Black Hat Europe 2012

March 14th 2012

Andy Davis

Research Director

Telephone: +44 (0) 208 401 0070
e-mail: andy.davis@ngssecure.com

NCC Group Plc, Manchester Technology Centre, Oxford Road, Manchester M1 7EF **www.nccgroup.com**

ngssecure
an ncc group company

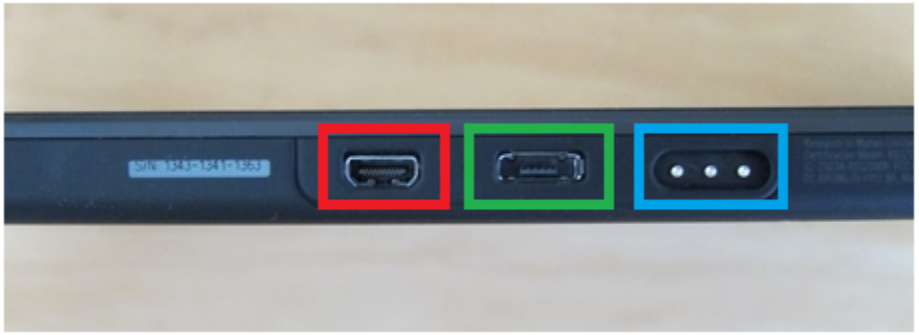
Agenda

- **Why am I talking about video interfaces?**
- Video interface history and overview
- A whole new world of acronyms – DDC and EDID
- The effects of KVM solutions
- Fuzzing EDID data
- CEC - Consumer Electronics Control
- HEC - HDMI Ethernet Channel
- HDCP - High-bandwidth Digital Content Protection
- Conclusion

ngssecure
an ncc group company

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)
- Hmm…microHDMI – what can I do with that? (red interface)

ngssecure
an ncc group company

HDMI is an output isn't it?

Well…yes and no

- Video **out**
- Audio **out**
- Display identification and capability advertisement **in**
- 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**

ngssecure
an ncc group company

Agenda

- Why am I talking about video interfaces?
- **Video interface history and overview**
- A whole new world of acronyms – DDC and EDID
- The effects of KVM solutions
- Fuzzing EDID data
- CEC - Consumer Electronics Control
- HEC - HDMI Ethernet Channel
- HDCP - High-bandwidth Digital Content Protection
- Conclusion

ngssecure
an ncc group company

Video interface history and overview

There have been many display standards developed over the years stretching back to the 1970's and probably earlier. Video display standards typically include information such as:

- Screen resolutions
- Colour modes and palette
- Refresh rates

Video interface standards are more likely to define:

- Transmission protocols
- Compression techniques
- Encryption schemes

Before discussing the security implications of display technologies lets discuss the main video and interface standards that are still in use today.

ngssecure
an ncc group company

VGA – Video Graphics Array

- The term VGA (Video Graphics Array) originally related to the display technology implemented on IBM PCs in the late 1980's.
- The name has become synonymous with both the video protocol standard and the physical connector type. Hence people talk about "VGA connectors" meaning the 15-pin D-type interface that everyone is familiar with:

- Analogue video standard – the separate Red, Green and Blue analogue video signals plus horizontal and vertical sync.

- Four pins were originally "reserved" to provide monitor identification data to the host machine; Only three monitor types were ever defined.

- The implementation of the VESA (Video Electronics Standards Association) DDC (Display Data Channel)standard changed all this (more on DDC later).

ngssecure
an ncc group company

DVI – Digital Visual Interface

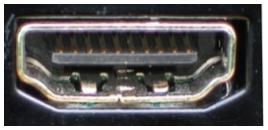
- DVI is a digital interface standard.
- Developed by the Digital Display Working Group (DDWG) to replace the VGA interface, which is viewed as an outdated legacy standard.

