Fraunhofer
FKIE

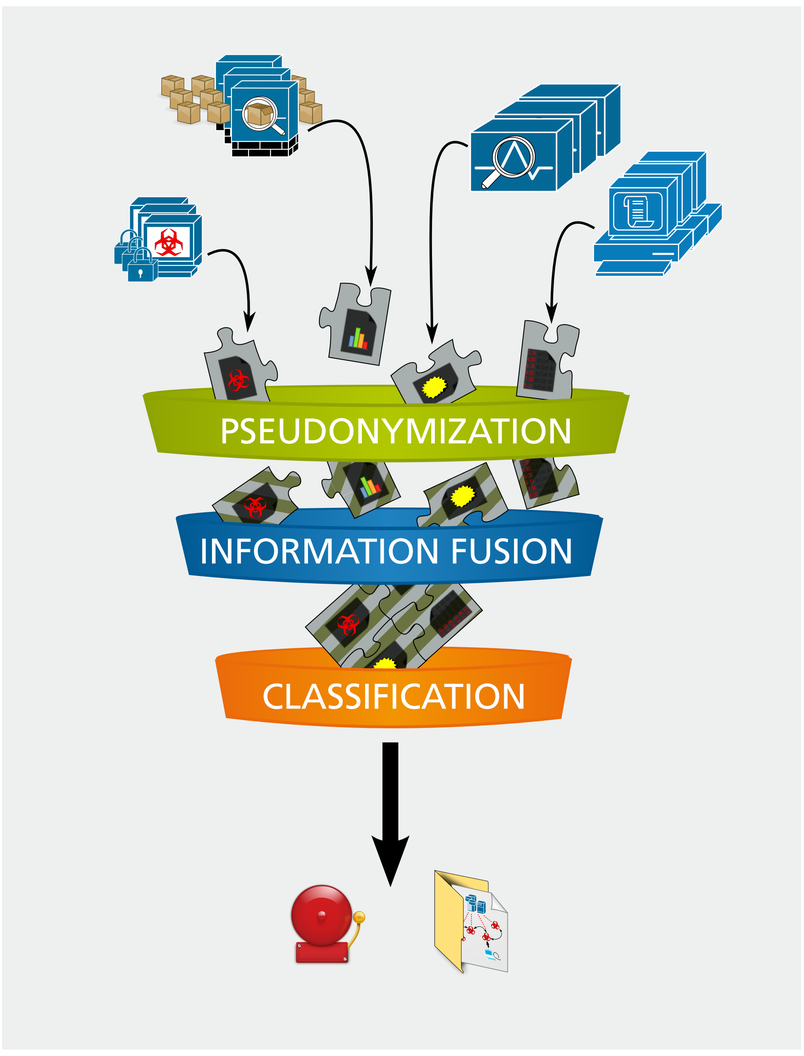
FRAUNHOFER INSTITUTE FOR COMMUNICATION, INFORMATION PROCESSING AND ERGONOMICS

DISTRIBUTED COOPERATIVE MONITORING FOR NETWORK ANOMALY DETECTION

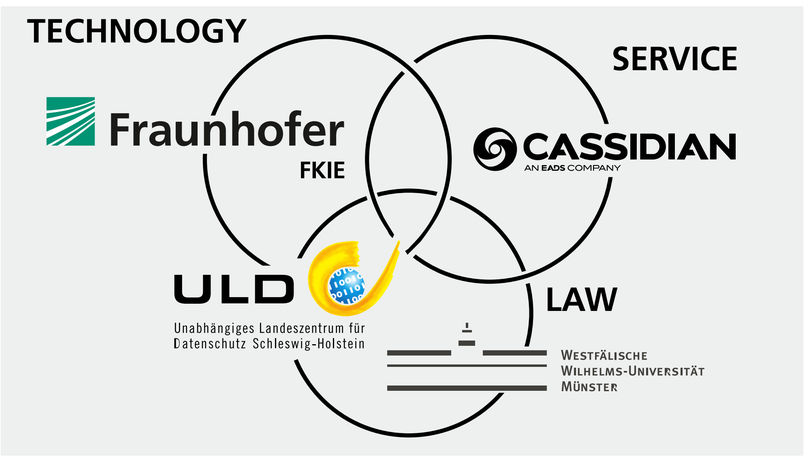
Till Elsner, Michael Meier, Arnold Sykosch, Matthias Wübbeling
{till.elsner, michael.meier, arnold.sykosch, matthias.wuebbeling}@fkie.fraunhofer.de

