BUILDING A DECENTRALIZED, COOPERATIVE, AND PRIVACY-PRESERVING MONITORING SYSTEM FOR TRUSTWORTHINESS: THE APPROACH OF THE EU FP7 DEMONS PROJECT

SAVERIO NICCOLINI AND FELIPE HUICI, NEC LABORATORIES EUROPE,
BRIAN TRAMMELL, ETH ZURICH
GIUSEPPE BIANCHI, CNIT / UNIVERSITY OF ROMA TOR VERGATA,
FABIO RICCIATO, FTW

INTRODUCTION

Providing or improving the trustworthiness of today's network infrastructure, in terms of resilience to malicious activity and failures, presents a set of difficult challenges.

First, today's threats and failures rarely confine themselves to a single administrative domain. Large-scale network "accidents," such as routing failures or software faults, can affect users on a global scale, to the point of temporarily knocking YouTube off the Internet [1]. Perhaps even more troubling, organized criminal enterprises leverage vulnerabilities on millions of hosts across many domains to build botnets, large-scale, distributed coordinated infrastructures supporting a range of malicious activities. Botnets are used to send spam, launch denial-of-service attacks, run extortion scams, and steal personal financial information though phishing, among other nefarious activities.

Second, the sheer volume of information flowing across the Internet calls for increasingly large and scalable monitoring and data analysis systems for tracking down anomalies and threats; current reports show Internet-wide traffic volumes in zettabytes and trends of continued traffic growth. Within this context, the traditional measurement approach of centralized storage and single-domain analysis of traffic information is just inadequate. The limitations of current systems are several and include performance and scalability limits, reaction times too long to counteract ongoing attacks, and lack of an inter-domain approach to face global phenomena.

Any approach designed to overcome such limitations and move on to the next generation of monitoring systems will ultimately have to handle massive amounts of data about users, and therefore must be designed to guarantee the level of privacy protection required by the legal provisions of each country. In particular, a customer's identifiable information should not be disclosed in the process. Besides the privacy and legal requirements, exchange of information across administrative domains must avoid revealing any business-critical information to potential competitors such as vantage points, traffic load, network structure internals, and customers' preferences, among others.

DEMONS PROJECT OVERVIEW

DEMONS (DEcentralized, cooperative, and privacy-preserving MONitoring for trustworthinesS) is an Integrated Project funded by the European Commission under the FP7 Programme. It comprises 13 partners, including three nationwide operators (Telefonica, France Telecom, Polish Telecom), a large multinational company (NEC), a large system integrator (Singular Logic), two SMEs (Optenet, Invea Tech), and five of the top European research centers and academic institutions (ETH, CNIT, FTW, ICCS, Institut Telecom). In addition, it involves, as subcontractor, a renowned multinational law firm (Baker & McKenzie) bringing into the project inter-jurisdictional regulatory requirements and relevant conformance assessment. The project started in September 2010 and will last 30 months.

DEMONS revolves around the recognition that large, globally distributed threats call for a distributed, high performance, cooperative inter-domain detection and mitigation infrastructure. DEMONS promotes a monitoring architecture consisting of three logical layers, as sketched in Fig. 1. The measurement layer is in charge of measurement and analysis primitives and the means to compose them. It seeks to design and implement flexible and programmable nodes to perform high-rate monitoring and data analysis. The coordination layer combines such programmable nodes into a distributed data processing system that ultimately provides summarized results, some of which can be exchanged across domains. The coordination layer performs these actions subject to the constraints imposed by node capabilities, access rights, and authorization permissions, data protection requirements, and any other application-specific workflow needs. The application layer permits rapid development and deployment of measurement and mitigation applications and incident response workflows (either automatic or involving human intervention as allowed by operator policies) by leveraging the services offered by the lower layers. Finally, privacy and business-protection principles permeate all layers, translating into tight access control and cryptographic protection solutions in order to allow effective cooperation across administrative domains and jurisdictional boundaries, as well as improved control of data disclosure within domains.

