As an Integrating Project strategy, DEMONS aims at addressing all the key aspects essential in monitoring approaches for the Future Internet. DEMONS’ ultimate goal is to i) design a more scalable, flexible and autonomic monitoring infrastructure, ii) exploit monitoring intelligence distributed inside programmable traffic probes and mediating devices, iii) improve monitoring applications’ performance, capability effectiveness (detection, reporting, and mitigation) and deployment easiness, iv) operating in compliance with the customers’ privacy rights, and v) taking advantage of cross-domain cooperation mechanisms to permit improved defence against global scale cooperative threats and operational failures.

Main Objectives

DEMONS envisions building a novel cooperative network monitoring and mitigation system based on a completely decentralized, application-aware, privacy-preserving, multi-jurisdictional monitoring infrastructure. Such an infrastructure will provide the detection, reporting and mitigation mechanisms needed to combat not only today’s threats, but also those of tomorrow. DEMONS aims to realize this infrastructure by applying novel distributed systems technologies and leveraging their native scalability and fault tolerance characteristics. In doing this, DEMONS will put special emphasis on privacy, trust, and legal issues arising from collecting and exporting data across operator domains and across multiple jurisdictions. These issues have previously prevented other security solutions from being widely deployed and have therefore rendered them ineffective.

Concept and Approach

The most important commonality among all of distributed threats is that events far away in the network topology can have serious effects on an organization’s own network. Merely observing the packets that comprise the “last mile” gives an incomplete picture of the environment and merely reacting to network conditions at this edge provides an inadequate means of response to threats. Handling a cooperative network attack or large-scale accident requires cooperative network defence and response. Such solution calls for a decentralized and scalable monitoring infrastructure to provide both detection and reporting of security and network disruption incidents across multiple domains and jurisdictions.
Scientific & Technical Approach

DEMONS Project considers a layered vision of the network monitoring activity, starting from the network where there are functions dealing directly with the traffic in order to get the very first information about what is happening. This set of functions, normally deployed in probes, composes the **Measurement Layer**.

In order to share all the information, even across boundaries, a communication and coordination overlay is needed. This overlay composes the **Coordination layer** and delivers information handling, orchestration and communication features.

At the top, we find the monitoring applications taking advantage of the lower layer features with the goal of identifying the potential threats in the network. This is the **Application Layer**.

Orthogonal to all these three layers, the **Privacy Layer** covers all the privacy issues derived from the intended collaboration and information sharing arising at any level (thus orthogonal). This layer shall provide all the required tools to keep the privacy while getting enough information to reach effective detection of threats.
DEMons Breakthroughs

DEMons main disruptive goal is crossing the traditional boundaries of network monitoring, proposing a highly distributed approach where key monitoring elements are no longer centralized and share their information with other elements in its own network and even beyond, breaking domain borders and allowing a full-scope monitoring activity, bringing it to a new level.

This decentralised monitoring infrastructure must take privacy and trust considerations into account.

Coordination capabilities plus a complete set of privacy protection tools (e.g. multi-party computation, filtering, fine-grained authorization, anonymization techniques, etc.) are needed to achieve such a inter-domain distributed analysis and mitigation, beyond all the data-sharing constraints. These are the most valuable assets to be delivered by the project.

Expected Impact

DEMons Project aims a very challenging problem in terms of scientific innovative breakthroughs but also have a strong commitment with the industry needs. Three important european operators (Telefónica, France Telecom and Telecom Polska) work together in the Project bringing their real problems in the monitoring field, and look for real solutions not far in the future. Thus, the Project seeks for a demonstration of the results in a production-like environment through inter and intra-domain trials. Moreover, there are plans to exploit DEMONS technologies after the conclusion of the Project in the actual operational networks. Beyond that, DEMONS looks for a wider adoption among operators and ISPs to reach a bigger set of collaborating networks delivering a much secure Internet. Dissemination activities will help in achieving that goal, along with the Project’s Advisory Board, composed in part by experts from 2 operators, who will help us to both improve and spread the solutions.
Dissemination

The project web-site (www.fp7-DEMONS.eu) has been set up for on-line dissemination of activities of the Project, public deliverables and news related to monitoring infrastructure with data protection research activities. The project will participate in the concertation and cluster meetings to develop projects level liaison. The partners will participate in the conferences to disseminate the results and towards developing potential interest towards developing harmonised standards. Project results will be contributed to ETSI, IETF and RIPE working groups.

The partners of the consortium foresee a significant exploitation potential in the near future from the project results. The project has number of public deliverables to disseminate the information to the stakeholders, so that third party industrial entities can be involved in the exploitation of results.

DEMONS
Large scale collaborative Project

Funding: The DEMONS Project receives research funding from the European Union’s Seventh Framework programme

Contract number: INFSO-ICT-257315

Coordinator: Telefónica I+D

Duration: Sep. 2010-Feb. 2013

Project partners

AUSTRIA | FTW
CZECH REPUBLIC | INVEA-Tech
FRANCE | France Telecom, Institut Telecom
GREECE | ICCS, Singular Logic
ITALY | CNIT
POLAND | Telekomunikacja Polska
SPAIN | Optenet, Telefónica I+D
SWITZERLAND | ETH Zürich, KYOS
UNITED KINGDOM | NEC Europe