System Architecture for collaborative security and privacy monitoring in multi-domain networks

Sathya Rao[1], Giuseppe Bianchi[2], Joaquin Garcia-Alfaro[3], Francisco Romero[4], Brian Trammell[5], Andreas Berger[6], [Georgios Lioudakis, Eugenia Papagianakopoulou, Mariza Koukovini][7], Karel Mittig[8]

1 KYOS, Switzerland; 2 CNIT, Italy; 3 Institut Telecom, France
4 TID, Spain; 5 ETHZ, Switzerland; 6 FTW, Austria
7 ICCS, Greece; 8 France Telecom, France

Abstract:

The System architecture presented in this paper is developed in DEMONS project of the European FP7 framework project to realize the trustworthy multi-domain network with collaborative and decentralized security and privacy monitoring system. The system architecture so developed comprises of five sub-systems: (i) programmable monitoring nodes called BlockMon nodes providing the monitoring infrastructure data plane, ii) BlockMon Controller, iii) Mitigation Control Point, in charge of providing a unique interface towards mitigation equipments, iv) an Inter-domain Exchange Point devised to provide gateway functionalities (at both control and data plane) from/to external administrative domains, and v) a Workflow Planner and Orchestrator Controller for authorization, brokerage, and run-time control service towards the deployed monitoring and mitigation primitives on the basis of the application needs, operational requirements, and regulatory provisions.

The DEMONS system architecture further comprises two external interfaces to the end users, namely i) a Programming and Administrative Interface through which the system and its components are programmed, administered and maintained, and ii) an Application User Interface through which the system is used for monitoring by users in a given domain, plus a number of dedicated interfaces among the internal DEMONS' sub-systems / components.

Introduction

Over the past decade, the Internet has become more challenging for operators, enterprises, and end-users. The Internet has evolved significantly, and people have come to depend on it for a number of activities such as voice and video communications, social networking, online banking, e-government and shopping. Trust is the core of social and economic activity in the Internet, and is the basis of economic transactions, social connections, and communication between people and organizations. As there is a need to be able to trust our network and services, the robustness of the Internet against security threats and operational failures is of significant importance.

Security threats, which once represented mere "hacking" or exploitation of hosts for little more than curiosity or vanity, have given way to sophisticated criminal operations [1] that exploit vulnerabilities in network devices and end systems to take over large numbers of nodes, arranging them into botnets, for spamming, phishing, extortion via distributed denial of service attacks, and personal information theft (e.g., credit card numbers) threatening end-user privacy and the importance of "information as an asset".

The most important commonality among all distributed threats is that events far away in the network topology can have serious effects on an organization's own network. Handling a cooperative network attack or large-scale accident requires *collaborative 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.

Such an infrastructure must take the following privacy and trust considerations into account:

- Even in the 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 has to do with data traffic, which from a privacy perspective of individuals poses a serious risk since these data may be differently combined, processed, used to encroach massively into the individual's private life. The network monitoring activities, as well as the underlying categories of data, have been subject of specific regulations, such as [2][3] in Europe. These concerns are only amplified when sharing information in order to carry out cooperative network defence activities. Information sharing is further complicated by the fact that such cooperative defence 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 not interested to share information with outside parties. Despite this, many incidents are cross-domain, so operators are forced to rely on a cooperative defence process which is both *informal*, based on links of trust between individuals at network operations centres (NOCs) and computer security incident response teams (CSIRTs); and *manual*, without any specific technological support beyond electronic mail and the public telephone network.

The core problem in collaborative network monitoring and mitigation is that incidents impacting the security and reliability of a given network today are complex, with threats widely distributed among attackers, intermediary systems, indirect targets, and direct targets, all potentially lying in different organizations, parts of the network, and national jurisdictions. The legal, organizational, and technical infrastructure to respond to these incidents must therefore be distributed and collaborative.

CONCEPT of DEMONS system for security and privacy monitoring

The base architecture for the DEMONS monitoring system envisions the integration of services and functionalities provided by different dedicated sub-systems, supporting operations roughly organized into the following three distinct layers.

- The **measurement layer** is in charge of performing measurement and analysis primitives and supporting means to compose them. The measurement layer revolves around software and hardware accelerated programmable monitoring nodes, capable of executing high-rate in-network monitoring and data analysis primitives implemented and deployed in a highly modular fashion [4].
- The **coordination layer** combines a potentially very large number of 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, thus guaranteeing that the right type and amount of monitoring information is accessed by (and delivered to) duly authorized parties [5]. The work in this area is based on the work carried out by the authors on the access control and authorisation framework for real-time monitoring applications to meet the needs of passive network monitoring [6]
- 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. It further provides tools and graphical interfaces for permitting easy management and exploitation of the supported monitoring primitives [7].

