Digital Investigation 11 (2014) 175–178

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Forensic analysis of smart TV: A current issue and call to arms

Iain Sutherland [a, b, c, *], Huw Read [a, c], Konstantinos Xynos [a]

[a] Faculty of Computing, Engineering and Science, University of South Wales, Treforest, CF37 1DL, UK
[b] ECU Security Research Institute, Perth, Australia
[c] Noroff University College, Norway

ARTICLE INFO

Article history:
Available online 27 June 2014

Keywords:
Smart television
Embedded device
Forensics
Linux
Android

ABSTRACT

A number of new entertainment systems have appeared on the market that have embedded computing capabilities. Smart Televisions have the ability to connect to networks, browse the web, purchase applications and play games. Early versions were based on proprietary operating systems; newer versions released from 2012 are based on existing operating systems such as Linux and Android. The question arises as to what sort of challenges and opportunities they present to the forensics examiner. Are these new platforms or simply new varieties of existing forms of devices? What data do they retain and how easy is it to access this data? This paper explores this as a future forensic need and asks if we are missing potential sources of forensic data and to what degree we are ready to process these systems as part of an investigation.

Introduction

Smart Televisions (smart TV) platforms represent two converging technologies, those of traditional television systems and computing platforms. The main purpose of these devices is currently to provide augmented interactive services in addition to broadcast television. The new generation of smart TVs have a range of capabilities that far exceed the delivery of audio and video and can include a variety of online interaction. Current functionality includes many of the features present in traditional computing systems and in mobile platforms. This includes internet connectivity; potentially offering instant messaging, games, voice and video over IP, web surfing and on-demand content. This expanding capability means an increasing possibility that these devices may retain information of user activities. These TV systems can be viewed as embedded devices, as they provide limited access to the underlying systems without specialist knowledge, software and in some cases, small amounts of hardware. The question for the forensic examiner is what data might be retained and how can this data be accessed?

There are a number of manufacturers with smart TVs in their product range. Examples include, but are not limited to, Samsung, LG, Sony, Panasonic, Toshiba and Philips. The different manufacturers offer different capabilities. The exact TV's functionality depends on the firmware setting of that device and on the applications downloaded to the device by the user. Typically the manufacturers provide applications from an App store. The firmware can be updated automatically if the user selects this option, otherwise the user can trigger an update manually.

Smart TV platforms continue to evolve at a rapid rate. The Samsung smart TV range has models using a Linux based operating system. Samsung's high end models include a built-in camera and microphone, enabling features such as gesture control and facial recognition. Currently, LG televisions are powered by Linux (using Saturn), but the purchase of webOS from HP suggests this may change in the near future (LG, 2013). The LG cloud provides the ability to exchange information between LG

* Corresponding author. Faculty of Computing, Engineering and Science, University of South Wales, Treforest, CF37 1DL, UK.
E-mail address: iain.sutherland@southwales.ac.uk (I. Sutherland).

http://dx.doi.org/10.1016/j.diin.2014.05.019
1742-2876/

phone and TV applications and there are already applications allowing tablets and phones to act as smart remotes to control televisions. The Linux systems now support open source development (Open webOS, 2014). The Google TV operating system can be found on various platforms. The manufactures that are supporting the Google TV platform include Sony, Hisense, LG, Vizio and more recently Asus (Pendlebury, 2013).

Smart TV: the current environment

The feature rich nature of smart TV combined with the possible domestic, commercial and educational environments, raise some interesting issues in terms of potential misuse and evidence of that misuse being captured on the device.

These systems require Internet connectivity to enable all of their functions. They often require high bandwidth connections to enable streaming video. This network connectivity can be achieved via a wireless or wired connection. This can provide a weak point within a wireless network as suggested by (Lee and Kim, 2013) as smart TV systems have already been shown to be vulnerable, with suggestions available for possibly attacking them via the network or infected applications (Lee and Kim, 2013). Overall the systems appear to have limited security, appearing to rely on reduced functionality, the absence of antivirus and firewalls exacerbates the problem. A recent examination of various smart TV security implementations suggested that all of the tested vendors had one or more vulnerabilities (Kuipers et al., 2012).

These systems are possibly too new for malware, but there is no reason why they should be any less vulnerable than other networked devices. Indeed the use of common Linux and Android Operating Systems may actually increase the risk of this form of misuse, as malware already exists for these operating systems. The use of an open source operating systems has the associated risks and advantages of the code being freely analysed for vulnerabilities, making these device easily explored and increases the potential for modification or misuse (LG Open Source, 2013).

