自己消去を可能にする HDD 認証強化

二村 和明† 矢崎 孝一† 中村 洋介† 郭 兆功† 山田 勇†

†(株)富士通研究所
郵便211－8588 川崎市中原区上小田中4－1－1
E-mail: {kazuaki.nimura, yasaki.kouichi, nkmr, guo.zhaogong, yamada.isamu}@jp.fujitsu.com

あらまし ハードディスク(HDD/SSD)のデータアクセスを保護する認証機構としてはパスワードが用いられる。また、PC のプリブート認証において生体認証など高度なユーザ認証を行う場合には、認証結果が正しければ PC に予め記憶しておいた正しい HDD パスワードを HDD に送り込み、認証結果が正しくなければ PC や HDD を使用させない仕組みが用意されることが多い。しかし HDD を抜き取られると、高度な認証は機能しない。本稿では HDD 単独で動作する認証強化方式について業界標準の TCG HDD を利用した方式を提案する。

Enhancement of hard drive authentication that enables self-wipe

Kazuaki NIMURA† Kouichi YASAKI† Yousuke NAKAMURA† Zhaogong GUO†
Isamu Yamada†

†Fujitsu Laboratories Ltd.
Kamikodanaka 4-1-1, Nakahara, Kawasaki, Kanagawa 211-8588 Japan
E-mail: {kazuaki.nimura, yasaki.kouichi, nkmr, guo.zhaogong, yamada.isamu}@jp.fujitsu.com

Abstract It is fairly common to link a password for hard drive and result of PC user authentication like user password or fingerprint authentication. When the user authentication pass, PC set the password for hard drive which has stored in PC to hard drive, or when it fail, the hard drive and/or PC cannot be used. However if a hard drive removed from PC, because there is no link with user authentication anymore, and because hard drive authentication uses password protection, it will be only protected by the password for hard drive after all. In this paper, to solve the problem, we introduce an enhanced authentication method for hard drive or solid state drive which works by itself.

1. はじめに

PC 盗難・紛失に対する情報漏洩の基本的な防止策として、データの暗号化、暗号鍵の保護、ユーザ認証が行われている。

データの暗号化では、ソフトウエアによるファイル・フォルダの暗号化、ディスク全体の暗号化や、ハードウエアによってディスク全体を暗号化するFDE(Full Disk Encryption)対応 HDD(Hard Disk Drive)/SSD(Solid State Drive)が利用されている。また、データ暗号化に使用する暗号鍵を保護するために、TPM(Trusted Platform Module)など耐タンパー性を持つハードウエアが用いられている。データと異なるデバイス上で鍵を管理することで、ハードディスクを抜いて別 PC でアクセスしようとしても、ディスク上に暗号鍵のヒントがなく、解読を困難にすることができる。

ユーザ認証では、パスワードだけでなく、生体認証や IC カードなどが用いられている。これは PC 起動時、OS 起動時に実行され、PC 起動/OS 起動の実行権がユーザにあるのかどうかを確認し不正ユーザを排除している。前者 PC 起動時におけるユーザ認証では、その認証結果が BIOS(Basic Input Output System)パスワード、HDD パスワードとリンクして用いられている場合が多い。すなわち、ユーザ認証の結果が正しい場合には、PC 側に予め記憶しておいた HDD パスワードを HDD に設定し、認証結果が正しくない場合には、HDD パスワードの設定は行わない仕組みである。

これらの防止策の組み合わせによって、PC 盗難・紛失時においても、情報漏えいが防止される。しかし上記防止策のユーザ認証機構は、PC 側にその殆どの部分が組み込まれているため、HDD を PC から抜き取ると機能しなくなる。抜き取られた HDD はパスワードが漏洩すると解析可能となる。

本稿では、HDDが抜き取られた状態でも高度な認証機構が働き、積極的に情報漏洩を防ぐ対策を、TCG (Trusted Computing Group)が策定した業界標準の HDD が備える機能を利用して実現することを提案する。また、実装後の動作結果についても報告する。

2. 課題と対策の検討

通常の場合、抜き取られた HDD は HDD パスワードとデータ暗号化によってのみ守られた状態となる。パスワードが漏洩すると、他のPCに接続されてHDDが解析されることもある。これを防ぐため、「どのPCに接続しても、そのホスト PC の危険度を判定し、自動消去などの情報漏えい対策機構が動作するよう、HDD に認証機構を内蔵する」。ここでいう”PC の危険度”とは、許可されていない PC、不正ユーザが操作する PC(何回もパスワード攻撃を行うPC)を指している。

