6Y-2

プラットフォーム遠隔認証

†早川 薫　　‡都井 紘　　‡塩谷 亮太　　‡五島 正裕　　‡坂井 修一
†東京大学工学部　電子情報工学科　　‡東京大学大学院　情報理工学系研究科

1　はじめに

近年のインターネットの普及により，著作物や商用コンテンツの多くが電子化されている．その一方でヒューマンエラーやマルウェアなどによる著作権侵害が後を絶たない．

コンテンツを開発，配布するサーバ側の対策として，よくデータの暗号化技術が用いられる．しかしクライアント側の復号処理を行うソフトウェアや実行するアプリケーション，OS そのものが情報を漏らすように改造されている場合の対策にはならない．暗号化以外にもサーバ側の対策が提案されているが，ソフトウェアレベルだけでは完全でないという報告もある [1].

そのため，コンテンツを利用するクライアント側のプラットフォームが，サーバ側の期待するものであるかの認証が必要となる．このように認証する側とされる側が離れているものを遠隔認証と言う．クライアント側の OS は遠隔認証を行う際は信用できないため，**OS の信頼性に依存しないプラットフォーム遠隔認証**を実装する．

プラットフォーム遠隔認証は以下の手順で行われる．まずクライアント側のプラットフォームのハッシュ値をサーバ側に送る．サーバ側は信頼できるプラットフォームのハッシュ値をあらかじめ用意しておき，送られてきたハッシュ値と比較する．2 つのハッシュ値が一致したら認証成功とする．

プラットフォーム遠隔認証に対する唯一の攻撃方法は，サーバ側にプラットフォームの正しいハッシュ値を送りつつ，実際に動作させるものはすり替えることである．そのため，あらゆるすり替えを防ぐ必要がある．

2　関連研究

プラットフォーム遠隔認証のひとつの技術として TPM [2, 3] を用いたものがある．これは TPM というハードウェアのみを信頼し，PC 起動時に全てのコンポーネントを改竄されることなく計測し，その結果であるハッシュ値を TPM 内に保存する．サーバ側に遠隔認証を要求されたら，そのハッシュ値を改竄されることなく安全にサーバ側に送る．サーバ側はそのハッシュ値を見て，クライアント側が安全なコンポーネントを利用しているかを検証する．これによりサーバ側はクライアント側のプラットフォームの安全性を確認できる．

2.1　Trusted Boot

TPM は Trusted Boot という方法でプラットフォームをすり替えられることなく計測し，結果を保存する．

PC を起動した際，最初に物理的に信頼できる TPM の CRTM から計測をし，各コンポーネントを起動する前にそれらの計測を行うことで，信頼できる領域を連鎖的に増やしていくものである．これにより計測結果であるハッシュ値の完全性を確立する．

PC が起動されると，まず CRTM が自分自身を計測する．CRTM の計測，及び実行が終わったら，BIOS の計測を CRTM が行う．BIOS の計測が終わったら BIOS を起動し制御権限を渡す．次に BIOS は ROM と MBR(Master Boot Record) の計測を行い，それらを起動し制御権限を渡す．同じ処理を OS に制御権限が渡されるまで繰り返す．各計測結果であるハッシュ値はそのつど PCR に保存しておく．

このようにあるコンポーネントは，先に改竄されることなく正しく計測されたコンポーネントにより計測され，その後に起動される．一番最初に計測される CRTM は物理的に保護されているため改竄されることがない．これにより計測したコンポーネントと実際に動作するコンポーネントが同一であることを保証できる．

2.2　問題点

この方法では，安全なコンポーネントのとりうるあらゆる状態をサーバ側は予測する必要がある．特にオープンソースのコンポーネントに対しては対応が難しくなる．またアップデートや修正パッチの多い現状を考えると，ひとつのコンポーネントがとりうる全ての状態をサーバ側が用意することは困難である．さらにこの手法は，コンポーネントを計測したタイミングと認証の要求がくるタイミングに時間差がある．そのためその間にプラットフォームのコンポーネントが変更された場合，それを通知する機構が必要となる．最後に，この手法ではプラットフォームの潜在的なバグなどによる危険性がないことを保証できない．

†Kaoru HAYAKAWA ‡Hiroshi TOI ‡Ryota SHIOYA ‡Masahiro GOSHIMA ‡Shuichi SAKAI
†Dept. of EEIC Eng, the Univ. of Tokyo
‡Dept. of Information and Communication Eng, the Univ. of Tokyo

3 提案手法

本研究はMMU内のTLBとDMACを拡張することで，サーバ側に遠隔認証を要求されたコンポーネントをクライアント側ですり替えられることなく計測，実行する方法を提案する．サーバ側は認証したいコンポーネントのみをクライアント側に計測，通知をする．その結果を検証することでプラットフォーム遠隔認証を確立できる．そのためサーバ側が用意する期待値は既存手法より少なくて済む．さらに本研究室で提案した情報漏洩防止プラットフォーム [4] と協調することで，プラットフォームの潜在的なバグによる情報漏洩も防止する．

クライアント側で起きうるすり替えは，ページのすり替えと入出力に関するすり替えの2種類である．

3.1 ページのすり替え防止

TLBを拡張してページのすり替えを防止する．アクセス制限を拡張し，特権プロセスのアクセス制限を加えることで，特権プロセスによるすり替えを防止する．

またページテーブルのMACを生成することで，ページテーブル自体がすり替えられることを防ぐ．

3.2 入出力に関するすり替え防止

DMACに暗号処理機能とハッシュ計測機構を追加する．スワップアウト時にデータを暗号化し，MACを生成する．スワップイン時に再度MACを生成し，スワップアウト時に生成したものと比較することですり替えを防止する．

3.3 TLBとDMACの協調によるすり替え防止

DMA転送時とページに関するすり替えが行われる可能性があるので，それをTLBとDMACの協調により防止する．

4 まとめ

本研究はサーバ側がクライアント側のプラットフォームを遠隔認証するためのものである．そのためにはあらゆるすり替えを防ぐ必要があることを述べた．

TPMを用いた手法は現実的に困難であり，クライアント側におけるすり替えを完全に防げてはいない．

本手法はクライアント側のページや入出力に関するすり替えの防止を，MMUを拡張することにより実装した．

参考文献

[1] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (Im)possibility of Obfuscating Programs. In *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, pp. 1–18. Springer-Verlag, 2001.

[2] Trusted Computing Group. *TCG Specification Architecture Overview*.

[3] Trusted Computing Group. *TPM Specification Version 1.2 Revision 103*.

[4] 横田侑樹, 塩谷亮太, 五島正裕, 坂井修一. 情報漏洩防止プラットフォーム. 電子情報通信学, 信学技報, vol. 109, no. 237, pp. 7–12, 2009.