THE ARCHITECTURE DESIGN FOR CONTENT-AWARE NETWORK SECURITY SERVICES

Radu LUPU[1], Eugen BORCOCI[2], Mihai STANCIU[3], Antonio PINTO[4]

Odată cu creşterea gradului de diversitate al tehnologiilor de reţea şi a gradului de integrare al aplicaţiilor utilizator, metodele tradiţionale de configurare ale mecanismelor de securitate nu mai pot asigura cele mai eficiente soluţii. Această lucrare propune o soluţie în domeniul serviciilor de securitate adaptive capabile să satisfacă nivelul de securitate cerut de către aplicaţii cu o utilizare minimă a resurselor de reţea. În acest articol propunem o nouă arhitectură de securitate orientată pe reţea care se bazează pe contextul de securitate al reţelei şi pe mecanisme orientate pe conţinut. Se vor prezenta şi defini principalele blocuri funcţionale de arhitectură şi se vor specifica interacţiunile dintre ele. Arhitectura de securitate a fost proiectată pentru a furniza serviciile de securitate inter-domeniu, numite sugestiv "trafic public", "conţinut secret" şi "comunicaţie privată", şi servicii de urmărire cu identificarea sursei de trafic şi controlul accesului distribuit.

With the ongoing increase of the network technologies' diversity and the integration of the user level applications, the legacy-style content-independent configuration of the security mechanisms cannot yields in efficient security solutions farther. Our work aims to contribute on the design of auto-reconfigurable (adaptive) security services that are capable to satisfy the application's security level required with minimal network resources' usage. In this paper we propose a new network-centric security architecture design that relies on the current network security conditions and content-aware mechanisms. The architecture main functional blocks and the corresponding relationships are defined. This architecture shall supply three inter-domain composite user security services, named "public traffic", "secret content" and "private communication", as well as, attack source traceback and distributed access control functionalities.

Keywords: content-aware network, security services, source traceback, distributed firewalling

[1] PhD stud, Dept. of Telecommunications, University POLITEHNICA of Bucharest, Romania, email: rlupu@elcom.pub.ro

[2] Prof, Dept. of Telecommunications, University POLITEHNICA of Bucharest, Romania, email: eugen.borcoci@elcom.pub.ro

[3] Associate Prof, Dept. of Telecommunications, University POLITEHNICA of Bucharest, Romania, email: mihai.staciu@elcom.pub.ro

[4] Assistant Prof, INESC Porto, University POLITEHNICA of Porto, Portugal, email: antonio.pinto@inescporto.pt

1. Introduction

While we more assist to the integration of the large diversity of the user level applications over the Internet, the efficient security mechanisms requirement becomes more and more acute. In this context, the legacy static configuration of the security mechanisms' parameters cannot allows for obtaining most efficient security solutions. Therefore, the design of the adaptive security mechanisms aroused as a new challenge to ensure highest security level with minimal resources consumption. Although, the content-aware approach for the security mechanisms' optimization lasts from several years, there are no such solutions to our knowledge published in the literature to provide end-to-end efficient security services. Most of the related solutions proposed are in the domain of flow's authentication and access control ([1], [2]). The solution defined in [3] with the scope limited to wireless access networks it is the most closed to our work.

This paper presents the network-centric security architecture we designed for the content-aware oriented services infrastructure being developed within Alicante project[2] (specified in the section below). The main goal of our security architecture is to provide security services for the Alicante data plane communications security. The security services we propose will take into account the network context risk level and leverage content-aware mechanisms in order to achieve the required user content security level with minimal network resource usage trade off. It is assumed the security mechanisms we will propose shall work in conjunction with lightweight cryptographic algorithms in order to minimize the negative impact on the network performance [6],[14]. Our solution assumes the end-users (i.e. content consumers-CC or content providers-CP) share trust relationships with the Alicante infrastructure. Based on our architecture we will investigate the existing Alicante infrastructure features to provide enhanced overlay mechanisms for data flow traceback and distributed filtering. Some related works have been published in [4] and [5], respectively.

Since the Alicante overall architecture is in its early phases of progress, the paper presents the first results we achieved within the security architecture design.