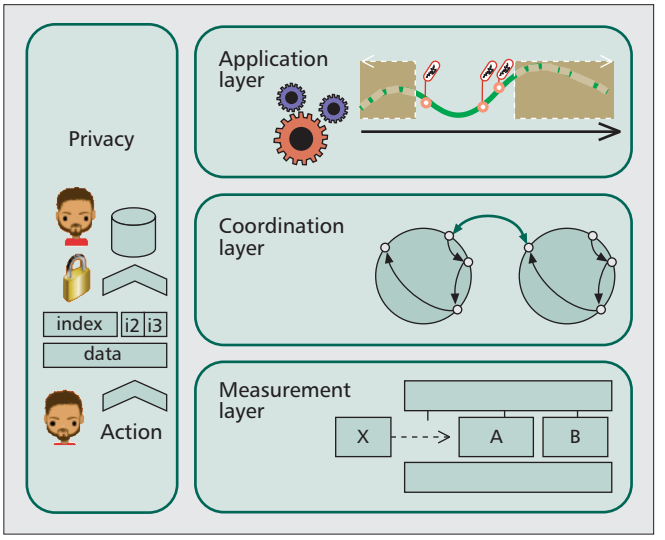

FIGURE 1: *The DEMONS architecture.*

DEMONS TECHNICAL APPROACH

DEMONS builds this vision on three key technical pillars: (1) a flexible modular monitoring node architecture; (2) dynamic and scalable monitoring overlays; and (3) inter-domain cooperation.

Flexible Modular Node Architecture

The architecture of a monitoring node is built around the notion of blocks, which are small units of processing (e.g., packet counting). Blocks are connected and communicate via

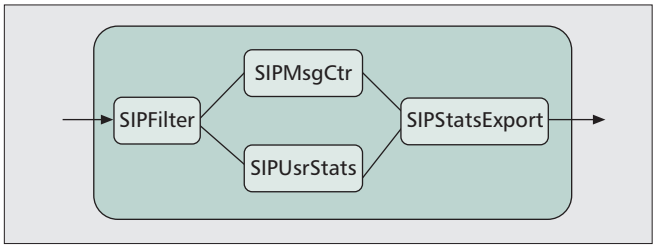

FIGURE 2: *Example of a node composition for SIP processing.*

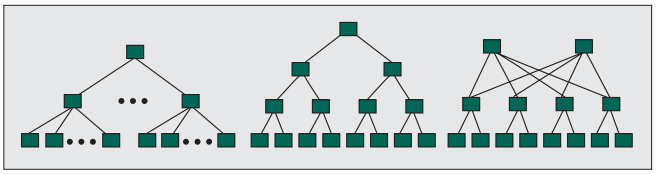

FIGURE 3: *Different overlay topologies. From left to right (1) an n-ary tree for coping with many probes and small aggregation delay (2) a deeper tree for greater data reduction and (3) a resilient fat-tree.*

gates, and the set of inter-connected blocks represents a composition. Multiple compositions, each belonging to a different monitoring task, may be dynamically deployed and operated in parallel on the same monitoring node. In essence, we bring about the advantages of a modular architecture permitting fast deployment through block reuse and composition [5] while retaining, similar to [6], the ability to efficiently and concurrently support multiple monitoring tasks..

Figure 2 shows one composition used to keep per-user and per-message type statistics about SIP traffic. It is worth pointing out that in reality a node (which could be mapped to a hardware probe, or a PC performing data reduction and analysis) will contain a number of compositions at any point in time, each belonging to a different monitoring application.

This modular architecture allows developers to quickly implement new applications by connecting existing blocks to new ones. The functionality of individual blocks ranges from generic counting and statistical operations to protocol-level parsers, complete implementations of complex anomaly detection algorithms, or even encapsulation of entire external software (e.g., Snort) or hardware (e.g., a NetFPGA) systems.

Further, nodes are equipped with a rich library of highly reusable computation- and memory-efficient probabilistic data structures (e.g., sketches and Bloom filters), with counting and rate/variation metering extensions.