- The uncompressed video signal data is transmitted using TMDS (Transition Minimised Differential Signalling)to reduce noise.
- For backward-compatibility DVI also includes analogue pins to transmit R,G,B and sync data (a la VGA).
- From a security perspective, the important thing is that DVI also supports DDC for display identification and capability advertisement.

ngssecure
an ncc group company

HDMI - High-Definition Multimedia Interface

- Most recent well-known video interface standard
- Not only used for in the world of IT, but more commonly in consumer electronics for transmitting video and audio data between devices such as Blu-ray players and flat screen TVs.

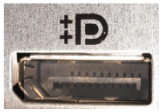


- Transmits encrypted uncompressed digital video and audio data (using TMDS like DVI)
- Supports DDC for display identification and capability advertisement
- Also it introduces a number of new technologies, which are potentially interesting from a security perspective; these include:
  - CEC – Consumer Electronics Control
  - HDCP - High-bandwidth Digital Content Protection
  - HEC – HDMI Ethernet Channel

ngssecure
an ncc group company

DisplayPort

- Developed by VESA to complement HDMI
- Effectively a royalty-free equivalent to HDMI (the HDMI royalty fee is US $0.04 per device and has an annual fee of US$10,000 for high-volume manufacturers).



- Uses packet-based data transmission (like Ethernet)
- Supports DDC and HDCP, in addition to DPCP (DisplayPort Content Protection)
- DisplayPort does not natively support CEC.
- Now, how does security fit into this discussion?

ngssecure
an ncc group company

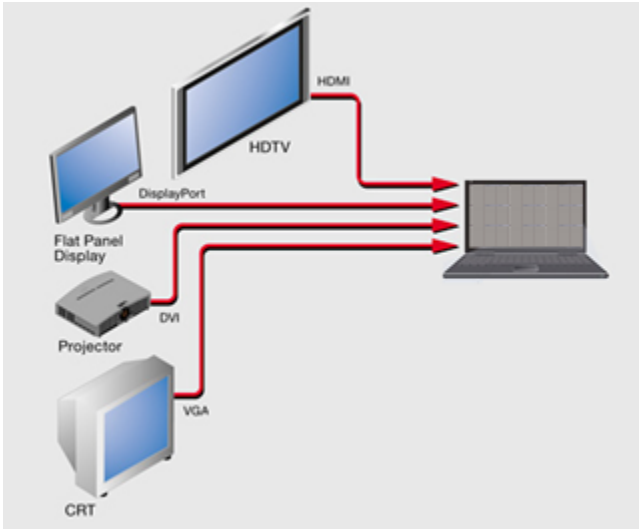
Agenda

- Why am I talking about video interfaces?
- Video interface history and overview
- **A whole new world of acronyms – DDC and EDID**
- The effects of KVM solutions
- Fuzzing EDID data
- CEC - Consumer Electronics Control
- HEC - HDMI Ethernet Channel
- HDCP - High-bandwidth Digital Content Protection
- Conclusion

ngssecure
an ncc group company

DDC - Display Data Channel

- Enables a connected display to communicate its supported display modes to the adapter and to enable the host device to adjust various monitor parameters to ensure the best video output is displayed.
- When a monitor is connected to a PC or a Mac there is a short delay before the video is displayed
- Data is **provided by the display** via DDC to facilitate "plug-and-play"
- Display capabilities are transmitted in a 128-byte block called an EDID (Extended Display Identification Data) structure.



ngssecure
an ncc group company

DDC versions

DDC version 1

- VGA reserved pins (ID0-ID3).
- Used a low-speed unidirectional serial protocol
- Continuously sent the EDID block via ID1 (clocked with the vertical sync)
- Very few vendors adopted DDC1.

DDC version 2

- Various sub-versions of DDC2 – most common is DDC2B
- Uses I^2C (Inter-Integrated Circuit) – two-wire serial protocol widely used for communication between chips on circuit boards.
- ID1 is used for the data line (called SDA)
- ID3 is used for the clock (called SCL)
- +5V used to power up the E^2PROM in the monitor that contains the EDID block so the EDID data can be read even if the monitor is powered off.