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 [8,9,10].

The schematic of the DEMONS system architecture is as shown in fig.1

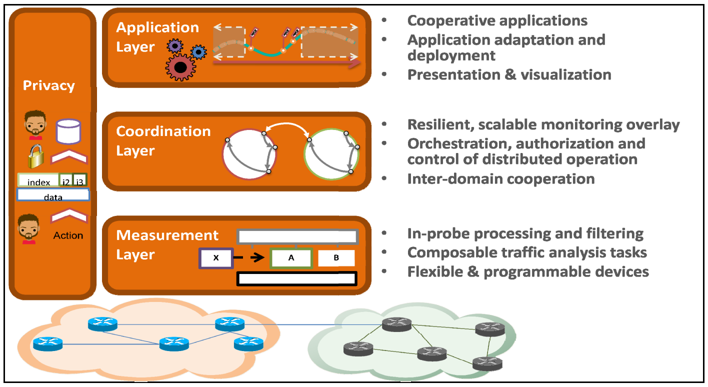
Privacy
index
i2
i3
data
Action
Application Layer
Coordination Layer
Measurement Layer
X
A
B
Cooperative applications
Application adaptation and deployment
Presentation & visualization
Resilient, scalable monitoring overlay
Orchestration, authorization and control of distributed operation
Inter-domain cooperation
In-probe processing and filtering
Composable traffic analysis tasks
Flexible & programmable devices

Figure 1: System architecture of collaborative security and privacy monitoring

Design principles

The design principles of DEMONS system architecture were evolved by analysis of different scenarios and use cases. These can be classified into 7 main issues:

1. **In-network monitoring via programmable nodes:** A key design principle in DEMONS is to push data processing as close as possible to the source, i.e., the network links. Such principle is a key enabler for impacting scalability, data reduction, and even data protection in future generation monitoring systems. To address this, the project has specified and designed flexible and programmable monitoring nodes called BlockMon Nodes.
2. **Distributed processing via a monitoring overlay:** This is achieved by specifying and designing the necessary primitives for creating and managing an overlay network formed by multiple distributed BlockMon nodes. 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 [8] 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. The monitoring overlay is devised to perform a particular monitoring and data analysis service involving multiple edge points in the operator's network.

3. **Application-oriented operation via workflow planning and orchestration:** DEMONS system aims at being application-centric, so that its operation is adapted to each specific application, being driven by the specific needs and requirements of such application. This is achieved by specifying and designing a control plane sub-system called Workflow Planning and Orchestration Controller (WPOC).
4. **Cross-Domain cooperation via Inter-domain exchange gateways:** This requires the collaboration across administrative domains to be supported by dedicated elements called Inter-domain eXchange Points (IXPs). Each operator maintains a *single* (logical) IXP in charge of handling the information exchange with other participating domains. This is achieved by promoting the integration of more advanced cooperation schemes leveraging cryptographic approaches in the IXP.
5. **Management of mitigation techniques via dedicated control plane interface:** DEMONS system architecture permits the convenient access to, and management of, mitigation strategies through a control-plane entity called Mitigation Control Point (MCP). The MCP provides the access to every specific strategy via a single (logical) interface, which maps multiple (registered) apparatus specific mitigation components.
6. **Improved usability via a Graphical User Interface:** DEMONS pays special attention to the usability of the entire system, by including a *Presentation layer* providing means to represent the results of the monitoring services and analyses, as well as means to configure and deploy such services and primitives, from the very high level of monitoring workflow down to the very low level of per-node analysis blocks.
7. **Interoperability via adoption of standards:** DEMONS aims at fostering interoperability, through the consistent adoption of standard-based solutions. The IPFIX protocol is used to export any set of observable properties for a flow [11], since IPFIX is neutral to any application or vendor implementation. The system also plans to use RID protocol across IXPs.

In the next section each of the sub-system and components are addressed briefly.

Overview of the system components

The DEMONS system architecture supports both intra-domain and Inter-domain network traffic analysis and incident mitigation.

In the **intra-domain** scenario, each administrative domain relies on a monitoring overlay infrastructure composed of distributed monitoring nodes which gather, in-network process, and deliver data information to an arbitrary number of end-points (storage, collectors, stream interfaces, mitigation control points, etc), under the control of a well specified monitoring control point. This collected and pre-processed data (especially for data reduction) is then controlled by a DEMONS' orchestration function which provides a service-oriented abstraction to the end users for accessing and using such data.