MonIKA

Todays society heavily relies on Internet infrastructure. Facing threats of a decentralized structure, securing this infrastructure becomes a continuously more challenging task. Cooperative monitoring helps to reveal anomalies that cannot be detected locally. This approach requires continuous sharing of information between autonomous parties. Passing on data may expose confidential or private information regarding network structure or customer identities. The MonIKA project aims to provide a solution that respects technical, legal, as well as organizational facets of this issue. The cooperating partners develop a framework for exchange and analysis of security related information across authority borders that is well embedded in necessary service structures and fulfills given legal requirements. The detection platform itself consists of three conceptual layers: pseudonymization, information fusion and classification. While the first step protects the data owners' interest in privacy preservation, the next step consolidates the information for classification analysis. This model provides comprehensive data for classification analysis targeting anomalies that would not be identified as such from a local viewpoint.



Conceptional architecture of the MonIKA project for anomaly detection in Internet infrastructures.

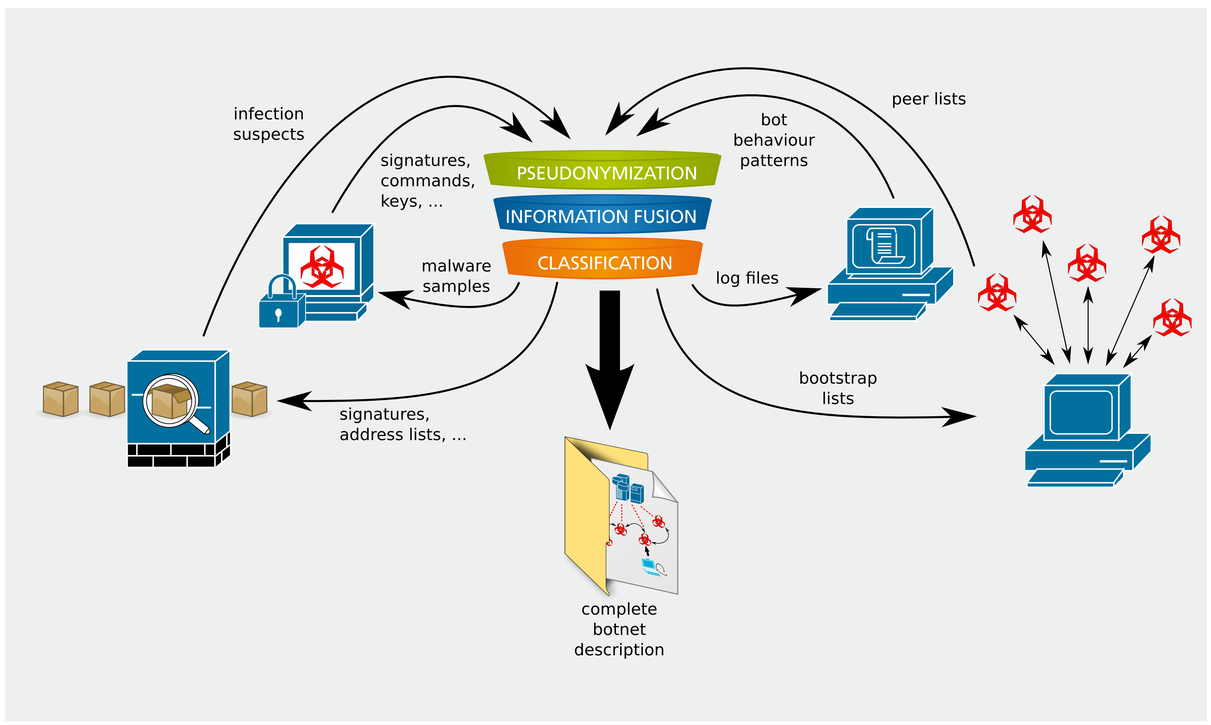


Views of collaborating partners inside MonIKA.

