Secure USB Bypassing Tool

By

Jewan Bang, Byeongyeong Yoo and Sangjin Lee

Presented At

The Digital Forensic Research Conference

DFRWS 2010 USA Portland, OR (Aug 2nd - 4th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http://dfrws.org
Secure USB Bypassing Tool

Authors: Jewan Bang, Byeongyeong Yoo and Sangjin Lee

Digital Forensics Research Center
Of Center of Information Security Technologies
Korea University
Introduce DFRC

- Most renowned & distinguished Research Center on Digital Forensics in Korea
- Most of research projects has funded by law enforcements and government
- One of Korea university's affiliated organizations
- About 30 Researcher is working on various area of digital forensics
  - 1 Professor, 2 Post-Doc, 7 Doctorate Course, 20 Master Course
- Overall Winner of 2009 DC3 Digital Forensics Challenge
  - Hosted by DoD Cyber Crime Center (DC3)
  - The DC3 Challenge encourages innovation from a broad range of individuals, teams, and institutions to provide technical solutions for computer forensic examiners in the lab as well as in the field

<table>
<thead>
<tr>
<th>Rank</th>
<th>Team Name</th>
<th>Team Type</th>
<th>Affiliation</th>
<th>Days Out</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DFRC</td>
<td>Group</td>
<td>Graduate Student</td>
<td>175</td>
<td>2014</td>
</tr>
<tr>
<td>2</td>
<td>Little Bobby Tables</td>
<td>Group</td>
<td>Graduate Student</td>
<td>102</td>
<td>1772</td>
</tr>
<tr>
<td>3</td>
<td>WilmU01</td>
<td>Group</td>
<td>Undergraduate Student</td>
<td>68</td>
<td>1732</td>
</tr>
<tr>
<td>4</td>
<td>DFAC</td>
<td>Individual</td>
<td>Government</td>
<td>207</td>
<td>1682</td>
</tr>
</tbody>
</table>
1. About Secure USB Flash Drive
2. Security Mechanisms of Secure USB Flash Drive
3. Methods of USB controller based access control
4. Secure USB Bypassing Tool (USB Lockpass)
5. Conclusions
Secure USB Flash Drive in the Field

- Accessing USB drive is locked.
- Entire Drive Imaging is impossible
- Drive size is not identical with Spec.
About Secure USB Flash Drive

- Most of the current USB Flash Drive provides a security solution
  - 300 USB flash Drive is selling in Korea.
  - 250 is capable of security feature.

- Such USB prevents private data exposure when lost

- When an investigator confiscates such secure USB, obtaining an evidence can be troublesome
  - In an emergency case, a decryption or bypassing process is required
Secure USB Flash Drive

Secure USB Flash Drive Type

Hardware Based

Flash Drive Controller Based

Encryption Chip Based

Software Based

Others (Fingerprint, …)

Data Encryption

Digital Forensics Research Center, Center for Information Security Technologies, Korea University
Secure USB provides security solution by encrypting data, or accessing data through an authentication process.

There exists Universal Command which is used in every USB, and Vendor Specific Command that is assigned to execute a particular action, by USB Controller manufacturer.

- Because it is Vendor Specific Command Controller dependent, identical controllers share the same Command system even if their manufacturers are different.
- Hence, the same controllers have the same access clearing command.
### Status of Market Shares of USB Controllers in 2008

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Market Share</th>
<th>Profit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phison</td>
<td>35.5%</td>
<td>$32.3</td>
</tr>
<tr>
<td>Silicon Motion (SMI)</td>
<td>23.2%</td>
<td>$21.1</td>
</tr>
<tr>
<td>Sandisk</td>
<td>14.9%</td>
<td>$13.6</td>
</tr>
<tr>
<td>Skymedi</td>
<td>9.0%</td>
<td>$8.2</td>
</tr>
<tr>
<td>Sony</td>
<td>7.4%</td>
<td>$6.7</td>
</tr>
<tr>
<td>AlcorMicro</td>
<td>3.2%</td>
<td>$2.9</td>
</tr>
<tr>
<td>Toshiba</td>
<td>3.1%</td>
<td>$2.8</td>
</tr>
<tr>
<td>Others</td>
<td>3.7%</td>
<td>$3.4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
<td><strong>$91.1</strong></td>
</tr>
</tbody>
</table>