In the **inter-domain** scenario, for each domain, the architecture appoints one specific *single* point for the exchange of monitoring data with the relevant peers in external domains, and for performing the relevant inter-domain monitoring cooperation primitives. This Inter-domain Exchange Point (IXP) acts as a gateway towards external domains, and takes care of any data crossing the boundary of the domain. Specifically, data internally gathered within a domain which is exported outside the domain itself will be passed to the IXP for export. Similarly, data coming from external domains will be forwarded to the IXP and then made available to analysis operations inside the domain.

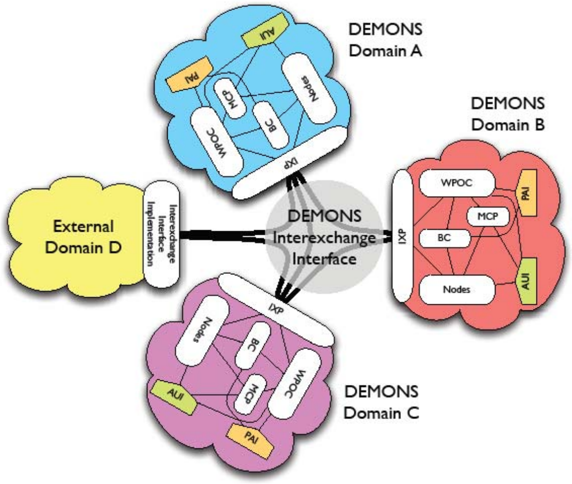

Figure 2: High level view of DEMONS domains

The decision to deploy an IXP gateway greatly simplifies the inter-domain architecture monitoring design, by providing a single, well-identified interface towards the external networks, and by concentrating all the critical security and data protection functionalities involving inter-domain monitoring in such a single point, thus making easier their control and deployment.

Fig.2 shows high level architecture of collaborative domains with IXP for exchange of inter-domain flows. An entity implementing such an IXP can be part of DEMONS domains, even though the architecture of such an entity may be different.
The components involved in such system architecture are:

- Workflow Planning and Orchestration Controller (WPOC) providing the central coordination point for DEMONS applications, regarding detection, mitigation and inter-domain transactions, and on the other aspect is the primary evaluation and authorization control point for both intra- and inter-domain invocations and requests [6];
- BlockMon Controller (BC), controlling the nodes in the BlockMon overlay,
- BlockMon Nodes performing data capture, import, and analysis, as well as result export for application presentation, mitigation, and inter-domain exchange,
- Mitigation Control Point (MCP) providing a common interface to the existing mitigation processes within an operator (e.g., a trouble ticketing system or automated nullrouting/ quarantining facility); and
- Inter-domain Exchange Point (IXP), which provides a single point of contact among DEMONS domains, coordinates cross-domain analysis requests, and mediates inter-domain data sharing and privacy protection.

The system also includes

- **Programming and Administrative Interface (PAI)** through which the system is programmed, administered, and maintained; and
- **Application User Interface (AUI)** is used by users for monitoring within a given domain. The AUI includes a **graphical user interface** (GUI) for presenting results, storing results for later analysis and presentation, and to generate new analysis requests for the WPOC based on results of running analyses.

The most important architectural characteristics of each component are the interfaces that they implement, and the services that they offer to each other. These interfaces are split into data and control interfaces. The control interfaces are split into deployment and invocation interfaces. The deployment interfaces are those used to “**program”** the DEMONS system, and result from user action via the Programming and Administrative Interface. The invocation interfaces are those used to ``**run**'' the DEMONS system, and in turn result from user action via the Application User Interface. The components and interfaces of the DEMONS architecture are shown in figure 3 with the communication links across different components.
The center of the DEMONS data plane is BlockMon; BlockMon is programmed in terms of *compositions* of *blocks*. A block is a small unit of processing and analysis, and a composition is an application or part of an application made up of one or more blocks connected together. Compositions are the base unit of meaningful application programming in DEMONS. Blockmon controller controls and configures the individual nodes in a BlockMon overlay [12].

The DEMONS control plane is centered around the concept of the *workflow*, a well-specified series of actions, along with their interaction patterns (both data-flow and control-flow), that are executed in order for a high-level purpose to be fulfilled.