Pseudonymization

Facing legal constraints and the requirement to preserve the participants privacy, a system is needed which makes sharing information possible while implementing a need-to-know principle. A full pseudonymization scheme allows passing very specific information on to third parties without exposing any other information than the intentionally shared. For example, a third party does not need to know ones IP address when all it needs to know is whether two participants are in the same subnet or not. This is possible with specially designed pseudonyms which allow testing for required information.

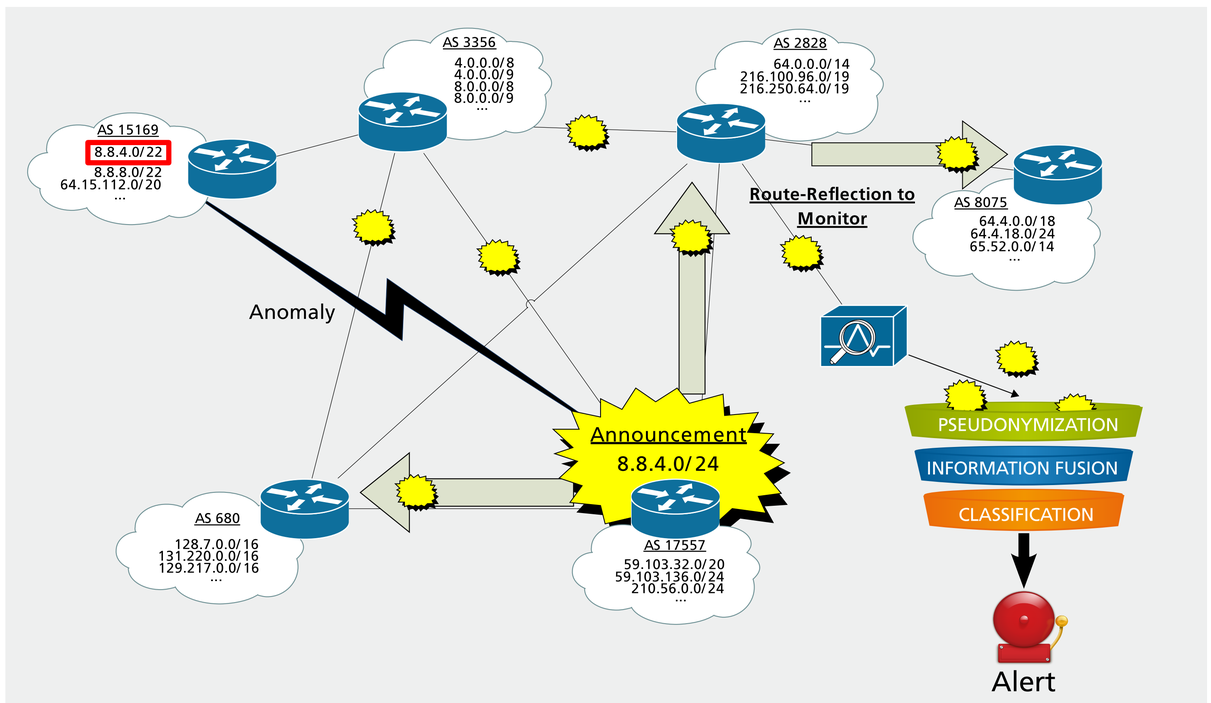
Fusion of Botnet Data



Fusion of Botnet data for a better understanding and reasoning on partial information.

With the heterogeneity of its components and the large diversity of techniques in use, Botnets feature a large range of properties. Different sensors can be applied to capture these properties in order to detect and monitor such Botnets.
MonIKA enables the exchange of different input and output information between sensors to make them work more efficiently and effectively and fuses all available information to present a more complete picture of a botnet.

Classification of BGP Anomalies



Detection of BGP anomalies using data of different view points.

Misconfiguration, hardware faults and attacks are causes of anomalies in inter-domain-routing. To detect targeted attacks as well as misconfiguration as early as possible, MonIKA uses geographically distributed monitors. If possible, the classification algorithms examine and classify occurring conflicts. Unclassifiable ones should be classified manually to support the automatic process. With the experience made by manually classifying conflicts, the automated classification algorithms can be improved.

SPONSORED BY THE
Federal Ministry of Education and Research

Fraunhofer FKIE · Westfälische Wilhelms-Universität Münster · CASSIDIAN AN EADS COMPANY · ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein