SPABox: Safeguarding Privacy and against Attacks at a MiddleBox

Jingyuan Fan
SUNY Buffalo

Chaowen Guan
SUNY Buffalo

Kui Ren
SUNY Buffalo

Chunming Qiao
SUNY Buffalo

Yong Cui
Tsinghua University

ABSTRACT

HTTPS is widely used over the Internet which encrypts traffic to provide secure and private data communication between clients and servers.

To cope with rapidly changing and sophisticated security attacks, network operators often deploy middlebox to perform Deep Packet Inspection (DPI) to detect attacks and potential security breaches, which requires from simple keyword matching to more advanced machine learning and data mining analysis. How can such middlebox work over HTTPS connection with encrypted traffic to support these DPI functionalities while preserving privacy?

In this paper, we present SPABox, a middlebox based system that supports both keyword based and data analysis based DPI functions over encrypted traffic. SPABox preserves privacy by using a novel protocol with a minimal overhead. We implement SPABox on a standard server and show that SPABox is practical for both long-lived and short-lived connection. Compared with the state-of-the-art Blindbox system (ACM SIGCOMM 2015), SPABox is more than 5 orders of magnitude faster and requires 7 orders of magnitude less bandwidth for system setup.

ACM ISBN 978-1-4503-2138-9.
DOI: 10.1145/1235