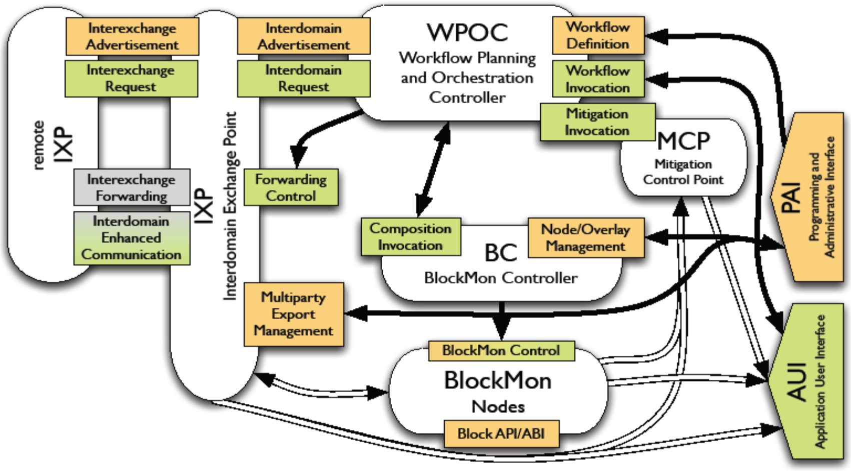

Figure 3: Interfaces in the DEMONS architecture

From a control plane's point of view, the execution environment can be seen as an infrastructure comprised of two layers:

• *Orchestration Layer*: its fundamental part is the pool of *Orchestrators*, each being a stateful component that plays the role of the workflow coordinator throughout its execution lifetime; among other functionalities, it is the entity that performs most of the work related with capabilities matching, it splits the workflow to the parts describing the behaviour of autonomous components and maintains the state of the execution.

• *Components Layer*: it consists of *Agents* that control "containers" of the underlying components, such as BCs, MCPs, IXPs or any other autonomous component. They are the entities responsible for the control communication with the Orchestrator of the workflow and the Agents of peer components, the transformation of the specified behaviour to a Platform Specific Model (PSM), as well as the tasks related with context generation, publication, retrieval and evaluation.

The WPOC is the central evaluation and authorisation control point regarding the definition of all DEMONS applications and must, therefore, interact on the one hand with the PAI and on the other with all the remaining control components of the architecture, namely the BC, the MCP and the IXP. During the Planning Phase, the WPOC is interfaced with:

- The *PAI* through the *WDI*, for the definition of workflows that are subsequently passed to the WPOC in the form of, e.g., BPMN models.
- The *IXP* through the *IAI*, for advertising services to the IXP and, inversely, for obtaining information about services available at remote domains, by exchanging, for instance, WSDL service descriptions.
- The *BC* through the *CII*, for being informed of the capabilities made available via the BC.
- The *MCP* through the *MII*, for being informed of the capabilities made available via the MCP.

The goal of the MCP is to dispatch mitigation instructions to mitigation equipment. It processes concrete policies produced by WPOC agents, and translates them into specific scripted commands for every mitigation apparatus. The WPOC agents are in charge of activating threat, as well as extracting new concrete mitigation rules from the active threats. Every mitigation apparatus is seen as an enforcement point that is applying the scripts derived from the mitigation rules. Registration of new mitigation capabilities is provided by WPOC agents via the DEMONS capabilities bus.

From an intra-domain perspective, the measurement layer (e.g., by blockmon nodes) provides the MCP with diagnosis data, e.g., events, logs, and alerts. The Alerts might come from different sources and with different formats. It is, therefore, necessary to post-process them, in order to normalize their format, as well as to reduce their volume and improve their semantics. The correlation process aims also at reducing the false positive rates and producing alerts with fewer contextual references (e.g., attack types).

The MCP holds decisional capabilities, e.g., depending on the specific domain where it is located, a concrete rule may provide different actions. For instance, depending on the topology of the domain, and the existing equipments for mitigation, a reconfiguration process may be instructed as a simply informative action (e.g., raise a ticket), or as a semi-automatic action (e.g., prepare the set of reconfiguration files that are required by the security officer).

DEMONS system architecture also defines the Inter-domain exchange points (IXP) to provide gateways functionalities for all the data exchanged across domains. Specifically, the IXP corresponds to a single component (at least on a logical point of view), designed as the communication entry point between intra-domain network and other domains. The IXP will provide a support for basic exchanges, corresponding to a minimal set of interactions that must be mandatorily supported by each IXP. Number of protocols are being considered for the information exchange across IXPs including IETF defined RID ("Realtime Internetwork Defense") protocol with the data model IODEF (the Incident Object Description Exchange Format). RID is a potential protocol since it is designed to support cooperative mitigation through traceback and mitigation of high-volume incidents (i.e., distributed denial of service attacks) closer to the source of the attack traffic. This is provided by the RID TraceRequest message, directed recursively upstream toward the source of traffic until an appropriate mitigation point is found.