上記対策を実現するために必要な構成要素を抽出すると、

- どの PC に接続しても、情報漏えい対策機構が動作する (Always works)
- 危険度の判定結果後、情報漏えいが発生し得ないよう自動消去を行う (Measure risks & execute)

となる。これら特性項目に対する具体的な実現方法について、以下で検討を行う。

2-1. Always works

どの PC に接続しても、情報漏えい対策機構(対策プログラム)が動作するためには、その接続形態に依存せず、対策機能(対策プログラム)が実行可能なように配置される必要がある。HDD の接続形態には以下の2種類がある。

(1) ブートデバイス

(2) 2nd HDD としての接続 (e-SATA/USB など)

(1)の利用形態においては、MBR(Master Boot Reccord)領域から始まり、OS が立ち上がるまでの起動パスのどこかに対策プログラムを実行するタイミングを設けることで実現できる。(2)の利用形態においては、一部の USB メモリで既に行われているパスワード認証を通過した後に記憶領

域にアクセス可能にする方式を適用することが考えられる。即ち、まず対策プログラムが置かれた領域だけをPC側に見せ、その他の領域はPC側から隠蔽し、対策プログラムの認証結果に応じて見せる/消去する。(1),(2)両方の形態で、対策プログラムが働くための HDD 構成としては、

i) 1 つのパーティションを暗号化せず、そのパーティション上に対策プログラムを実装する構成
ii) 上述のように、認証結果に応じて、データが入ったディスク内容の見せる/隠す機構があるデバイスを利用して実装する構成

がある。本稿の実装では、ii)の方法での一例を実現した。

2-2. Measure risks & execute

接続するPCの危険度の高さは、

- 対策プログラムが実行するユーザ認証の失敗回数
- 対策プログラムが記憶している機器 ID と一致するかどうか

で判定する。

PC の危険度が高い場合には、消去を実行する。消去は、NIST(National Institute of Standards and Technology)で定められている上書き消去を実行する前に、短時間で実行が完了する暗号鍵消去を実行し、情報漏えいを防ぐ。消去する暗号鍵は、解析の難しさという観点から暗号鍵の再設定を行うことができないハードウェアベースのものが最適である。

3. 対策の実装

以下では、TCG によって策定された HDD 仕様によって、前述した対策が実現できることを示す。また、実装に際して使用した EFI(Extensible Firmware Interface)に関して、その概要を示す。そして実装の動作・フローについて説明を行う。

3-1. TCG HDD

本稿で略記する TCG HDD とは、国際標準化団体 TCG にて策定されたストレージセキュリティの仕様である TCG Storage Architecture Core Specification[1] と Opal SSC(Opal Security Subsystem Class)[2]に準拠した HDD/SSD を指している。

以下では、認証、暗号化、および消去に関して、従来技術と比較しながら TCG HDD が提供する機能についてまとめる。

これまでの認証では、ATA Security feature set で規定された Master/User の2種類の HDD パスワードを用いて行われてきた。TCG HDD による認証では、同じく ATA で規定した Trusted Computing feature set の中の Trusted Send/Receive コマンドを利用して[3]、複数のパスワードを用いて行うことが可能となる (Admin1～4/User1～8 のパスワード設定が可能)[1]。従来との機能的な違いは、パスワード入力回数に制限を設ける試行リミット(Authentication Attempt Limits with C_PIN Objects)[1]を有している点である。これは予め指定されたパスワード試行の失敗上限回数を超えると、それ以降のパスワード試行は必ず失敗と見なす仕様となっている。上限回数に達するまでの認証失敗は、電源が切られたらクリアする方法と、電源が切られてたとしても累積カウントする方法が選択できるようになっている。

暗号化に関しては、ディスク全体暗号(FDE)だけでなく、部分暗号(LBA 値によって指定した領域毎に暗号鍵を設定する)機能を備えている。

消去に関しては、ATA security Feature Set に Enhanced Secure Erase/Secure Erase コマンドが規定されている。これにより、HDD の上書き消去、FDE 対応 HDD の暗号鍵の消去を行うことができる。TCG HDD では、Trusted Send/Recive コマンドである genkey コマンドによって暗号鍵の再生成が実行される。

