ISSN 2395-1621

Detecting Tunneled Video Streams Using Traffic Analysis

[#1]Vidya Sudam Waghmare, [#2]Prof.Yashwant Ingle

[1]vidhiwaghmare@gmail.com
[2]Yashingle.vnit@gmail.com

RMDSchoolofEngineering Warje,Pune-411058

ABSTRACT

Detecting access to video streaming websites is the first step for an organization to regulate unwanted accesses to such sites by its employees. Adversaries often adopt circumvention techniques using proxy servers and Virtual Private Networks (VPNs) in order to avoid such detection. Traffic analysis based technique that can detect such tunneled traffic at an organization's firewall using signatures found in traffic amount and timing in targeted video traffic. We present the detection results on the traffic data for several popular video streaming sites

Keywords: traffic analysis, website fingerprinting, virtual private networks, machine learning, classifiers.

ARTICLE INFO

Article History

Received:30th December 2015

Received in revised form :

31st December 2015

Accepted:1st December , 2015

Published online :

2nd December 2015

I. INTRODUCTION

Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Traffic Analysis (TA) stems from the decade-old practice of detecting anomalies from the frequency of encrypted telegrams used for exchanging military information. Even in today's network, T A is an effective means of side-channeling because there is no practical way of masking the traffic entirely, since masking the traffic requires the channel to be constantly busy.The primary goal of T A in the networking context is to reveal knowledge of network traffic without accessing the packet contents.

The used information for T A is typically metadata such as packet size and packet timing. TA has been used as a means to uncover the language used in a session for encrypted Voice over Internet Protocols (VoIP) in and further used to uncover certain key phrases in . It is also proven to be effective to other protocols such as HTTP . The use of traffic analysis in identifying other protocols is an active area of research. Because of the above advantages, T A stands out as a competent technology to recognize video streaming traffic that is tunneled over VPNs.

Symptoms and medications are two important types of information that can be obtained from clinical notes. Symptom related information such as diseases, syndromes, signs, diagnose etc., can be used to analyze diseases for patients. In addition, valuable medication information is commonly embedded in unstructured text narratives spanning multiple sections in clinical documents[5]. Medication information from clinical notes is often expressed with medication names

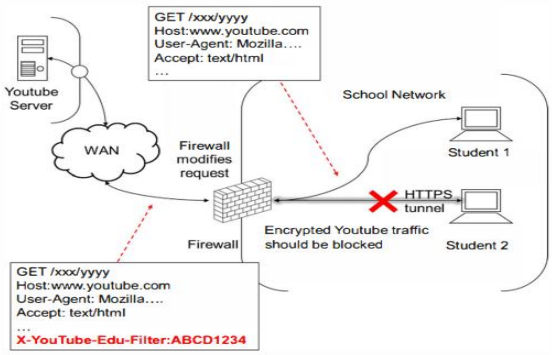

Fig 1.Structure and mechanism for YouTube for Schools

© 2015, IERJ All Rights Reserved

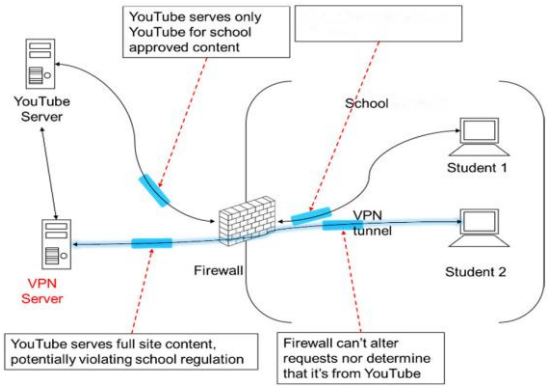

Fig 2. Bypassing Firewall Rules Using VPN

II. RELATEDWORK

Video Streaming Protocols

"Streaming" represents when data is sent in such a format that processing based on partial data is possible. As a result, neither the server nor the client needs to obtain the data in its entirety before serving or processing it. Streaming protocols are at the core of the services provided by video streaming websites due to its obvious advantages. Video files are usually large, but their temporal locality of information is significant since only a small portion of the data is needed at any time. Therefore, streaming of video can save a significant amount of storage space on both server and client side, as well as saving bandwidth and processing power needed for encoding and decoding video.