Negotiation of inter-domain policies and exchanged data will be dynamically configured by the WPOC according to the negotiated services. In order to secure the inter-domain exchanges against any mis-configuration, those negotiated policies will not in any way provide more rights than the one defined within the access control part.

The interaction with the DEMONS architecture and supported services will be managed mainly by two external interfaces presented to the users of the system: the *Programming and Administrative Interface (PAI)* and *the Application User Interface (AUI)*.

The PAI will constitute a graphical programming and deployment interface that will permit the expert user to directly interact through the NOM with the internal BlockMon primitives, in order to implement and deploy blocks, define block compositions and configure BlockMon nodes. It will also provide for the specification of workflows that will subsequently be passed to the WPOC through the WDI for validation.

The AUI will be provided to the very end user of the DEMONS system. On the one hand, it will allow, through the WII, the invocation of previously defined monitoring applications, also permitting the user to interact with them throughout the execution of the corresponding workflows. On the other hand, it will present monitoring results as well as information on the internals of the architecture and running applications that can be of interest to the end user (e.g., error reports).

Conclusions

The paper provided an overview of the DEMONS system architecture for collaborative security and privacy monitoring in multi-domain networks. The proposed architecture supports two modes of operation, namely i) intra-domain and ii) inter-domain network traffic analysis and incident mitigation, each mode characterized by different and complementary requirements (scalability, resilience, support for operator-specific workflow processes and policies, and performance effectiveness being primary concerns in the intra-domain case; security, privacy, protection of business information confidentiality, and in more generality tight control of inter-domain cooperation being central in the inter-domain case).

The architecture revolves around five major sub-systems (components) and two external interfaces. The subsystems comprise i) a Workflow Planning and Orchestration Controller (WPOC) coordinating the supported monitoring and mitigation services and the inter-domain transactions, and managing the relevant authorization based on semantic access control policies; ii) a BlockMon Controller (BC) which controls distributed monitoring nodes forming a monitoring overlay; iii) the BlockMon nodes, devices performing (programmable) data capture, import, and analysis ; iv) a Mitigation Control Point (MCP), acting as interface towards mitigation equipments and strategies, and v) an Inter-domain Exchange Point (IXP) permitting inter-domain cooperation and controlled monitoring information exchange. The envisioned external interfaces include a) a Programming and Administrative Interface which permits monitoring application deployment to program and configure the specific monitoring operation, and b) an Application User Interface devised to permit the usage of the deployed monitoring infrastructure.

The graphical user interface will provide an authentication and authorization mechanism, in order to control the access to both the PAI and AUI and their subcomponents.

Acknowledgement

This work was done as part of DEMONS research project (contract number 257315) partially funded by the European Commission under its 7th framework Program. The views and conclusions contained in this paper are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements of the European Commission

References

[1] "A walk on the dark side", The Economist, 30 August 2007.

[2] 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector; European Parliament and Council: Directive (Directive on privacy and electronic communications). Official Journal of the European Communities L 201 (July 2002).

[3] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive; European Parliament and Council. 2002/58/EC. Official Journal of the European Communities L 105 (April 2006).

[4] DeliverableD3.1: Measurement layer Principles: SoA Survey, www.fp7-demons.eu

[5] DeliverableD4.1: Decentralized coordination layer principles: SoA Review, www.fp7-demons.eu

[6] Combining monitoring and privacy-protection perspectives in a semantic model for IP traffic measurements. Computer and Information Sciences, Lecture Notes in Electrical Engineering. Vol. 62, Springer Netherlands, 2010.

[7] DeliverableD5.1: DEMONS internal deliverable; Application layer components: SoA review

[8} A Scalable distributed information management system; P. SIGCOMM'04, Yalagandula and M. Dahlin, New York, 2004.

[9] Deliverable D2.1: Privacy preservation techniques: SoA review, www.fp7-demons.eu

[10] New directions in privacy-preserving anomaly detection for network traffic. NDA '08: Proceedings of the 1st ACM workshop on Network data anonymization (New York, NY, USA, 2008); Bianchi G. et al.

[11] An introduction to IP flow information export. Trammel B, Boschi E; IEEE Communications Magazine 49, 4 (Apr. 2011).

[12] Blockmon: A Modular System for Flexible High-Performance Traffic Monitoring and Analysis; Andrea di Pietro et al. Infocom 2012.