2007 USB Controller Market Shares (Revenue in Millions of Dollars), iSuppli Corp (Applied Market Intelligence)
Secure USB Command Flow

- Request Authentication Information
Secure USB unlock methods:

✅ Type 1: Sending an unlock command

- Defined unlock command exists
- Chipset
  - USBEST UT163, SMI SM321-325, Skymedi SK6211/6281
Secure USB unlock methods:

**Type 2: Obtaining authentication information**

- Sending defined unlock command with authentication information
- Chipset
  - AlcorMicro AU6983
Secure USB unlock methods:

- Applies when secured area exists in the back of unsecured area
- Resetting secured area’s starting address to unsecured area’s starting address
- Denying access to general area : it has to be obtained in advance

- Chipset
  - Phsion PS2136
USBest UT163/UT165 series

✔ USBest UT163 series
  – SINGANG MyStick, AXXEN i-BAR, Transcend JetFlash
    • Get Password Command
      – 0xF8000000 02000000 01000000 (12 bytes)
    • Unlock Command
      – 0xFC000000 00000000 0100 (10 bytes)

✔ USBest UT165 series
  – EK Black Cat, SELFIC SWING MINI, Kingmax Superstick
    • Get Password Command
      – 0xF8000000 04000000 01000000 (12 bytes)
SMI SM321~325 series

- LG XTICK, Memorive T3, Zyrus Mini Swing

- **Get Password Command**
  - 0xF0050000 00000000 00000001 00000000 (16bytes)

- **Unlock Command**
  - 0xF1110000 00000000 00000001 00000000 (16bytes)
Skymedi SK6281/SK6211 series

✓ Skymedi SK6281 series
  – AXXEN SKY CANDY, PLEOMAX, Kingston DataTraveler
    • Get Password Command
      – 0xD4000000 00010000 0000 (10bytes)
    • Unlock Command
      – 0xD8040000 00000000 0000 (10bytes)

✓ Skymedi SK6211 series
  – LUXL-V Swing
    • Get Password Command
      – 0xD4000000 00010000 0000 (10bytes)
    • Unlock Command
      – 0xF1100000 00000000 0000001 00000000 (16bytes)
AlcorMicro AU6983 series

- Transcend JetFlash

- Get Authorization Command
  - 0x4000000 00010000 0000

- Unlock Command
  - 0x74000000 00000000 0000 with [AUTHINFO]
Phison PS2136 series

- PLEOMAX PUB-S80

- Get Secure Area Command
  - 0x0605494F 464F0000 0000

- Set Secure Area Size
  - 0x06060100 00000000 00000000 with
    0xD000000 0802 [SIZEINFO] 000000000000
Sandisk Contour

- Sandisk Contour

- Get Initialize Command
  - 0xFF210000 00000000 00000000 00000000

- Password Command
  - 0xFFFFA20000 00000000 00000000 00000000 with [INITINFO]
✓ Toshiba

– Toshiba TransDrive

- Set Authorization Command
  – 0xFF570000 00000000 0000 with [HASHINFO]

- Unlock Command
  – 0xFF540000 00000000 0000 with [HASHINFO]
Detoured around by various USB controllers

