このポリシに基づいて、保護ファイルのデータ(保護データ)を読み込んだプロセスにアクセス制御を課すことで、データを保護します。つまり保護データを読み込んだプロセスはSalviaの監視対象となり、USBメモリへの書込みやネットワーク上への送信といった、ポリシに違反するようなアクセスが行われた時は、データ漏洩が発生する可能性があると判断してアクセスを拒否するのです。

コンパイラと協調させ、データフロー単位でデータの流れを管理することに成功しました。

最新の成果として、私たちはSalviaのアクセス制御の粒度をさらに細かくしたDF-Salviaを開発しました。

Salviaの問題点の一つは、過剰にアクセスを制限してしまう可能性があることでした。プロセスを監視対象とした場合、過去に読み込まれた全保護ファイルが監視過程に含まれるため、一旦保護データを読み込むプロセスを経ると、その後の過程で保護データが含まれないファイルを書き込むことなども拒否されるという事態が発生してしまうのです。

そこで私たちは、コンパイラと協調させることでプロセスをさらに細かく分割し、より小さいデータフロー単位で管理・制御できるようにしました。コンパイラとは、プログラミング言語で記述されたソフトウェアの設計図（ソースコード）をコンピュータが実現できる形式（実行コード）に変換するソフトウェアです。この変換時、一般的に、コンパイラは実行コードを速く、より小さいサイズにする最適化を行います。最適化のためには、プログラム中でデータが変数間をどう伝播するかといった変数定義の流れ、すなわちデータフローを把握する必要があり、私たちはこのデータフロー解析の技術を利用し、データフローごとにポリシを管理できるようにしました。

DF-Salviaが実際にアクセスを制御できるかどうかを実験した結果、正確にデータフローを識別してデータフロー単位でのアクセス制御を行い、過剰なアクセス制限も発生しないことを確かめました。これによって「監視すべき」データフローと「監視不要」のデータフローを明確に区分して管理できるようになり、セキュリティ向上とアクセスの柔軟性の両方を達成できました。

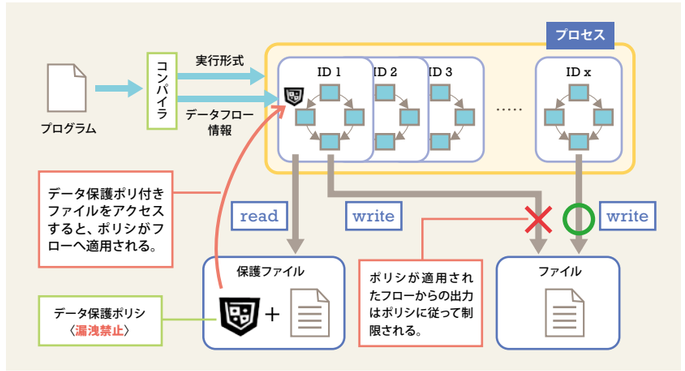
多様なセキュリティ管理を実現する可能性が広がっています。

さらなる課題は、コンパイラによるデータフローグラフの自動再生です。今回のプロトタイプではデータフローグラフを人的に生成し、コンパイラに与えて実験しました。現在は、動的な情報漏洩検出に必要なデータフローグラフをソースプログラムからコンパイラが自動生成する研究を進めています。

DF-Salviaの強みは、Linuxという既存のOS内に実装できる上、C言語を対象としたソースコードの解析を可能にする点です。実現すれば、既存のソフトウェア資産を含め、あらゆるソフトウェアシステムに適応できます。企業の顧客情報などの多様なデータベースの管理、Webやメールの管理など、非常に広範、かつ重要な分野で情報セキュリティの大きな力となるに違いありません。

毛利公一 准教授
Koichi Mouri

情報漏洩を防止するDF-Salvia



（注1）**ウィルス・ワーム** …「ウィルス」とは、コンピュータに感染して破壊活動を行ったりトラブルを引き起こしたりするプログラムのことで、通常、感染経路としてネットワークやフロッピーディスク、CD-ROMなどを通じてシステム内に侵入する。ネットワークを使って自己増殖するものは特に「ワーム」と呼ばれる。

（注1）**USB** … Universal Serial Bus。キーボードやマウス、モデム、ジョイスティックなどの周辺機器とパソコンを結ぶデータ伝送路の規格のひとつ。

●参考文献／**1** プライバシアウェアOS Salviaにおける共有メモリアクセス制御手法 情報処理学会論文誌、情報処理学会、Vol. 50、No. 9、1984-1996（2009） **2** Privacy-aware OS Salviaにおけるデータフローを主体としたアクセス制御手法 第71回全国大会講演論文集、情報処理学会、Vol. 3、353-354（2009） **3** リムーバブルメディアを経由した情報漏洩を防止する手法 コンピュータセキュリティシンポジウム2008（CSS2008）論文集、情報処理学会、Vol. 2008、No. 8、211-216（2008）

●連絡先／立命館大学 びわこ・くさつキャンパス（BKC）毛利研究室　電話：（外線）077-561-5061　HP：http://www.asl.cs.ritsumei.ac.jp/