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

About us

✓ 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

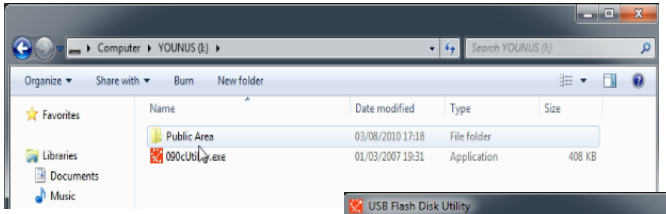
Overall - By Points

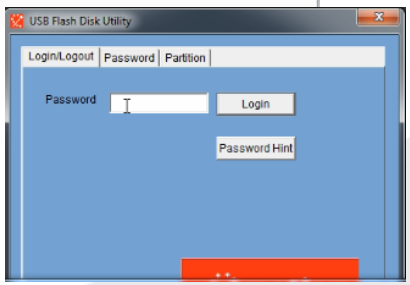
Rank	Team Name	Team Type	Affiliation	Days Out	Score
1	DFRC	Group	Graduate Student	175	2014
2	Little Bobby Tables	Group	Graduate Student	102	1772
3	WilmU01	Group	Undergraduate Student	68	1732
4	DFAC	Individual	Government	207	1682

Agenda

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



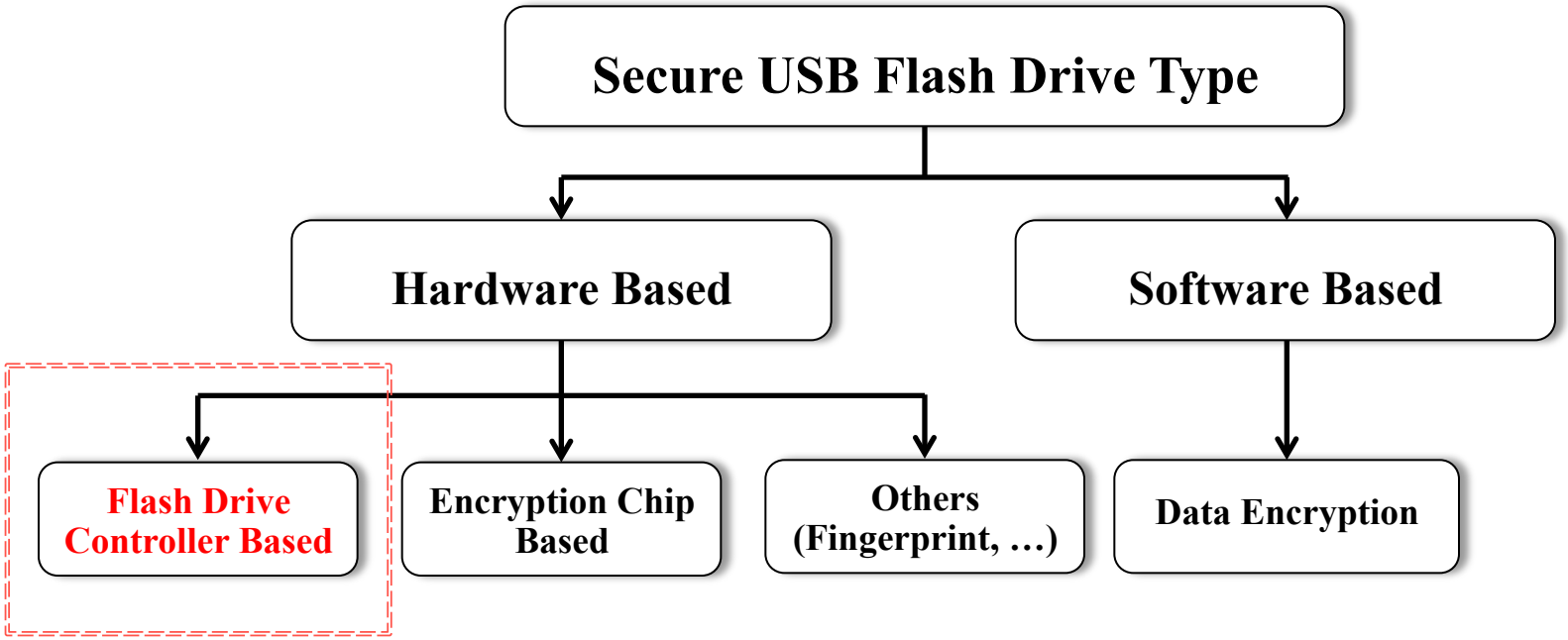


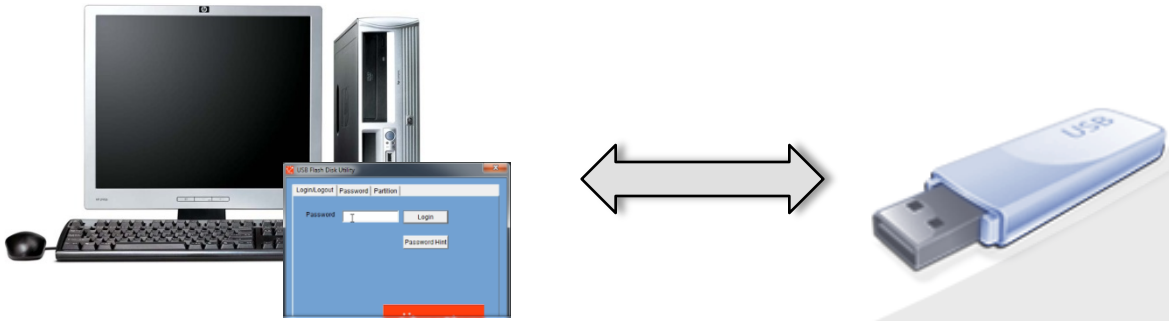
- **Accessing USB drive is locked.**
- **Entire Drive Imaging is impossible**
- **Drive size is not identical with Spec.**

About Secure USB Flash Drive

- ✓ **Most of the current USB Flash Drive provides a se curity solution**
