様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　１８　日現在

機関番号：　８２６２６
研究種目：　基盤研究(B)（一般）
研究期間：　2015～2017
課題番号：　１５Ｈ０２７１２

研究課題名（和文）サイバーエスピオナージを防止するデバイス管理技術

研究課題名（英文）Device Management which protects cyber espionage

研究代表者
須崎　有康（Suzaki, Kuniyasu）

国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員

研究者番号：５０３５７２７４

交付決定額（研究期間全体）：（直接経費）　　14,100,000円

研究成果の概要（和文）：USBの高性能化により、高解像度のカメラやマイクや大容量ストレージが接続可能であり、これを用いた盗聴や大容量データ窃取が可能となった。この攻撃を防ぐために個々のUSBデバイスに物理的に改竄不可能なIDを物理的困難関数（個々のIC固有の回路遅延を使った技術）で付加し、それれぞのUSBデバイスをOSの起動する前に識別・認証するハイパーバイザーを開発した。この開発により、既存のBadUSB(USBキーボードに化けて悪意のあるコマンドを入力する攻撃)が防げることを確認した。

研究成果の概要（英文）：The Universal Serial Bus (USB) supports a diverse and wide-ranging set of device types, which include high-resolution camera, microphone and mass storage. These devices also enable eavesdropping and big data theft. In order to prevent these attacks, individual USB device is added the tamper-proof ID which is created from PUF (Physically Unclonable Function based on each circuit delay). The authentication mechanism is developed by the hypervisor and the USB device is authenticated with the ID before the OS. The developed technology can prevent the attack of BadUSB (which disguises a USB keyboard and types malicious commands).

研究分野：　コンピュータセキュリティ

キーワード：　コンピュータセキュリティ　仮想化　アクセス制御　デバイス認証技術

１．研究開始当初の背景

近年のデバイスは高性能化しており、これの高性能デバイスを使ったサイバーエスピオナージの脅威が高まっている。例えば、攻撃技術の会議である WOOT'14 では 10 メガピクセルの解像度のカメラがあれば『目に映ったスマートフォンの画面』を内蔵カメラから見ることでパスワードが推定できると発表された。また、ジャイロセンサーから得られる情報を使って周囲の音声を解析する手法がスタンフォード大学で開発され、USENIX Security 14 で発表されている。デバイスにサイバーエスピオナージの機能が組み込まれている疑いのあるデバイス製品も出ている。中国に本社のあるファーウェイ（Huawei）社の無線 LAN 製品が米国政府の安全保障を脅かす可能性があるとする調査報告が出され、携帯通信事業者各社に対し、同社との取引を取りやめるよう勧告したこともあった。

サイバーエスピオナージでは外部からのサイバー攻撃ばかりでなく、内部犯による不用意なデバイス接続も考慮しなくてはならない。例えば、ベネッセコーポレーションによる個人情報漏洩事件では、容疑者は大量のデータを貸与 PC から私物のスマートフォンにコピーし、持ち出していたとされる。貸与 PC は USB メモリへのデータ書き込みを禁止する設定だった報じられて、この禁止設定は Active Directory のグループポリシーの設定による USB メモリの使用制限だと類推されている。この禁止設定ではスマートフォンに特有のファイル転送方式 MTP（Media Transfer Protocol）の使用を制限できずに漏洩事件に発展してしまった。また、イランの核開発施設を狙った StuxNet もインターネットと接続しないエアーギャップを内部の協力者が回避して USB メモリを制御システムに接続したために感染したと言われている。

モバイル端末は社外作業や医療現場で活用されているが、企業では不要なデバイスや不審なデバイスは安全確保のために社員用では無効にしたい（図１）。しかし、多くのモバイル端末ではデバイスは組み込みであり、また USB を通した接続も簡単なために無効化するのが容易ではない。

