クライアントおよびサーバ双方からの情報漏えいを防止するアクセス制御技術の研究開発
(111603011)

Access Control to prevent information leakage from both client and server

研究代表者
須崎　有康　独立行政法人産業技術総合研究所
Kuniyasu Suzaki　National Institute of Advanced Industrial Science and Technology

研究分担者
古原　和邦 †　川出　智幸 ††　井上　宜子 ††
Kazukuni Kobara†　Tomoyuki Kawade††　Nobuko Inoue††
†独立行政法人産業技術総合研究所　††サイエンスパーク株式会社
†National Institute of Advanced Industrial Science and Technology　††Science Park, Inc.

研究期間　平成 23 年度～平成 25 年度

概要
情報漏えいはネットワークの盗聴ばかりでなく、プロバイダ管理者からの覗き見／持ち出しや利用者のクライアント端末を経由したものが少なくない。一旦漏えいが起こるとファイルが暗号化されていたとしてもパスワードのオフライン全数探索が可能となったり、リバースエンジニアリングによって解読される危険性がある。また、漏えいはクライアント端末経由からの不用意な印刷や画面のカットアンドペーストからも起こる。これらを解決するためにインターネットで公開するファイルが手元のクライアントから漏えいせず、且つサーバからも漏えいさせないアクセス制御技術を開発した。

１．まえがき

近年の情報漏えいはネットワークの暗号化が普及したことにより、ネットワーク自体からの盗聴は少ない。むしろ正当なアクセス権を有するプロバイダ管理者からの覗き見や利用者のクライアント端末からが多くなっている。一旦漏えいが起こるとファイルが暗号化されていたとしてもパスワードのオフライン全数探索が可能となる。また、リバースエンジニアリングによって思わぬ脆弱性が見つかり、解読される危険性もある。また、情報漏えいは紙媒体からも多く、不用意な印刷を抑制する必要もある。画面のカットアンドペーストによる持ち出しも防がなければならない。このため近年普及しているネットワークストレージでは、機密情報を含んだファイルが外部に漏れることを防止するアクセス制御や鍵管理などの対策を総合的に施す必要がある。

これらの問題を解決するためにインターネットで公開するファイルはピースに分割・暗号化されてサーバ上での覗き見を防ぐ技術を開発する。分割・暗号化されたファイルはクライアントの仮想ストレージでのみで復号される。仮想ストレージはアクセス制御が施され、アプリケーションからファイルを開くことはできるが、アプリケーションからファイルがコピー、印刷、カットアンドペーストは出来ない。さらにアクセス制御で使う暗号鍵が漏えいした場合に無効化できる技術やアクセス制御のドライバが管理する情報を守るハイパーバイザーを作成することで被害を最小限に抑える堅牢なシステムとする。

２．研究開発内容及び成果

上記の目的のために、具体的な研究課題は以下の３つに分けて、開発を行った。

課題 A) ファイルがサーバから漏えいしない技術
課題 B) ファイルがクライアント端末からコピーされない技術
課題 C) ドライバへの攻撃検出および鍵の無効化による高信頼クライアント技術