- The SDA and SCL pins are present on all the video interfaces discussed in this presentation

ngssecure
an ncc group company

E-DDC - Enhanced Display Data Channel

- [Display vendors] "We need to send more data"…
- E-DDC utilises a segment pointer which enables up to 32K bytes of display information to be retrieved using the E-EDID (Enhanced EDID) standard.
- Standard EDID block is 128 bytes in length, "extension blocks" can be used, each of which are also 128 bytes in length.
- DDC2 allowed one EDID block followed by one extension block
- E-DID up to 32K bytes can be addressed (256 x 128 byte blocks)
- All this data needs to be parsed and parsers = potential vulnerabilities

ngssecure
an ncc group company

The EDID structure – VESA block

- Header
- Vendor and product information
- EDID version and revision
- Video input definition
- Display transfer characteristics
- Colour characteristics
- Established timings
- Standard timing information
- Descriptor blocks (up to four)
  - Detailed Timing Descriptor
  - Other Monitor Descriptor
  - Monitor Range Limits Descriptor
  - Additional White Point Descriptor
- Extension flag
- Checksum

ngssecure
an ncc group company

EDID extension blocks

- EIA/CEA-861 extension
- Video Timing Block Extension
- Display Information Extension
- **Localised String Extension** (potential for buffer overflows)
- Block Map

When extension blocks are used, there are a number of rules that must be followed:

- The VESA block (Block 0) is always required
- At least one CEA extension block is required
- If more than one extension block is used they must all be the same EDID version
- if more than two blocks (including the VESA + CEA blocks) are used then a "Block Map" block is required to define the blocks after the VESA block.

ngssecure
an ncc group company

Localised String Extension

05	05h	String Table Size	28h	00101000
06	06h	String Table Header – UTF 8	00h	00000000
07	07h	Language ID structure – Default Neutral String Table	00h	00000000
08	08h		00h	00000000
09	09h		00h	00000000
10	0Ah		00h	00000000
11	0Bh	Manufacturer Name Data Length	0Eh	00001110
12	0Ch	'D'	44h	01000100
13	0Dh	'i'	69h	01101001
14	0Eh	's'	73h	01110011
15	0Fh	'p'	70h	01110000
16	10h	'l'	6Ch	01101100
17	11h	'a'	61h	01100001
18	12h	'y'	79h	01111001
19	13h	's'	73h	01110011
20	14h	','	2Ch	00101100
21	15h	' '	20h	00100000
22	16h	'I'	49h	01001001
23	17h	'n'	6Eh	01101110
24	18h	'c'	63h	01100011
25	19h	'.'	2Eh	00101110
26	1Ah	Model Name String Length	06h	01100000
27	1Bh	'F'	46h	01000110
28	1Ch	'C'	43h	01000011
29	1Dh	'1'	31h	00110001
30	1Eh	'9'	39h	00111001
31	1Fh	'0'	30h	00110000
32	20h	'1'	31h	00110001
33	21h	Serial Number Data String Length	0Ch	00001100
34	22h	'0'	30h	00110000
35	23h	'3'	33h	00110011

ngssecure
an ncc group company

Agenda

- Why am I talking about video interfaces?
- Video interface history and overview
- A whole new world of acronyms – DDC and EDID
- **The effects of KVM solutions**
- Fuzzing EDID data
- CEC - Consumer Electronics Control
- HEC - HDMI Ethernet Channel
- HDCP - High-bandwidth Digital Content Protection
- Conclusion

ngssecure
an ncc group company

KVM solutions and EDID

EDID data may be adversely affected by KVM based on how the data is processed by the device. There are three possible scenarios:

- No support – the KVM switch cannot handle the data and therefore, the host will not be able to determine any capabilities about the connected display. In some cases the host may assume that a generic monitor is attached and use "safe" settings.

- Fake EDID – the KVM switch generates the EDID data, which may not be appropriate for the connected display

- Pass-through – the KVM switch communicates with the display in order to obtain the EDID data and then sends this on to the host. This can confuse either the host by causing it to re-detect the display or confuse the display resulting in it entering or exiting from power-save mode.

