Privacy Preservation Techniques to establish Trustworthiness for Distributed, Inter-Provider Monitoring

J. Seedorf, S. Niccolini, A. Sarma
NEC Laboratories Europe
Heidelberg, Germany
seedorf/niccolini/sarma@neclab.eu

B. Trammell
ETH Zurich
Zurich, Switzerland
trammell@tik.ee.ethz.ch

G. Bianchi
University of Rome
Rome, Italy
giuseppe.bianchi@uniroma2.it

November 29, 2010

1 Introduction and Background

The increasing scale of the Internet and the growing heterogeneity of applications and devices attached to it, combined with the distributed impact and cascading nature of operational failures and the widespread diffusion of large-scale, inter-domain, coordinated attack infrastructures such as botnets, call for a novel approach to the design, deployment, and operation of threat monitoring and mitigation infrastructure. The EU research project DEMONS[1] fosters a new, resilient, scalable, and privacy-preserving approach to network monitoring and security management through the design of a trustworthy, coordinated monitoring network, composed on flexible and programmable nodes capable of supporting in-network traffic processing and analysis tasks. As its main goal, the DEMONS project is building the infrastructure of a novel cooperative network monitoring and mitigation system which is completely decentralized, application-aware, and *privacy-preserving*.

In this paper, we highlight the privacy considerations for decentralized, inter-domain network monitoring. We then present the DEMONS vision and approach for an architecture which enables large-scale, distributed network monitoring in a privacy preserving way. Our view is that the use of adequate privacy-preservation techniques is necessary to a) ensure trustworthiness in such a system by its user as well as to b) enable legal compliance in a multi-jurisdictional scenario.

2 Privacy Considerations for Network Monitoring

The process of monitoring networks poses severe concerns on the protection of the network customers' privacy, acknowledged by European legislation as a fundamental right of the individual [1] [2] [3]. Even in a single-organization case, network traffic monitoring activities, especially at higher layers of the network stack, pose a serious risk to individual privacy, since they may result in tracking the personal online activities of end users without their knowledge. Monitoring activities undertaken without transparency or accountability with respect to data processing (i.e., without privacy-awareness) lead to a loss of trust in the network as a whole. As a result, care must be taken that privacy concerns are addressed, and that privacy rights and data protection laws are not violated.

Network monitoring is necessarily concerned with traffic data, which from a privacy perspective of individuals poses a serious risk. An individual's network traffic may be combined and analyzed in any number of ways, and these activities may encroach severely into the individual's private sphere. These concerns are only amplified when sharing information in order to carry out cooperative network defense activities. Information sharing is further complicated by the fact that such cooperative defense activities will often cross jurisdictional boundaries, requiring the collection, storage and processing of network traffic data to comply with data protection laws of several different jurisdictions. Trust among operators is also an important consideration. Operators are generally loath to share information with outside parties. Despite this, many incidents are cross-domain, so operators are forced to rely on a cooperative defense process which is both informal, based on links of trust between individuals at network operations centers (NOCs) and computer security incident response teams (CSIRTs); and manual, without any specific technological support beyond electronic mail and the public telephone network.

3 The DEMONS Vision and Approach: Privacy-Preservation Techniques to enable Trustworthy Network Monitoring

The privacy issues detailed in section 2 have previously prevented large-scale monitoring solutions from being widely deployed and have therefore rendered them ineffective. It is therefore absolutely necessary to take such privacy consider-

[1]This work was partially supported by DEMONS, a research project supported by the European Commission under its 7th Framework Program (contract no. 257315). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the DEMONS project or the European Commission.

ations into account when designing a decentralized monitoring system. Hence, the overall DEMONS architecture will put special emphasis on privacy, trust, and legal issues arising from collecting and exporting data across operator domains and across multiple jurisdictions.

3.1 Vision of Privacy-Preserving Network Monitoring

Loosely speaking, DEMONS' general driving design principle 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. In order to accomplish such a vision, two complementary challenges must be addressed:

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

In the following subsection, we briefly describe the DEMONS' approach devised to jointly respond to these two challenges.

3.2 Technical Approach

In order to apply and extend the *necessity* principle clearly expressed by the European directives [2] [3] to a network-wide scale and cross-domain scenario, the DEMONS technical approach to privacy-preservation comprises four complementary scientific and technological research directions:

- **in-network processing and application-tailored data reduction**: Privacy preservation may practically be achieved without any cryptographic privacy enhancement technology but simply by specifying which type of data a monitoring application strictly requires for its operation. For example, if only flows exceeding a given profile are of interest for a performance monitoring application, then information about other conforming flows should not be conveyed. In practice, this requires a major rethinking of the current arrangement of most measurement systems and applications, where the data collection phase precedes a subsequent separate data processing function typically running over the entirety of raw gathered data.
- **privacy preserving access control of monitoring resources and data**: A privacy preserving access control framework, specifically tailored to the needs and requirements of the monitoring environment, can be used to control access to traffic data, monitoring resources, mitigation functions and countermeasures, traffic analysis functions and modules, and permitting monitoring alerts and reports, allowing only entities authorized for a specific function and purpose to use privacy-sensitive data.
- **monitoring data protection technologies**: New cryptographic approaches to privacy protection in traffic data generated by monitoring activities can be applied by identifying and validating practical cryptographic approaches which are capable of coping with the processing constraints and high throughputs of a given monitoring scenario.
- **privacy and business information preserving inter-domain cooperation mechanisms**: In an inter-domain scenario, where cooperation among multiple actors would enable an improved threat detection, the design of technical solutions which permit the safe exchange of monitoring information (alerts, reports, and even data when applicable) must be addressed. One approach under investigation is to rely on the well-established field of Secure Multiparty Computation (SMC): A secure computation is achieved if none of the participants, performing operations on data shared by different entities, neither reveals secrets nor learns anything except its input and the result.

4 Conclusion

The vision of the EU project DEMONS calls for a network monitoring architecture which puts special emphasis on privacy, trust, and legal issues arising from collecting and exporting data across operator domains and across multiple jurisdictions. In this paper, we motivated this vision and briefly outlined the corresponding technical approach for attaining the goal of a privacy-preserving monitoring infrastructure. Ultimately, achieving this vision by developing adequate privacy-preservation techniques will ensure users' trustworthiness and legal compliance.

References

[1] *Charter of Fundamental Rights of the European Union, O.J. C 364/1, 18.12.2000*

[2] *Directive 2002/58/EC of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communication), O.J. L 201/37, 31 July 2002*

[3] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; O. J. L. 281, 23 November 1995*