Security function can be detoured around by various USB controllers

<table>
<thead>
<tr>
<th>Controller</th>
<th>Security configuration condition checking</th>
<th>Whether password is obtained</th>
<th>Whether security certification can be detoured around</th>
</tr>
</thead>
<tbody>
<tr>
<td>USBest UT163</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Skymedi SK6281</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>SMI SM321 ~ SM325</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Phison PS2136</td>
<td>O</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>USBest UT165</td>
<td>O</td>
<td>O</td>
<td>X</td>
</tr>
<tr>
<td>Skymedi SK6211</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>AlcorMicro AU6983</td>
<td>O</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>Sandisk Cruzer Contour</td>
<td>O</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>Toshiba</td>
<td>O</td>
<td>X</td>
<td>O</td>
</tr>
</tbody>
</table>
Structure of the Secure USB bypassing tool

- User Interface Parts
- Disk Imaging Module
- USB Unlock Module
- USB Device Recognition Module
- Registry Analysis Module

Current Registry State

Command transmission

Response received

Report
Secure USB Drive Bypass

USB LOCKPASS v1.5

Security USB Memory Bypass  USB Memory Trace  USB Memory Security Application Trace  USB Memory Image

USB Memory Drive Selection

H:\AXXEN PASSION-bar USB Device

USB Memory Information

USB Memory Name: AXXEN PASSION-bar USB Device
Vendor ID: 1516
Product ID: 1603
Security Area: YES
Memory Size: 1.06GB
Serial Number: 200802190000000059188E06
USB Controller: Skymed SK8281
Password Information: PaSs@# (Hint:PassHint)

[07:49:10] Finished USB Memory Information Update
[07:49:23] Investigator Name: Jeewon Bang
[07:49:23] Case Information: EVIDENCE
[07:49:25] AXXEN PASSION-bar USB Device 200802190000000059188E06 Password (Hint: Information Acquisition)
### USB Drive Trace

![USB Drive Trace](image)

**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USBSTOR**
USB Drive Security Application Trace

<table>
<thead>
<tr>
<th>Product Group</th>
<th>USB Chip</th>
<th>Application Trace</th>
<th>First Execution</th>
<th>Last Execution</th>
</tr>
</thead>
<tbody>
<tr>
<td>XTICK, MEMORY, ZYRUS</td>
<td>SMI</td>
<td>OSB C UTILITY.EXE</td>
<td>2016-04-13 07:21:45</td>
<td>2016-04-19 07:21:45</td>
</tr>
<tr>
<td>SILICON POWER</td>
<td>Pilsen</td>
<td>LOCK.EXE</td>
<td>2016-04-11 20:30:08</td>
<td>2016-04-19 08:12:37</td>
</tr>
</tbody>
</table>

%systemroot%\Prefetch\*.pf
USB Drive Imaging

USB LOCKPASS v1.5

USB Memory Drive Selection
- H:\AIXXEN PASSION-bar USB Device

USB Memory Drive Imaging
- USB Memory Name: AIXXEN PASSION-bar USB Device
- Memory Size: 2,000 GB
- File Selection: C:\EVIDENCE03 IMAGE
- MD5: 1870C1B976E6ABBF7DF0E36529E6BB36
- SHA1: CP2013AEC2140E2A34895AC54A4A9760DAE02E22

Log:
- [07:51:52] Starting USB Memory Information Update
- [07:51:52] Finished USB Memory Information Update
- [07:52:02] AIXXEN PASSION-bar USB Device (S/N: 200802 90000000058988EDf) Selection
- [07:52:10] AIXXEN PASSION-bar USB Device (S/N: 200802 90000000058988EDf) Disk Imaging Start
- [08:01:54] AIXXEN PASSION-bar USB Device (S/N: 200802 90000000058988EDf) Disk Imaging Finished

Digital Forensics Research Center, Center for Information Security Technologies, Korea University
Conclusions

✓ Secure USB ByPasing tool
  – Most secure USB Drive access is controlled, based on its Controller
  – However, it does not send authentication information but simply sends unlock command to access
  – Make it to support most of the controllers by utilizing a tool through an analysis.

✓ Future Research
  – Analyzing more Controller based secure USB’s authentication bypassing methods
  – Hardware(Encryption chip) based encryption and USB analysis
Thank you for attention