Announcement and Call for Papers

ManTra'20: 1st ACM SIGCOMM Workshop on Traffic Manipulation

August 14, 2020, New York City, USA

The first ACM SIGCOMM Workshop on Traffic Manipulation (ManTra'20) will be co-located with the ACM SIGCOMM conference and will be held at Columbia University, New York City, USA

Important Dates

- Paper Submission Due: 1 May 2020
- Acceptance Notification: 31 May 2020
- Workshop: 14 August 2020

Program Co-Chairs

Radia Perlman, *DELL/EMC*
Haya Shulman, *Fraunhofer Institute for Secure Information Technology SIT*

Program Committee

Mark Allman, *International Computer Science Institute (ICSI)*
Steven Bellovin, *Columbia University*
Danny Dolev, *The Hebrew University of Jerusalem*
Nick Feamster, *University of Chicago*
Amir Herzberg, *University of Connecticut*
Trent Jaeger, *The Pennsylvania State University*
Charlie Kaufman, *DELL/EMC*
Adrian Perrig, *ETH Zurich*
Zhiyun Qian, *UC Riverside*
Jennifer Rexford, *Princeton*
Michael Waidner, *Technische Universität Darmstadt*
Bing Wang, *University of Connecticut*

Web and Hotcrp Chair

Markus Brandt, *Fraunhofer Institute for Secure Information Technology SIT*

Overview

Network attacks using traffic manipulation can have profound societal consequences. These attacks are increasing in frequency, sophistication, and stealthiness. Motivations behind these attacks vary from financial, political, terrorism, and more. These attacks can be performed by off-path or by on-path (Man-in-the-Middle (MitM)) attackers or by malicious operators.
Traffic manipulations include attacks injecting malicious packets into the communication stream (e.g., injecting malicious scripts into TCP connections), manipulating time over NTP, attacking the IP layer by exploiting IP fragmentation for DNS cache poisoning, as well as redirecting communication, e.g., via BGP prefix hijacks. Traffic manipulation attacks aim to cause various types of denial of service, theft of crypto-currency, distribution of malware, disruption of governmental or financial organisations, censorship or surveillance.

The ManTra workshop provides a forum for researchers, practitioners, network operators, and the Internet standards community to present and discuss the state of the art in traffic manipulation attacks and countermeasures. The

workshop considers different types of attackers, from very strong ones such as the corrupt operators and MitM adversaries to weak off-path attackers and different type of attacks, all that utilise manipulation of traffic for achieving the attack goal, as well as the defences against them. The attacks can be sophisticated, utilising corruption of multiple building blocks in concert, or simple, against one specific system or protocol.

The goal of the ManTra workshop is to provide a venue that focuses exclusively on traffic manipulation attacks in the Internet and countermeasures against them, presenting a broad view of technologies and approaches for manipulating traffic (from injections into the communication stream to hijacking communication), evaluations and simulations thereof, identification of new techniques and vulnerabilities, bringing together researchers and practitioners in all areas of computer, networks and systems security for studying the problems and paving the ways towards deployment of defences. Works which identify new vulnerabilities allowing traffic manipulation attacks, works which evaluate attacks in the wild, or works that perform measurements to understand the scope or extent of the attacks as well as techniques used to launch them in the wild are all welcome.

Topics of Interest

Refereed paper submissions are solicited in all areas relating to research in traffic manipulations (incl. injections into all layers of TCP/IP and traffic hijacks) and defences, including but not limited to:

- Inter/Intra-domain routing security
- BGP/DNS security
- Privacy aspects of defences against traffic manipulation attacks
- Deployment of defences for routing against traffic hijacks (RPKI, BGPsec,...)
- Deployment of defences against DNS cache poisoning (DNSSEC,...)
- Internet measurements and simulations of attacks and defences
- Attacks against Internet Exchange Points
- In-network defences (e.g., in the data plane)
- Practical crypto-based defences
- Deployability and usability studies
- Leveraging traffic hijacks for sophisticated attacks against other systems and applications
- IP spoofing
- TCP/UDP/IP injection attacks
- Techniques for bypassing challenge-response authentication (ports, sequence numbers, ...)
- Sensor/Ad-hoc networks
- TCP/IP layers including link and physical layers
- Software Defined Networks (SDN)
- SDN data/control plane injections/hijacks

Submission Instructions

Mantra'20 welcomes original submissions of unpublished work from academia, independent researchers, students, hackers, industry. The submissions must not be under consideration at another conference or journal. Submitted papers must be in PDF format, at most six (6) pages long, including all figures, tables, and unlimited number of pages for references, in two-column 10pt ACM format. Papers must include authors names and affiliations for single-blind peer reviewing by the PC. Authors of accepted papers are expected to present their papers at the workshop. The proceedings will be included in the ACM Digital Library.

Systematisation of Knowledge

ManTra'20 welcomes also Systematisation of Knowledge (SoK) papers that evaluate and systemise state of the art in traffic manipulation. Such works include surveys and taxonomy of aspects related to traffic manipulation as well as papers that provide validation (through simulations or evaluations) of theories or folklore beliefs.

Workshop Format

The workshop will consist of presentations of peer-reviewed papers accepted for publication, of invited talks, mini-tutorials, and a panel discussion to encourage interaction among attendees. Everyone can register to participate in the workshop.