# DNSSM: A Large Scale Passive DNS Security Monitoring Framework

*Samuel Marchal, Jérôme François, Cynthia Wagner, Radu State, Alexandre Dulaunoy, Thomas Engel, Olivier Festor*

UNIVERSITÉ DU LUXEMBOURG

SnT

Fonds National de la Recherche Luxembourg

SMT

# Outline

SMT

# Outline

SNT

# Overview of DNS

- DNS (Domain Name System) is the service that maps a domain name to its associated IP addresses

  `www.example.com` $\Longrightarrow$ `123.45.6.78`

- DNS is the service that allows to find information about a domain :
  - A : IPv4 address
  - AAAA : IPv6 address
  - MX : Mail server
  - NS : Authoritative DNS server
  - TXT : any information

SNT

# Why DNS monitoring ?

- DNS:
  - critical Internet service
  - threats: cache poisoning, typosquatting, DNS tunnelling, fast/double-flux
    $\Rightarrow$ enhance: phishing, botnet C&C communications, covered channel communications etc.

  $\Rightarrow$ Patterns in DNS packet fields and DNS querying behavior
- Passive DNS monitoring to detect:
  - worm infected hosts
  - malicious backdoor communication
  - botnet participating hosts
  - phishing websites hosting

SNT

# Existing solutions

- Mainly use supervised classification techniques
  - SVM, tree, rules, etc.
  - require malicious data for training
- Targeted identification of malicious domains
  - C&C communication involved domains
  - Phishing domains
  - Spamming domains
  - etc.

SMT

# Outline

SNT

# Clustering

*Automated clustering technique for online analysis*

- No previous knowledge
- Group domains regarding their activity
- DNS information $\Rightarrow$ Domain activity
- Disclose the raise of new threats
- K-means clustering
- 10 relevant features

SNT

# Features

*For each domain observed:*

- Number of IP addresses
- IP scattering : entropy based and position weighted
- mean TTL
- Requests count
- Period of observation
- Requests per hour
- Name servers count
- Number of subdomains
- Blacklisted flag

