18-731 Project Proposal: Chromecast Traffic Analysis

Alison Kao
Carnegie Mellon University
ackao@andrew.cmu.edu

Philip Lee
Carnegie Mellon University
plee2@andrew.cmu.edu

Wellington Lee
Carnegie Mellon University
wklee@andrew.cmu.edu

I. Project Description

The Chromecast is a streaming device developed by Google to allow users to view media on the connected TV "cast" from devices such as a computer or mobile phone or tablet. This allows any user to cheaply convert a TV into a smart internet connected device. The second generation of the Chromecast was released on September 29, 2015. There are differences in protocols used by the two generations for communication, so our project will be targeted on this newer device. This will allow our research to be relevant to the current available product sold by Google.

The goal of this project is to discover possible vulnerabilities with the Chromecast in a setting where the attacker is not connected to the same network as the Chromecast. Our initial step will be to determine any basic privacy issues from sniffed data. The useful leaked data would contain information of device being used, media being streamed, account information, and other personal details. Further research, if time permits, will be into the effects of multiple Chromecasts in the same physical area with the same general goal of determining the data being cast from a particular Chromecast.

II. Related Work

Work directly related to the Chromecast is very scarce. From our preliminary research, the only work done on Chromecasts examined the traffic caused by utilizing the Chromecast in various ways, such as idling, streaming, and mirroring content. The work showed that control packets to the Chromecast are in clear text, allow possible replay attacks or session hijacking attacks. Also, private information is leaked through these packets, such as YouTube account, video, and device information. Tekeoglu et al.[1] also mention methods to help determine the presence of a Chromecast behind a NAT device based on behavioral patterns. This will be useful for us to help determining the existence of the Chromecast while not connected to the network. It is important to note that these experiments and tests were done on the first generation Chromecast on the same network.

NDSS '16, 21-24 February 2016, San Diego, CA, USA

http://dx.doi.org/10.14722/ndss.2016.23xxx

Chromecast is vulnerable to a deauth attack common to wireless devices. The attack works in by sending a deauth packet which will cause the Chromecast to revert to configuration mode. In this mode, the Chromecast broadcasts its own wireless network for setup, allowing malicious entities to hijack the device. Dan Petro of Bishop Fox (a global security consulting firm) demonstrated this vulnerability by creating the RickMote, which attempts to deauth any Chromecast device within range and stream the Rick Astely video "Never Gonna Give You Up" [2]. Kaspersky Lab reconfirmed this issue recently in November of 2015.

The new Chromecast uses multicast Domain Name System (mDNS) for discovery purposes. There are a few published vulnerabilities with mDNS, but initial research shows very few that are relevant towards our goal. The previous generation Chromecast utilized DIAL, which allowed commands to be sent to return device information, such as the app or video currently active or local information such as available wifi and detailed device information. No such related capabilities have been published for the newest Chromecast.

III. Outline of Research Contribution

IV. Timeline of Implementation Milestones

V. Evaluation Metrics

References

[1] Ali Tekeoglu, Ali Tosun, ?A Closer Look into Privacy and Security of Chromecast Multimedia Cloud Communications?, IEEE INFOCOM?15, International Workshop on Multimedia Cloud Communication, Hong Kong, April 2015

[2] http://www.bishopfox.com/blog/2014/07/rickmote-controller-hacking-one-chromecast-time/