Privacy protection is the Key for building Trust in ICT technologies and to empower the citizens of the information Society with the future Internet. The FP7 project PRISM addressed this challenge and has developed the technical solutions for privacy aware network monitoring with the novel system architecture that can facilitate the appropriate and acceptable privacy legislation provisions.

PRISM: Privacy-Aware secure Monitoring

An FP7 European Project

http://www.fp7-prism.eu

The need for network monitoring

Traffic monitoring is vital for the life of networks, irrespective of the specific network kind, size and technical features. This simple and self-evident statement has lead to a steady development in the network monitoring area, providing specific technical solutions allowing in-depth analysis of network traffic. Network monitoring is indeed essential for efficiently supporting network functioning and management, for guaranteeing network and users' security for example against attacks, intrusions, infections, for detecting anomalies and for enabling troubleshooting.

Privacy and monitoring: a zero-sum game?

The other side of the coin is that any monitoring process, in order to be effective, must be fed with a significantly large amount of data and information, and such data and information often represent personal data of network users. It follows that network monitoring has to come to grips with the privacy legislation that is aimed at protecting users' privacy and confidentiality by posing specific requirements to the collection and use of users' personal data and information.

Some attempts to mitigate the risks for users' privacy have been made in the sense of limiting the information gathered, yet the problem still stands. limiting data capture to the packet header part or to the flow/call signalling information can mitigate the risk for users' privacy but it still allows to gather a large amount of information (e.g. who connects to whom, the applications used, when connection starts and its frequency). Moreover, anonymization techniques do not offer the complete solution. When too strong, essential information needed to operate monitoring applications may be lost; when too loose, users' privacy may be at the stake of powerful statistical traffic analysis attacks.

Apparently, a dichotomy emerges. On one side, the need to protect citizens and network infrastructures from attacks and threats calls for effective monitoring approaches. On the other side, the more efficient and granular the monitoring process becomes, the greater the risk of privacy infringements. To date, the problem of where to set the trade-off bar of such an assumed zero-sum game has been mainly tackled by legislature.

The PRISM answer

The PRISM project has contributed to show that, in the network monitoring scenario (but we expect this to hold in much more general cases), the above mentioned dichotomy is false. Besides the specific technical accomplishments, which are only briefly summarized later on, we believe that the PRISM case should be carefully scrutinized by policy makers, which may not be aware of how technology brings about win-win solutions, and which should take into much stronger account the actual existence of technical approaches and solutions when drafting legislative acts.

PRISM approach

PRISM envisions a consistent and general driving principle in its technical approach. Loosely speaking, it consists in the "translation", in technically addressable terms, of what we conveniently refer to as the "necessity" principle which lays at the basis of the European data protection regulation.

Indeed, European regulation underlines that "*only the kind and amount of data that are functional and necessary to the specific processing purpose that is pursued*" should be collected and processed. It hence holds that data protection should not be considered as a static, one-size-fits-all function valid for "all" monitoring tasks, and that any attempt to address privacy issues only through the design of stand-alone, context-free, and monitoring applications independent protection primitives should be considered myopic. Rather, the level of access or disclosure of data should be carefully tailored to the specific purpose of the applications and entities that require access to the data.

PRISM has accomplished this target through two complementary technical directions:

1. An improved understanding, and the consequent formal specification through semantic modeling techniques, of what is the minimal personally identifiable information a *given* monitoring application actually needs for providing its results and achieving its purpose; and
2. The development of technical means devised to guarantee that only said minimal data will ultimately be conveyed to each considered monitoring application.

In its technical specification activities, The PRISM project has embraced the "Privacy by Design" principle, indeed highlighted by Ms Viviane Reding (Member of the European Commission responsible for Information Society and Media Privacy) in her recent speech at Brussels, European Parliament, for the Data Protection Day (28 January 2010), as "*…a principle that is in the interest of both citizens and businesses. Privacy by Design will lead to better protection for individuals, as well as to trust and confidence in new services and products that will in turn have a positive impact on the economy*".

Moreover, the technology solutions proposed by the PRISM project have been designed and conceived from the very first stage bearing in mind the privacy regulatory framework, and explicitly including, as a project partner, a renowned law firm with specific expertise on privacy matters. Indeed PRISM activities, in addition to the 'traditional' performance and security assessment, has also included a dedicated "regulatory assessment" aimed at evidencing if, and how, the PRISM solutions are able to guarantee compliance with applicable privacy legislation.