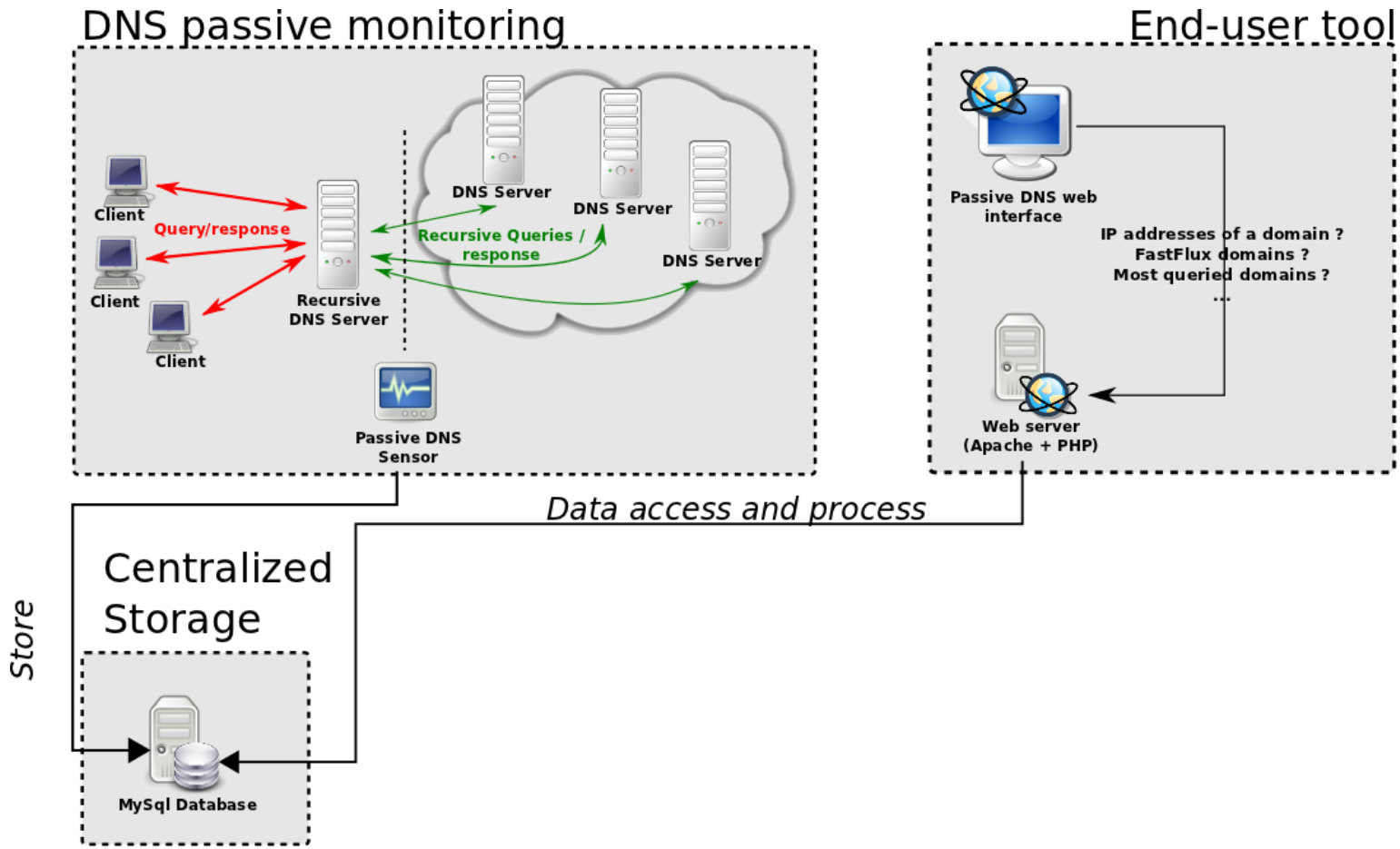
SMT

# User interface

*DNSSM is an approach for automated analysis of DNS (passive traffic)*

- Manual assistance in tracking anomalies:
  - Feed with cap file
  - All DNS packet fields extracted
  - MySQL database storage model
  - Web interface
  - Fast and efficient mining functions
  - Integrates with existing blacklist tools to assist in tagging data
  - Detection of fast/double flux domains, DNS tunnelling, etc.
  - Freely downloadable at: `https://gforge.inria.fr/\docman/view.php/3526/7602/kit_dns_anomalies.tar.gz`

