2014

A forensic overview of the LG Smart TV

Iain Sutherland
Edith Cowan University

Konstantino Xynos
University of South Wales, UK

Huw Read
Noroff University College

Andy Jones
Edith Cowan University

Tom Drange
Noroff University College

DOI: 10.4225/75/57b3e69dfb881

12th Australian Digital Forensics Conference. Held on the 1-3 December, 2014 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.

A FORENSIC OVERVIEW OF THE LG SMART TV

Iain Sutherland[1,3], Konstantinos Xynos[2], Huw Read[1, 2], Andy Jones[3], Tom Drange[1]
Noroff University College[1], Norway
Corresponding author: iain.sutherland@noroff.no
Faculty of Computing, Engineering and Science[2] University of South Wales, UK
Security Research Institute[3], Edith Cowan University, Perth, Australia

Abstract

The emerging Smart TV platform will likely replace traditional television sets over time as the entertainment and communication centrepiece in people's homes. Given its expanded functionality and now, its online presence, there is a need to identify how they may become part of forensic investigations. The purpose of this paper is to introduce the area of Smart TVs and the potential forensic value these systems present in combination with their ever advancing functionality and capabilities. We provide an overview of Smart TV systems highlighting functionality and potential issues. We also take an initial look at two particular models, from the same manufacturer, to highlight the different range of material that may be available to the forensic examiner and provide an outline to investigators of the steps necessary to ensure relevant forensic data can be captured for processing, as part of an investigation. We then discuss the need for future work to improve access for forensic investigators.

Keywords:
Smart Television, Embedded Device, Digital Forensics, LG Smart TV

INTRODUCTION

The television set has evolved from John Logie Baird's electromechanical system of the 1920's to the current range of digital, colour, high definition, widescreen television sets. The latest iteration of these systems sees the convergence of two technologies; the home computer and the television, to create a new type of embedded computing platform. A Smart TV platform provides interactive services in addition to broadcast television. The functionality of these systems is significantly more than just the delivery of audio and video content. Current Smart TV systems now offer much of the interactivity and network capabilities associated with desktop, laptop and mobile platforms. They are network enabled devices with the ability to browse the web and purchase applications. Applications (apps) present on these systems offer games, video conferencing and web-browsing in addition to on-demand content. This expanding capability means an increasing possibility that these devices may retain information of user actions, and so provide evidence that may show, or disprove illicit activities. The uptake of these systems is increasing with estimates of 40-60 million units shipped in 2012 and predictions (Tarr, 2013) suggesting 102-140 million units, by 2015/16. Smart TV platforms continue to evolve at a rapid rate with a number of bodies attempting to standardise the delivery of products and services such as the Open IPTV Forum (OPIF, 2012), and the Smart TV Alliance (Alliance, 2014).

THE SMART TV ENVIRONMENT

Smart TV manufacturers include Hisense (Hisense, 2014), Samsung (Samsung, 2014), LG (LG, 2014), Sony (Sony, 2014), Panasonic (Panasonic, 2014), Toshiba (Toshiba, 2014), Vizio (Vizio, 2014), and Philips (Phillips, 2014). The different manufacturers offer a variety of technical features across the product range. The exact functionality provided by the TV depends on the make, model, extra peripherals attached and any extra applications that may be downloaded from an 'App store' by the end user. Early versions of Smart TV systems were based on proprietary operating systems; versions from 2012 onwards are based on existing operating systems such as Linux and Android. There are some notable similarities and distinct differences in the various

product ranges: The Samsung Smart TV range runs on an Android based operating system. Samsung's high end models include built-in camera and microphone, enabling features such as hand gesture control, voice control and facial recognition (Samsung, 2014). The Google TV operating system (Android based) can be found on various platforms. The manufacturers that are supporting the Google TV platform include Sony, Hisense, LG, Vizio and more recently Asus (Pendlebury, 2013). Sony has an Android based operating system. Some models also offer Near Field Communication (NFC) with certain NFC enabled devices. LG televisions use a Linux based operating system, with a move to webOS in the near future (LG, 2013a). It could be argued that Linux systems and the different variants are in a better position to make use of the open source community support that comes with open source development (OpenWebOS, 2014).