  - 300 USB lash Drive is selling in Korea.
  - 250 is capable of security feature.
- ✓ **Such USB prevents private data exposure when lo st**
- ✓ **When an investigator confiscates such secure US B, obtaining an evidence can be troublesome**
  - In an emergency case, a decryption or bypassing process is required

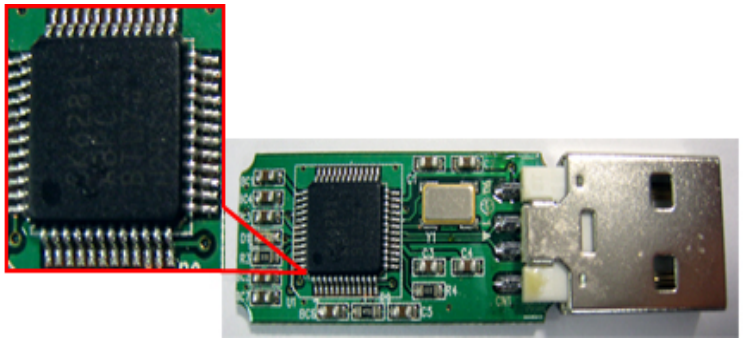
Secure USB Flash Drive





Secure USB Flash Drive

- ✓ **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

Million Dollars

	Manufacturer	Market Share	Profit
1	Phison	35.5%	$32.3
2	Silicon Motion (SMI)	23.2%	$21.1
3	Sandisk	14.9%	$13.6
4	Skymedi	9.0%	$8.2
5	Sony	7.4%	$6.7
6	AlcorMicro	3.2%	$2.9
7	Toshiba	3.1%	$2.8
8	Others	3.7%	$3.4
	Total	100%	$91.1

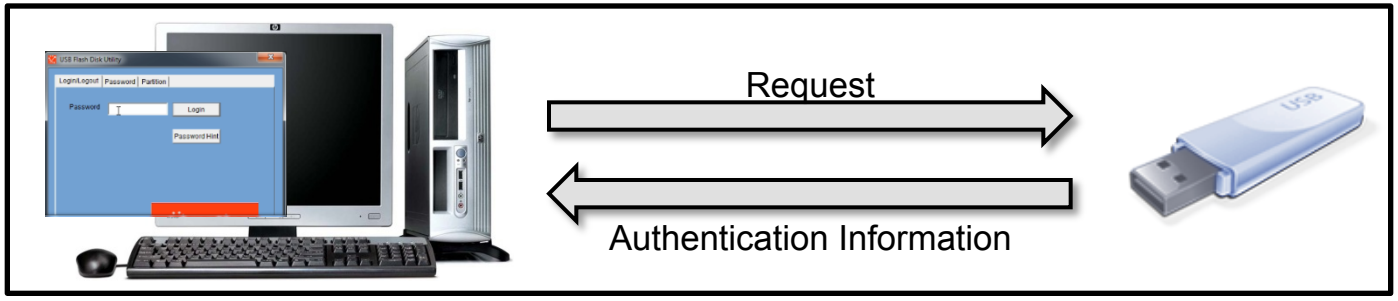
2007 USB Controller Market Shares(Revenue in Millions of Dollars), iSuppli Corp (Applied Market Intelligence)

