Digital Investigation 25 (2018) 78–89

Contents lists available at ScienceDirect

Digital Investigation

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

I know what you streamed last night: On the security and privacy of streaming

Alexios Nikas [a], Efthimios Alepis [b], Constantinos Patsakis [b, *]

[a] University College London, Gower Street, WC1E 6BT, London, UK
[b] Department of Informatics, University of Piraeus, 80 Karaoli & Dimitriou Str, 18534 Piraeus, Greece

ARTICLE INFO

Article history:
Received 3 January 2018
Received in revised form
15 February 2018
Accepted 12 March 2018
Available online 21 March 2018

Keywords:
Security
Privacy
Streaming
Malware
IoT

ABSTRACT

Streaming media are currently conquering traditional multimedia by means of services like Netflix, Amazon Prime and Hulu which provide to millions of users worldwide with paid subscriptions in order to watch the desired content on-demand. Simultaneously, numerous applications and services infringing this content by sharing it for free have emerged. The latter has given ground to a new market based on illegal downloads which monetizes from ads and custom hardware, often aggregating peers to maximize multimedia content sharing. Regardless of the ethical and legal issues involved, the users of such streaming services are millions and they are severely exposed to various threats, mainly due to poor hardware and software configurations. Recent attacks have also shown that they may, in turn, endanger others as well. This work details these threats and presents new attacks on these systems as well as forensic evidence that can be collected in specific cases.

Introduction

The deployment of Internet of Things (IoT) devices and services is accelerating and most major mobile network operators consider Machine-To-Machine (M2M) communication networks as a significant source of new revenue (Dhillon et al., 2017). However, whilst IoT is characterized by heterogeneous technologies that concur to the provisioning of innovative services in various application domains, meeting respective security and privacy requirements in these domains becomes increasingly important (Sicari et al., 2015). In the light of the radical changes occurred in the telecommunication industry over the last decade, a series of novel services and applications have been enabled. For instance, the increase in the available data bandwidth allowed for the sharing and consuming of multimedia content from almost all our devices, utilizing local and remote network settings. Foreseeing this shift, service providers have correspondingly redesigned their service and content delivery mechanisms. This evolution is so disruptive that has totally changed the media market as people are continuously leaving traditional media, whether this is newspapers or TV, and are shifting towards their corresponding on-line peers. The most important factor attracting people towards this turn is the fact that they can choose the content they want at the time they want it. This incentive is rather significant since, up to recently, traditional media due to their nature could not serve content on demand.

Focusing on multimedia, primarily the discussion points towards sports and entertainment. Film studios and subscription TV providers are following this trend by shifting their services to on-demand content delivery, streaming content to the corresponding subscribers for a predefined cost. However, since the focus is on digital content which replicates rather easily, people are allowed to share content with others who are not authorised to. In fact, unauthorised multimedia content sharing has become an increasing online illegal trend. For instance, recently many mobile apps that illegally stream famous movies and TV series are uploaded in mobile app stores (Ernesto, 2017; Johnson et al., 2015). Yet, the effectiveness of current measures to counter pirated content is not apparent (Sudler, 2013; Lauinger et al., 2013; Danaher et al., 2015, 2017; Reimers, 2016).

In spite of the ethical and legal aspects of these user actions, this work studies the security and privacy implications of working with this kind of apps and devices, as the amount of users who use such solutions are in the scale of millions. After a thorough investigation into the related scientific literature we have come up with the

* Corresponding author.
E-mail addresses: alexios.nikas.17@ucl.ac.uk (A. Nikas), talepis@unipi.gr (E. Alepis), kpatsak@unipi.gr (C. Patsakis).

https://doi.org/10.1016/j.diin.2018.03.004
1742-2876/

conclusion that this is the first work to study these applications under this perspective. Namely, through our conducted experiments we have successfully identified more than 100,000 users worldwide who are using similar services and apps while they are having their devices directly connected to the Internet with poorly configured security settings, e.g. using default user names and passwords. This inevitably exposes them to numerous security and privacy threats which are thoroughly analysed hereafter. Going a step further from the personal security and privacy issues, our results also indicate that the number of the devices that could be used for campaigns such as the recent Ukraine power grid cyberattacks or as bots for the next Mirai is beyond any measure, and even worse, the methods to penetrate thousands of them already exist.

Ethical considerations

While all the information used throughout this work has been erroneously made public, mainly due to misconfigurations or to the data owner's lack of knowledge, we deliberately refrain from identifying the users and we opted not to collect personal data apart from those necessary for the production of statistics and screenshots so as to illustrate the problem's magnitude. Despite the "public" nature of these data, we follow Zimmer's approach (Zimmer, 2010):

> "*this logic of "but the data is already public" is an all-too-familiar refrain used to gloss over thorny ethical concerns*".