Smart TVs have caught the attention of the hacking community (SamyGo, 2014) who are already modifying the TV to overcome the limitations in the systems. There are currently a variety of hacking forums looking at the possibility of modifying the firmware contained in these televisions mainly for extending their capabilities e.g. to play various media formats. The OpenLGTV forum (The OpenLGTV forum, 2013) is one example of a group focused on modifying the open source code on LG Saturn platforms. The SamyGo Forum has a number of posts providing instructions on modifying the smart TV to support P2P software including installing torrent clients (SamyGo Forum, 2014). There are also examples of tools and code available for rooting other manufacturers' smart TVs (e.g. Sony (Edwards, 2012)).

The possibility of malicious attacks on some of these weaknesses has also been highlighted as a potential risk (Lee and Kim, 2013, Kuipers et al., 2012, Grattafiori and Yavor, 2013). Issues of data protection have already arisen (Telecompaper, 2013) with one supplier being investigated by a national regulator for recording personal data on viewing behaviour, web and application use. Vulnerable smart TV sets could be a potential boon to criminals who are already established in the "ransomware" field. There have been many examples of malicious software devised to hijack and ransom users files (Gazet., 2010). Worse, a particularly sinister malware, Revoyem (Mimoso, 2013), redirects users to a child porn themed page, whereupon the ransomware takes over and demands payment to "clean" the system. This type of threat aimed at the smart TV could be particularly unpleasant considering the typical family use of such a device. Remote Access Tools or RATs are a problem; people have been caught out with webcams being remote controlled. The same is true with Smart TVs with built-in camera and microphone. If this was compromised, then in theory this could be used to monitor the TV's users. This has already been demonstrated as a potential risk in currently available systems (Grattafiori. and Yavor, 2013). A compromised smart TV could potentially be used to attack other computers on the same home network, or to form part of a botnet. One security company (Proofpoint, 2014) found evidence of smart devices (including a refrigerator) already being exploited by malware. Some smart TVs contain speech recognition (Samsung, 2013) – could this feature be used to extract a user's biometric data?

Forensic issues

Smart TVs are becoming increasingly popular with estimates of 40–60 million units shipped in 2012 and projections of 55% of the global market (Tarr, 2013, DisplaySearch, 2012). Estimates suggest 102–140 million units by 2015/16 and that by 2017 around 73% of flat panel TV shipments will be smart TVs and almost all TVs will have the ability to communicate via IP (Watkins, 2014). It should be noted that for 2012, the estimated number of TV units shipped would appear to be considerably more than the number of games units shipped in the same year (ABI Research, 2013). The forensics community has invested considerable effort in games forensics (examples are (Xynos et al., 2010, Burke and Craiger, 2007 and Conrad et al., 2007). To date, there appears to be no material available referring to the forensic examination of any smart TV or to guide the forensic examiner in the extraction and analysis of data.

These systems may not ship with a hard drive (although many have the ability to connect an external drive to use as a recording device) but they have solid-state storage for the operating system and for recording user configuration settings on the device. Therefore the investigator has three potential options for accessing possible data from the TV's embedded systems. The first is recording the limited details displayed on the device by interacting with the system. The second is to connect via a network or serial port to interrogate the system. The third and most invasive is to disassemble the system and de-solder the memory chips in-order to access the data.

Dismantling, extracting and interrogating memory chips requires specialist knowledge and hardware. When

considering the forensic analysis of embedded systems, Van der Knijff (van der Knijff, 2002) suggested that due to the difficulty of extracting data from embedded systems, a number of questions should be considered. This was aimed at assessing the risk of expending considerable effort against the possibility of the device yielding little information (van der Knijff, 2002). Although in the case of smart TVs there are routes available to accessing the file system, the assessment suggested by Van der Knijff can be applied:

A. The likelihood of relevant digital clues being present which linked to an individual
B. The universality of methods and techniques
C. The availability of assistance from the industry
D. The possibilities of deploying methods and techniques without specialist knowledge or equipment

This paper applies this assessment to smart TVs in general to explore the current value in processing these devices as part of an investigation, exploring the idea that smart TV systems should be an item of significant importance on the investigator's agenda.