3-1-1. MBR shadowing と PBA

“Always works”に関連する、TCG HDD の特徴的な機能として MBR(Master Boot Record) shadowing と、PBA(pre boot authentication)用に用意された PBA 領域がある。PBA 領域は、通常の OS やアプリをインストールするユーザ領域とは別に用意された HDD 領域(図 1 のイメージ 1 のことを指している。PBA 領域は、認証されたユーザのみが書き込み可能であり、それ以外のユーザは read only という属性を持つ。PBA 領域に対策プログラムを組み込むことで、パスワード認証、生体認証、IC カード認証といった高度なユーザ認証が可能になる。PBA 領域とユーザ領域は動的に切り替えられ、認証結果が正しかった場合に TCG HDD に切り替えを指示することによって、ユーザ領域イメージにアクセスできるようになる。この切替を行うのが、MBR shodowing 機能である。MBR shadowing 機能が一度 Enable されると、電源の投入時には、PBA 領域のみが見えるように機能し、ユーザ領域を隠蔽するモードがデフォルト設定になる。そのため、PC 起動時には PBA 領域に記録された OS ブート・対策プログラムが必ず実行されることになる。

消去に関しては、鍵の再生成を瞬時に行うことで実現される[4]。暗号鍵は TCG HDD 内で自動生成されるものであり、外部から設定するインタフェースを持たない。また、PBA 領域は消去命令が発行された場合であっても影響を受けず、PBA 領域のイメージをそのまま残すことができる。

また、TCG HDD は Trusted Send/Receive コマンドのみでアクセス可能な 1KB 以上のデータストレージ(DataStore)を持っている。Datastore は、認証のリファレンス値、ログなど、PBA で利用する重要なデータを格納するために用意された格納領域である。

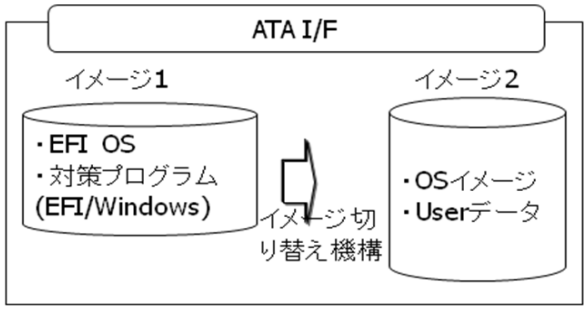

図 1. TCG HDD

3-2. EFI

TCG HDD にてプリブート認証を行うためには、PBA 領域への OS 搭載が必要となる。この OS 選択は任意に行うことができるが、本稿では以下のような好ましい特徴を備える EFI(Extensible Firmware Interface)を利用することにした。

- EFI は、BIOS に変わるファームウエアとして利用されており[5]、既存のプリブート認証との連携がとり易い。
- 開発環境が、無償でオープンソースとして提供されている[6]
- EFI では、EFI Platform Initialization 上で HDD Driver や表示系 Driver といった様々なデバイスを司る EFI Drivers を動作させる仕組みが標準で備わっており、またドライバも Linux 系ドライバを流用できることから、新しいデバイスへの対応が容易 (図 2)。
- OS を CALL する前に EFI アプリを動作させる仕組みや、再起動せずに、EFI をサポートした OS だけでなく、通常の OS を呼び出す Legacy ブートをサポートしている。

3-3. 実装の構成

対策プログラムを配置している場所は図 1 の通りである。TCG HDD がもつイメージ切替機構を利用し、イメージ 1 を FAT32 でフォーマットして、EFI OS 環境、EFI 用対策プログラム、Windows

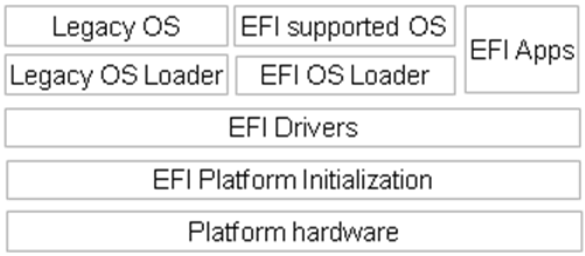

図 2. EFI のレイヤ

用対策プログラムを配置している。TCG HDD がブートデバイスとして接続されたときには、EFI OS/EFI 上で動作する対策プログラムが実行され、2nd HDD として接続されたときには、Windows 版対策プログラムが実行される仕組みである。