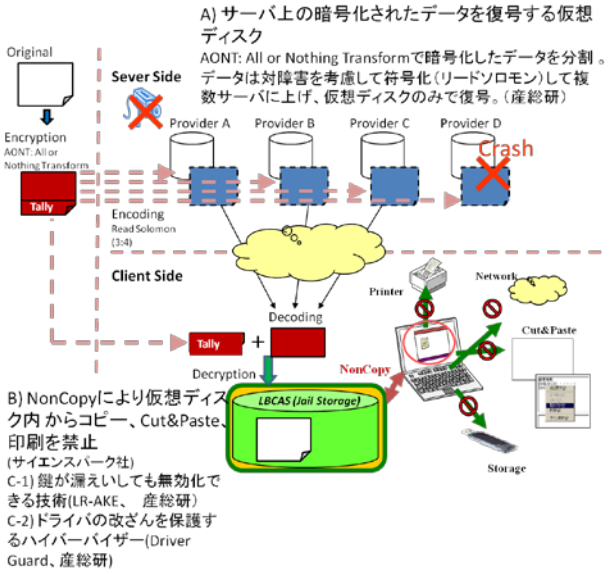

図１　開発したシステムの全体図

課題 A)の成果としては、符号冗長化技術(AONT: All or Nothing Transform 暗号と Split Tally 割符)と分散配信技術(Reed-Solomon 符号化)を組み合わせたネットワークストレージシステム LBCAS: LoopBack Contests addressable Storage を開発した。AONT はワンタイムパッド暗号の一種であり、全暗号データを集めない限り、元のデータに戻すことができない。これに割符(Split Tally)技術を適用することにより、サーバにアップロードするデータとユーザのクライアントマシンにセキュアに保存する割符に分けることで、攻撃者がサーバにアップロードしたデータを全て集めても全内容を解読できない。データは割り符があるクライアント上の LBCAS の仮想ストレージ上のみで復号される。仮想ストレージへのアクセスは課題 B) で開発される NonCopy により制限することで情報漏えいを防いでいる。LBCAS の実装は Windows 7 と Linux に対応する２つのバージョンを作成した。

Windows7 版では Callback File System(CBFS)を使い、Linux では FUSE(File system in USEr space)を使った実装した。また、LBCAS は各種の最適化技術を組み合わせることで、40MB/s 程度の性能が達成できた。この性能はセキュリティ機能有するとして実用範囲である。

課題 B)の成果としては、LBCAS の仮想ディスクからファイルがアプリケーションから開くことができるが、印刷や画面コピーなどを禁止する NonCopy の技術を開発した(図 2)。NonCopy はアクセス制御対象のストレージにアクセスしたプロセスを管理下に置き、そのプロセスから実行されるファイルのコピー、印刷、カットアンドペーストなどの API を抑制する（図中の①)。アクセス対象のストレージ以外にプロセスが書き込み要求を出した場合、その要求はフィルタドライバでフックされ（図中の②)、書き込み要求が抑制される。ただし、アクセス対象のプロセスも元のストレージ対してはアクセス制御されずにファイルの更新が可能となっている。ネットワークへの通信もフィルタドライバで抑制され（図中の③)、ネットワーク越しに情報が漏えいすることを抑制している。アクセス対象のプロセスからの印刷はプロセスが使う DLL ライブラリを置き換えることで抑制される（図中の④)。カットアンドペーストにはついては Windows のグローバルフックの機能を活用して、アクセス対象のプロセスが GUI の Clipboard にデータを保存し、他のプロセスに切り替えた場合に Clipboard 上のデータを消すことでアクセス制御を実現している。

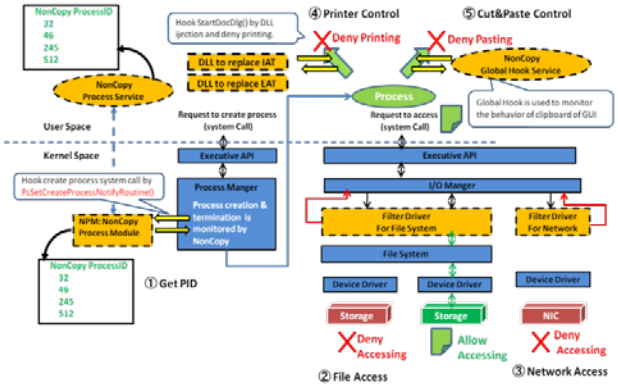

図 2　NonCopy によるアクセス制御の実装詳細

課題 C-1)の成果としては、NonCopy ドライバのメモリを守るハイパーバイザーDriverGuard の開発を行った。DriverGuard はオープンソースの BitVisor に監視機能を付加したものである。VM Introspection の機能により、Windows7 の動作を監視し、デバイスドライバーのコードおよび重要データに不正なアクセスが起こった場合は、そのアクセスをフックして、ユーザに警告する。