There are many video streaming protocols

1. Real Time Streaming Protocol (RTSP)
2. Real Time Message Protocol (RTMP)
3. HTTP progressive downloading
4.Smooth Streaming

RTSP

RTSP was first developed by RealNetworks, Netscape, and Columbia University in 1996, and then standardized in 1998 RTSP provides a client with methods to connect to a stream server, obtain information about a certain streaming source and initiate a streaming session. It is, however, is not responsible for transmission of the stream. Real Time Protocol (RTP) and Real Time Control Protocol (RTCP) are used for the actual transfer process. RTP is usually used in conjunction with RTCP. RTP is responsible for transferring data, while RTCP is responsible for giving feedback to the streaming server or a client for quality control and bandwidth control. Collectively, these three protocols are known as the RTSP protocol stack. RTSP is based on Transmission Control Protocol (TCP), while RTP and RTCP are all based on User Datagram Protocol (UDP).

A depiction of the different channels used in the RTSP stack is shown in Fig. RTSP is used by YouTube when Adobe Flash Player is not available. Such situation includes when accessing Server Original Video

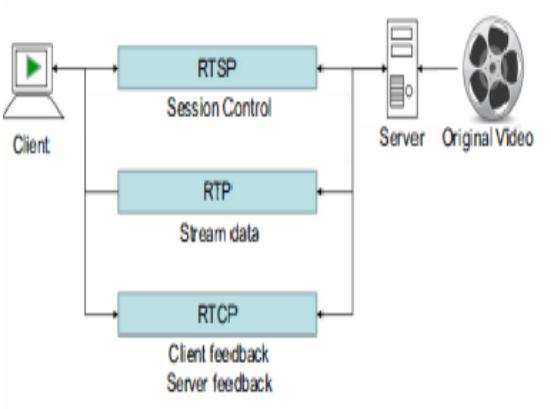

Fig.3 . RTSP

RTMP

RTMP is first developed by Macromedia as a protocol to stream audio/video over the Internet for use of Flash player. It is popularized by the widespread adoption of Flash player as a cross- platform streaming client. The main distinction of RTMP compared to the standardized RTSP stack is that RTMP uses only one TCP based connection for session control, data link, and quality control. Its ability is similar to that of RTSP. YouTube's default player is based on Adobe Flash Player and
therefore uses RTMP.

SMOOTH STREAMING

Smooth Streaming is an HTTP based streaming protocol developed by Microsoft for use with its Silver light rich-client framework . On a Smooth Streaming server, a video content is saved as small slices, each of which is only a few seconds long. Multiple versions of the same slice with different quality factors are prepared. The client downloads the slices at a certain rate via HTTP, measures the network condition and downloads slices of lesser qualities when the network is congested to ensure that the video playback is smooth. This protocol is also used by Nettlix video streaming services.

As "wrapper protocols", streaming mechanisms are generally designed to work with any video or audio encoding standard ("co dec" for short), and therefore do not restrict the type of stream data sent over them. This is possible because of the inherent "streaming" nature of video. Older codecs that do not consider streaming to be a high priority, like Motion Picture Expert Group (MPEG) are also designed such that the video can
be played in one sequential read [10]. The design foreshadows the application of video streaming because the player does not need the entire file. Instead only a small and localized portion is needed at any time to play the video. The same design remains in today's popular video codecs

III. DISCUSSION

VIRTUAL PRIVATE NETWORK

A VPN extends a private network across public networks.VPN keeps the privacy of sensitive information by putting the network traffic through a secure tunnel. The tunnel ensures that the message body, and the real source/destination information are encrypted between the 2 ends of the tunnel. The tunnel can be stretched across public networks, where it is possible for adversaries to tap into the

© 2015, IERJ All Rights Reserved

traffic yet unable to decrypt the information or reveal the actual source and destination.

There are many variations of VPN in terms of the tunneling protocol a VPN uses to create a secured tunnel. Two of thE p opular protocols in use are the Internet Protocol Security (IPsec), and the Secure Socket Layer/Transport Layer Security (SSLlTLS). IPsec works at the network layer, whereas SSLlTLS works at the transport layer. Their capabilities on protecting the traffic payload are similar, but their difference lies in the way they protect the metadata of the packets being transported.

