What the HEC? Security implications of HDMI Ethernet Channel and other related protocols

Andy Davis, Research Director NCC Group
UK Offices
Manchester - Head Office
Cheltenham
Edinburgh
Leatherhead
London
Thame

North American Offices
San Francisco
Atlanta
New York
Seattle

Australian Offices
Sydney

European Offices
Amsterdam - Netherlands
Munich – Germany
Zurich - Switzerland
Agenda

• Why am I talking about video interfaces?
• What does HDMI bring with it?
• The CEC protocol – enabling the user to expend as little energy as possible
• CECSTeR – The CEC Security Testing Resource
• The HEC protocol – you mean I get network access too?
• HEC internals and potential security issues
• Conclusion
Why am I talking about video interfaces?

- It all started with a BlackBerry PlayBook research project...
- I was investigating USB security at the time (green interface)

- What other ports are available?
- A power connector (blue interface) – probably not that exciting…
- Hmm…microHDMI – what can I do with that? (red interface)
HDMI is an output isn’t it?

Well…yes and no

• Video out
• Audio out
• Display identification and capability advertisement in via EDID
• Remote control via CEC in and out
• Network data via HEC in and out
• Encryption and authentication data via HDCP and DPCP in and out
HDMI - High-Definition Multimedia Interface

- [http://www.hdmi.org/manufacturer/specification.aspx](http://www.hdmi.org/manufacturer/specification.aspx) (HDMI adopters only)
- Transmits encrypted uncompressed digital video and audio data using TMDS (Transition-Minimised Differential Signalling)
- Supports Enhanced DDC for display identification and capability advertisement
- Also it introduces a number of new technologies, which are potentially interesting from a security perspective; these include:
  - CEC – Consumer Electronics Control
  - CDC – Capability Discovery and Control
  - HDCP - High-bandwidth Digital Content Protection
  - HEC – HDMI Ethernet Channel
CEC – I’ve not heard of that before…

Trade names for CEC are:

- BRAVIA Link and BRAVIA Sync (Sony)
- VIERA Link, HDAVI Control, EZ-Sync (Panasonic)
- Anynet+ (Samsung)
- Aquos Link (Sharp)
- SimpLink (LG)
- EasyLink (Philips)

etc…
CEC - Consumer Electronics Control

Purpose:
• Control two or more HDMI devices using a single remote control
• Devices can control each other without user-intervention.

Physical:
• The architecture of CEC is an inverted tree
• One-wire bidirectional serial bus (AV.link)

Logical:
• Up to ten AV devices can be connected and the topology of a connected system is auto-discovered by the protocol.
Supported CEC commands

- One Touch Play, System Standby
- Pre-set Transfer, One Touch Record
- Timer Programming, System Information
- Deck Control, Tuner Control
- OSD Display, Device Menu Control
- Routing Control, Remote Control Pass
- Device OSD Name Transfer, System Audio Control
The CEC protocol

**CEC Block layout:**

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>-</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information bits</td>
<td>EOM</td>
<td>ACK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CEC Header block:**

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>-</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source logical address</td>
<td>Destination logical address</td>
<td>EOM</td>
<td>ACK</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CEC Message:**

- Messages are either Directed or Broadcast
- Logical addresses are 0x0 – 0xF (0 always TV, F always broadcast)
- Physical addresses x.x.x.x (TV = 0.0.0.0)
Can we fuzz CEC?

- Feature rich protocol - could potentially yield some interesting security vulnerabilities in different implementations
- Publicly available Arduino - CEC interface circuit:
  
  - USB-CEC Adapter from Pulse Eight:
  
  ![USB-CEC Adapter from Pulse Eight](image)
  
  - USB-CEC Bridge from RainShadow Tech:
  
  ![USB-CEC Bridge from RainShadow Tech](image)
Introducing **CECSTeR**

- **Consumer Electronics Control Security Testing Resource**
- Download it here - [http://tinyurl.com/ncctools](http://tinyurl.com/ncctools)
- Supports CEC and CDC (more on that later)
- Capture and display traffic
- Send arbitrary commands
- Fuzz the protocols
- Time for a demo…
HDMI Connectivity for the demo

- Sony TV – 0.0.0.0
- HDMI A/V Switch – 1.0.0.0
- CECSTeR – 2.0.0.0
- Sony PS3 – 1.1.0.0
- BlackBerry PlayBook – 1.2.0.0
What are the fuzzer results?