The paper is organized as follows. In the beginning, the introductory section gives the reasons that motivated our work. It is followed in Section 2 by the overall presentation of the content-aware architecture designed in the Alicante project with highlight on the main functional layers objectives. Section 3 starts with specification of the enhanced security services we intend to design and develop. Thereafter, it is presented the overall security architecture we designed in order to implement the content-aware security services with emphasis on the objectives of the main functional components. Then, it is specified the functional structure of the main architecture components and the related interactions. The paper ends

[2] EU funded project Alicante FP7 IP No. 248652 (2010-2013)

with Section 4 that concludes on the current status of the work and points out the objectives of the future work.

2. The Alicante network infrastructure

The Alicante project aims to design and develop a complex network and services infrastructure complying with the "Future Internet" philosophy, based on the new concept of "Content Aware Networking" (CAN). Furthermore, this project focus on the design of the content-aware mechanisms for the media/data flow transport optimization eventually enabling more flexible network services. Thus, the Alicante infrastructure manage to replace the legacy model of rigid users role with a new dynamically one that allows the end user to exchange its role from content consumer to content/service provider. Amongst the user level applications supposed to be run on top of the Alicante infrastructure are IPTv and P2P.

Fig. 1 provides a high-level view of the general Alicante architecture. The main business actors within Alicante infrastructure are: the EU (End-User) - is an actor (human plus a set of terminals or processes), which may consume, produce and manage media services and content; the SP (Service Provider) – it provides high level media services and aggregates content from multiple CPs for delivering it to the EUs; and the CANP (CAN Provider) - is a new Alicante business actor that offers content-aware network services to the upper layer entities (Service or User Environments), through combination of the slices of virtualized infrastructure from NPs together into a functional virtual CAN.

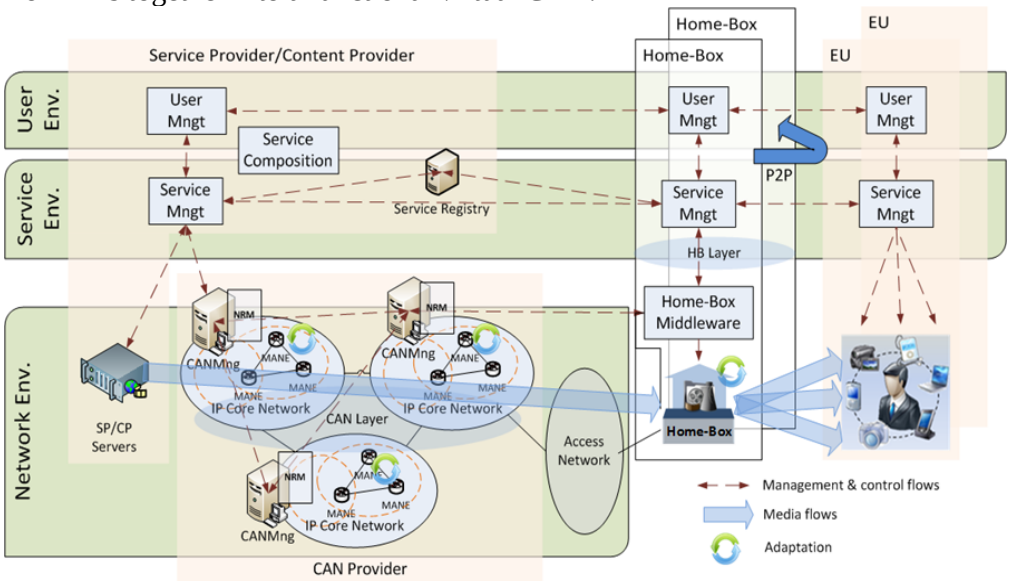

Fig. 1. Alicante General Functional Architecture

The architecture has been organized on several environments and layers (see Fig. 1):