課題 C-2)の成果としては、鍵が漏えいしても無効化が出来る技術 LR-AKE(Leakage-Resilient Authenticated Key Exchange)を活用してユーザが異なる場合に LBCAS 上のデータの再利用を禁止した。LR-AKE は鍵そのものを分散管理する事で運用管理者を含む攻撃者からの漏洩を防ぐ事ができる技術、およびファイルの暗号化で利用者の成りすましや保存データの漏えいを防止するシステムである。暗号化したデータを LBCAS および NonCopy で公開した場合にユーザ毎の識別ができ、ユーザに鍵自体を見せずにデータの復号が出来るようにした。LR-AKE の鍵管理は NonCopy によるアクセス制御内で行われるため、ユーザも LR-AKE の鍵を直接触ることが出来ない。また、あるユーザが他人に鍵を渡すことができずに使い回しされることがない。

個々の要素技術の全てを統合することで、サーバおよびクライアントが情報漏えいしない技術をハイ発ができた。

３．今後の研究開発成果の展開及び波及効果創出への取り組み

本課題について関心を持たれたホスティングサービス企業（ドリームアーツ沖縄と北海道総合通信網株式会社）があり、開発技術の応用を検討している。両者は日本の両端に位置して、災害にデータのバックアップやサーバの代替えなどできるインフラを考えている。

既に両社のホスティングサービスを使った実験的なシステムは作成しており、フィージビリティスタディを通して技術展開を行う。フィージビリティスタディ先としては、大分県立短期工科大学校を想定している。ここでは、開発したストレージシステムを改良して課題提出で使われる。このシステムでは教師が課題ファイルをクラウドストレージに保存すると自動的に暗号化される。生徒は個々のシステムを通して課題ファイルを復号することが出来るが、ファイル自体をコピーしたりカットアンドペーストしたりすることはできない。生徒は任意のアプリケーションで課題ファイルに回答を書き込み、教師に提出することができるのみである。これにより、教師と生徒は 1 対多の関係でファイルのやり取りを安全に行うシステム上で、課題ファイルおよび生徒の回答の情報漏えいを防止できることを確認する。

４．むすび

クライアントおよびサーバ双方からの情報漏えいを防止するアクセス制御技術は産総研の持つインターネット仮想ディスク LBCAS と鍵管理技術 LR-AKE、サイエンスパーク株式会社の持つ NonCopy を改良し、有機的に組み合わせることで実現できた。今後は大分県で予定しているフィージビリティスタディを通して実際の活用に向けた展開を行う予定である。

【誌上発表リスト】

[1] K.Suzaki、T.Yagi、K.Kobara and T.Ishiyama, “Kernel Memory Protection by an Insertable Hypervisor which has VM Introspection and Stealth Breakpoints”、Springer Lecture Notes Computer Science,、Vol.8639 pp48-6（2014 年 8 月 27 日）

[2] 須崎有康、八木豊志樹、古原和邦、石山智祥、村上純一、鵜飼裕司、“BitVisor をベースとした既存 Windows のドライバメモリ保護”、情報処理学会 BitVisor Summit（東京都文京区）（2012 年 12 月 4 日）

[3] 須崎有康、古原和邦、井上宜子、川出智幸、小路幸市郎、村上純一、鵜飼裕司、“クライアントおよびサーバ双方からの情報漏えいを防止するアクセス制御技術の研究開発”、暗号と情報セキュリティシンポジウム SCIS2012（金沢市）（2012 年 2 月 2 日）

【国際標準提案リスト】

[1] IETF 、Internet-Draft 、"Augmented Password-Authenticated Key Exchange for Transport Layer Security (TLS)" 、(2013 年 09 月)

【受賞リスト】

[1] 古原和邦、第 25 回中小企業優秀新技術産学官連携特別賞、"情報漏洩に強い２要素認証 ＬＲ−ＡＫＥ"、(2013 年 4 月 8 日)