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