また、TCG HDD を以下のように構成する。

- TCG HDD のイメージ切り替えを行うレジスタ(MBR_DONE)への制御権を User1,User2 に付与する。
- User1 のパスワード = hash(機器 ID)
- User2 のパスワード = hash(ユーザパスワード)

ここで機器 ID としては、PC の不揮発性記憶領域 (NVRAM) に保存されている BIOS UUID(Universally Unique Identifier)など、その PC へのアクセス権がないユーザが入手できない固有の ID を利用する。機器 ID を登録済の PC を”登録 PC”、登録していない PC を”登録外 PC”と呼ぶこととする。登録 PC が複数ある場合には、User3～User8 以降のパスワードとして登録し、その UserX に対して MBR_DONE へのアクセス権を付与する。対策プログラムは、機器情報の収集や、ユーザパスワード入力画面を出し、収集した情報を用いて TCG HDD に対してパスワード認証を試みる、その結果、登録外 PC であったり、不正ユーザによるパスワード攻撃だと判定すれば、ユーザ領域の暗号鍵消去を実行する。また、TCG HDD を PC に接続したときの構成を図 3 に示している。PBA 領域の設定は、PC 出荷前や OS インストール前に行う必要がなく、その必要性が生じたときに、ユーザ領域の OS が稼働している状態で設定を行うことができる。そして再起動することで、認証機構が HDD 内で有効となる。

PBA 領域からユーザ領域へのイメージ切替では、EFI の legacy OS loader, BIOS の Int13 命令を利用して、対策プログラム実行後すぐにユーザ領域の OS が立ち上がるよう実装し、また 2nd Disk 接続形態では、認証 OK 時に、接続バスドライバ(例えば USB バスドライバ)の再起動によって、HDD を再接続することなく、ディスクイメージが見えるよう実装した。

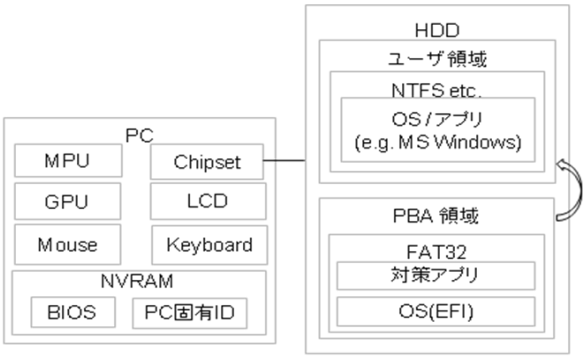

図3. 実装の構成

3-4. 動作フロー

機能を実装した TCG HDD/対策プログラムは、図 4 のようなユースケースにおいて、図 5 の動作フローに従って動作する。

4. 評価

登録 PC(PC1)として、FMV-A8260(Intel Celeron CPU 1.86GHz, メモリ 2GB, BIOS は EFI 非対応)を使用した。また、登録外 PC(PC2)として他社製 PC(Intel Atom N270, 1.6GHz メモリ 1GB,BIOS は EFI 非対応)を使用した。