Smart TVs require an active Internet connection with the minimum recommended bandwidth being between 1.5Mbps, and 3.0Mbps with 5.0Mbps for HD content (LG, 2013a). In some models this is achieved with an integrated wireless receiver, in others an additional wireless card or wired connection is required. This connectivity can create security issues, as the current generation of Smart TV's appear to lack any built-in or installable antivirus, firewalls and other security controls. An assessment (Kuipers, Starck, & Heikkinen, 2012) of the security of various Smart TVs suggested that all of the tested systems had one or more vulnerabilities. A Smart TV can therefore provide a weak point within a network (SeungJin & Seungjoo, 2013), the possibility of accessing and modifying these systems has not escaped the notice of the hacking community. Users such as SamyGo (SamyGo, 2014) are already modifying the Smart TV platforms to enable additional functionality. The possibly of malicious attacks has also already been highlighted as a very possible risk (SeungJin & Seungjoo, 2013), (Kuipers et al., 2012), (Grattafiori & Yavor, 2013). Other issues have arisen in relation to security and privacy as manufacturers already propose this as an ideal marketing platform with the ability to devise specific advertisements and provide feedback to the advertisement's effectiveness. This has led to concerns of possible abuse with the Dutch national regulator reprimanding a supplier for capturing data on viewing behaviour, web and application use without providing sufficient information to the end user (Telecompaper, 2013). This has also been recently highlighted as an issue with the LG systems by another security researcher (DoctorBeets, 2013) who found issues with the Smart AD (LG, 2012b) service running on the LG System. There are also examples of tools and code available for gaining root access to Sony Smart TVs (CFSworks/nimue, 2014).

The increasing capability, connectivity and acceptance of these systems suggests there is a need to understand their potential value from an investigator's perspective (Sutherland, Read, & Xynos, 2014). Smart TVs are embedded devices, there is no easy access to the operating system or file systems without specialist knowledge. This presents a challenge for both the investigator and an individual wishing to maliciously alter information or settings. Malicious alterations are possible (Grattafiori & Yavor, 2013), but in most instances the required skill level is quite high, needing specialised software and, if accessing the TV locally, requires specific RS232 / USB cables and software.

THE LG SMART TV

This work focuses on the LG Smart TV, (using model 42LS570T-ZB and model 55LA740V.) The LG platform was chosen for analysis for three reasons: The system has been made partly open source (LG, 2013b) by the manufacturer, allowing potential modification and code analysis in future work. LG has also made both extensive support and documentation available, (LG, 2013b). Although this paper is focused on investigating the system at a high-level via the user interface, access to open source documentation and some of the sites dedicated to modifying the firmware highlight just some of the possible problems a more in depth analysis of these systems will encounter. Secondly LG may be regarded as one of the main manufacturers in the Smart TV sector, thirdly these systems were made available to the authors at the time of writing.

Specific features of the LG Smart System include web browsing (including email), video-on-demand via a number of service providers, Web 2.0 interactivity and social networking features including LG's own mashup

interface to combine social networking with broadcast/video (LG, 2012a), LG Premium video news video on-demand and other features that require network connectivity (LG, 2012a).

LG documentation (LG, 2012a) suggests a total of around 2.5GB of internal data storage is provided within similar products in the range. It is assumed that this is the total available for all of the TVs processing and storage requirements. While not large, this still represents a significant amount of potential data, although some of this space is reserved for applications (for the models tested in this paper, around 387MB).

One possible reason for the popularity of the LG Smart TV platform to the coding enthusiast is the extensive amount of information available. The OpenLGTV forum (OpenLGTV, 2013) is one example of a group focused on modifying the open source code on LG Linux based Saturn processor platforms. The LG Smart TV manual (LG, 2012a) also provides some instructions on connecting and controlling the system from a PC although that requires knowledge of the commands and some specific equipment including serial cables to connect a PC to the TV.