- **User environment (UE):** it creates and manages complete User Profiles necessary for efficient services provision. For instance, the User Management (UMng) modules in the figure are involved in dealing with user–related information, and management/control. UE's functionalities enable the End-Users to be (1) media service and content producers, managers, consumers and providers and (2) completely decoupled from the terminal they use;
- **Service environment (SE):** assures the full service management (creation, provisioning, offering, delivery, control), enhanced with composition of services and the delivery of content to End-Users throughout the network. The Service Management (SMng) modules in the figure, located at SP/CP, inside the Home-Box (HB) and inside the EU terminals, are involved in dealing with services–related information and management/control. Service Registry functionality is also included in SE. The SE uses the overlay connectivity services of the CAN layer and is also involved in the process for efficient adaptation of the services/content according to the End-Users' context. User mobility features, content producer features, security and privacy are other functionalities to be considered at SE level;
- **Virtual HB layer:** is a novel layer proposed by Alicante project. Thanks to this virtual HB layer, one can elaborate Network and Context-Aware Applications and deliver the necessary inputs to create Content-Aware Networks. The adaptation, mobility, security and overall exploitation of media services and content (creation, management, consumption, delivery, adaptation) are being assured through a specific middleware at this layer. Also, it provides a flexible logical infrastructure, capable to be organized in a hierarchical unicast/multicast distribution tree mode, in a distributed mode (e.g. P2P) or both;
- **Network environment (NE)** is composed of:
    - **A Virtual CAN (VCAN) layer**: a novel layer proposed by Alicante, offering virtual connectivity services on the top of a multi-domain IP infrastructure. The VCAN offers enhanced support for packet payload inspection, processing and caching in network equipment. It can improve data delivery via classifying and controlling messages in terms of content, application and individual subscribers, per flow adaptations, network security via content-based monitoring and filtering. Content based routing will also be provided through this layer. Multi-domain CANs can be composed, if necessary. The main modules managing the CANS are the CAN Managers, one per IP domain;

- **Traditional IP network/transport layer**: is responsible for the CANs instantiation via its Network Resource Managers (NRM) at request of the CAN Manager. The specific components, to instantiate the CANs, are the Media-Aware Network Elements (MANE), i.e. the new CAN routers, and the CAN managers, along with the interfaces, monitoring and security features;
- **Access networks:** which are out of the scope of Alicante innovation. The objective is to be compliant and use traditional existing access network technologies.

Further details on the Alicante architecture are available within the project's report [7].

3. The CAN Security Architecture

The main goal of this architecture is to ensure the protection of the data plane communications that span the CAN (multi)domain(s). More specifically, the following security functionalities will be implemented by our architecture:

- content-aware enhanced data packet confidentiality, integrity and authenticity;
- data flow source traceback and distributed access control policy enforcement (suitable as an IPS reactive subsystem)

Fig. 2, shows the security related concepts that we are designing and developing within Alicante CAN layer. Let be assumed the CC_A entity required the SP to establish an IPTv session with CP protected by the security service, named "Secret contain".

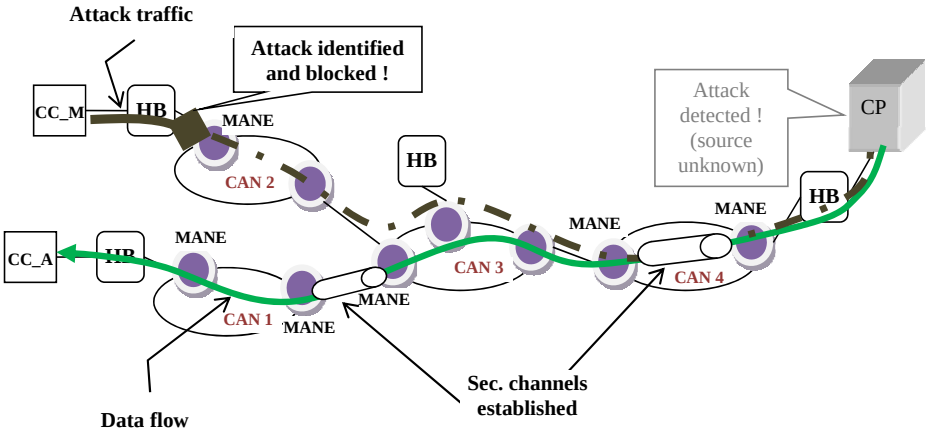

Fig. 2. Conceptual view of the CAN layer security services

Furthermore, upon SP's related solicitation toward the CAN layer, the later asses e2e the corresponding data path risk level and concludes the flow has to pass two

vulnerable network segments located within CAN4 and between CAN1-CAN3, respectively. Consequently, CAN layer require the MANE routers to establish two security channels (see Fig. above), in order to guarantee E2E data flow security level. Later, CP entity detected an (D)DoS attack whose source(s) could not be identified.
Therefore, the CP requires the SP, via HB to find out the source and filter the malicious traffic as close as possible to the origin(s). In turn, the CAN layer task results in identification of all the MANEs (or HBs) entities forwarding the malicious traffic. Therefore, the subset of the MANEs in the neighborhood of the access networks is configured to filter the traffic.

