A NAIVE IMPLEMENTATION OF BLINDBOX: PROTOCOL I

Deep Packet Inspection over Encrypted Traffic

OUTLINE

- Introduction and Motivation
- BlindBox
  - System Overview
  - Threat Model
  - Evaluation Highlights
- A Naive Implementation of BlindBox: Protocol I
  - System Overview
  - Demo
  - Limitations
- Questions?

INTRODUCTION AND MOTIVATION

WHAT IS DEEP PACKET INSPECTION (DPI)?

- In-network middleboxes use DPI to examine and alter packets
- Used to enforce security policies
  - Intrusion detection/prevention, exfiltration prevention, parental filtering etc.

DPI AND HTTPS

- HTTPS and other encryption protocols have dramatically grown in usage
- Packet payloads are encrypted, middleboxes can no longer inspect them
- To enable inspection, some systems support *insecure* HTTPS
    - Main-in-the-middle attack on SSL

Functionality of Middleboxes

or

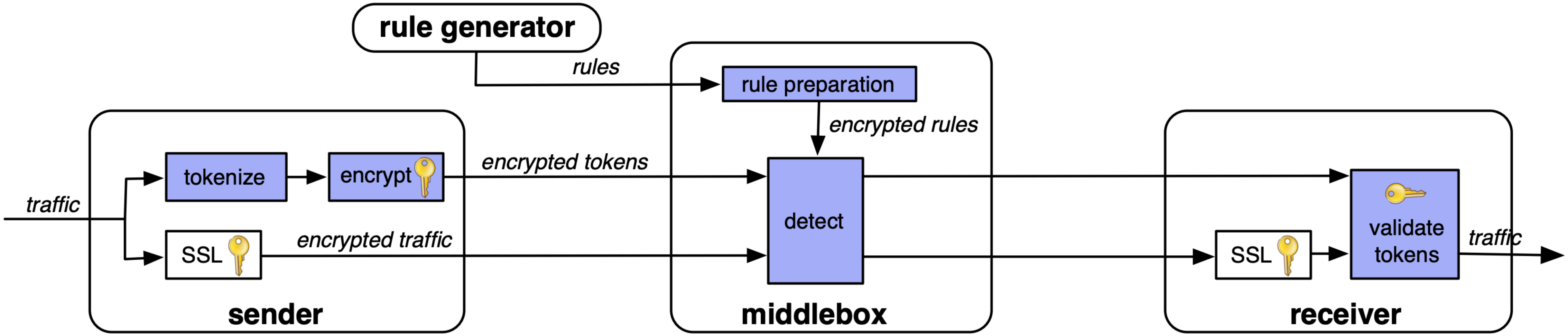
Privacy from Encryption

Can we get both?

BLINDBOX

BLINDBOX: BOTH PRIVACY AND DPI

- Detection
  - Middlebox receives both SSL-encrypted traffic and encrypted tokens
  - Detect module searches for matches between encrypted rules and encrypted tokens
- Receive
  - Receiver decrypts and authenticates traffic using normal SSL
  - Receiver also checks that encrypted tokens were encrypted properly by sender



THREAT MODEL SUMMARY

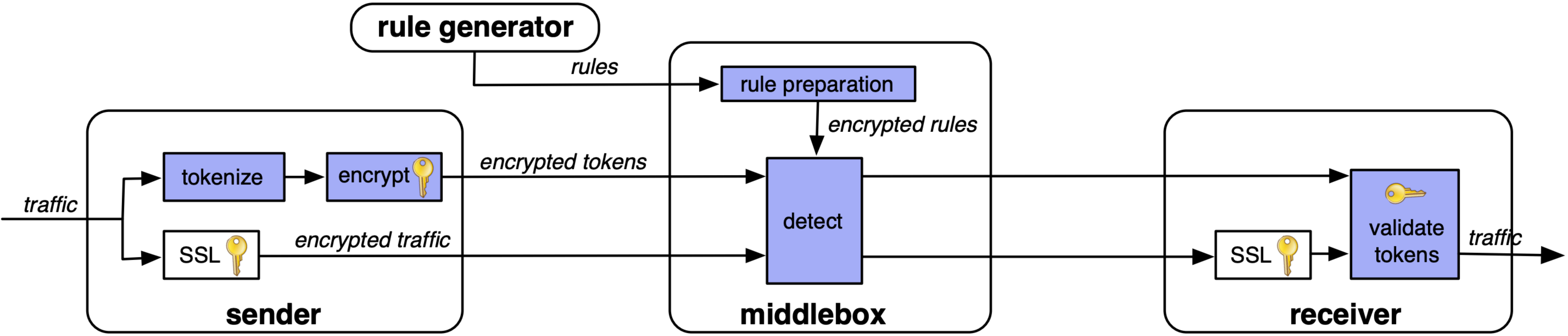
- Clients
  - Want to protect privacy from middlebox AND protection from each other
  - Requires: at least one client must be honest
- Middlebox
  - Honest but curious
  - Can only see what is necessary to enforce security policy
- Rule Generator
  - Must be trusted by both middlebox and clients
  - Cannot actually observe or alter traffic

