A Trusted Knowledge Management System for Multi-layer Threat Analysis

Thanasis Petsas [1], Kazuya Okada [2], Hajime Tazaki [3], Gregory Blanc [4], and Pawel Pawliński [5]

[1] Institute of Computer Science, Foundation for Research and Technology—Hellas, Greece
[2] Nara Institute of Science and Technology, Japan
[3] The University of Tokyo, Japan
[4] Institute Mines-Télécom / Télécom SudParis, CNRS UMR 5157 SAMOVAR, France
[5] CERT Polska, Poland

petsas@ics.forth.gr, kazuya-o@is.naist.jp, tazaki@nc.u-tokyo.ac.jp,
gregory.blanc@telecom-sudparis.eu, pawel.pawlinski@cert.pl

Motivation

- **Widespread attacks**
  - Large scale attacks against infrastructures or endpoints [1]
- **New technological advances**
  - New generations of malicious code are increasingly stealthy, powerful and pervasive [2]
- The European Union, Japan and US develop national cybersecurity programs
- *A shared need for better understanding of this kind of large scale threats*
- Basic requirements
  - Handling large volumes of data collected from distributed probes
  - Performing efficient cross-layer analysis

Trusted Knowledge Management System (tKMS)

tKMS

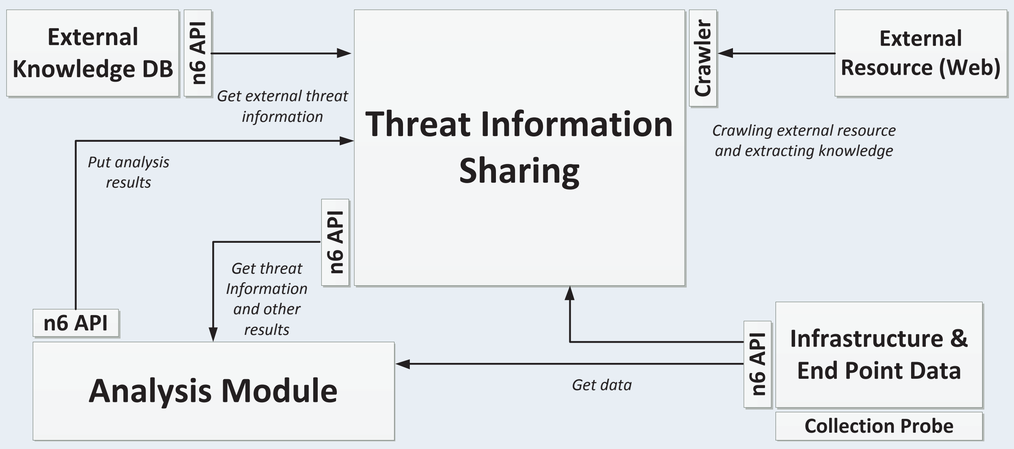
The system will cover a huge set of data sources, analysis modules and a common data sharing format.

Information, stored in tKMS, will be used for direct feedback to the policy enforcement points (PEPs).

Main features

- Great variety of sensors
- Actionable information for cyberdefense systems
- Common lightweight data sharing format (n6 API)
- Preservation of data confidentiality across the different components

tKMS Architecture



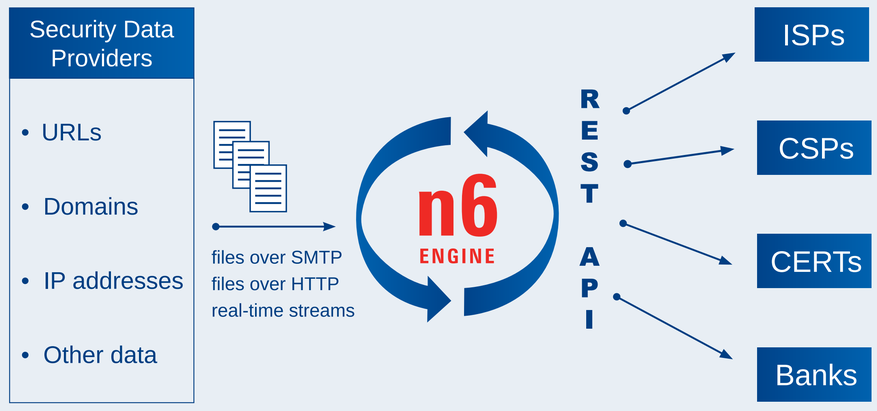
Components Description

- **External Knowledge System**
  - A source of cyber-threat information in a standard format (e.g., vulnerabilities database)
- **External Resources**
  - Sources that do not provide any data sharing interface (e.g., data gathered from crawlers)
- **Threat Information Sharing**
  - Manages and correlates data from Analysis Modules, External Knowledge systems, etc.
- **Analysis Module**
  - Detects cyber-threats by analyzing infrastructure and end point layers data
- **Infrastructure & End Point Data**
  - Data collected from infrastructure or end point devices by means of probes

Data Sources

- **Traffic data**
- **DNS server traces**
- **Topology information**
- **Telescope traces**
- **Early warning systems**
- **Spam archives**
- **Web sources**
- **User behavior traces**
- **Sinkhole data**
- **Honeypots and Sandboxes**

Common Data Exchange Format



The n6 platform

- A platform for acquisition and exchange of data regarding Internet threats
- Provides a simple REST-ful API for data retrieval
  - defines both query and response formats
- Communication over HTTPS with mandatory authentication via TLS client certificates, to ensure confidentiality and trustworthiness
- Event-based data model for all types of security information (JSON format)
- Efficient, reliable and fast delivery of large volumes of network incident data
- A good candidate for exchange of heterogeneous datasets

n6 platform website: http://n6.cert.pl/

Cross-layer Analysis

Development of cross-layer correlation techniques for the identification of specific threat campaigns

- Simple techniques, e.g., time or address correlation
- More advanced techniques, i.e., data mining and machine learning algorithms
- Enable the threat analysis platform to utilize automatic knowledge collection capabilities

About NECOMA

Nippon-European Cyberdefense-Oriented Multilayer threat Analysis (NECOMA) addresses the aspects of

- **Data collection**
  - Leveraging past and current work on the topic
- **Threat data analysis**
  - Not only from the perspective of understanding attackers and vulnerabilities, but also from the point of view of the target and victim
- **Develop and demonstrated new cyberdefense mechanisms**
  - leveraging the above metrics for deployment and evaluation

These three aspects will be analyzed both from an infrastructure perspective and end points. The results of the NECOMA project will be showcased in demonstrators that will highlight the innovations of the project and prepare exploitation

NECOMA website: http://www.necoma-project.eu/

References

[1] Martin Brown. Pakistan hijacks youtube. http://www.renesys.com/2008/02/pakistan-hijacks-youtube-1/.

[2] David Kushner. The real story of stuxnet. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

This work was supported in part by the FP7 project NECOMA funded by the European Commission under Grant Agreement No. 608533 and the Ministry of Internal Affairs and Communication (MIC) in Japan.