Detecting Parallel Covert Data Transmission Channels in Video Conferencing Using Machine Learning / Ofir Joseph

Abstract

Covert communication channels are a concept in which a policy-breaking method is used in order to covertly transmit data from inside an organization to an external or accessible point. VoIP and Video systems are exposed to such attacks on different layers, such as the underlying real-time transport protocol (RTP) which uses Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packet streams to punch a hole through Network address translation (NAT). This paper presents different innovative attack methods utilizing covert communication and RTP channels to spread malware or to create a data leak channel between different organizations. The demonstrated attacks are based on a UDP punch hole created using Skype peer-to-peer video conferencing communication. The different attack methods were successfully able to transmit a small text file in an undetectable manner by observing the communication channel, and without causing interruption to the audio/video channels or creating a noticeable disturbance to the quality. While these attacks are hard to detect by the eye, we show that applying classical Machine Learning algorithms to detect these covert channels on statistical features sampled from the communication channel is effective for one type of attack.

The research findings and results presented in this thesis have been published in the Electronics journal, emphasizing the importance and impact of the study.

Joseph O, Elmalech A, Hajaj C. Detecting Parallel Covert Data Transmission Channels in Video Conferencing Using Machine Learning. Electronics. 2023; 12(5):1091. https://doi.org/10.3390/electronics12051091

MMS Number: 9926933509905776