# Architecture

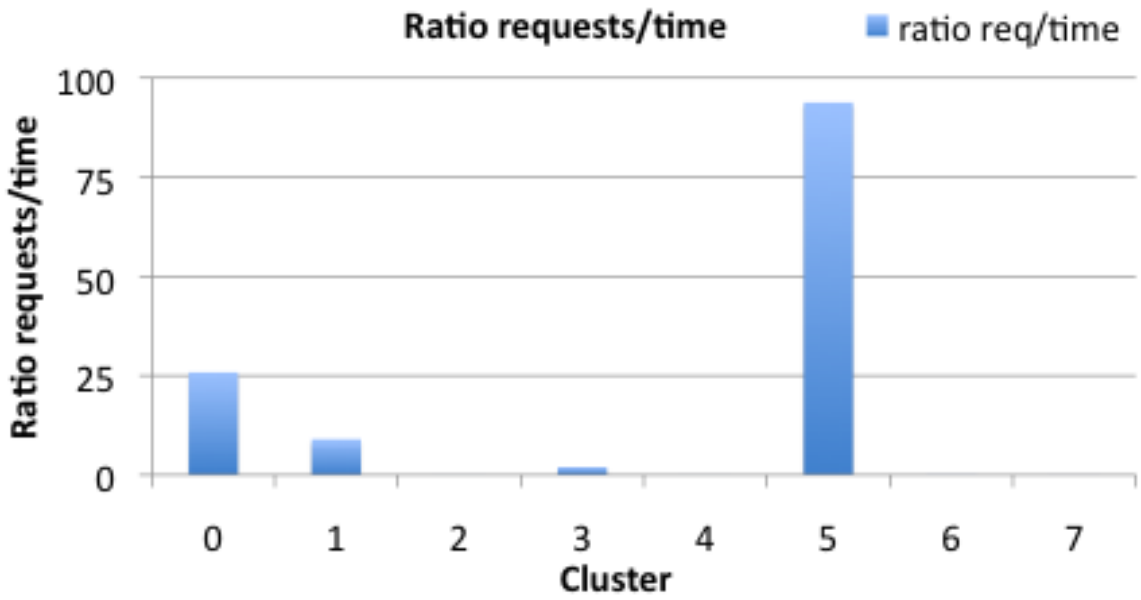


SMT

# Outline

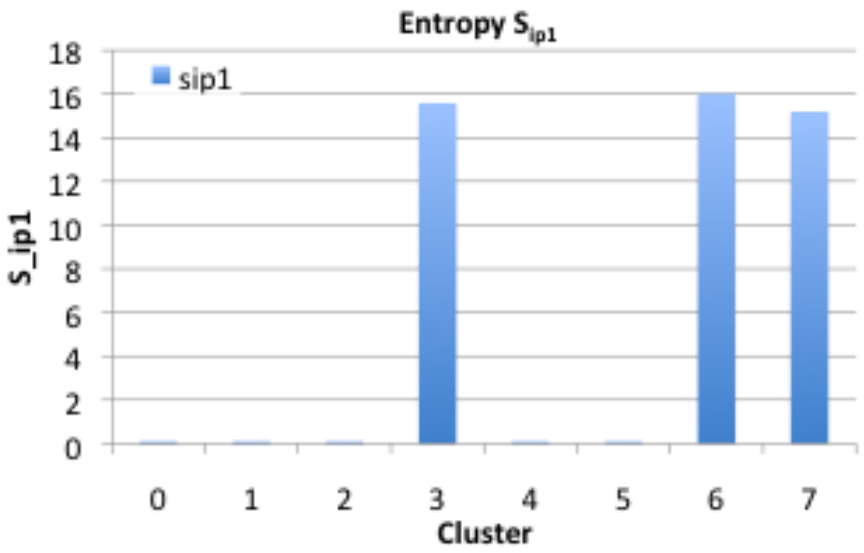
# Experiments

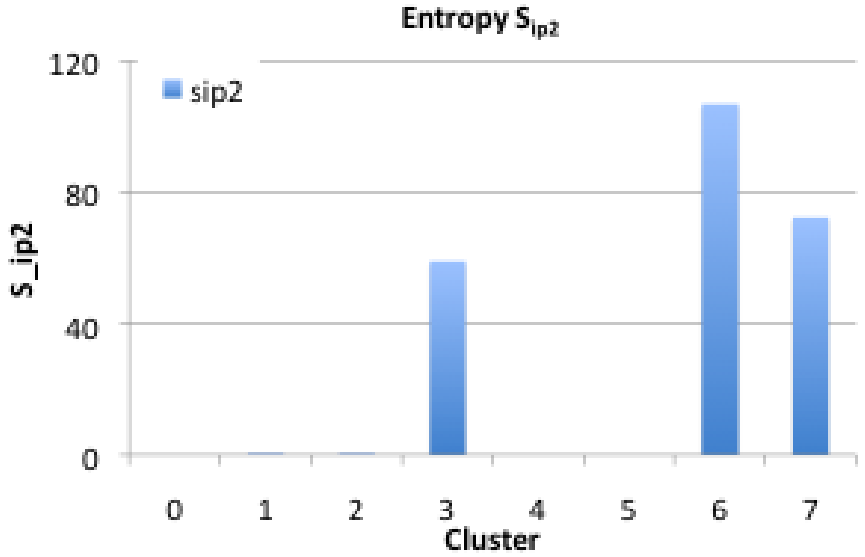
- 2 datasets ($\neq$ location, $\neq$ type of network, $\neq$ users, $\neq$ quantity)
- Automatic results from k-means: 8 clusters exhibiting different properties




- Cluster 5: apple.com, amazon.fr, adobe.com(highly popular websites)