A) Content-aware data packets' security functionality
The following three composite security services will be implemented at CAN layer to be offered at the user interface of the service provider (SP):

- **"Public traffic"**: it means no security or privacy guarantees;
- **"Secret contain"**: to ensure the confidentiality and authenticity of the packets' payload;
- **"Private communications"**: to ensure the confidentiality and authenticity of the entire packet (payload+header). This way, an unauthorized party cannot find out the type of traffic (i.e. what application the user is running), the peers IP addresses and the content of the packets

The security functionalities will benefit from the native CAN layer capabilities in order to efficiently provide security services while guarantees the highest level of security for packets transferred through the network. The CAN layer strategy is to evaluate end-to-end security level of the data path along all CAN domains and discretely apply the security mechanisms only where and when necessary to guarantee the required security level with respect to the security service invoked (pointed out above).
Furthermore, the security functionality at the CAN layer is responsible with network and content-aware adaptation of the security mechanisms parameters, such as: type of cryptographic algorithm, key lifetime, key length with respect to the network conditions and traffic characteristics.
The following inputs will be provided to the security mechanisms in order to enable the security services with features mentioned above (see Fig. 3):

- user flow characteristics (e.g. sensitivity w.r.t. threats, statistics);
- CANP policies (e.g. access control, range of security level);
- network conditions (e.g. data path risk level)

In order to attain the required flexibility the related security architecture was designed according to the hop-by-hop security model on the top of the CAN

infrastructure. This approach implies that trust relationships shall be established between:

- all MANEs routers within each the CAN domain, implicitly associated at the same security domain. They can be established in the form of security associations (SA), either statically at the moment of each MANE router installation or dynamically through participation of the CAN layer (e.g. SecDispatcher entity acting as a broker, see Fig. 4). The complexity of the related SA management procedure is O(n2) for the former method and the O(n) for the later;
- MANEs entities that belongs to adjacent CAN security domains. In this case the related SA management procedure relies on the SA (i.e. trust) statically established between the SecDispatcher entities assigned to the each corresponding CAN security domain;
- all user HBs entities. In this case the related SA management procedure relies on the SA (i.e. trust) statically established between each HB entity and the corresponding SecDispatcher associated with the serving CANP.

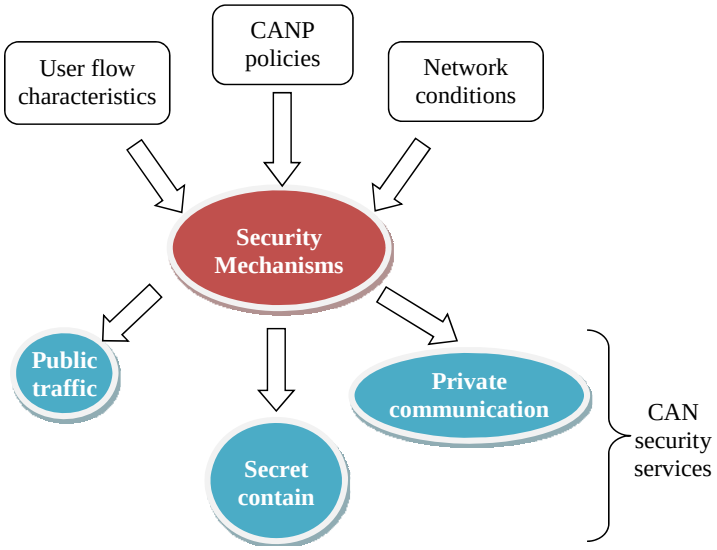

Fig. 3. Input-output of the CAN layer security mechanisms

To support the privacy of the user communications (for implementing “Private communications” service), the security mechanisms should be developed at the OSI network level. This is a challenging task in the context of the content-aware technologies. Therefore, special mechanisms are expected to be designed and employed in order to ensure proper functioning of the other network services. One direction that may be researched is to apply security encapsulation mechanism

(e.g. IPSec ESP [8],[10]) in conjunction with some mapping and tagging mechanisms (e.g. security level label).