Dynamic and Scalable Monitoring Overlays

In order to perform a particular monitoring and data analysis task, a control plane element called node control takes care of arranging nodes into a peer-to-peer (p2p) overlay. The adopted solution advances the state of the art with respect to Distributed Aggregation Trees [3] by decoupling the p2p routing from the algorithm used to build the overlay's topology. In this way, DEMONS is able to support a large range of topologies, including trees of variable depth, fat-trees, and other, non-tree topologies (Fig. 3).

In addition, the node control takes care of dynamically reconfiguring the overlay's topology, which allows adaptation to current traffic and analysis loads. Further, the node control can deploy new software on-the-fly, allowing for easy maintenance and quick addition of new functionality. Note that all such operations are subject to strict privacy and access control checks and that a single physical infrastructure can simultaneously support a number of different overlays, each mapping to a different monitoring application.

Inter-Domain Cooperation

In DEMONS the cooperation across administrative domains is supported by dedicated elements called Interdomain eXchange Points (IXPs). Each operator maintains an IXP in charge of handling the information exchange with other participating domains.

To preserve business confidentiality and customer privacy, the project is promoting the adoption of scalable and performance-effective Secure Multi-party Computation (SMC) methods whose viability in the network monitoring domain has been recently addressed [2]. Promising research directions currently under exploration include the combination of SMC techniques with probabilistic data structures like Bloom Filters to perform common inter-domain tasks in a more scalable way [4], as well as the design of novel cryptographic techniques for conditioning the sharing of inter-domain data to the occurrence of specific alarm conditions or anomalous events.

ENVISIONED IMPACT

Besides the prospective scientific advances, the project will ensure an important level of impact through a number of activities. First, the block-based node architecture currently under development is scheduled to be released as open source at the beginning of 2012. Second, test sites for collaborative inter-domain monitoring are planned to be deployed among the DEMONS operator partners. Candidate use cases to be demonstrated are (D)DoS mitigation, botnet identification, and VoIP anomaly detection. Moreover, DEMONS aims to extend (and is massively contributing to) existing standards, most notably the IETF IP Flow Information eXport (IPFIX) protocol. Finally, through the active participation in, and current chairing of, the ETSI's Identity and access management for Networks and Services (INS) "Industry Specification Group," DEMONS aims at spreading awareness, in the industry and operators arena, about the security benefits of inter-domain monitoring information sharing, as well as concretely promoting the adoption of technical means to secure inter-domain cooperation and protect the relevant monitoring data exchange.

CONCLUSION

The aim of DEMONS is to significantly improve the trustworthiness of today's Internet by empowering the operators' ability to detect and react to global-scale incidents and malicious activity. To this end, DEMONS follows an integrated approach to network monitoring whose key elements are the distribution of programmable monitoring tasks across cooperative monitoring nodes, and the deployment of inter-domain collaborative mechanisms that preserve the privacy of customers' and operators' data.

ACKNOWLEDGEMENT

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.

REFERENCES

[1] Ars Technica, "Insecure Routing Redirects YouTube to Pakistan," http://arstechnica.com/old/content/2008/02/insecure-routing-redirects-youtube-to-pakistan.ars
[2] M. Burkhart *et al.*, "SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics," *Proc.19th USENIX Security Symp.*, Washington, DC, Aug. 2010.
[3] P. Yalagandula and M. Dahlin, "A Scalable Distributed Information Management System," *SIGCOMM '04*, New York, NY, USA, 2004.
[4] F. Ricciato and M. Burkhart, "Reduce to the Max: A Simple Approach for Massive-Scale Privacy-Preserving Collaborative Network Measurements," *Proc. TMA 2011 Wksp.*, Vienna, Apr. 2011.
[5] E. Kohler *et al.*, "The Click Modular Router," *ACM Trans. Comput. Syst.*, vol. 18, no. 3, Aug. 2000.
[6] G. Iannaccone *et al.*, "UK the Como White Paper," http://como.intel-research.net/.