Secure USB Command Flow

✓ Secure USB Command Flow

000022: Bulk or Interrupt Transfer (DOWN), 18.05.2009 20:54:17.171 +0.0
Pipe Handle: 0x89231a24 (Endpoint Address: 0x1)
Send 0x1f bytes to the device

```
55 53 42 43 B8 62 2A 89 10 02 00 00 80 00 0C F8  USBC¸b*□....□..ø
00 00 00 02 00 00 00 01 00 00 00 00 00 00 00 00  ................
```

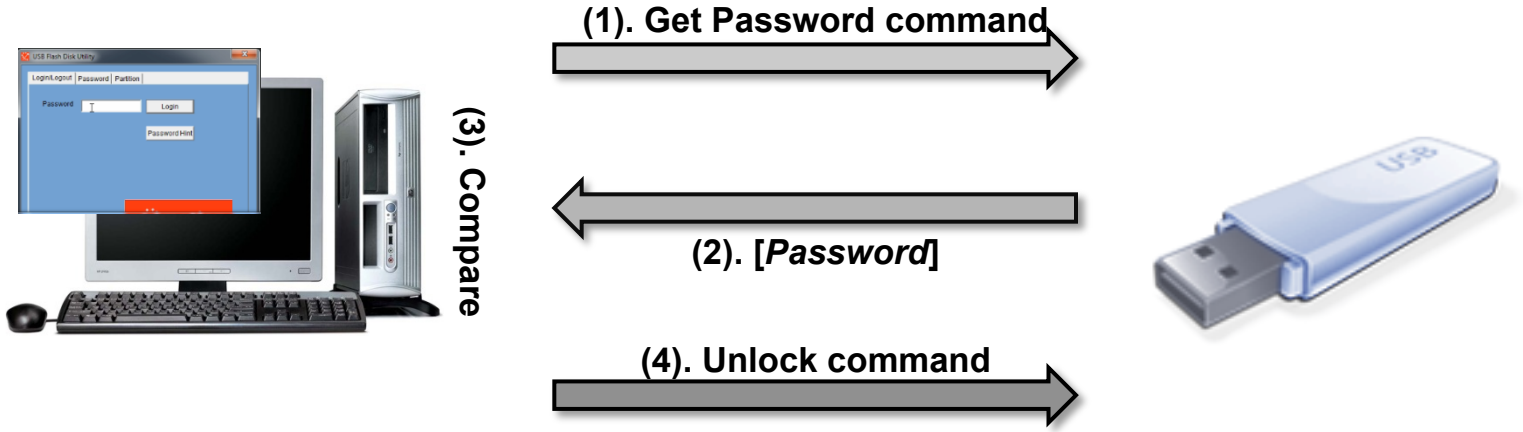


000171: Bulk or Interrupt Transfer (UP), 18.05.2009 22:56:22.328 +0.0. Status: 0x00000000
Pipe Handle: 0x8a370b94 (Endpoint Address: 0x81)
Get 0x210 bytes from the device

```
12 01 00 02 00 00 00 40 FE 13 21 1F 00 01 01 02  .......@þ.!.....
03 01 04 03 09 04 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 10 03 50 4C  ..............PL
4F 4D 41 58 00 00 00 00 00 00 00 00 00 00 00 00  EOMAX...........
00 00 00 00 00 00 10 03 50 55 42 2D 53 38 30 00  ........PUB-S80.
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
1A 03 34 00 45 00 37 00 36 00 30 00 43 00 30 00  ..4.E.7.6.0.C.0.
30 00 30 00 36 00 45 00 46 00 1A 03 30 00 38 00  0.0.6.E.F...0.8.
31 00 34 00 31 00 43 00 30 00 34 00 30 00 04 01  1.4.1.C.0.4.0...
38 00 39 00 01 05 10 08 01 1A FF 01 50 55 42 2D  8.9.......ÿ.PUB-
53 38 30 20 20 20 20 20 20 20 20 20 D5 02 00 00  S80          Õ...
50 4C 45 4F 4D 41 58 20 50 4D 41 50 00 00 00 00  PLEOMAX PMAP....
```

Secure USB unlock methods:

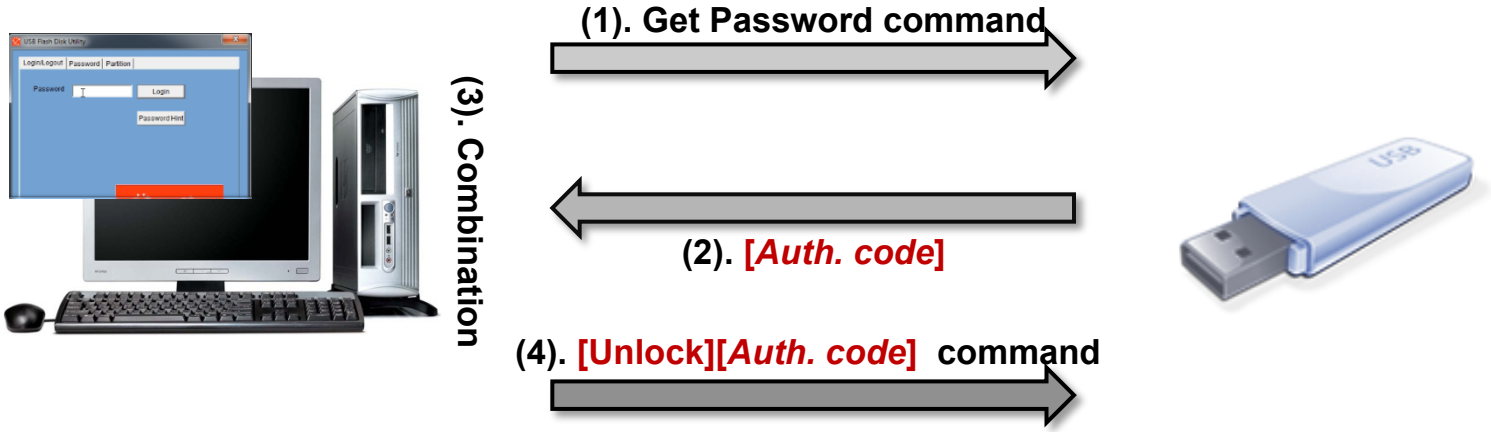
✓ Type 1: Sending an unlock command



- **Defined unlock command exists**
- **Chipset**
  - **USBEST UT163, SMI SM321~325, Skymedi SK6211/6281**

Secure USB unlock methods:

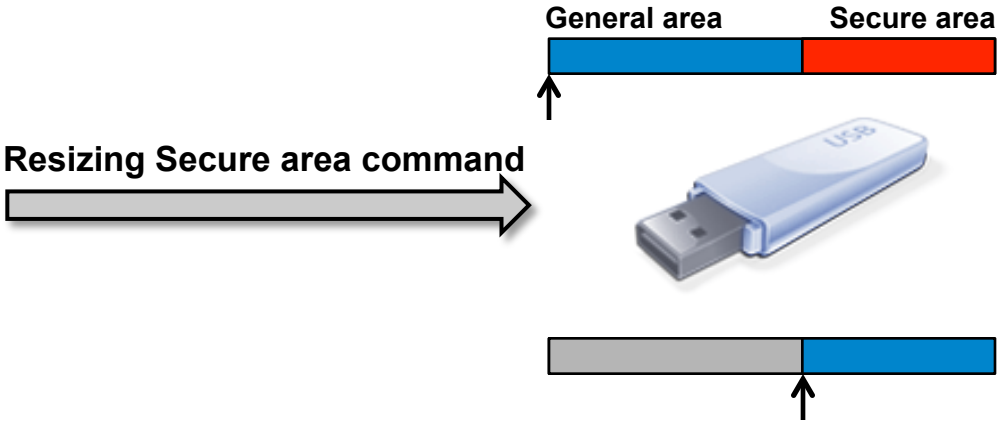
✓ Type 2: Obtaining authentication information



- Sending defined unlock command with authentication information
- Chipset
  - AlcorMicro AU6983

Secure USB unlock methods:

✓ Type 3: Resizing Secured Area



- 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 (12bytes)
  - Unlock Command
    - 0xFC000000 00000000 0100 (10bytes)

✓ USBest UT165 series

- EK Black Cat, SELFIC SWING MINI, Kingmax Superstick
  - Get Password Command
    - 0xF8000000 04000000 01000000 (12bytes)

✓ 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
    - 0xF1110000 00000000 00000001 00000000 (16bytes)

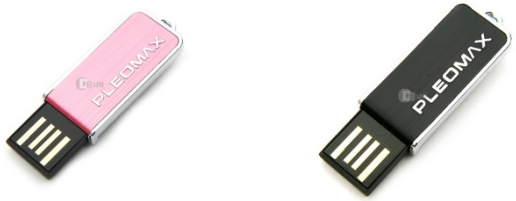
✓ AlcorMicro AU6983 series

– **Transcend JetFlash**

- **Get Authorization Command**
  - **0xD4000000 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

    0x0D000000 0802[*SIZEINFO*]000000000000

Sandisk Contour

✓ Sandisk Contour

– Sandisk Contour

- **Get Initialize Command**
  - 0xFF210000 00000000 00000000 00000000
- **Password Command**
  - 0xFFA20000 00000000 00000000 00000000 **with [*INITINFO*]**