B) Distributed access control and data flows' traceback functionalities

CAN Layer security in Alicante will pursue a content-aware approach that will be enforced by MANE routers over data in motion. Such security enforcement will be done accordingly to policies and filtering rules obtained from SecDispatcher@CANMng (see Fig. 4). In turn SecDispatcher@ CANMng will compute policies and traffic filtering rules by executing security related algorithms over information gathered by Monitoring subsystem. Additionally, MANE routers are expected to derive filtering rules from packet inspection, and to inform SecDispatcher@CANMng about those rules.

Content-aware security technologies typically perform deep content inspection of data traversing a security element placed in a specific point in the network. These security elements should also be capable of performing some level of remedial action.

The use of security specific network elements to perform content-aware inspection is mainly due to performance issues, thus avoiding bottlenecks as this equipment have high computational power to perform the required per packet processing. Alicante vision differs from this approach as it is based on MANE routers, which will be used to construct CANs. Content awareness is then obtained on the top of the flow awareness classification already present in the MANE routers, combined with data obtained from monitoring, and policies and traffic filtering rules obtained from SecDispatcher@CANMng. Additionally, it is foreseen that MANE equipment may also be able to compute traffic filtering rules on their one.

An example of a traffic filtering rule could be to drop all traffic matching a set composed of: source IP; source port number; destination IP; destination port number. An example of a policy, i.e. more generic than a traffic filtering rule, would be to limit the maximum number of active connections for a given source in a period of time. Based on this policy, MANE equipment would be able to derive traffic filtering rules and to enforce them.

On the other side, due its content-aware mechanisms the CAN layer, also, allows data flows source traceback. This feature may be provided together with above firewalling mechanisms as a service for intrusion prevention systems implementation. The source traceback procedure will be initiated by some attack detection module (outside Alicante project research work) via HB entity located near the target resource of the attack (i.e. CC/CP). The attack traffic's parameters are forwarded by HB to the corresponding SecDispatcher@CANMng module. This one, in turn, will collaborate with homologous entities from the other CANP

domains until all the MANE(s) routers located close to the attack source(s) are identified and eventually the malicious traffic is filtered.

The architecture design

Fig. 4, presents the main functional entities involved in deploying Alicante security services (pointed out above). The main entities are: SecDispatcher@CANMng and MANE/HB. Their functional objectives, the preliminary structure and interactions are outlined below. Each SecDispatcher is assigned to one CANP (located within CANMng) being in charge with the security decision role, while the MANE routers and HBs have more a security enforcement role. SecDispatcher shall be capable to tell the appropriate MANEs/HBs entities when to build up security channels (e.g. IPSec ESP) or to enforce access control policies. Moreover, SecDispatchers shall be able to collaborate in order to localize the source(s) of the attacks detected by other means considered outside the scope of the Alicante project.