Relevant digital clues

Considering the range of functionality described above, the need for a forensic analysis of a smart TV could arise from either the activity or misuse of the owner, or as a result of a network compromise by a malicious entity, the same as a laptop or desktop computing platform. Considering the range of functionality of some systems, it is possible to state a number of tentative assumptions on the type of data held on smart TV systems. This would vary from manufacturer to manufacturer and potentially from model to model, but might include:

- Network configuration
- Viewing behaviour and application use
- Web browser use (potentially including login details)
- There may be the potential to determine associated devices:
  - Some TV applications are available to enable other devices to act as remotes to the TV, an example being the smart controller app for the iPad/iPhone to control LG smart TVs. This might allow some activity to be more closely tied to an individual if a passcode protected device accesses the smart tv.
  - Some Smart TVs may also permit the sharing of images from other devices, these images may also be stored on the smart TV.
  - Most of the smart TV systems contain ports (typically USB) to allow the connection of storage devices
- If compromised/rooted then evidence of the compromise may be contained on the device

It may be the case that certain information is lost on powering down the device, in which case live analysis options could be considered. In domestic locations these systems are commonly on the same power bar as video recording equipment and frequently left powered on in standby mode.

Universality of methods and techniques

At least a proportion of these devices run well-known operating systems that investigators are already familiar with and therefore tools and techniques developed for these systems may be applicable to smart TV systems. A best case scenario is that tools and techniques will work across the full range of an operating system type for a particular manufacturer. The worst case scenario is that specific tools and techniques would be required for each model or series.

The availability of assistance from the industry

The fact that some systems use versions of open source operating systems means there should be a body of available knowledge in this subject area. There are numerous support sites (LG TV-Audio, 2014, Samsung Support, 2014) providing a variety of support from downloading manuals to upgrading firmware. Typically contact and support information is readily available. An assumption can also be made that customer focused nature of the manufacturers may mean a more open response than that of say the games console industry, although manufacturers of other embedded systems such as mobile phones have been slow to provide assistance due to the proprietary nature of the system firmware (Al-Zarouni, 2006).

The need for specialist knowledge or equipment

Although smart TVs are solid state embedded systems, they are potentially easy to access with the correct cables. In some cases an RS232 interface and some emulation software are the core requirements along with the time to experiment with some of the remote control commands to access the appropriate 'engineer mode'. There is an issue of potential expense in that errors can result in 'bricking' a device. For instance the process to rooting a smart TV that contains Android OS is very similar to that of rooting phones. This means that techniques from other fields can lend themselves when analysing such devices.

The way forward

The above review suggests smart TVs should be explored as potential sources of evidence and that possible techniques for access are already available (The OpenLGTV forum, 2012). Although there are surveys that suggest some users do not connect the systems to a network (Analysys Mason, 2013), there may still be data of value on the device as to simple usage. This trend will change in the future as more on-demand content is made available and viewers change their viewing habits.

For now, smart TVs appear to be a neglected source of potential evidence as they can be misused by the owner, they can be attacked over a network and have already be shown to be vulnerable. Sales figures suggest that smart TV systems are likely to be the most significant embedded

devices needing forensic analysis. Action is needed to aid the investigative process. This could include increased effort on the analysis of the most commonly sold devices to determine what information is retained in the device and if more widespread analysis is required.

Actions by industry could include the development of appropriate equipment to support the rapid analysis of this type of device. There are hardware kits such as Xry and Celldeck for cellular phone analysis. It would seem a logical step to develop similar resources for smart TV systems that access the device and aid the interpretation of captured data.

References

ABI Research, Despite 25% annual decline in 2012 game console shipments, there is still room for optimism, [updated 2013; cited 16.06.24]. Available from: https://www.abiresearch.com/press/despite-25-annual-decline-in-2012-game-console-shi.

Analysys Mason, Most smart-TV owners do not connect their TVs to the Internet: manufacturers must respond. http://www.analysysmason.com/About-Us/News/Insight/smart-TV-May2013/#.Ukhs7hbZf8s. [accessed 16.06.2014].

Al-Zarouni M. Mobile handset forensic evidence: a challenge for law enforcement. In: Proceedings of the 4th Australian digital forensics Conference, Edith Cowan University, Perth Western Australia, December 4th 2006; 2006. http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1023&context=adf.

Burke PK, Craiger P. Xbox forensics. J Digital Forensic Pract 2007;1(4):275–82. http://dx.doi.org/10.1080/15567280701417991.

Conrad S, Dorn G, Craiger JP. Forensic analysis of a Sony Playstation 3 gaming console; 2007 [6th Annual Conference on the International Federation of Information Processing].