PRISM technical achievements

We refer the reader interested into details to the PRISM project documentation (reports, deliverables, publications) available on the PRISM web site. At a glance, key PRISM contributions include:

- the specification, design, and assessment of a two-tiered integrated monitoring architecture, which places monitoring intelligence and data protection capabilities as close as possible to the actual source of monitored data, and specifically over traffic capturing probes called "PRISM front-ends";
- the design and implementation of hardware accelerated computationally and memory efficient "on-the-fly" traffic analysis algorithms capable of detecting, and delivering to the PRISM back-end, traffic flows of interest for each considered monitoring application (for instance suspicious flows in the case of intrusion detection or anomaly detection applications), therefore filtering away *at data gathering time* well behaving traffic; we remark that this proposed operation not only yields obvious privacy gains, but also achieves significant improvements in data reduction, improvements which make the adoption of these algorithms and mechanisms extremely appealing for increased network monitoring infrastructure scalability;
- the design and implementation of hardware-accelerated per-flow data protection cryptographic primitives, which permit monitoring parties to selectively access data only if specific monitoring conditions are met;
- the design and implementation of a semantic rich access control model, providing an extremely fine-grained level of authorization permissions (based on roles and purposes of the monitoring entities), and incorporating in its design European data protection provisions;
- The proof-of-concept seamless adaptation of already existing monitoring applications, including an intrusion detection system, a performance monitoring application, and a traffic classification application, to the privacy-preserving PRISM operation;
- The consistent adoption of standard-based data export protocols for interoperability and faster deployment, and their extensions for supporting protected traffic data.

A glance to the future

In terms of perspectives and impact of the PRISM project, we believe that the above clearly proves that the initial aim that has moved the PRISM project has been achieved. Now the following goal is that the project results do not remain only a good impression on the work performed throughout the project life, but that they become the starting point for a real-world deployment of privacy preserving monitoring.

The PRISM project has contributed to show that this approach is feasible even in very challenging scenarios such as that of monitoring high speed network infrastructures, and that data protection approaches may be synergic with data reduction and scalability goals. It is now up to policy makers to open the door of legislation to technical concepts and principles, to providers who are in the front line to benefit of Privacy by Design technologies, to users to ask for their privacy rights to be protected in their exploitation of new technologies and services.

We strongly believe that an increased awareness, especially among non technicians, about the actual existence, viability, and deployability of powerful and mature privacy preserving technologies will permit to constructively face “the end of privacy” threat (quoting the title of a well known book from Charles Sykes). Technicians know, and PRISM results are a striking example, that we can have both privacy and defense against attacks and threats, and that the “game” between privacy and security-through-control is a non zero sum one. We hope that the political, institutional, and social world may significantly open to such encouraging messages, and react accordingly. Some steps have been already made, but a lot has still to be done. We have already lost time, and if we wait further, it could be too late for preventing misusage of our monitored online behavior and for recovering our fundamental right to our private lives.

The PRISM Consortium

Telscom AG, Switzerland	Sathya Rao (Project Manager) rao@telscom.ch
Consorzio Nazionale Interuniversitario per le Telecomunicazioni, Italy	Giuseppe Bianchi (S&T coordinator) giuseppe.bianchi@cnit.it
Studio Professionale Associato a Baker & McKenzie, Italy	Francesca Gaudino francesca.gaudino@bakernet.com
Hitachi Europe, Switzerland	Elisa Boschi boschie@tik.ee.ethz.ch
Institute of Communication and Computer Systems – National Technical University of Athens, Greece	Georgios Lioudakis gelioud@icbnet.ece.ntua.gr
Fraunhofer Institute for Open Communication Systems, Germany	Carsten Schmoll carsten.schmoll@fokus.fraunhofer.de
Forschungszentrum Telekommunikation Wien, Austria	Ivan Gojmerac gojmerac@ftw.at
Salzburg Research Forschungsgesellschaft m.b.H, Austria	Felix Strohmeier felix.strohmeier@salzburgresearch.at
Nettare s.r.l., Italy	Nicola Bonelli nicola.bonelli@nettare.net