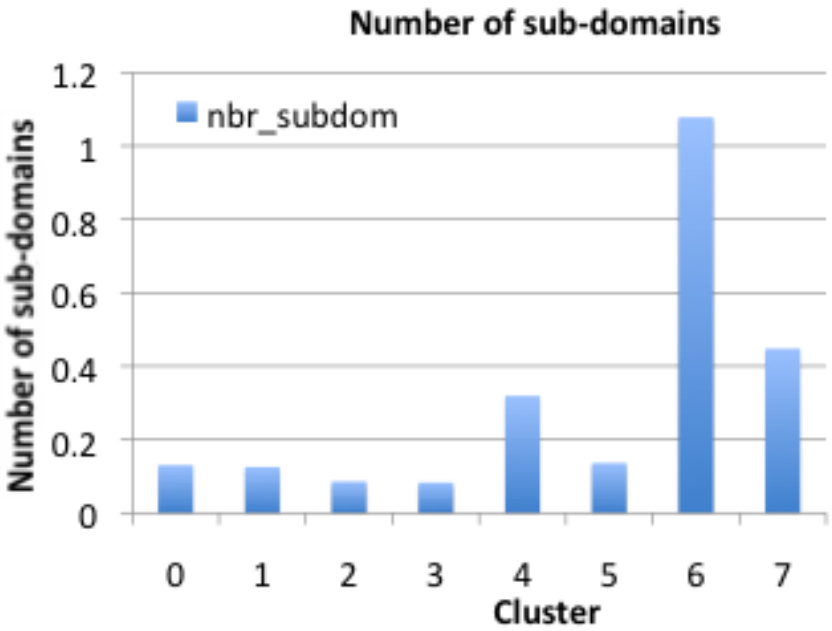
# Results

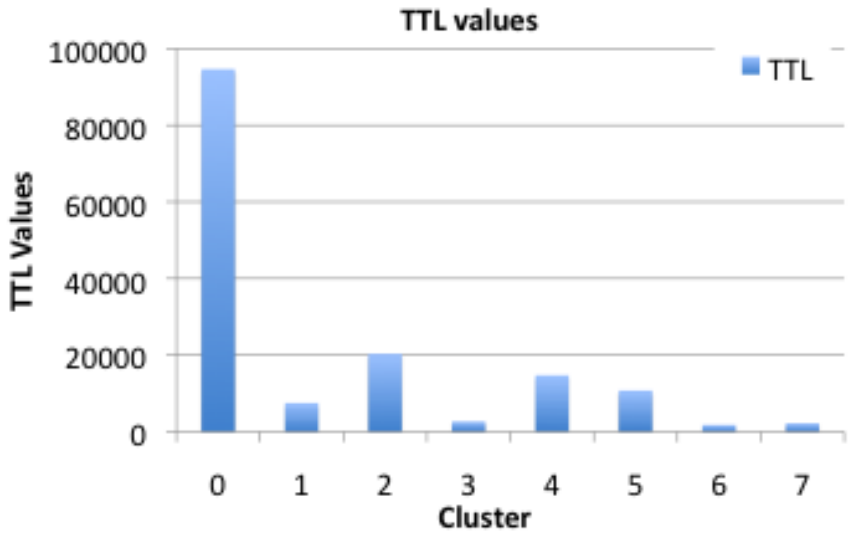



- Cluster 6: google.com. skype.com, facebook.com (higly popular web sites)
- Cluster 7: tradedoubler.com, doubleclick.net, quantcast.com (user tracking)
- Cluster 3: akamai, cloudfront.net (CDN)

# Results




- Cluster 0: small websites with low popularity

SMT

# Outline

SnT

# Conclusion

- Passive DNS monitoring solution
  - Analysis of domain names activity
  - Relevant data mining algorithm (unsupervised clustering techniques)
  - Efficiency proved on two different datasets
  - Freely downloadable interface
- Applications:
  - Investigate cyber security fraud
  - Debug DNS deployment
  - Penetration testing

# DNSSM: A Large Scale Passive DNS Security Monitoring Framework

*Samuel Marchal, Jérôme François, Cynthia Wagner, Radu State, Alexandre Dulaunoy, Thomas Engel, Olivier Festor*

UNIVERSITÉ DU LUXEMBOURG

SnT

Fonds National de la Recherche Luxembourg