Secure, dependable and trusted Infrastructure

PRISM

Privacy-Aware secure Monitoring

The PRISM project proposes to develop a two-tier privacy-compliant integrated monitoring architecture. A first (front-end) tier of data protection mechanisms will be directly enforced at the traffic probe device, thereby guaranteeing that the data delivered to the controller will be already privacy-protected. A second (back-end) tier will enforce access procedures to the collected data and will orchestrate the operation of reversing, when strictly needed, the data protection mechanisms set forth by the first tier.

At A Glance: PRISM

Privacy-aware Secure Monitoring

Project Coordinator

Dr. Sathya Rao
TELSCOM AG
Aarwilweg 20
3074 Muri
Switzerland
Tel: +41 31 3762033
Fax: +41 31 3762031
Email: Rao@Telscom.ch

Partners: Telscom (CH), Consorzio Nazionale Interuniversitario per le Telecomunicazioni (IT), Fraunhofer Institure for Open Communication System (DE), Forschungszentrum Telekommunikation Wien (AT), Hitachi Europe (FR), Institure oif Communicatoin abd Computger Systens (GR), Nettare (IT), Salzburg Research Forschungsgesellschaft (AT)

Duration: Mar. 2008 – *May 2010*

Contract Number: INFSO-ICT-*215350*

Project website: www.fp7-Prism.eu

Main Objectives

PRISM aims at devising a privacy-preserving network monitoring system with guaranteed enforcement of data protection legislation. This will be accomplished by pursuing privacy-compliant technologies and solutions including the following objectives:

- Design of a two-tier monitoring architecture with data protection reversion bound to third-party cooperation
- “Blind” intrusion detection
- Extension and promotion of standard-based data export protocols
- Design of monitoring application friendly data protection mechanisms
- High performance front-end implementation
- Secure and high-performing back-end implementation
- Design of a privacy-aware back-end middleware
- Regulatory compliancy
- Innovative approaches to privacy-respectful monitoring application design
- Integrated trial

Privacy and data protection in ICT leads to increased trust

Concept

Privacy is of great concern to users of the Internet, and is a critical part of a user experience. The PRISM project investigates the possibility to preserve the customers' privacy, by avoiding disclosure of raw captured data even inside the controller domain itself, while preserving the capability of running monitoring applications, including the possibility to detect and react to attacks and trace back abuses (thus improving public security). The PRISM technology aims at being fully legally compliant with data privacy protection regulation on one side, and to the security legislation on the other side.

European Commission
Information Society and Media

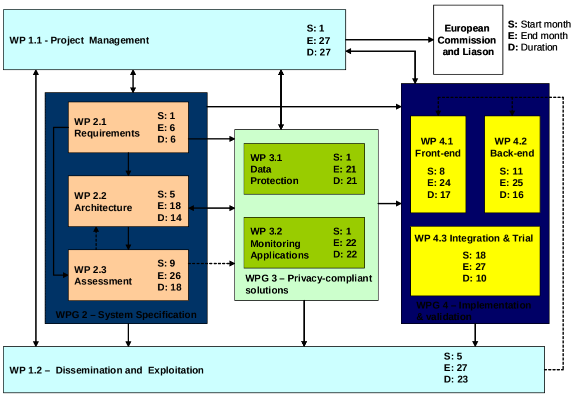
SEVENTH FRAMEWORK PROGRAMME

SEVENTH FRAMEWORK PROGRAMME

Technical Approach

The goal of the PRISM project is to devise network monitoring technologies and architectures, which guarantee enforcement of data protection legislation. This will be accomplished through the specification, design, implementation and validation of a two-tiered network monitoring system. The overall work plan of PRISM is structured into 4 work-package groups.