My CEC targets:
• Sony PS3 – no results
• Panasonic Blu-ray player (DMP-BD45) – “random” lockups
• BlackBerry PlayBook (very limited CEC functionality) - no results
• XBMC (using Pulse-eight USB-CEC Adapter) – Permanent DoS
  • It “bricked” the Pulse-eight adapter!
• Potentially interesting commands include:
  • “Vendor command” – Opcode 0x89
  • “Set OSD string” – opcode 0x64
  • “Set OSD name” – opcode 0x47
  • “CDC command” – opcode 0xF8
HEC - HDMI Ethernet Channel

• Introduced in HDMI v1.4 (latest version is 1.4a)

• Consolidates video, audio, and data streams into a single HDMI cable

• The primary intention is to reduce the amount of cables required to connect AV devices together.

• Uses CDC (Capability Discovery and Control) to control Ethernet channels
CDC (Capability Discovery and Control)

CDC is used to:
- Discover potential HDMI Ethernet channels
- Activate and deactivate channels
- Communicate status of channels

CDC messages are sent with the CEC “CDC Message” (0xF8) opcode
All CDC messages are sent to the CEC logical broadcast address (0xF)

CDC message format:

<table>
<thead>
<tr>
<th>CEC Header Block</th>
<th>CEC Opcode Block (0xF8)</th>
<th>Initiator Physical Addr</th>
<th>CDC Opcode Block</th>
<th>CDC Operand Blocks</th>
</tr>
</thead>
</table>
HEC (CDC) Messages

The following messages are used for Capability Discovery and Control:

- `<CDC_HEC_InquireState>`
- `<CDC_HEC_ReportState>`
- `<CDC_HEC_SetState>`
- `<CDC_HEC_RequestDeactivation>`
- `<CDC_HEC_NotifyAlive>`
- `<CDC_HEC_Discover>`
- `<CDC_HEC_SetStateAdjacent>`
HEC potential combinations

Possible HECs within a certain HDMI network:

(referenced from HDMI specification v1.4a)
HEC States

• PHEC (Potential HDMI Ethernet Channel) – part of a PHEC if at least one HDMI connection is HEC capable

• VHEC (Verified HDMI Ethernet Channel) – part of a VHEC after CDC has confirmed HEC capability of all devices in a PHEC via a <CDC_HEC_Discover> message

• AHEC (Active HDMI Ethernet Channel) – part of an AHEC after activation of all devices in a VHEC via a <CDC_HEC_SetState> message
Network loop prevention

- Routing loops such as shown here are managed using RSTP (Rapid Spanning Tree Protocol)
Network loop prevention

- Routing loops such as shown here are managed using RSTP (Rapid Spanning Tree Protocol)
- HEC2 is disabled to remove the loop
Network loop prevention

- Routing loops such as shown here are managed using RSTP (Rapid Spanning Tree Protocol)
- HEC2 is disabled to remove the loop
- If HEC1 link is broken, HEC2 is restored
Queue control

- Devices in a HEC network are expected to prioritise traffic. Time sensitive application traffic should be forwarded with higher priority than activities such as file downloads:
  - On-line gaming
  - Video
  - VoIP
- This is achieved using a 3 bit priority field in VLAN tags
This is all very interesting, but...

- I’m never going to be pentesting a home AV network!
- HDMI connectors are appearing on new laptops and PCs – soon these protocols will be implemented in all the major operating systems

- If I found a bug in an HDMI enabled TV, so what?
- Plasma/LCD TVs are becoming part of the corporate network infrastructure

- So how could HDMI protocols affect corporate users?
HEC Risk #1 – Corporate boundary breach

- Network-enabled projectors and TVs could circumvent corporate security boundaries
- Will users be aware of the capabilities of this technology within their own devices?
HEC Risk #2 – Endpoint Protection Circumvention

- HDMI could be used to connect unauthorised network-enabled devices to the corporate network

- Endpoint Protection systems (unless they are HEC-aware) will be unable to detect this

- Unauthorised devices could introduce malware or exfiltrate sensitive data
HEC Risk #3 – Unauthorised Network Extension

- HDMI could be used to create an unauthorised extension to the corporate network
- This “private network” would not be visible to corporate network monitoring tool / NIDS devices
Testing HDMI Ethernet Channel

Have I tested any HEC-enabled devices?
no…
The only device I could find that supports HEC is the T+A Blu-ray receiver:

It costs £6000!
Another corporate HDMI security risk

Remember hardware-based key loggers?

Here’s an HDMI video logger - VideoGhost:

  - “2GB storage”
  - “7 year battery life”

This is potentially much more powerful than a key logger!
Conclusions

- As users demand more and more “seamless” functionality in a plug-and-play world there will be a greater need for bi-directional data to be flowing in A/V links between devices.
- HDMI Ethernet Channel could have a major impact on corporate security, but the technology is still very new and largely unsupported.
- As well as checking for hardware key loggers you should now also be checking for video loggers connected to your corporate workstations.
- Before long every laptop will have an HDMI port and they will all support CEC, CDC and HEC!
Questions?

Andy Davis, Research Director NCC Group
andy.davis@nccgroup.com