✓ Toshiba

– Toshiba TransDrive

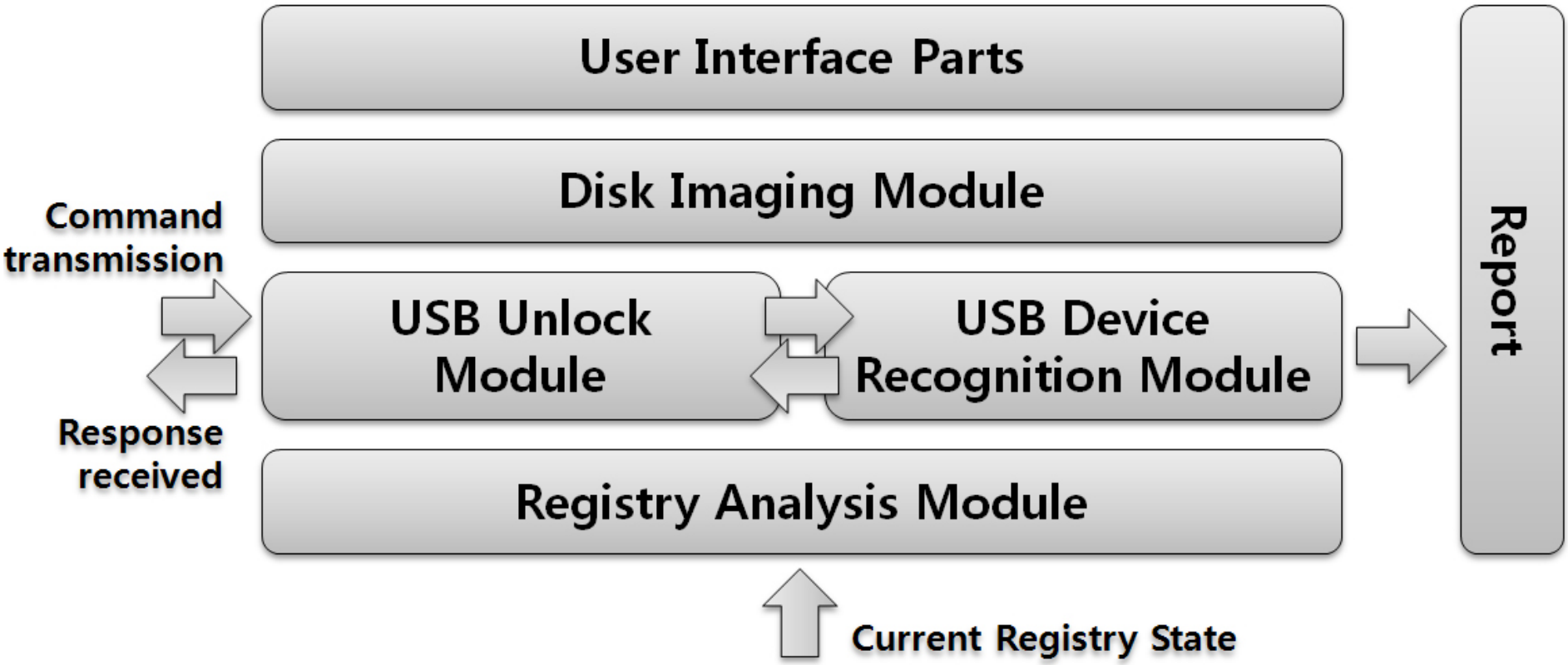
- **Set Authorization Command**
  - 0xFF570000 00000000 0000 with [*HASHINFO*]
- **Unlock Command**
  - 0xFF540000 00000000 0000 with [*HASHINFO*]