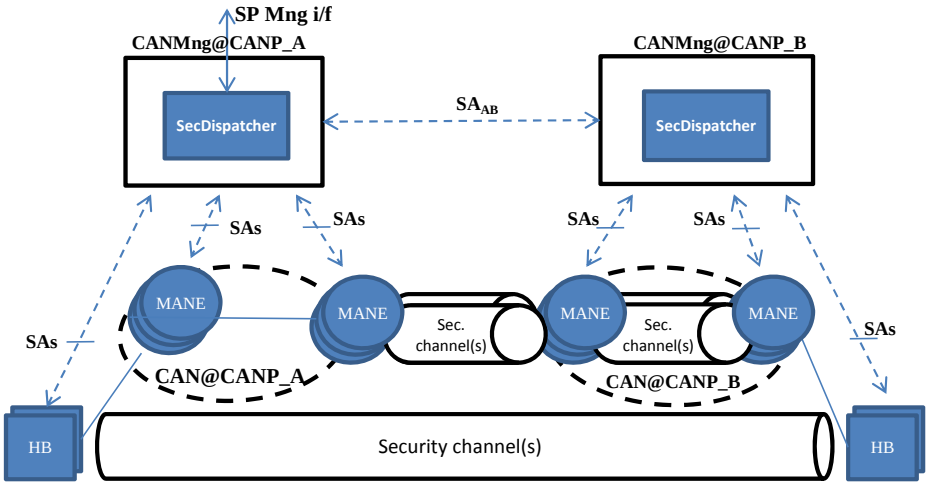

Fig. 4. Overall security architecture design

A minimal network of trust relationships has been defined between the entities as illustrated by the bidirectional vertices, such that security services may be enabled end-to-end. These trust relationships are implemented through static established security associations, denoted SAs. The main goals of SAs defined between CANMng and MANEs/HBs entities belonging to the same CANP domain are to protect their communication and to support dynamic security associations establishment (and trust) in between MANEs/HBs. SA_{AB}'s goal is to extend chain of trust, e2e over several CANP domains. The security of the interface between CANMng and SP entity is outside of the scope of research in the Alicante project.

An ordinary solution could be employed for protection of the communications on this interface.
The main functional objectives of the MANE/HB component are:

- attacks' identification (e.g. port-scan, IP spoofing, replay);
- to enforce traffic filtering rules (based on PckCtx, instructions of CANMng);
- security associations (SA) control by "SA control" module, as requested by "SecControl" module (e.g. key establishment control);
- to enforce per packet security services (authentication, integrity, confidentiality) at IP layer, that are requested by the "CAN SecDispatcher"@CANMng module;
- secure encapsulation/decapsulation of the IP packets;
- management of the security policies database (SPD), configured statically and/or dynamically;
- management of the SAs database (SAD), established dynamically by "Sec Control" module

SecDispatcher@CANMng module carries out collaborative work with homologous entities from other CANPs, in order to implement the following security functions:

- access control policies definition and distribution;
- large scale attacks' identification (e.g. network scans based on MANE port-scan information, DDoS);
- attack flows' traceback to enable source identification and to block the malicious traffic in the proximity of the source;
- the CAN's related security policies management (e.g. SA lifetime control, key length, cryptographic algorithms required for latency trade-off, per content security policy enforcement w.r.t. data path);
- coordination of the end-to-end deployment of the Alicante's 3-level security services: "Public communication", "Secret contain" and "Privacy communication" based on the inputs in Fig. 3;
- figure out in a collaboratively manner whether a certain requested Alicante security service can be provided end-to-end (over several CANP domains);
- initiation of the requests directed to the MANEs for implementation of the elementary security services (e.g. authentication, confidentiality) for a given packet flow or aggregated flows;
- (optional) key management services for intra/inter-domain security mechanisms

The Fig. 5, illustrates the main functional blocks of the MANE router and the related interfaces that are involved in implementation of the Alicante's security services:

- "**Local Sec. Policies**" to provide statically configured local policies to the "Sec. Control" module in order to be enforced;
- "**Sec. control**" has the coordinator role for the blocks and implements the interfaces with the other security architecture layers;
- "**Content descriptor analysis**" provides information about the data flow content for "Sec control" module decisions. Its work may be controlled by the "Sec control" directives;
- "**Malicious traffic detection/identification**" it is a plug-in that specifies the attacks' signatures;
- "**CAN Monitoring**" provides information about statistic characteristics of the data flow for "Sec control" module decisions;

