High performance encrypted network traffic inspection using hardware accelerators

Eva Papadogiannaki and Sotiris Ioannidis
FORTH-ICS

Motivation

- By 2019, 80% of network traffic will be encrypted
- Traditional network inspection techniques that focus on packet contents are becoming insufficient

In an encrypted network packet, we can only inspect the header - not the payload

- Network traffic speeds are constantly increasing

Need to accelerate the packet processing procedure

FORTH

State of the Art

- Traffic decryption before inspection
  (e.g. BlindBox, Symantec's ETM)

- Encrypted traffic analysis using ML techniques; feasibility of classification using packet metadata
  (e.g. Conti et al.)

FORTH

State of the Art

- Traffic decryption before inspection
  (e.g. BlindBox, Symantec's ETM)

  ✗ **- Could cause privacy violations**
  - Expensive processing

- Encrypted traffic analysis using ML techniques; feasibility of classification using packet metadata
  (e.g. Conti et al.)

  ✗ **- No real implementation**

FORTH

Our solution

1. Build signatures generated using network packet metadata sequences (e.g. packet size, packet direction)

2. Develop a network inspection engine that searches for these signatures against the network traffic

3. Accelerate the packet processing procedure using GPUs

FORTH

Methodology, Evaluation

Come by our poster …

Thank you!

High performance encrypted network traffic inspection using hardware accelerators

Eva Papadogiannaki and Sotiris Ioannidis
FORTH-ICS