Detoured around by various USB controllers

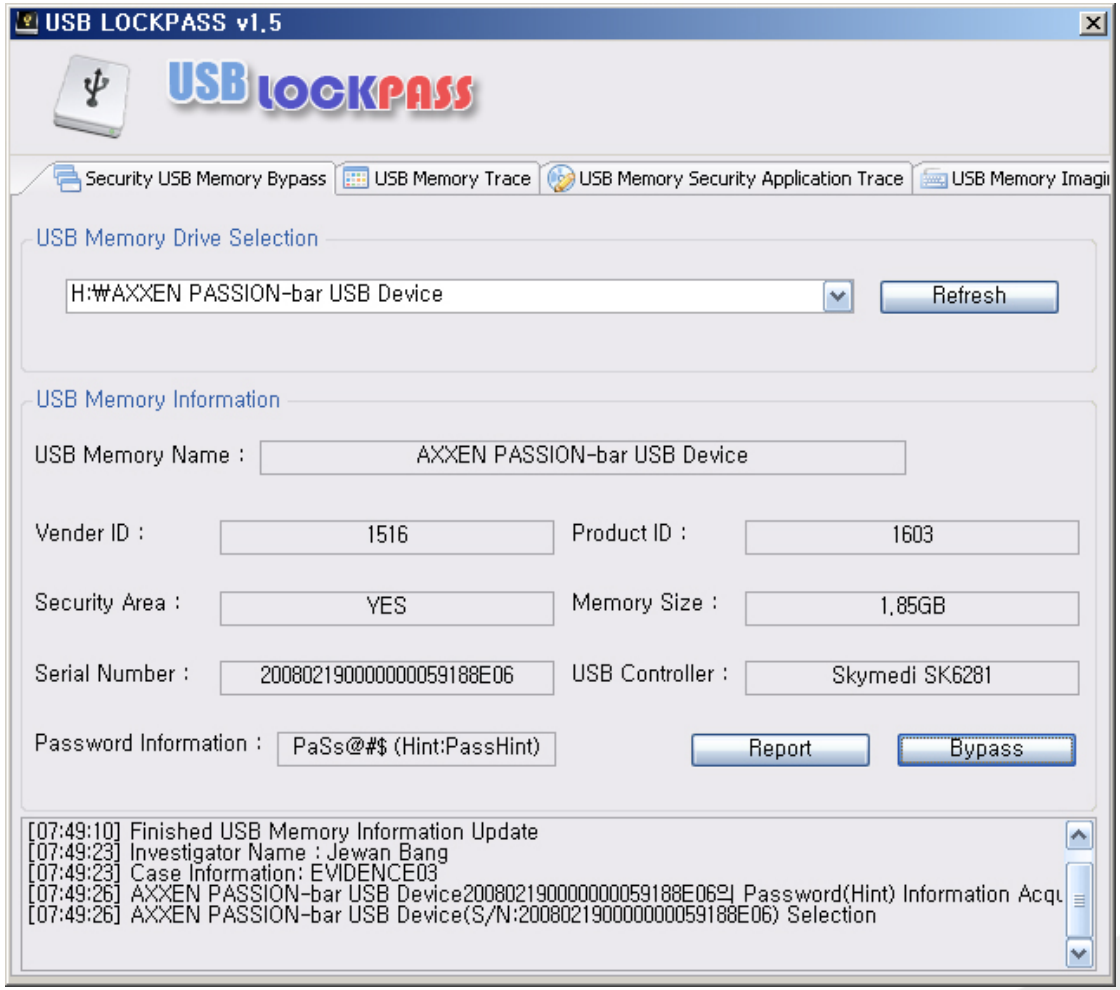
- ✓ **Security function can be detoured around by various USB controllers**

Controller	Security configuration condition checking	Whether password is obtained	Whether security certification can be detoured around
