USB Forensics and Pentesting

Dr. Phil Polstra
@ppolstra
PhD, CISSP, CEH

http://philpolstra.com

Dr. Phil Polstra
PhD, CISSP, CEH
@ppolstra
http://philpolstra.com

USB Mass Storage: Communication

USBMS Communication

- Bulk-Only Mass Storage (aka BBB or USBMS) protocol used
- All communications use bulk endpoints
- Three phases: CBW, data-transport (optional), CSW
- Commands sent to drive using a Command Block Wrapper (CBW)
- CBW contains Command Block (CB) with actual command
- Nearly all drives use a (reduced) SCSI command set
- Commands requiring data transport will send/receive on bulk endpoints
- All transactions are terminated by a Command Status Wrapper (CSW)

Command Block Wrapper

```
typedef struct _USB_MSI_CBW {
    unsigned long dCBWSignature; //0x43425355
    unsigned long dCBWTag; // associates CBW with CSW
    unsigned long dCBWDataTransferLength; // bytes
send
    unsigned char bCBWFlags; // bit 7 0=OUT, 1=IN rest
0
    unsigned char bCBWLUN; // logical unit number
    unsigned char bCBWCBLength; // 3 hi bits zero
    unsigned char bCBWCB[16]; // the actual command
                                        block (>= 6 bytes)
} USB_MSI_CBW;
```

Command Block

- 6-16 bytes depending on command
- Command is first byte
- Format Unit Example:

```
typedef struct _CB_FORMAT_UNIT {
   unsigned char OperationCode; //must be 0x04
   unsigned char LUN:3; // logical unit number (usually zero)
   unsigned char FmtData:1; // if 1, extra parameters follow
com
   unsigned char CmpLst:1; // 0/1=partial/complete defect list
   unsigned char DefectListFormat:3; //000 = 32-bit LBAs
   unsigned char VendorSpecific; //vendor specific code
   unsigned short Interleave; //0x0000 = use vendor default
   unsigned char Control;
} CB_FORMAT_UNIT;
```

Command Block Example

Read (10) Example:

```
typedef struct _CB_READ10 {
   unsigned char OperationCode; //must be 0x28
   unsigned char RelativeAddress:1; // normally 0
   unsigned char Resv:2;
   unsigned char FUA:1; // 1=force unit access, no cache
   unsigned char DPO:1; // 1=disable page out
   unsigned char LUN:3; //logical unit number
   unsigned long LBA; //logical block address (sector
number)
   unsigned char Reserved;
   unsigned short TransferLength;
   unsigned char Control;
} CB_READ10;
```

Common Commands

Some Common SCSI Commands:

FORMAT_UNIT=0x4, //req
INQUIRY=0x12, //req
MODE_SELECT6=0x15,
MODE_SELECT10=0x55,
MODE_SENSE6=0x1A,
MODE_SENSE10=0x5A,
READ6=0x08, //req
READ10=0x28, //req
READ12=0xA8,
READ_CAPACITY10=0x25, //req
READ_FORMAT_CAPACITIES=0x23,
REPORT_LUNS=0xA0, //req
REQUEST_SENSE=0x03, //req
SEND_DIAGNOSTIC=0x1D, //req
START_STOP_UNIT=0x1B,
SYNCHRONIZE_CACHE10=0x35,
TEST_UNIT_READ=0x00, //req
VERIFY10=0x2F,
WRITE6=0x0A, //req
WRITE10=0x2A,
WRITE12=0xAA

Command Status Wrapper

Read Sense command can be used for details on failed operations

```
typedef struct _USB_MSI_CSW {
   unsigned long dCSWSignature; //0x53425355
   unsigned long dCSWTag; // associate CB
   unsigned long dCSWDataResidue; //
         difference between requested data and
         actual
   unsigned char bCSWStatus; //00=pass,
          01=fail, 02=phase error, reset
} USB_MSI_CSW;
```

Command Demo