When performing any security testing against the processing of EDID data it is important that no KVM switch is present between the "display" and the target host.

ngssecure
an ncc group company

Agenda

- Why am I talking about video interfaces?
- Video interface history and overview
- A whole new world of acronyms – DDC and EDID
- The effects of KVM solutions
- **Fuzzing EDID data**
- CEC - Consumer Electronics Control
- HEC - HDMI Ethernet Channel
- HDCP - High-bandwidth Digital Content Protection
- Conclusion

ngssecure
an ncc group company

EDID fuzzing

- We will emulate a display device to the extent that "valid" albeit malformed EDID data can be provided to the video display interface on a host via the E-DDC protocol using I^2C.
- Use a microcontroller that supports I^2C - Arduino Duemilanove microcontroller - I^2C supported by default in the "Wire" library.
- Remaining challenges:
  - Replicating the E-DDC protocol
  - Repeatedly emulating the attachment and detachment of the "display"
  - Iterating through the different elements of the EDID blocks

ngssecure
an ncc group company

EDID fuzzing (2)

Replicating the E-DDC protocol
- Minor changes to the "wire" library required
- Disable the internal pull-up resistors (use external ones instead)
- Configure interrupt handlers for incoming messages and when data is required

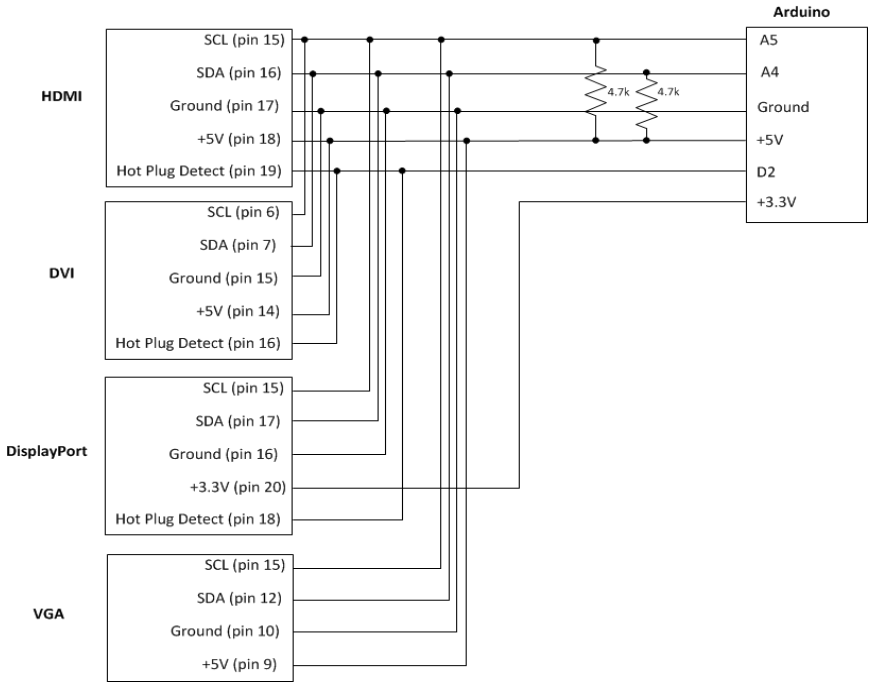
Repeatedly emulating the attachment and detachment of the "display"
- Can easily be achieved with DVI, HDMI and DisplayPort interfaces using the "hotplug" pin
    - +5V - a display is connected low
    - GND - the display has been disconnected.
- The "display" can be virtually unplugged (by the Arduino) and then plugged back in for each fuzz test case (not for VGA yet)

Iterating through the different elements of the EDID blocks
- Easily achieved by looping through any bytes of interest within each EDID block and modifying them based on different test cases.

ngssecure
an ncc group company

Fuzzer hardware and firmware

- The circuit is extremely simple, as each video interface connects directly (via pull-up resistors) to outputs on the Arduino microcontroller