FORENSIC ANALYSIS AND METHODOLOGY

The review of the LG Smart TV suggests that these devices can be explored as potential sources of evidence and although possible techniques for more comprehensive access are available, they have not yet been explored. These TVs have already been highlighted as a potential source of forensic evidence (Sutherland et al., 2014). 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. Has the TV been used to stream / play illegal content? Has the system been compromised? Is the webcam being used to generate illegal content? Has the webbrowser been used to facilitate criminal activity? There are a number of potential types of misuse.

Due to the varied nature of Smart TV systems, creating a detailed forensic checklist is a considerable task. This is compounded by the fact that there are a number of manufacturers, all with different models and a range of firmware and applications. The firmware can be updated automatically if the user has selected this option, otherwise the user can trigger an update manually. Special care must be taken as this may alter the underlying behaviour and even layout of the system: applications, products and services can be revised, updated or withdrawn. The investigator would not only have to be confident of dealing with a specific manufacturer and model, but possibly a specific firmware revision for that model. For the forensics examiner a similar comparison can be made to the PC world; where evidence can come from different operating systems including the different functionality, which is also very dependent on the numerous programs installed (Applications / Apps in the case of the TV). The key difference is that the systems are for now, less well known. Also despite the hacking forums and the instructions on how to connect a PC via a RS232 connection it is considerably more difficult to access the user data within the device than a PC, with the additional risk that incorrect commands can render the device inoperable (i.e., brick the device). Each make, model and firmware revision is different and provides its own challenges. 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 from them.

The following methodology highlights the possible types of information that might be available and the appropriate order to explore the device via the user interface. This minimally invasive approach removes the need for specialist equipment or training, instead it provides guidance for interrogating the system.

Methodology for Analysis of an LG Smart TV

This work focusses on the general areas of interest within the LG Smart TV (e.g., LED Smart TV model: 42LS570T-ZB and 3D LED Smart TV model: 55LA740V). The analysis process proposed for the LG Smart TV

suggests 10 steps for acquiring potential information. The ordering of the steps ensures that the data, most likely to be revised or altered, is captured first.

1. Record Analysis:
   Minimally invasive access is used to collect the data via the user interface, so following similar good practice guides (ACPO, 2012) there is the need to create a visual record of the investigator's actions on the system. The video capture of the analysis is required as the investigators actions will inevitably alter the state of the device.

2. Physical Set up:
   a. Review of connections – existence of any external USB drives that are currently connected or available to be connected. HDMI connections for other media devices (and potentially other computer systems), PC connections, networked connections Games systems cable boxes etc.
   b. Check model number to determine if wireless capability is available on the particular model (indicating other possible connected devices).
   c. Check to see if LAN cable (i.e., network cable) is present and connected.

3. Power Status:
   If the system is not powered on (i.e., showing a picture), check to see if the system is in standby mode or off. The power light/ standby light is a configurable option and may be altered by a technically advanced user. One method of determining the status of the Smart TV is to use a mobile device (e.g., phone or tablet) with the LG remote application installed. If the Smart TV is in standby then this would appear in the list of devices offering a connection. As with computers, a Smart TV may remain logged in to some applications which can then accessed (see step 10.)

4. Recent History:
   The first step in determining user activity is to check the recent history in the TV, as the investigator's actions will alter and update this list.

   Model: 42LS570T-ZB: `My Apps > Home > Recent`

   Model: 55LA740V with Magic Remote: Press "Smart" on the right side of the remote control

   This provides a scroll bar on the bottom section of the screen. This includes 'Recent' which holds the last 10 actions / apps used on the TV system including video / images viewed on external USB devices, recent channels and from other sources (see 'Smart Share' below). The list provides the name and in some cases a thumbnail image of video / images providing an indication of what was viewed. These are retained in the 'recent' list if the TV is switched to standby, powered off, or even if the USB device has been removed providing evidence that external content was displayed using the Smart TV.

