Cyber Defense from Covert Channel Cyber-attack over video stream payload

Prof. Ofer Hadar and Yoram Segal

TOPICS WITHIN HORIZON 2020 PROJECTS

IDENTIFIER	TYPE	TOPIC	DEADLINE
SU-ICT-01-2018	IA	Dynamic countering of cyber-attacks	28 August 2018
SU-ICT-02-2020	RIA	Building blocks for resilience in evolving ICT systems	19 November 2019
SU-ICT-03-2018	RIA	Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap	29 May 2018

Video Attack Motivation

Popularity

- Multimedia traffic occupies roughly 50% of total internet bandwidth

Capacity

- Image size and video bit rate may reach tens of Mbit, hence an attacker can conceal big amounts of data.

Undetectable

- Image and video payload may be degraded by the attacker invisibility to the Human Visual System (HVS)

Permissive standard

- A hacker can change and embed data into the video payload without exceeding the standard

Research conducted in the field, headed by Prof. Ofer Hadar

- Manipulating DCT & motion vectors of a compressed video stream (H264 standard)
- The research focused on prevention (not detection) of the malicious data from attacking the victim.
- The team demonstrate how an attacker can create a covert channel with a reasonable bandwidth in a video stream.
- The study received attention from various media channels, including radio channels, newspapers and social networks.

- Y. Amsalem, A. Poznov. A. Bedinerman, M. Kotcher, and **O. Hadar**, "Cyberattack/defense algorithms based on data hiding in compressed video stream," in *SPIE Optics + Photonics conference*, 9-13 August 2015, San Diego, California (USA).
- R. Segal, E. Segal and **O. Hadar,** "Cyber Attack/Defense Based on Estimated Motion Vectors Via Covered Channel," in ***TRUDEVICE 2016***: Workshop on Trustworthy Manufacturing and Utilization of Secure Devices, 14th -16th November 2016, Barcelona, Spain.
- R. Segal, R. Birman, E. Hadas and **O. Hadar**, "Defense from Covert Channel Cyber-attack over video stream payload," in RESCUE 2017 workshop, part of the 22nd IEEE European Test Symposium, Limassol, May 25-26, 2017, Cyprus, May 25-26.
- R. Dubin. A. Dvir, O. Pele, and **O. Hadar**, "I Know What You Saw Last Minute – The Chrome Browser Case," in Balckhat Europe 2016, 1st-4th November 2016, London, UK.
- R. Dubin[S], A. Dvir[PI], O. Pele[PI] and **O. Hadar**[PI], "I Know What You Saw Last Minute – Encrypted HTTP Adaptive Video Streaming Title Classification" under final review in *IEEE Transactions on Information Forensics & Security*. (NOC = 0, IF = 2.441, IF (last 5 years) = 3.266. JR = 10/105, Q1).

Future topics for research and development under the H2020

- Authentication Methods & Standards for Video Compression
- Machine Learning & Data Mining tools for Video Attack detection
- Study the video rate distortion as a function of manipulated Compression Algorithm Payload Data (CAPD) such as DCT coefficients, Intra-Prediction parameters and Motion Vectors.
- Minimize the data redundancy in the video compress domain in order to block potential covert channel
- Attack Detection & System Immunization

Short description of the type and role of partner(s) we are seeking

- Yoram Segal is one of the H2020 proposal evaluator (independent experts) and he has vast experience H2020 proposal there for we are willing to establish the consortium and / or join one existing.
- We need At least 20 legal entities that are active in the Cyber field.
- They must be independent of each other and be established in at least nine different Member States or Associated countries.
- We are ready to lead the establishment of the Consortium. The coordinator will be define as part of the establishment process.
- Please email to Yoram Segal: yoramse@post.bgu.ac.il or to Prof. Ofer Hadar: ofer.hadar2@gmail.com