USBest UT163	O	O	O
Skymedi SK6281	O	O	O
SMI SM321 ~ SM325	O	O	O
Phison PS2136	O	X	O
USBest UT165	O	O	X
Skymedi SK6211	O	O	O
AlcorMicro AU6983	O	X	O
Sandisk Cruzer Contour	O	X	O
Toshiba	O	X	O

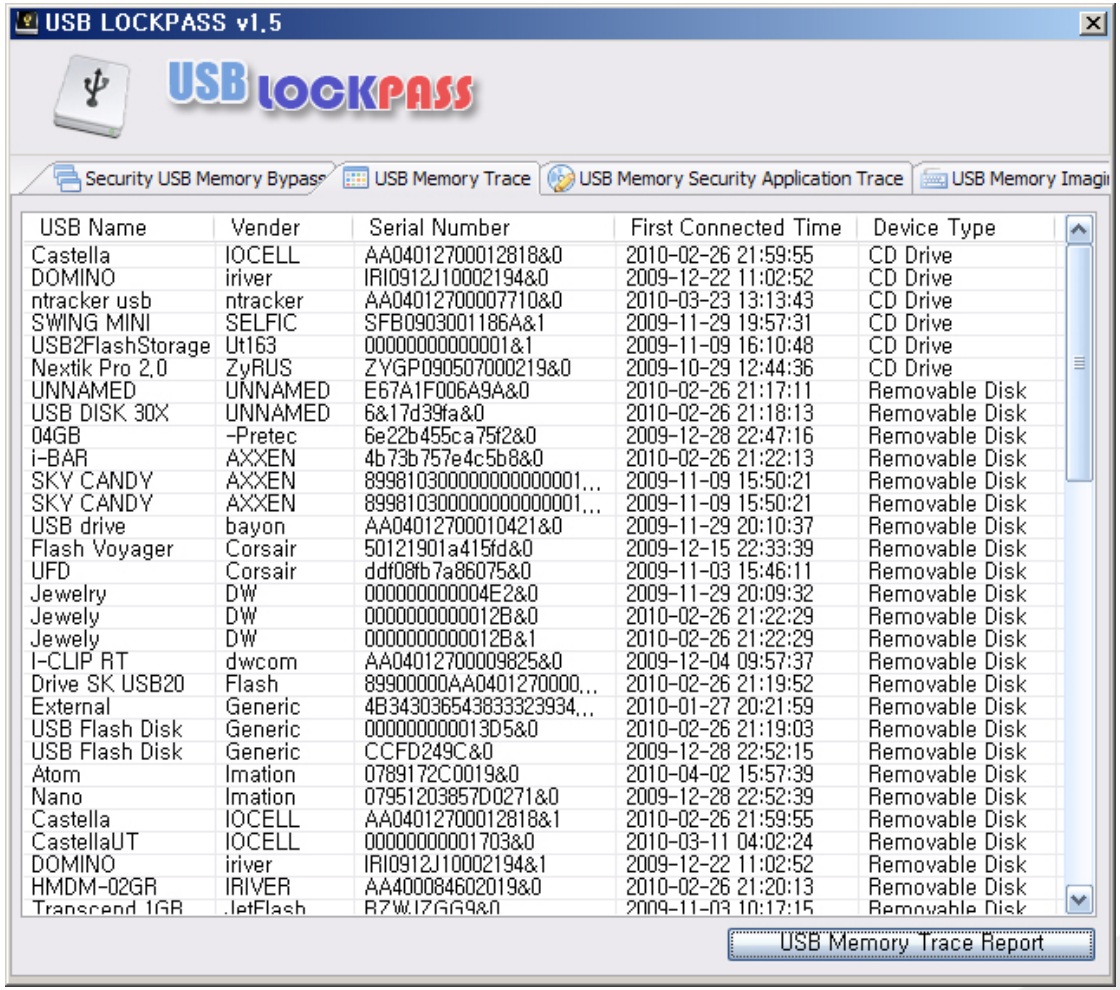
Structure of the Secure USB bypassing tool



