[Work in Progress] 研究報告

低価格で普及可能な簡易 USB チェッカーの試作

安東　孝二[†1]　　向阪　秋良[†1]

Prototyping of Affordable & Portable Simple USB Checker

1. 背景

2014 年 8 月に開催された Black Hat 2014 USA において Karsten Nohl と Jacob Lell により、”BadUSB – On Accessories that Turn Evil”というブリーフィングが行われ、USB の脆弱性を用いた BadUSB と呼ぶ攻撃法のデモが行われた．ここで指摘された USB の脆弱性は単純かつ深刻なものであった．USB デバイスには必ず制御ソフト(firmware)が備わっているが、多くの USB デバイスではその制御ソフトは第三者が書き換え可能だということが示されたのである．
彼らはこの時、危険すぎるという理由で制御ソフト書き換えソフトウェアのソースコードは公開されたなかったが、同 9 月に開催された DerbyCon 4.0 の発表 ”Making BadUSB Work For You” の中で、この手法を可能にするソフトウェアが公開されるべきだと考えた Adam Caudill と Brandon Wilson は独自の制御ソフト書き換えソフトウェア ”Psychson” を GitHub に公開した．これは Phison 社製チップが搭載された USB メモリの制御ソフト書き換えツールであり、誰でも BadUSB を悪用できる状態となっている。

2. 問題点

BadUSB での攻撃に対してアンチウイルスソフトは無力である．USB プロトコルに不正はなく、アンチウイルスソフトでは制御ソフト自体のチェックが不可能だからである．また多くのデバイスに USB が採用されていることから攻撃方法も多岐にわたる．USB キーボードにはキーロガーを紛れ込ませ、USB ストレージからは任意のコマンドを実行させ、USB ネットワークアダプタには悪意のあるサーバにデータを流すことも原理的に可能である．

効果的対策はほとんど考えられないため、USB を使わないことが最善であるが、ほとんどのコンピュータのキーボードデバイスが USB 接続であることを考えても、USB 自体を全廃することは難しい．また、ネットワーク以外でのファイルのやり取りの多くは USB メモリに移行しており、利便性との兼ね合いからもすべての利用を取りやめることは現実的に不可能である．

3. 考察

全ての対策を万全に行うことは不可能であるため、可能性の高い攻撃方法に対応することで被害を緩和することを考える．顕在化している BadUSB を用いた攻撃方法のほとんどは USB メモリをキーボードなどの HID(Human Interface Device)として機能させることでコンソールの権限を奪うことを出発点としている．そのため USB デバイスの接続に際し期待しない HID を検出することが有効な対策となる．加えて、HID を接続した場合に期待しない入力は不審であり検出されるべきである．

4. 試作

一般的に我々は PC 以外の USB ホストを持っていないが、PC を守るためには PC 以外の USB ホストが接続されたデバイスの振る舞いをチェックすることが望ましい．ただし、USB プロトコルアナライザは一般に PC より高価であり通常の利用には馴染まない．

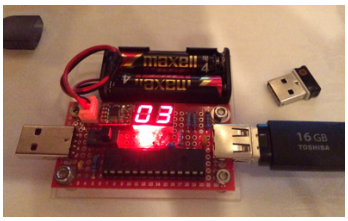

図 1　USBCheker 試作機

そこで、今回は USB デバイスの振る舞いチェックのための安価なデバイス、「USBCheker」を試作することとした．広く対策を行うには 1 人に 1 台利用できる程度の価格であることも重要と考え、安価でプログラムを改変されない USB ホストであり、モバイル化も可能なものとして、試作機では USB ホスト機能を持つ PIC マイコン（PIC24FJ64GB002）を利用した．

現在の機能は ClassID の表示（複数 ID にも対応）と HID からの入力パケットの検出である．

今後、このデバイスの妥当性と技術的問題点を議論していくとともに、協力者による様々なデバイスでの実験を重ねていく予定である．

†1 株式会社　mokha
mokha Ltd., Bunkyo, Tokyo 113-0033, Japan