The Arduino firmware can be downloaded from:

http://www.ngssecure.com/research/research-overview/Public-Tools.aspx

ngssecure
an ncc group company

Findings so far

BlackBerry PlayBook

- No luck with buffer overflows associated with the Localised String Extension block
- Fuzzed the VESA block to iterate through every value of every byte in the block whilst monitoring the state of the host
- The PlayBook stopped responding to EDID requests. The code that triggered the bug (which was in an open source library) looked similar to this:

```
for (x = 0; x < 6; y++) {
…
}
```

- "y++" should have been "x++" and as a result caused an infinite loop
- The bug subsequently triggered another bug which killed the system logger daemon

ngssecure
an ncc group company

Findings so far (2)

NVIDIA Windows driver

- Various crashes associated with *nvlddmkm.sys* (the Windows Vista / Windows 7 kernel mode driver)
- These are still being investigated and have not yet been reported to NVIDIA

ngssecure
an ncc group company

Agenda

- Why am I talking about video interfaces?
- Video interface history and overview
- A whole new world of acronyms – DDC and EDID
- The effects of KVM solutions
- Fuzzing EDID data
- **CEC - Consumer Electronics Control**
- HEC - HDMI Ethernet Channel
- HDCP - High-bandwidth Digital Content Protection
- Conclusion

ngssecure
an ncc group company

CEC - Consumer Electronics Control

- Control two or more HDMI devices using a single remote control
- Devices can control each other without user-intervention.
- The architecture of CEC is an inverted tree with the “root” node (display) at the top, “branch” nodes (video switches) below and connected to “leaf” nodes (devices such as Blu-ray players).
- The user should only need to perform the minimal number of tasks
- One-wire bidirectional serial bus (AV.link)
- Up to ten AV devices can be connected and the topology of a connected system is auto-discovered by the protocol.

ngssecure
an ncc group company

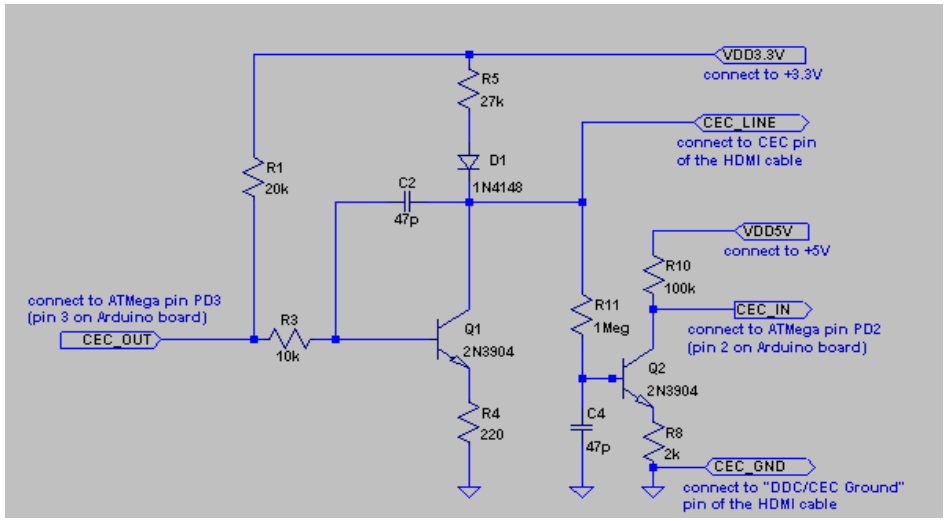
What can CEC do?

- **One Touch Play:** the device will become active source when playback starts
- **System Standby:** switches all connected devices to standby
- **Preset Transfer:** transfers the tuner channel setup to another TV set
- **One Touch Record:** start recording immediately
- **Timer Programming:** allow one device (e.g. a TV set or HTPC) to set the timer programming of another (e.g. a PVR,/DVR or DVD-recorder)
- **System Information:** checks all components for bus addresses and configuration
- **Tuner Control:** control the tuner of another device
- **OSD Display:** use the On Screen Display of the TV set to display text
- **Device Menu Control:** use the menus of another device
- **Routing Control:** control the switching of signal sources
- **Remote Control Pass Through:** pass through remote control commands

ngssecure
an ncc group company

Can we fuzz CEC?