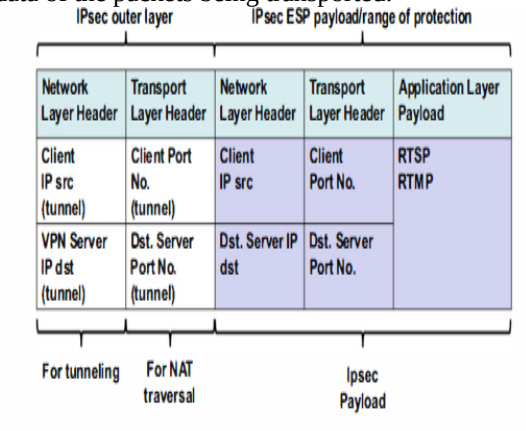

Fig 4.IPsec

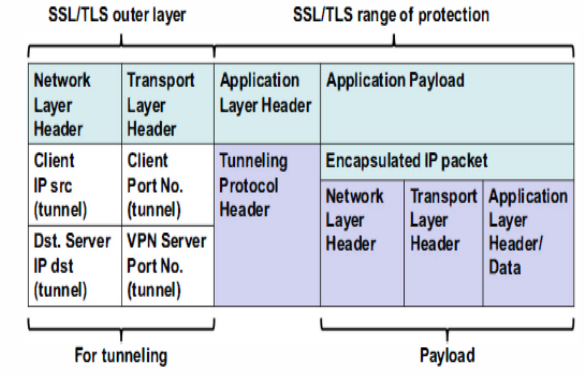

Fig.5SSL

IV. CONCLUSION AND FUTURE SCOPE

Thus conclude that, solve the problem of detecting video streaming traffic tunneled through VPN or proxy servers. It was proven that with Traffic Analysis (TA) based recognition methods, it is possible to recognize video streaming traffic
tunneled through a certain VPN service with low false positive rate, even when the classifier deals with traffic from hosts that are unknown in the training process

REFERENCES

[I] Sandvine Incorporated, "Sandvine Global Internet Phenomena Report 2014 I H," 14 May 2014. [Online]. Available:
https:llwww.sandvine.comldownloads/generallglobal-internet-phenomena 120 I 4/1 h-20 I 4-global-internet-phenomena-report.pdf. [Accessed 0 I Sep 2014].
[2] Google. Inc, "How YouTube for Schools Works," [Online]. Available:
https:llsupport.google.com/youtube/answerI2695317?hl=en. [Accessed 01 Sep 2014].
[3] I. Phantom Technologies, "iBossTM Introduces Encrypted YouTube
[4] T. Dierks and E. Rescorla, {The Transport Layer Security (TLS) Protocol Version 1.2}, IETF, 2008.
[5] T. Rowan, "{VPN technology: IPSEC vs SSL}," Network Security, vol. 2007, no. 12, pp. 13-17, #dec# 2007.
[6] J.-F. Raymond, "{Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems}," in Designing Privacy Enhancing Technologies, vol.
2009, H. Federrath, Ed., Berlin, Heidelberg, Springer Berlin Heidelberg, 2001, pp. 10-29.
[7] C. V. Wright, L. Ballard, F. Monrose and G. M. Masson, "Language Identification of Encrypted VoIP Traffic: Alejandra Y Roberto or Alice and Bob?," in Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, Berkeley, CA, USA, 2007.
[8] C. V. Wright, 1. Ballard, S. E. Coull, F. Monrose and G. M. Masson, "Spot
Me if You Can: Uncovering Spoken Phrases in Encrypted VoIP Conversations," in Proceedings of the 2008 IEEE Symposium on Security
and Privacy, Washington, DC, USA, 2008.
[9] A. Panchenko, L. Niessen, A. Zinnen and T. Engel, "Website Fingerprinting in Onion Routing Based Anonymization Networks," in
Proceedings of the 10th Annual ACM Workshop on Privacy in the
Electronic Society, New York, NY, USA, 20 II.
[10] D. Herrmann, R. Wendolsky and H. Federrath, "Website Fingerprinting:
Attacking Popular Privacy Enhancing Technologies with the Multinomial Naive-bayes Classifier," in Proceedings of the 2009 ACM Workshop on
Cloud Computing Security, New York, NY, USA, 2009.
[11] K. P. Dyer, S. E. Coull, T. Ristenpart and T. Shrimpton, "Peek-a-Boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail," in
Proceedings of the 2012 IEEE Symposium on Security and Privacy, Washington, DC, USA, 2012

© 2015, IERJ All Rights Reserved