DisplaySearch, Smart TV Shipments Grow 15% Worldwide in 2012, According to NPD DisplaySearch. [updated 2012; cited 18.06.2014]. Available from: http://www.displaysearch.com/cps/rde/xchg/displaysearch/hs.xsl/121017_smart_tv_shipments_grow_worldwide_in_2012.asp

Edwards S., Nimue a simple Python script for jailbreaking Sony Bravia TVs. [updated 2014; cited 16.06.2014]. Available from: https://github.com/CFSworks/nimue.

Gazet A. Comparative analysis of various ransomware virii. J Comput Virology 2010;6(1):77–90 [February 2010].

Grattafiori A, Yavor J. The outer limits: hacking the Samsung smart TV, Blackhat briefing 2013; 2013. http://www.blackhat.com/us-13/briefings.html#Grattafiorihttp://www.samsung.com/us/2013-smart-tv/-smart-tv-5.

van der Knijff. Embedded systems analysis, Chapter. In: Casey E, editor. Handbook of computer crime investigation. Academic Press; 2002.

Kuipers R, Starck E, Heikkinen H. Smart TV hacking: crash testing your home entertainment; 2012 [Codenomicon Whitepaper]http://www.codenomicon.com/resources/whitepapers/codenomicon-wp-smart-tv-fuzzing.pdf.

Lee S. and Kim S. Hacking, surveilling and deceiving victims on smart TV, Blackhat Briefing 2013, [updated 2013, cited 16.06.2014]. Available from: https://media.blackhat.com/us-13/US-13-Lee-Hacking-Surveilling-and-Deceiving-Victims-on-Smart-TV-Slides.pdf.

LG, LG Electronics acquires webOS from HP to enhance smart TV. [updated 2013; cited 16.06.2014]. Available from: http://www.lg.com/us/press-release/webos-release.

LG Open Source Code Distribution. [updated 2013; cited 16.06.2014]. Available from: http://www.lg.com/global/support/opensource/index.

LG TV-audio and video support. [updated 2014, cited 28.05.2014]. Available from: http://www.lg.com/uk/tv-audio-video.

Mimoso M., Revoyem ransomware sinks to new low [updated 2013; cited 16.06.2014]. Available from: http://threatpost.com/revoyem-ransomware-sinks-to-new-low.

Open webOS. [updated 2014; cited 28.05.2014]. Available from: http://www.openwebosproject.org.

Pendlebury T., Asus to release Google TV device, [updated 2013, cited 16.06.2014]. Available from:http://ces.cnet.com/8301-34451_1-57562090/asus-to-release-google-tv-device/.

Proofpoint, Proofpoint uncovers Internet of Things (IoT) Cyberattack., [updated 2014; cited 16.06.2014]. Available from: http://www.proofpoint.com/about-us/press-releases/01162014.php.

Samsung Support. [updated 2014; cited 28.05.2014]. Available from: http://www.samsung.com/us/support/.

Samsung Smart TV Voice Control, [updated 2013; cited 16.06.2014]. Available at: http://www.samsung.com/global/microsite/tv/2013_vi/voice_control.html.

SamyGo Forum. Index Page, [updated 2014; cited 28.05.2014]. Available from: http://forum.samygo.tv/index.php.

SamyGo, Samsung TV Firmware Hacking. [updated 2014; cited 28.05.2014]. Available from: http://samygo.tv/.

Tarr G., IHS: smart TVs rise to 27% of TV shipments, [updated 2013; cited 16.06.2014]. Available from: http://www.twice.com/articletype/news/ihs-smart-tvs-rise-27-tv-shipments/105108.

Telecompaper, Smart TV maker told to improve info on data collection. [updated 2013, cited 16.06.2014]. Available from: http://www.telecompaper.com/news/smart-tv-maker-told-to-improve-info-on-data-collection-962460.

The OpenLGTV forum. Main Page [updated 2013, cited 16.06.2014]. Available from: http://openlgtv.org.ru/wiki/index.php/Main_Page.

The OpenLGTV forum. Debug mode and connections. [updated 2012, cited 16.06.2014]. Available from: http://openlgtv.org.ru/wiki/index.php/Debug_mode_connection.

Watkins D. 2013. Smart TV shipments grew 55 percent, [updated 2014, cited 16.06.2014]. Available from: https://www.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5472.

Xynos K, Harries S, Sutherland I, Davies G, Blyth AJC. Xbox 360: a digital forensic investigation of the hard disk drive. Digit Investig 2010;6(3–4):104–11.