HDMI-WALK: Attacking HDMI Distribution Networks via Consumer Electronics Control Protocol

Luis C. Puche Rondon, M.S.
Leonardo Babun, M.S.
Kemal Akkaya, Ph.D.
A. Selcuk Uluagac, Ph.D.

Annual Computer Security Applications Conference (ACSAC)
Session: Embedded Security
San Juan, Puerto Rico. December 13, 2019
Outline

- Introduction
  - A/V, HDMI, CEC
  - HDMI Distributions
  - CEC Propagation
- HDMI-Walk
  - Overview
  - Architecture and Threat Model
- Attack Implementation
- Concluding Remarks
Introduction: A/V

- Audio Video devices exist everywhere.
- Close to 10 billion HDMI devices distributed and sold worldwide.
- Push for integration created the Consumer Electronics Control Protocol (CEC).
HDMI Distributions

- Distribution of HDMI signal is not limited to simple 1-to-1 communication.
- Devices can be interconnected with switches, hubs and splitters.
CEC Introduction

- Consumer Electronics Control (CEC) was created for control as a bus architecture.

- Under different trade names:
  - Anynet+ (Samsung)
  - AquosLink (Sharp)
  - BRAVIA Link (Sony)
  - CEC (Hitachi)
  - CEC-LINK (Toshiba)
  - SimpLink (LG)
  - VieraLink (Panasonic)
  - Easylink (Philips)

  And Many others…
CEC Propagation

- Propagation of CEC, not the same as CEC control. A device may propagate without allowing control.
- Propagation capabilities of devices is often not documented.
- Example: A non-CEC capable TV allows communication between two devices connected to the TV ports.
Threat Model

- Purpose is to use HDMI-Walk to leverage CEC to manipulate, control and cause undesired operation in HDMI distributions.
- Mallory inserts (or compromises) an HDMI device within a distribution and communicates to it.
Threats

- **Malicious Scanning:** Mallory, scans an HDMI distribution to gather information about devices.
- **Eavesdropping:** Mallory, using the CEC distribution to eavesdrop on information while not being present.
- **Information Theft:** For instance, an attacker leveraging CEC communication to transfer captured audio through HDMI to their device.
- **Facilitation of Attacks:** Such as removing time constraints by using CEC to transfer Wireless Handshake at a later date.
- **Denial of Service:** Mallory disrupts the availability of a system using input change commands.
HDMI-WALK: Architecture

- HDMI-Walk is the concept of leveraging CEC communication and propagation of CEC signals over HDMI devices to perform attacks.

- There are four modules:
Testbed and Software

- Created an HDMI testbed with common devices.
- Used a Raspberry Pis as the attacker devices.

<table>
<thead>
<tr>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharp Smart TV.</td>
</tr>
<tr>
<td>Samsung UN26EH4000F</td>
</tr>
<tr>
<td>Monoprice Blackbird 3x1 HDMI Switch</td>
</tr>
<tr>
<td>Wyrestorm - 1x4 HDMI 1.3b Splitter</td>
</tr>
<tr>
<td>Chromecast NC2-6A5</td>
</tr>
<tr>
<td>Sony STR-ZA2100ES</td>
</tr>
<tr>
<td>Raspberry 3 Model B x2</td>
</tr>
<tr>
<td>TP-Link TL-WN722N V1 Adapter</td>
</tr>
<tr>
<td>Motorola G5 Plus Phone</td>
</tr>
<tr>
<td>TP-Link TL-WR841N Router</td>
</tr>
</tbody>
</table>
Software Modules

- Implemented various software modules with open-source tools.
  - CEC File I/O
  - CEC SND/RCV
  - CEC Scanner
  - Microphone Module
  - CEC Sniffer
  - Wireless Module
  - Remote Access Module

<table>
<thead>
<tr>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pulse Eight LibCEC 4.0.2</td>
</tr>
<tr>
<td>Python 3.6.1</td>
</tr>
<tr>
<td>Aircrack-ng 1.2-rc4</td>
</tr>
<tr>
<td>Eclipse IDE</td>
</tr>
<tr>
<td>PyAudio v0.2.11</td>
</tr>
<tr>
<td>Jersey JAX-RS</td>
</tr>
<tr>
<td>Raspbian Version 9</td>
</tr>
<tr>
<td>Swagger.io</td>
</tr>
<tr>
<td>Java 1.8</td>
</tr>
<tr>
<td>AWS Elastic Beanstalk</td>
</tr>
</tbody>
</table>
### Attack 1: Topology Inference

- Implemented HDMI-Walk to gather information on all the devices in an HDMI distribution.
  - Information gathering, ‘walking’ over the distribution.
  - Leakage of information either to a remote or a local client.

