Entwicklung eines Treibers für einen Filmscanner mittels USB-Sniffing und Reverse Engineering

Hugo Platzer

Reflecta CrystalScan 7200

- Für Kleinbilddias / -negative
- Per USB verbunden
- Software nur für Windows / Mac
- Versuch, einen Linux-Treiber zu entwickeln ohne entsprechende Dokumentation

Reverse Engineering

- Prozess des „Engineering“ (von der Spezifikation zum Produkt) in umgekehrter Richtung
- Versuch, aus für den Konsumenten verfügbaren Daten (Maschinencode, Mitlauschen an Schnittstellen) Protokolle rekonstruieren
- Rechtliche Grauzone
- Um Einverständnis gebeten: Hersteller war kooperativ

Der USB-Standard

- ein Anschluss für alle Klassen von Geräten
- Alle Kommunikation geht vom Host aus
- Verschiedene Übertragungsmodi (Control, Bulk, Interrupt, Isochronous)

USB-Sniffing

- Mitschneiden der Kommunikation zwischen Gerät und Windows-Software
- Kernelmodul `usbmon`
  - Zugang zu vom Linux-Kernel abgearbeiteten USB-Transfers
  - Schwierigkeiten bei langer Payload
- Wireshark
  - Netzwerk-Sniffer, der sich auch für USB eignet
  - sowohl zur Aufzeichnung als auch Analyse
  - Deaktivierung aller Protokolle außer USB
- VirtualBox
  - Windows in virtueller Maschine unter Linux ausführen
  - USB-Passthrough gibt Windows Zugang zum Scanner

usbmon: unvollständige Payload

- Bei großen Paketen wird Payload nach 60KB abgeschnitten
- visuell: Risse im rekonstruierten Bild
- gelöst durch einfachen Kernel-Patch

Analyse der Aufzeichnung

- Versuche, Bilddaten aus Aufzeichnung zu rekonstruieren
- Beispiel: Rohdaten der Bulk-Transfers: Schließen auf Little-Endian 16bit Pixelwerte
- Ermitteln von: Offset, Zeilenlänge, Farbkanäle (Interleaving), Offsets

Ansteuern des Scanners

- Grundidee: aufgezeichnete Befehle zum Gerät wieder abspielen, eingehende Daten speichern
- Kommunikation läuft nach gewissen Mustern ab
- Warten auch wichtig: Zeitdiagramm
- Welche Bytes haben welche Funktion?
  - Wiederhole Scan mit jeweils einem geänderten Parameter
  - Beispiel: Auflösung, Farbmodus, Scanbereich

Bildverarbeitung

- Helligkeitsunterschiede pro Spalte ausgleichen
- Gammakorrektur, Wertebereich, Farbbalance
- Staub- / Kratzerkorrektur (Digital ICE, Inpainting)

Ausblick: SANE

- Das Linux-Scannerframework
- hat Treiber für CrystalScan 7200, funktioniert aber nicht
- meine Software in SANE integrieren

Live-Demo