5. Connected Devices:
   The Smart TV configuration and connected devices can be determined by checking the devices recognized as inputs for the Smart TV. This can be a number of devices and is located under:

   `Inputs`

   This can indicate any other devices connected to the Smart TV such as streaming PCs which may hold further evidence.

6. Network status:

The MAC address of the system and the IP address (obtained using DHCP on the local network). This may be used to identify or eliminate the Smart TV during a live network investigation.

`Settings > Network (planet symbol)`

7. Versions and Serial numbers:
   The Electronic Serial Number (ESN), the unique device identifier for the device (Association, 2013), model number, browser version and MAC address can also be determined by:

   `Settings > Product / Service Info (question mark symbol)`

   This location can also supply the MAC address of the device and the Widevine DRM information for the television (LG, 2012a).

8. Smart Share:
   This is essentially a log of shared files including those shared over WiFi and from USB devices. This will list the nine most recently watched and nine newly added media. There are more options at the top of each of these to provide a more comprehensive list. These can be cleared by the user and appear to be cleared periodically by the device. On the more advanced model (55LA740V) this log also contains camera memory and possible DLNA (Digital Living Network Alliance) Servers.

   Model: 42LS570T-ZB: `MyApps > Smart Share`

   Model: 55LA740V with Magic Remote: Press "Smart" on the right side of the remote control > `Smart Share`

9. Web Browsing:
   The Smart TV has a limited Web browser that includes bookmarked / favourite pages and a web history. The favourites page has an option to store 12 locations. The default settings record the browser history. The Smart TV interface on the model 42LS570T-ZB provides no details of time or dates in relation to web history. This is rather an ordered list of sites visited by the user. On the 55LA740V however, the time and date is provided.

10. Other Applications including social media applications:
    This overview explores some of the information available as a result of applications being used on the Smart TV. These applications are the default ones for these particular make and models (42LS570T-ZB and 55LA740V).

    - Facebook and Twitter Apps are pre-installed on the TV and the default configuration enables automatic sign-on. There is the possibility that because these are not perceived as computing devices, owners may not sign out as they would on a PC enabling forensic investigators to access social media information.

    - Skype is also pre-installed however will not run if it does not detect appropriate camera equipment. If the requirements are met, it does maintain a history of recently called contacts.

    - LG Apps includes the LG Cloud a free application which offers 5GB storage via an account. Potential evidence such as video and images can be streamed directly to the Smart TV. As with the other apps mentioned, LG Cloud has an automatic sign-in feature. Given the time needed to enter a password via a remote control interface, many users may opt to enable it.

These 10 steps provide aspects of the system configuration and recent usage. It should be noted that a more in depth and forensically sound approach requires access to the underlying operating system of the Smart TV. This could provide additional information such as timestamps, file carving for artifacts and if the system had been compromised.

CONCLUSION

This paper reviews features of Smart TV systems outlining the functionality and highlighting some of the problems including some security issues. It has also examined some of the potential types of evidence that may be found on Smart TVs; including applications (like Facebook, Skype, etc) that could provide a good source of evidence or even further insights that may be required in an investigation. Given the remote control as the main source of input into a Smart TV, the use of the automatic sign-on feature present in many of the communication/social media applications should not go overlooked. Where a user may be more security conscious when using a desktop based web browser, the Smart TV itself may provide a quick way to viewing recent posts and updates. In addition to a plethora of user activity, these systems may also contain extra evidence items as a result of the owner extending functionality, via rooting, or in the rare case when the system has been exploited via the network (Kuipers et al., 2012).

The paper has also outlined an example method for two LG models of Smart TV. It focused on 10 steps to explore how the system may have been used. To avoid the use of specialist hardware and software this is conducted via the user interface and the activities of the user and investigator should be video recorded.

The authors have identified the need for further work in the following areas: experimental work to provide a detailed forensic process, the constant updating of the capturing process as the devices get updated and evolve, monitoring of vulnerabilities that are produced and the ability to install custom software at will (e.g., rooting). The first of these is to explore issues of gaining access to the LG Smart TV via the serial RS232 connection. This would enable a more detailed analysis of the information available within the operating system of this particular manufacturer's range and it would provide a richer picture of the user's utilisation of the system.There is a strong suggestion that Smart TV systems are likely to be one of the most significant embedded domestic devices needing forensic analysis.