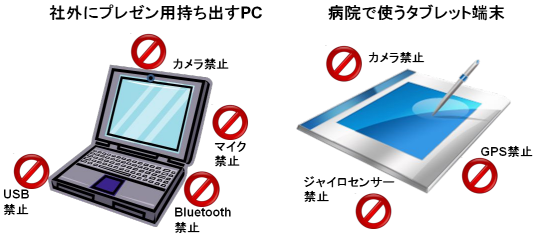

図 1 管理者が行いたいデバイス利用制限

モバイル端末によっては BIOS 等の設定で無効化できるものもあるが、全ての機器で使えるものではなく、特定のデバイスのみを許可するような設定は行えない。USB ポートガードなどの製品もあるが、信頼の根拠が利用者のモラルに頼っており、工学的な安全性が確保されていない。

２．研究の目的

研究目的（概要）

モバイル端末は社外作業や医療現場で活用されているが、高性能なデバイス(カメラ、GPS、ジャイロセンサー)が標準で装備され、これらを悪用したサイバーエスピオナージ(電子的諜報活動)の危険性が指摘されている。残念ながら OS や BIOS による利用禁止機能は不十分であり、また、モバイル端末は管理者の手が届き難く、従業員による改竄の危険性もある。これらの問題を解決するために、(1)OS とは独立に管理者が利用可能デバイスを設定できる技術、および管理者以外に改竄されないようにセキュアチップ TPM などを使った改竄防止技術、(2)半導体の個体識別技術の物理的困難関数 PUF と連携した認証技術を研究する。また、(3)開発する技術の根拠を示すリスクアセスメントおよびテストベッドで実際のマルウェアを使った評価も行い、工学的な有効性を示す。

３．研究の方法

(1) 既存の OS を保護するために、認証技術はハイパーバイザーとして作成し、OS 以前に USB デバイスを事前識別・認証する技術を開発した。この技術開発は USB が挿入された際に起こる割り込みを隠ぺいするため、ハイパーバイザーで一時的にダミーUSB デバイスを認識させた後、デバイスが正当なものであれば、再度認識させるようにした。

また、ハイパーバイザーは内部犯行にも耐えられるように TPM: Trusted Platform Module 内の鍵はハイパーバイザーを含める Trusted Boot 時にのみ取り出せる仕組みを使い、既存 OS を暗号化した。既存 OS はハイパーバイザーが起動したときのみ、動作可能となる。また、Secure Boot を使って、ハイパーバイザーと既存 OS のカーネル以外は起動できない設定として、内部犯行者が改ざんできないようにした。

(2) 個々のデバイスの回路遅延を識別子とする物理的困難関数 PUF(Physically Unclonable Function)は耐タンパー性を持ち、同一工場の同一ラインで製造されても個別デバイスで異なる。この性質を USB の個別デバイス認証に活用した。

(3) 開発された USB デバイス認証技術が活用される条件を調べるために論文サーベイやインターネット検索を、模擬 BadUSB コードや MTP プロトコルによるデータ窃取の方式を調査した。

４．研究成果

高性能デバイスを悪用したサイバーエス

ピオナージ（電子的諜報活動）を防ぐデバイス管理技術を確立するために、OS とは独立に USB デバイスを事前識別・認証するハイパーバイザーを開発した。

(1) オープンソースの BitVisor をベースに OS の認識前に個々の USB デバイスを識別・認証できるハイパーバイザーを作成した。作成したハイパーバイザーと USB 認証の構成図は下記になる。ハイバーバイザー内で USB デバイスの識別（図 2 右の Access Hook）と PUF によるチャレンジレスポンスによる認証（図 2 左の PUF Verificaion）を行う。