EVALUATION HIGHLIGHTS

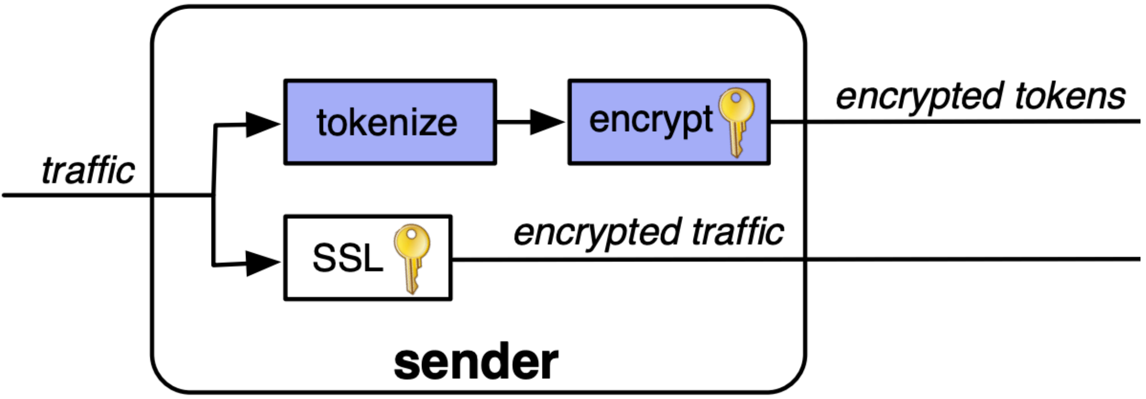
- Functionality:
  - Seems to cover the majority of use cases, esp. with protocol III
- Detection Time: Similar to existing IDS
  - 186Mbps with BlindBox (compare to Snort at 85Mbps)
- Transmission Time: Reasonable overhead
  - Page load completion time increases by 0.15-1x (ignoring setup)
- Setup Time: Very slow
  - 97 secs for 3000 rules
  - This could be OK when connections are persistent

A NAIVE IMPLEMENTATION OF BLINDBOX: PROTOCOL I

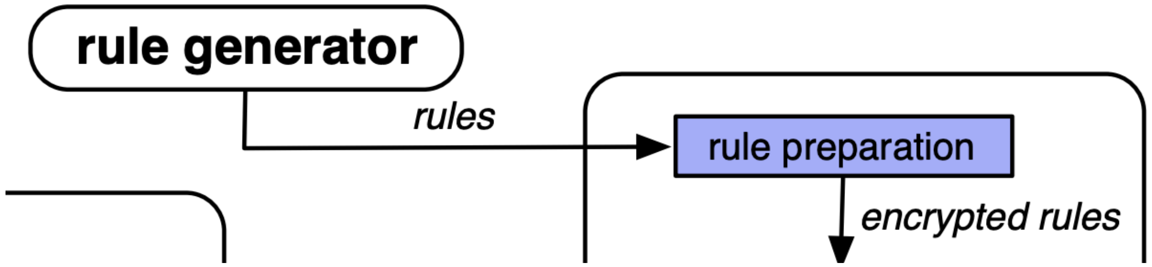
BLINDBOX: PROTOCOL I



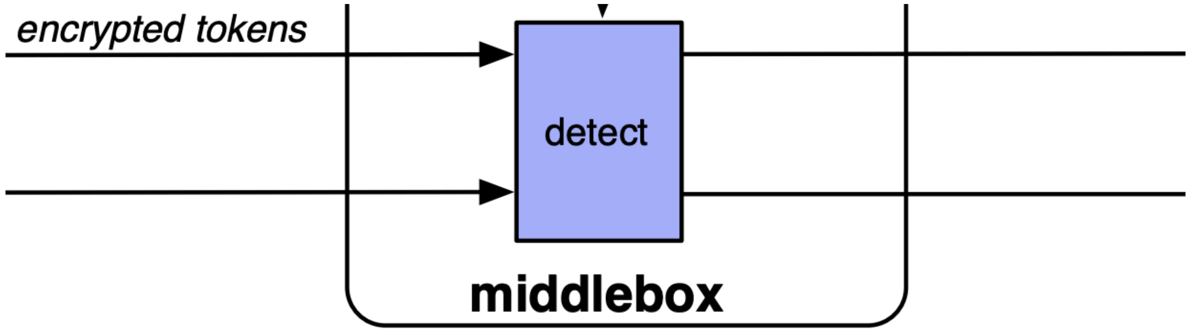
SENDER.PY


traffic
tokenize
encrypt
encrypted tokens
SSL
encrypted traffic
sender

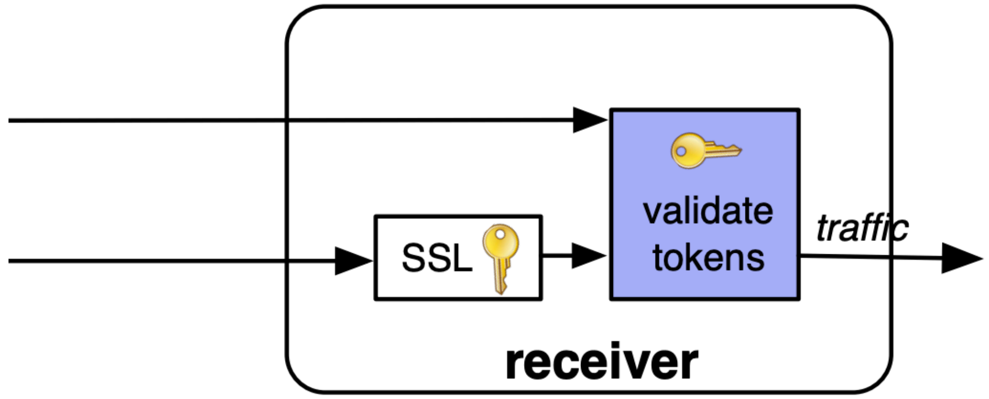
RULE_GENERATOR.PY



MIDDLEBOX.P4



RECEIVER.PY



DEMO

LIMITATIONS

QUESTIONS AND COMMENTS?

Thank you.