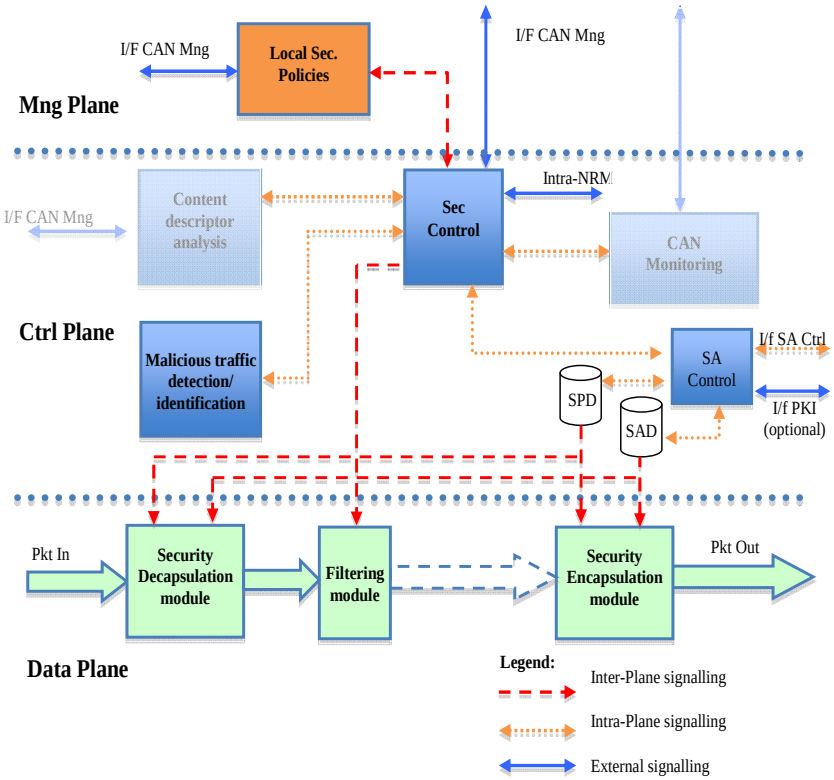

Fig. 5. The MANE's security architecture

- "**SA Control**" in charge with security associations (re)establishment (including security parameters negotiation, and cryptographic key establishment procedures);
- "**SPD database**" specifies the rules to enforce security measures;
- "**SAD database**" specifies the existing SAs (established statically or dynamically);
- "**Security Encapsulation module**" applies cryptographic transformations over the data flows in order to support the required security guarantees, according to SPD and SAD specifications;
- "**Security Decapsulation module**" removes the cryptographic transformations over data flows, according to SPD and SAD specifications;
- "**Filtering module**" in charge with access control rules enforcement, received from "Sec control" module

The Fig. 6, illustrates the main functional blocks of the CAN layer and the related interfaces that are involved in implementation of the Alicante's security services:

- "**CAN Sec. Policies**" provides the statically configured CAN policies to the "CAN Sec. Dispatcher" module in order to be enforced;
- "**CAN Sec. Dispatcher**" it is in charge with the coordination of the security blocks at the CAN layer and implements the interfaces with the other layers of the Alicante's architecture. It is responsible with the implementation of several functionalities (as mentioned above);
- "**CAN Provisioning**" sends directives to the "CAN Sec. Dispatcher" in order to initiate some of the CAN security services;

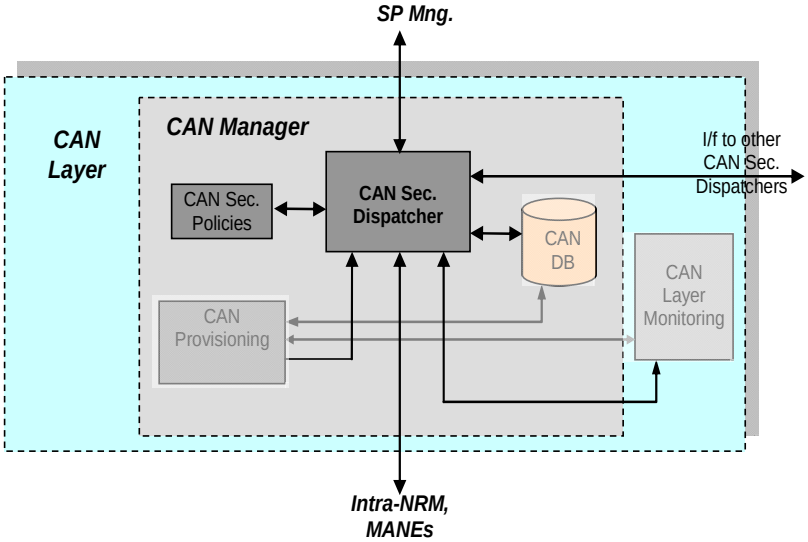

Fig. 5. The CAN layer security architecture

- "**CAN database**" specifies the security characteristics of the CAN infrastructure (e.g. the initial security parameters and context);
- "**CAN Layer Monitoring**" provides information about statistic characteristics of the traffic at the aggregated level for "CAN Sec. Dispatcher" module decisions.