These WPGs are further subdivided into ten work-packages. The interdependencies of these workpackages are shown below:



WP 1.1 - Project Management S: 1 E: 27 D: 27
European Commission and Liason
S: Start month
E: End month
D: Duration
WP 2.1 Requirements S: 1 E: 6 D: 6
WP 2.2 Architecture S: 5 E: 18 D: 14
WP 2.3 Assessment S: 9 E: 26 D: 18
WPG 2 – System Specification
WP 3.1 Data Protection S: 1 E: 21 D: 21
WP 3.2 Monitoring Applications S: 1 E: 22 D: 22
WPG 3 – Privacy-compliant solutions
WP 4.1 Front-end S: 8 E: 24 D: 17
WP 4.2 Back-end S: 11 E: 25 D: 16
WP 4.3 Integration & Trial S: 18 E: 27 D: 10
WPG 4 – Implementation & validation
WP 1.2 – Dissemination and Exploitation S: 5 E: 27 D: 23

Note: Solid lines indicate direct input from a WP (or WPG) to another. Dashed line indicate the feedback from a WP (or a WPG) to another. Obviously, WPs in WPG1 have/receive direct impact on/from all other WPs.

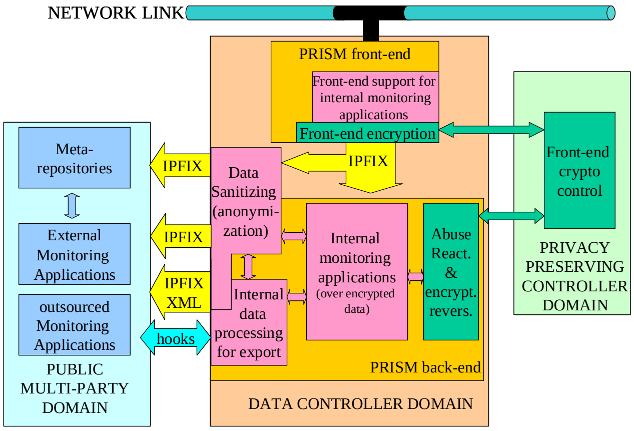
PRISM System Architecture

PRISM system architecture has 4 functional blocks:

PRISM Front-end – This component is meant to be a "Black-Box" traffic probe, "cryptographically controlled" by an entity, in the figure referred to as third-party privacy-preserving controller. The PRISM front-end is devised to capture data on the network link(s), protect them according to suitably designed data protection mechanisms whose secrets are provided by the Privacy-Preserving Controller, and deliver them to the back-end system through standard-based data export protocols, IPFIX being the technology of choice.

Privacy-Preserving Controller – This entity accomplishes the task of providing and maintaining the crypto secrets, which are used by the data protection mechanisms enforced on the front-end.

PRISM back-end – This part of the system is in charge of collecting, storing and processing the front-end protected data traces. Monitoring applications running on the back-end will operate on encrypted traces, and when strictly necessary and/or mandated by regulatory provisions. it will interoperate with the privacy preserving controller to selectively revert the data protection mechanisms set forth at the front-end.



NETWORK LINK
PRISM front-end
Front-end support for internal monitoring applications
Front-end encryption
Meta-repositories
External Monitoring Applications
outsourced Monitoring Applications
PUBLIC MULTI-PARTY DOMAIN
IPFIX
IPFIX
IPFIX XML
hooks
Data Sanitizing (anonymi-zation)
IPFIX
Internal data processing for export
Internal monitoring applications (over encrypted data)
Abuse React. & encrypt. revers.
PRISM back-end
DATA CONTROLLER DOMAIN
Front-end crypto control
PRIVACY PRESERVING CONTROLLER DOMAIN

Public Domain – Finally, collected data traces and/or derived statistics will be further sanitised through robust anonymization mechanisms. These will allow disclosure of data traces and/or related derived information to the public community, to meta-repositories, and to externally operated monitoring applications.

Expected Impact

Privacy is of great concern to most users of the Internet, and is a critical part of satisfactory user experience.

The PRISM front-end can be also independently exploited as a traffic-probing device, regardless of the data protection mechanisms implemented, because of modular design planned.

The operators can use the back-end role-based access control technology to improve their control and management of the access and processing procedures over data gathered in raw form.

The Privacy-Preserving Controller can be deployed as a privacy authority that can become an important exploitation opportunity.

Dissemination and Exploitation

The project web-site (www.fp7-prism.eu) will be set up for on-line dissemination of activities of the project, public deliverables and news related to privacy 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 on privacy compliant monitoring and data export is likely to impact the IP Flow Information Export (IPFIX) and Packet Sampling (PSAMP) standardization groups at the IETF. Experiences with the metrics and measurement methods used will be contributed to IETF/IPPM and ETSI/STQ working groups.