Secure USB Drive Bypass

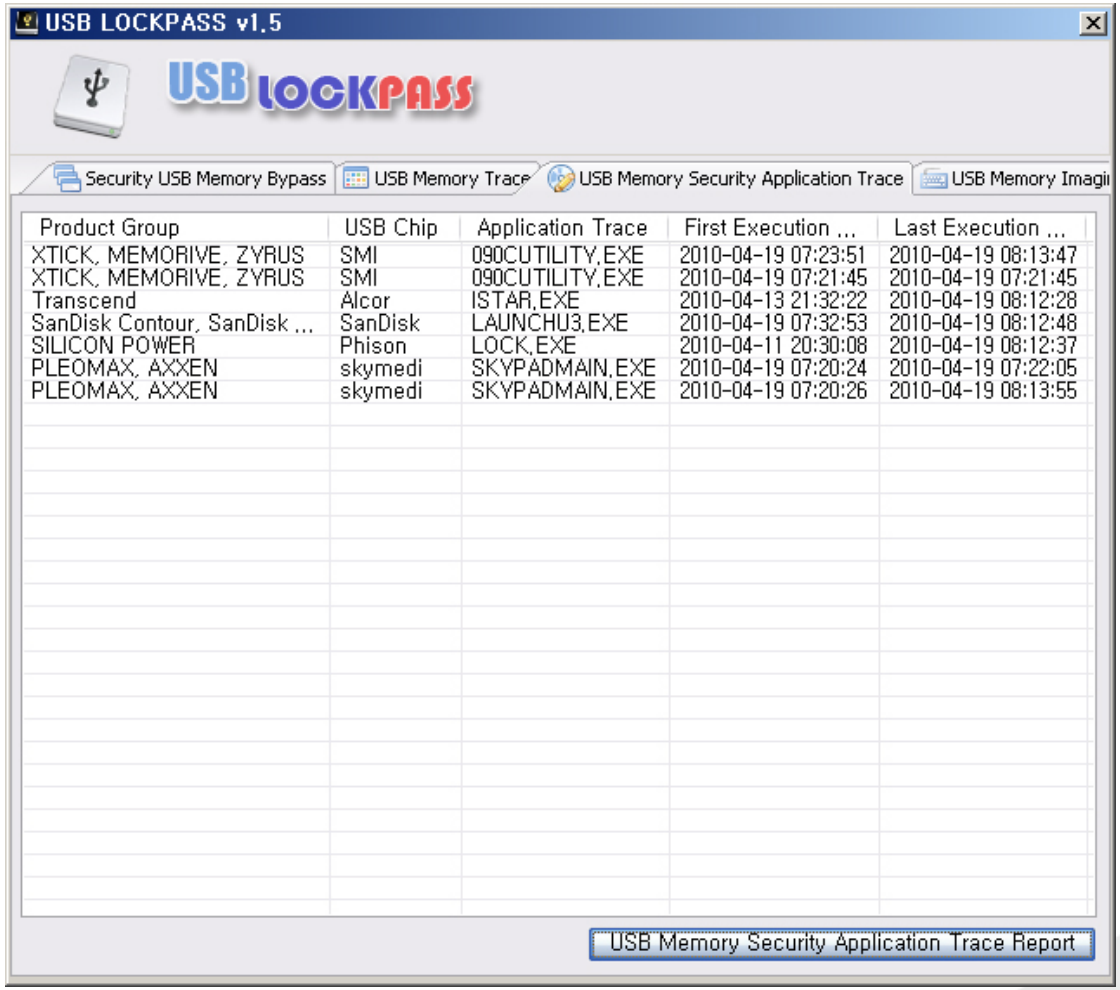


USB Drive Trace



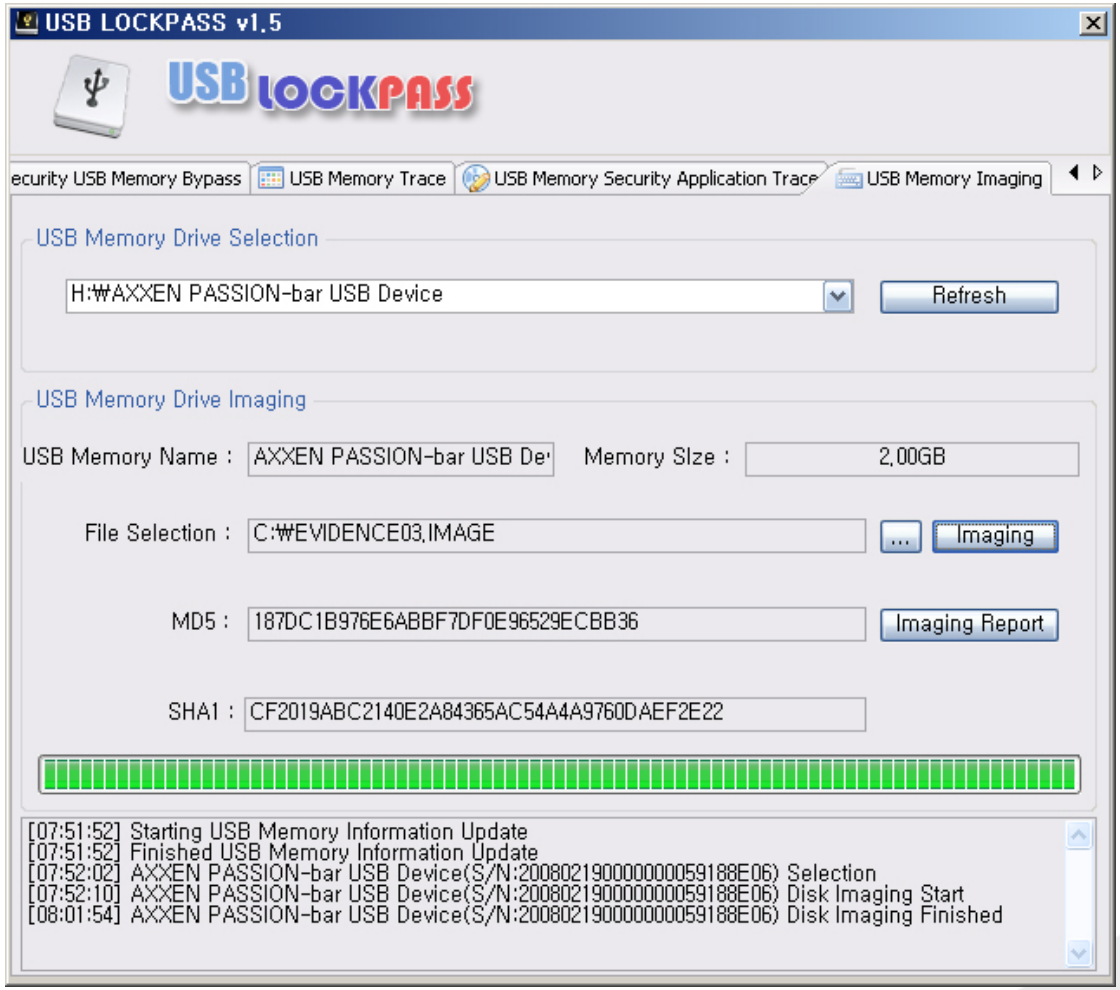
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USBSTOR

USB Drive Security Application Trace



%systemroot%\Prefetch*.pf

USB Drive Imaging



Conclusions

- ✓ **Secure USB ByPassing tool**
  - Most secure USB Drive access is controlled, based on its Controller
  - However, it does not send authentication information but simply send s 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 bypass ing methods
  - Hardware(Encryption chip) based encryption and USB analysis

Thank you for attention

jwbang@korea.ac.kr