PRESTO

PRocessing Encrypted Streams for Traffic Oversight

Project ANR-19-CE39-0011
Coordinator: David Pointcheval
Paris, ANR kick-off meeting, 2019
Traffic Analysis: Cybersecurity

Scenarii:

- Mitigate cyber attacks:
  - detect intrusion attempts
  - avoid (distributed) denial of service
  - block malwares
- Forensic analysis
- Protect users: content filtering

Requirements:

- Real-time analysis of data streams
- Afterwards study on disk storage and data streams
- Construction of models for analysis
Traffic Analysis: Encrypted Streams

Data analysis:

- Design of models
- Decision from data streams

Some techniques known on cleartext

Encrypted data:

- But https has replaced http: flows are encrypted
- GDPR: General Data Protection Regulation

Data must be analyzed or kept in an encrypted way
State of the Art

- Use of the meta-data/header:
  Because of encrypted flows, only headers are available in clear
  - good for intrusion detection, (D)DoS prevention
  - not enough for content filtering, malware detection, forensic

- Cryptographic primitives:
  Searchable encryption (a.k.a. Encryption with Keyword Search)
  - can improve intrusion detection and (D)DoS prevention
  - can help for malware detection and content filtering
  Fully homomorphic encryption (FHE) and multi-party computation (MPC)
  - can address forensic analysis and models re-inforcement
Goal of the Project

PRESTO
PRocessing Encrypted Streams for Traffi

WP1: Requirements and design of new architecture
WP2: Cryptographic primitives
WP3: Prototype specification and implementations

→ Improve/adapt cryptographic primitives for cybersecurity
Concrete Use-Cases

› Content filtering:
  - on-line and real-time control of encrypted stream
  - off-line model re-inforcement

› (Distributed) Denial of service detection:
  - real-time detection from a combination of cleartext header information
  - and encrypted stream

› Forensic analysis:
  - no time constraint
  - analysis of disks and/or logs
WP1
Requirements and design of new architecture

Specification of the use-cases

Design of the architecture

- On-line analysis of cleartext or encrypted stream
- Off-line analysis (model improvement or forensic)
Adapt and improve primitives (ENS and Orange Labs)

- Public-Key Encryption with Keyword Search
- Functional Encryption
- Fully Homomorphic Encryption
- Multi-Party Computation
Still considering the three use-cases

- Implementation of the cryptographic primitives
- Prototypes for the three use-cases
  - Content filtering (LORIA)
  - Forensic analysis (IMT)
  - DDoS attack mitigation (6cure)
- Validation