REFERENCES

ACPO. (2012). Association of Chief Police Officers: Good practice guide for digital evidence. from http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf

Alliance, S. T. (2014). Smart TV Alliance: Our mission.

Association, T. I. (2013). TIA: Electronic Serial Number.

CFSworks/nimue. (2014). Nimue a simple Python script for jailbreaking Sony Bravia TVs. from https://github.com/CFSworks/nimue

DoctorBeets. (2013). LG Smart TVs logging USB filenames and viewing info to LG servers (Blog entry 15 November 2013). from http://doctorbeet.blogspot.co.uk/2013/11/lg-smart-tvs-logging-usb-filenames-and.html

Grattafiori, A., & Yavor, J. (2013). The Outer Limits: Hacking the Samsung Smart TV, Blackhat briefing 2013. from http://www.blackhat.com/us-13/briefings.html#Grattafiori

Hisense. (2014). Hisense Televisions. from http://www.hisense-usa.com/tvs/

Kuipers, R., Starck, E., & Heikkinen, H. (2012). Smart TV Hacking: Crash Testing Your Home Entertainment, Codenomicon Whitepaper. from http://www.codenomicon.com/resources/whitepapers/codenomicon-wp-smart-tv-fuzzing.pdf

LG. (2012a). LG Smart TV User Guide.

LG. (2012b). Smart AD (No Longer available). from http://lgsmartad.com/main/main.lge

LG. (2013a). LG Electronics Acquires webOS from HP to Enhance Smart TV. from http://www.lg.com/us/press-release/webos-release

LG. (2013b). LG Open Source Code Distribution System from http://www.lg.com/global/support/opensource/index
LG. (2014). Smart TV. from http://www.lg.com/uk/smart-tvs
OpenLGTV. (2013). The OpenLGTV forum. from http://openlgtv.org.ru/wiki/index.php/Main_Page
OpenWebOS. (2014). The Open webOS Project. from http://www.openwebosproject.org
OPIF. (2012). Open IPTV Forum: About us. from http://www.oipf.tv/about-us
Panasonic. (2014). Welcome to Smart Viera. from http://www.panasonic.com/promos/learn/smart-viera/
Pendlebury, T. (2013). Asus to release Google TV Device. from http://ces.cnet.com/8301-34451_1-57562090/asus-to-release-google-tv-device
Phillips. (2014). Welcome to Phillips Smart TV. from http://www.philips.com/content/global/country-selectors/www/en/smarttv.html
Samsung. (2014). Samsung Smart TV. from http://www.samsung.com/us/experience/smart-tv/
SamyGo. (2014). Samsung TV Firmware Hacking. from http://samygo.tv/
http://sourceforge.net/projects/samygo/
SeungJin, L., & Seungjoo, K. (2013). Hacking Surveilling and Deceiving Victims on Smart TV, BlackHat 2013. from https://media.blackhat.com/us-13/US-13-Lee-Hacking-Surveilling-and-Deceiving-Victims-on-Smart-TV-Slides.pdf
Sony. (2014). Sony UK. from http://www.sony.co.uk/
Sutherland, I., Read, H., & Xynos, K. (2014). Forensic analysis of Smart TV: A Current Issue and Call to Arms. *Digital Investigation: Special Edition on Embedded Forensics: Edited by Pavel Gladyshev*. doi: 10.1016/j.diin.2014.05.019
Tarr, G. (2013). IHS: Smart TVs Rise To 27% Of TV Shipments. from http://www.twice.com/news/tv/ihs-smart-tvs-rise-27-tv-shipments/3471
Telecompaper. (2013). Smart TV maker told to improve info on data collection.
Toshiba. (2014). Toshiba Smart TV. from http://www.toshiba.eu/television/consumer-tvs/smart/
Vizio. (2014). Smart TV. from http://www.vizio.com/tvs.html