4. Conclusion

In this paper we have presented the new security architecture we designed to provide security services based on content-aware security mechanisms to enable optimization of the network resources utilization. More specifically, we proposed an architectural solution capable to involve the mechanisms only "where and when" necessary with respect to the network context risk level, traffic characteristics (e.g. volume, redundancy, security level) and CANs' security policies. Since we adopted a network-centric approach, our design relies on a priori established trust relationship between end-user and the CAN infrastructure provider and between CAN providers themselves. However, no trust relationship is necessary to be shared between end-user and low level network provider. It may be an advantage since CAN providers are less numerous than network providers. In addition, this approach supports the legacy applications to satisfy the new, more stringent, security related requirements.

The location of the security mechanisms for packets encryption/decryption remains an open issue, which will be decided later, based on the performance evaluations. For instance, their localization within MANE routers that are quite heavy loaded with data packets seems to require the use of lightweight cryptographic algorithms, in order to maintain the communications delay acceptable and reduce the conditions arising the network congestion. A lower latency alternative, at the price of more bandwidth consumption is to place those mechanisms on the HB (Home-Box) entities.

On the other side, our architecture make use of the CAN features to enable specialized integrated functionalities for attack identification, flow traceback and distributed firewalling in support of IPS response subsystem.

Acknowledgement

The authors would like to thank the European Commission for funding our research work within the framework of the Alicante project FP7 ICT No. 248652-IP.

REFERENCES

[1]. *M.Covington, P.Fogla, Z.Zhan, M.Ahmad*, A context-aware security architecture for emerging applications, Proceedings of the 18th ACSAC'02 Int'l conference, 2002

[2]. *M.Lacoste, G.Privat, F.Ramparany*, Evaluating confidence in context for context-aware security, Ed. Springer, LNCS 2007, Vol. 4794, 2007

[3]. *C.Hager*, Context-aware and adaptive security for wireless networks, 2004 http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.106.7384

[4]. *J.Mirkovic, S.Dietrich, D.Dittrich, P.Reiher*, Internet Denial of Service: Attack and Defense Mechanisms, Ed. Prentice Hall, 2004

[5]. *D.Cook, W.Morein, A.Keromytis, V.Misra, D.Rubenstein*, WebSOS: Protecting Web Servers from DDoS attacks, Proceedings of the 11th Int'l ICON Conference, Web Page http://www1.cs.columbia.edu/~angelos/ Papers/websos.pdf, 2003

[6]. *T.Eisenbarth, S.Kumar, C.Paar, A.Pschmann, L.Uhsadel*, A survey of lightweight cryptography implementations, IEEE Design & Test of Computers, 2007

[7]. *D.Negru, Y.Chen, S.Ait-Chellouche, P.Rodrigues, E.Borcoci, R.Iorga, S.Radulescu, R.Lupu, G. Xilouris, G.Gardikis, et al*, D2.1: ALICANTE Overall System and Components Definition and Specifications, IST Alicante project No. 248652, Deliverable D2.1, 2010, http://alicante.labri.fr

[8]. *S.Kent, K.Seo*, Security Architecture for Internet Protocol, IETF, http://www.ietf.org, RFC4301, 2005

[9]. *S.Kent*, IP Authentication Header, IETF, http://www.ietf.org, RFC 4302, 2005

[10]. *S.Kent*, IP Encapsulating Security Payload (ESP), IETF, http://www.ietf.org, RFC 4303, 2005

[11]. *C. Kaufman*, The Internet Key Exchange Protocol (IKEv2), IETF, http://www.ietf.org, RFC 4306, 2005

[12]. *S. Bellovin*, Distributed firewalls, Web Page http://www.research.att.com/~smb/papers/ distfw.html

[13]. *W.Cheswick, S.Bellovin*, Firewalls and Internet Security: Repelling the Wily Hacker, Ed. Addison-Wesley, Reading MA, 1994

[14]. *S.J.Knapskog, A. Gutscher, S.Kiesel, C.Paris, T.Brekne, A.Zwierki, A.Zuquete, R.Lupu, M.Fiedler, et al*, A Report on security concepts for mobile and wireless IP networks. A state of the art report on security for mobile users, IST EuroNGI project No. 507613, Deliverable D.JRA.6.3.1, http://www.eurongi.org/member/WP_JRA_63/

[15]. *W.Stallings, L. Brown*, Computer Security. Principles and Practice, Ed. Prentice Hall, 2008