During our experiments we did not penetrate any of the users' devices since we attempted to confirm our claims by performing no more actions than those absolutely necessary. Similar approaches have already been taken in the literature e.g. (Bodenheim et al., 2014; Balthasar Martin, 2017).

Structure of this work

The rest of this work is organised as follows. In the next section we review the related work. Then, in Section Target applications and services we discuss potential target applications and services and provide some usage statistics. In Section The Kodi use case we focus on the specific use case of Kodi, an app used by millions of users, for which two malicious applications were implemented to simulate two of the most serious attacks. Apart from discussing further threats exposed by similar services, we also present forensics methods which are targeted towards the Kodi platform, allowing an investigator to efficiently collect relevant information from respective devices. Furthermore, in Section Solutions we outline measures that could improve the security of such applications and the article concludes in Section Conclusions where our findings are analysed and discussed.

Related work

IoT has penetrated our daily lives and businesses as the number of IoT devices in use have surpassed the number of smartphones, tablets and PCs combined. Consequently, streaming applications over Peer-To-Peer (P2P) systems, as an inextricable part of the IoT, have gained an enormous popularity too. To this end, Liu et al. (2008) provide a survey on the existing P2P solutions for live and on-demand video streaming. Their work illustrates representative P2P streaming systems, including tree, multi-tree and mesh based systems. They also describe the challenges and solutions of providing live as well as on-demand video streaming in P2P environments. Nevertheless, it seems that both the scientific literature and the available software solutions have not yet reached maturity as far as the security aspects of this domain are concerned. Indeed, Gheorghe et al. (2011) state that regarding P2P streaming applications there are neither best practices in system design, nor widely accepted attack models, nor measurement based studies on security threats to P2P streaming, nor even general surveys investigating specific security aspects of these systems.

Fischlin et al. approach the security of channels designed to securely convey a stream of data from one party to another by narrowing the gap between real-world transport layer security protocols (Fischlin et al., 2015). Their approach sheds light, in a formal way, on recent attacks, in particular concerning the use of HTTP over TLS, confirming a disjunction between applications' expectations on the one hand and the guarantees that secure streaming channels provide on the other. They conclude by highlighting the need for detailed API specifications and security guarantees for such protocols. For more on streaming systems one may refer to (Liu et al., 2008).

The prevailing shift towards streaming pirated content is prominently depicted in the recent survey of YouGov[1] which highlights that approximately 5 million people in Britain are using pirated streaming services while this number is expected to be increased in the near future by more than 2.5 million. On top of that, companies have been reported to ship Kodi boxes with pirate streaming addons preinstalled (Ernesto, 2018). In spite of that, the task of identifying the pirated content, especially when users collude, is not trivial (Furon and Doërr, 2010) and the effectiveness of current measures is questionable (Sudler, 2013; Lauinger et al., 2013; Danaher et al., 2015, 2017; Reimers, 2016).

Lee et al. (2010) illustrate attacks on commercial on-line music streaming services that lead to a copyright infringement and they propose countermeasures for on-line commercial music streaming services. In particular, they analyse three vulnerabilities for respective portal sites and present the actual attack scenario and processes. Finally, they conclude their work by suggesting music streaming service countermeasures for the discussed vulnerabilities.

Niemietz et al. (2015) investigate attack models for Smart-TVs and their apps while they focus on analysing the security of Smart-TV devices. They examine off-the-self TVs from major vendors and report vulnerabilities including, among others, unencrypted traffic in popular apps, poor implementation of TLS and stealing of device data and credentials.

Tools like ZMap (Durumeric et al., 2013), which enable fast scanning of the whole Internet to identify individual machines, when integrated into search engines they can give rise to powerful technologies such as Shodan (Matherly, 2009), the most well-known search engine for Internet-connected devices. As a matter of fact, using Shodan researchers have managed to identify thousands of vulnerable devices (Bodenheim et al., 2014) that could be trivially exploited due to their poor configuration, the usage of default credentials, etc.

Target applications and services

During our research we studied an extensive number of platforms in order to provide a more holistic overview of the current landscape. Since the content of services such as Netflix and Hulu is considered legitimate, our study targeted on platforms that are known to host illegal content. Apparently, not all of these platforms are illegal as they primarily serve many legitimate services necessary to several applications. Nonetheless, there is the risk of

[1] https://yougov.co.uk/news/2017/04/20/almost-five-million-britons-use-illegal-tv-streami/.