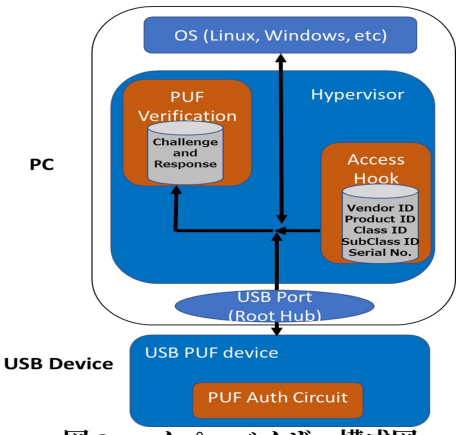

図 2 ハイパーバイザー構成図

BitVisor 単体では、耐タンパー技術を有しないため、TPM の鍵が BitVisor を含める Trusted Boot でのみ取り出せる仕組み、その鍵で暗号化した OS を起動する仕組みを開発した。また、この仕組みを Secure Boot と組み合わせて、指定されたハイパーバイザーと OS カーネルのみが起動できるようにした。これにより、内部犯行者が情報取得を試みても OS イメージは登録されていない USB デバイスと接続することができないようになった。

(2) USB デバイスには物理複製困難関数(PUF: Physically Unclonable Function)の機能を付加し、接続先の PC ではハイパーバイザーにより OS が認識する以前に PUF 認証を行う技術を開発した。PUF は産総研で開発されている物理攻撃評価ボードである Zuiho をベースに開発した。PUF には産総研で開発した PL-PUF: Pseudo Linear Shift Feedback Shift Register PUF を使った。

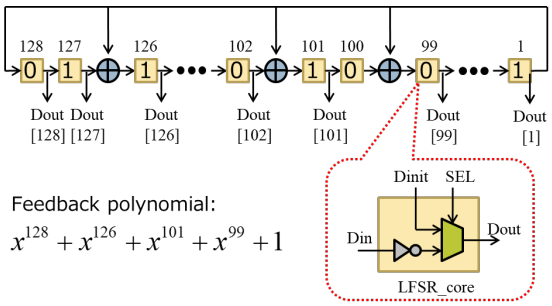

図 3 PL-PUF の回路構成図

PL-PUF は図 3 に示す回路構成をしており、ビット長が長いチャレンジアンドレスポンスに対応することができる。この開発により、通常の USB デバイスに PUF 認証回路を付加するのに 100 円以下で可能なことを評価した。

(3) 開発した技術を使って既存の BadUSB 攻撃(USB メモリを USB キーボードとして認識させ、悪意のあるコマンドを入力する攻撃)が防げることを確認した。更に 2014 年のベネッセの情報漏えいで使われたと考えられているスマートフォンの特殊なプロトコル(PTP: Picture Transfer Protocol あるいは MTP: Media Transfer Protocol)を使っても、デバイス（スマートフォン）がハイパーバイザーに登録されていなければ攻撃を防げることを確認した。

(4) 更に研究を進めるに当たって、PUF にチャレンジアンドレスポンスの安定性に問題があることが判明し、安定したチャレンジアンドレスポンスであるかと検証できる技術を開発した。この技術では USB ハブの電源を制御する Per-Port Power Switching (PPPS)の機能使えば USB デバイスの抜き差しがソフトウェアから自動化できることに注目した。この機能とハイパーバイザーを連携させて自動的に USB-PUF デバイス認証を確認できる機能を作成した。この技術により、PUF ではチャレンジするデータによってはそのレスポンスがエラー訂正の範囲内に入らずに認証に使えない問題を機械的に調査できるようになった。

5．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　0　件）

〔学会発表〕（計　0　件）

〔図書〕（計　0　件）

〔産業財産権〕

○出願状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0　件）

名称：
発明者：

権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
https://staff.aist.go.jp/k.suzaki/

６．研究組織
(1)研究代表者
須崎有康（Suzaki, Kunyasu）
国立研究開発法人産業技術総合研究所・情報・人間工学領域・主任研究員
研究者番号：50357274

(2)研究分担者
堀洋平（Hori, Yohei）
国立研究開発法人産業技術総合研究所・エレクトロニクス・製造領域・主任研究員
研究者番号：60530368

(3)連携研究者
古原和邦（Kobara, Kazukuni）
国立研究開発法人産業技術総合研究所・情報・人間工学領域・総括研究主幹
研究者番号：70323649