- Feature rich protocol - could potentially yield some interesting security vulnerabilities in different implementations
- Arduino library - http://code.google.com/p/cec-arduino/
- Publicly available Arduino - CEC interface circuit:



- Fuzzer currently in development (using libCEC and the USB-CEC Adapter from Pulse Eight)

ngssecure
an ncc group company

Agenda

- Why am I talking about video interfaces?
- Video interface history and overview
- A whole new world of acronyms – DDC and EDID
- The effects of KVM solutions
- Fuzzing EDID data
- CEC - Consumer Electronics Control
- **HEC - HDMI Ethernet Channel**
- HDCP - High-bandwidth Digital Content Protection
- Conclusion

ngssecure
an ncc group company

HEC - HDMI Ethernet Channel

- Introduced in HDMI v1.4 (latest version)
- Consolidates video, audio, and data streams into a single HDMI cable
- Ethernet channel is physically combined with audio return functionality onto a single pair of wires:
  - Ethernet only
  - Audio only
  - Both simultaneously.
- The primary intention is to reduce the amount of cables required to connect AV devices together.
- More and more AV devices with embedded OS's communicating with the Internet this could result in these mini networks becoming targets for malware which may result in them joining botnets in the future.

ngssecure
an ncc group company

Agenda

- Why am I talking about video interfaces?
- Video interface history and overview
- A whole new world of acronyms – DDC and EDID
- The effects of KVM solutions
- Fuzzing EDID data
- CEC - Consumer Electronics Control
- HEC - HDMI Ethernet Channel
- **HDCP - High-bandwidth Digital Content Protection**
- Conclusion

ngssecure
an ncc group company

HDCP - High-bandwidth Digital Content Protection

- Digital copy protection developed by Intel Corporation
- Designed to prevent encrypted video and audio content from being displayed on unauthorised devices, which could potentially copy the digital content to a non-encrypted form.
- Uses three cryptographic mechanisms:
  - **Authentication** prevents non-licensed devices from receiving content
  - **Encryption** of the data prevents eavesdropping of information and man-in-the-middle attacks
  - **Key revocation** prevents devices that have been compromised from receiving data.
- In September 2010, an HDCP master key that allows for the generation of valid device keys was publicly disclosed which effectively renders the key revocation feature of HDCP useless
- Anecdotal evidence that the key was reverse engineered rather than leaked by using a number of device keys

ngssecure
an ncc group company

Agenda

- Why am I talking about video interfaces?
- Video interface history and overview
- A whole new world of acronyms – DDC and EDID
- The effects of KVM solutions
- Fuzzing EDID data
- CEC - Consumer Electronics Control
- HEC - HDMI Ethernet Channel
- HDCP - High-bandwidth Digital Content Protection
- **Conclusion**

ngssecure
an ncc group company

Conclusions

- Many people are completely unaware that video displays send data which is subsequently processed by the connected device
- 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
- There are vulnerabilities in EDID parsers and potentially CEC parsers too
- Further areas for research for NGS Secure include:
  - The investigation of more creative datasets of EDID block combinations using the Block Map standard
  - Adding more "intelligence" to the EDID fuzzer so that it's more than just a "bit flipper"
  - Identifying a technique to emulate a VGA cable insertion/removal
  - Completing the CEC fuzzing project and using it to test a representative sample of devices
- I've only scratched the surface of these technologies and how they may potentially be attacked

ngssecure
an ncc group company

Questions?

Please complete your feedback forms...

Andy Davis

Research Director

Telephone: +44 (0) 208 401 0070

e-mail: andy.davis@ngssecure.com

NCC Group Plc, Manchester Technology Centre, Oxford Road, Manchester M1 7EF **www.nccgroup.com**

ngssecure

an ncc group company