BlindIDS: Market-Compliant and Privacy-Friendly Intrusion Detection System over Encrypted Traffic

Sébastien Canard

Orange Labs (France)

Abstract :

The goal of network intrusion detection is to inspect network traffic in order to identify threats and known attack patterns. One of its key features is Deep Packet Inspection (DPI), that extracts the content of network packets and compares it against a set of detection signatures. While DPI is commonly used to protect networks and information systems, it requires direct access to the traffic content, which makes it blinded against encrypted network protocols such as HTTPS. So far, a difficult choice was to be made between the privacy of network users and security through the inspection of their traffic content to detect attacks or malicious activities. This paper presents a novel approach that bridges the gap between network security and privacy. It makes possible to perform DPI directly on encrypted traffic, without knowing neither the traffic content, nor the patterns of detection signatures. The relevance of our work is that it preserves the delicate balance in the security market ecosystem. Indeed, security editors will be able to protect their distinctive detection signatures and supply service providers only with encrypted attack patterns. In addition, service providers will be able to integrate the encrypted signatures in their architectures and perform DPI without compromising the privacy of network communications. Finally, users will be able to preserve their privacy through traffic encryption, while also benefiting from network security services. The extensive experiments conducted in this paper prove that, compared to existing encryption schemes, our solution reduces by 3 orders of magnitude the connection setup time for new users, and by 6 orders of magnitude the consumed memory space on the DPI appliance.

Joint work with Aïda Diop, Nizar Kheir, Marie Paindavoine, Mohamed Sabt.