Defense Against Covert Channel Cyber-attack Over Video Stream Payload

Researchers

Prof. Ofer Hadar
hadar@bgu.ac.il

Yoram Segal
yoramse@post.bgu.ac.il

Publications

R. Dubin, A. Dvir, O. Pele and O. Hadar, "I know what you saw last minute: Encrypted HTTP adaptive video streaming title classification," IEEE Transactions on Information Forensics & Security, Vol. 12, No. 12, pp. 3039-3049, 2017.

R. Segal, R. Birman, E. Hadas and O. Hadar, "Defense from covert channel cyber attack over video stream payload," RESCUE 2017 workshop, 22nd IEEE European Test Symposium, Limassol, 2017.

R. Segal , E. Segal and O. Hadar, "Cyber attack/defense based on estimated motion vectors via covered channel," TRUDEVICE Workshop Barcelona, 2016.

R. Dubin. A. Dvir, O. Pele, and O. Hadar, "I Know what you saw last minute: The Chrome browser case," Blackhat Europe 2016, London, 2016.

Y. Amsalem, A. Poznov. A. Bedinerman, M. Kotcher, and O. Hadar, "Cyber attack/defense algorithms based on data hiding in compressed video stream," SPIE Optics + Photonics Conference, San Diego, 2015.

Goals

Video streaming and image downloading account for 50% of Internet traffic today, a figure which is expected to rise to 67% of Web traffic by 2020. These attack routes provide a lot of space to implant malicious code (the image size and video bitrate may reach tens of megabits). Moreover, such covert channels do not utilize the computer's legitimate data transfer system and malware detection systems, enabling attackers to transfer data while evading detection. This research is aimed at investigating this attack model and developing countermeasures against this growing threat.

Description

In this project, researchers showed how the video compression domain can be used as a "backdoor" for cyber-attacks. In addition to demonstrating how to establish this channel, researchers showed the ease with which video streams can be used as a vehicle for passing sequences of commands and performing malicious actions remotely on a targeted computer; more specifically, they were able to create a covert channel with sufficient bandwidth to allow them to remotely control the computer without compromising the quality of the video stream. They also demonstrated how an attacker can exploit the estimated motion vector in the ubiquitous H.264 video stream. This can be done via proxies in near real-time with a limited amount of CPU consumption. The attack was demonstrated on several different platforms to show that the security breach is not hardware dependent.

Having shown the feasibility of this attack model, the researchers are now focusing on developing countermeasures. Their proposed Coucou solution, is based on advanced techniques aimed at providing a comprehensive solution against attacks conducted over video streams via covert channels. The techniques under development leverage the attack model and work on the frequency domain and motion vectors, without decreasing runtime or compromising image quality. The researchers are pursuing local solutions (the proposed technique is based on inserting random noise into the stream and allows the client to choose his/her protection level. Network and system solutions are also being considered, including a technique that involves changing and increasing the standard of compression to add a digital signature to the video stream.