<table>
<thead>
<tr>
<th>Info</th>
<th>Addr 00</th>
<th>Addr 01</th>
<th>Addr 02</th>
<th>Addr 04</th>
<th>Addr 05</th>
</tr>
</thead>
<tbody>
<tr>
<td>P. Addr</td>
<td>0.0.0.0</td>
<td>f.f.f.f</td>
<td>4.0.0.0</td>
<td>3.0.0.0</td>
<td>1.0.0.0</td>
</tr>
<tr>
<td>Active</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Vendor</td>
<td>Unk</td>
<td>Unk</td>
<td>Pulse-Eight</td>
<td>Google</td>
<td>Sony</td>
</tr>
<tr>
<td>OSD Str</td>
<td>TV</td>
<td>RPI</td>
<td>CECTestr</td>
<td>Chromecast</td>
<td>STR-ZA2100</td>
</tr>
<tr>
<td>CEC Ver</td>
<td>1.4</td>
<td>1.3a</td>
<td>1.4</td>
<td>1.4</td>
<td>1.4</td>
</tr>
<tr>
<td>Pow Status</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
<td>Standby</td>
</tr>
<tr>
<td>Language</td>
<td>Eng</td>
<td>Eng</td>
<td>Eng</td>
<td>Unk</td>
<td>Unk</td>
</tr>
</tbody>
</table>
Attack 2: CEC-Eavesdropping

- Implemented to demonstrate eavesdropping with CEC.
  - Insertion of mic-capable listener into a distribution.
  - Activation of the microphone and recording from client to listener.
  - Client requests the audio data, which is then serialized and transferred through CEC to the client.
This attack was successful, we managed to record and transfer small audio data files through CEC from listener to client.
Attack 3: WPA/WPA2 Handshake

- Aim to facilitate WPA/WPA2 Handshake theft attacks by removing attack limitations.
  - Attack listener is placed in a location where it can capture secure network communication.
  - Client triggers the listeners wireless attack module. This activates sniffing for a specific BSSID. All in passive monitoring.
  - Retrieval: after a given amount of time, the handshake can be retrieved by the attacker.
Attack 3: WPA/WPA2 Handshake

- Local CEC triggers proved successful in initiating the scanning without direct access to the listener device.
- The handshake packet was then captured, cleaned, and transferred with HDMI File I/O to the client.
Attack 4: Targeted Device Attack

- In this attack, we target a specific device and cause undesired operation.
  - The listener awaits for power state change commands from a specified device (a TV).
  - Once power state change is detected (commands ‘84’, ‘87’ and ‘80’), the listener automatically sends a shutoff command.

```plaintext
Disruption Mode Active: True
Welcome to Listener-mode, enter:
  q - quit, d - disrupt mode
Listener Mode (Q to exit): Logger: >> 0f:84:00:00:00:00:
Power on detected! Sending shutoff command!
Sent 36
[command received] 84:00:00:00
Logger: >> 0f:87:1f:00:08
Power on detected! Sending shutoff command!
Sent 36
```
Attack 5: Display Broadcast DoS

- These attacks demonstrate abuse of broadcast functions to cause a DoS state in a display.
  - Once active, the listener begins broadcasting input change commands over the distribution, rendering compatible devices unusable.
Conclusions and Future Works

- HDMI devices are everywhere.
- HDMI-Walk demonstrates that CEC may be leveraged to perform attacks.
- A variety of attacks can be performed through CEC with open source tools and relatively easy implementation.

- Develop security mechanisms for CEC.
- Find vendor-specific vulnerabilities accessible through the CEC protocol.
This work is partially supported by the U.S. National Science Foundation under awards: NSF-CAREER-CNS-1453647 and NSF-1663051.
Thank You!

Name: Luis Puche Rondon

Email: lpuch002@fiu.edu

Personal Web: http://myweb.fiu.edu/lpuch002/

Lab Web: https://csl.fiu.edu/