TCG HDD の PBA 領域に搭載する EFI(OS)と、

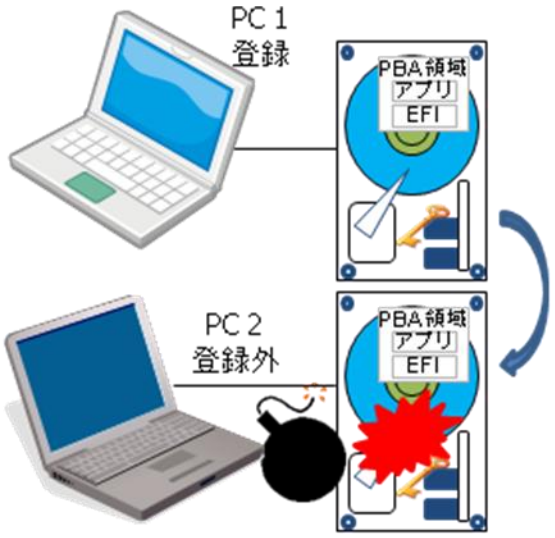

図 4. ユースケース

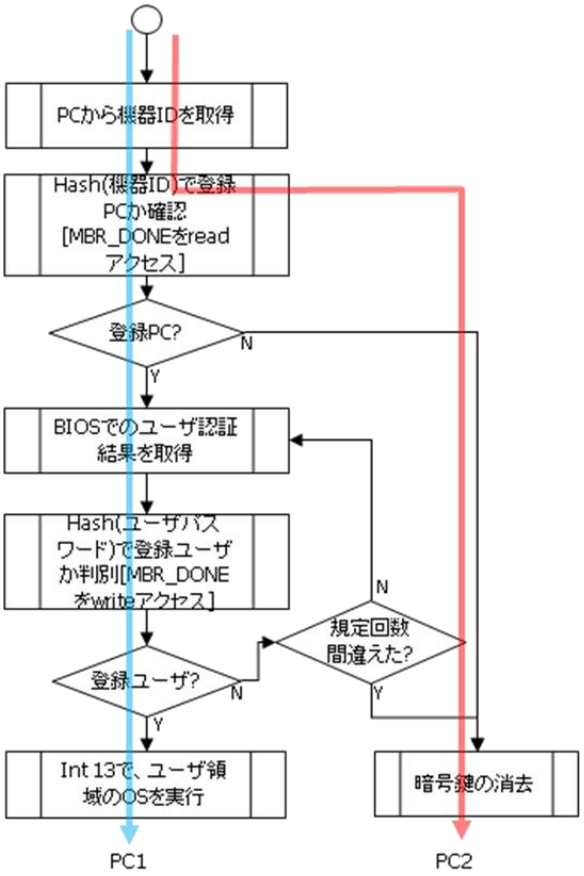

図 5. 動作フロー

開発した対策プログラムを合計したイメージのサイズは 1.1MByte 程度である。開発した対策プログラムを用いて TCG HDD に PC1 の機器 ID を登録し、以下の動作を確認した(図 4)。

・登録 PC に、対策プログラムを搭載した TCG HDD を接続して、PC を起動した場合に、登録 PC として認識され、その後従来通りユーザ領域の OS(Windows Vista, Windows XP, or Fedora Linux)が起動すること。PC の通常 BIOS/OS 起動時間に加えて EFI(OS)と対策プログラム実行に要する時間は 2.2 秒であった。

・登録外 PC に TCG HDD を接続して、PC を起動した場合に、登録 PC とは認識されず、TCG HDD のユーザ領域全体が消去されること。この時、通常の BIOS 起動時間に加えて、EFI(OS)と対策プログラム実行に要する時間は minimun 2.2 秒であった。この時間は個々の PC の BIOS 実装に依存し、BIOS によって HDD 認識に要する時間により異なる。

・2nd HDD として USB 接続し、認証を実行した場合に、登録 PC ではデータを閲覧でき、登録外 PC では消去が実行されること。

5. まとめ

これまで HDD を抜き取られると高度な認証は機能しなかった。これを解決するための HDD 単独で動作する新しい認証強化策を提案した。また PC 業界でデファクトスタンダードとなる TCG Opal SSC 仕様の HDD に、ソフトウエアを追加実装することでその認証強化策が実現できることを示した。

参考文献

[1]TCG Storage Architecture Core Specification, Specification Version 2.00 Final, Revision 1.00, 20 April, 2009
www.trustedcomputinggroup.org/files/static_page_files/B6811067-1D09-3519-ADDAFC18E3A87CB2/Storage_Architecture_Core_Spec_v2_r1-Final.pdf

[2]TCG Storage Security Subsystem Class: Opal, Specification Version 1.0, Revision 2.00, April 20, 2009
www.trustedcomputinggroup.org/developers/storage/specifications

[3]AT Attachment 8 - ATA/ATAPI Command Set (ATA8-ACS), Revision 6, June 25, 2008

[4]Jason Cox, Trusted Computing Group Truseted Storage Specification, Education
www.snia.org/events/storage-developer2008/presentations/tuesday/CoxJason_TCG_Trusted_Storage_Specification.pdf

[5]Unified Extensible Firmware Interface Specification, Version 2.3, May, 2009
www.uefi.org/home

[6]EFI and Framework Open Source Community
www.tianocore.org/