A Context-Aware Security Framework for Next Generation Mobile Networks

Matteo Bandinelli, Federica Paganelli, Gianluca Vannuccini, and Dino Giuli

Università degli Studi di Firenze
Department of Electronics and Telecommunications, via S. Marta 3, Florence, Italy
{matteo.bandinelli,g.vannuccini}@gmail.com,
{federica.paganelli,dino.giuli}@unifi.it

Abstract. The openness and heterogeneity of next generation communication networks are now highlighting more security issues than those of traditional communication environments. Moreover users' security requirements can often change in mobile communication environments, depending on the situation in which the user is immersed. Our objective is to define a context-aware security framework for addressing the problems of end-to-end security on behalf of end-users. Based on context data acquisition and aggregation features, the framework uses contextual graphs to define security policies encompassing actions at different layers of communication systems' architecture, while adapting to changing circumstances.

Keywords: context-aware security, multi-layer security policy, security context, contextual graph, next generation communication networks.

1 Introduction

The emerging vision from research in Next Generation Networks (NGN) is that of an All-IP network of heterogeneous networks, integrating different access technologies seamlessly with respect to end users. This approach implies to move from traditional vertical architectures towards the definition of a common architecture providing open interfaces for heterogeneous communication and application service providers [15].

The openness and heterogeneity of NGN communication networks are now highlighting more security issues than those of traditional communication environments. Roberts et al. [18] provide a brief analysis of challenges for security implied by NGN architectures. For instance, mobility and heterogeneity of user devices as envisaged by NGN architectures are likely to present physical security threats, since control and configuration of the devices are directly managed by end users and not by network security administrators. Another issue is how to provide end users with secure end-to-end communication in a heterogeneous network infrastructure, with rapidly changing security requirements related to user's mobile environment.

The term "context-aware security" is widely used to identify an emerging research field trying to cope with the above-mentioned issues by applying a context-aware system design approach [5],[13],[14]. Most existing works ([1],[5],[14],[20]) focus on

A.U. Schmidt and S. Lian (Eds.): MobiSec 2009, LNICST 17, pp. 134 – 147, 2009.

context-based security policies for adaptive authentication and authorization services at the application layer. Such an approach is quite limited with respect to the issues of the upcoming NGN scenario, where a more comprehensive approach for enforcing security actions at different layers of the communication architecture is needed.

Therefore, our objective is to define a context-aware security framework capable of defining security policies with proper adaptation to changing circumstances in order to address the problems of end-to-end security on behalf of end-users. Adaptive security policies are here conceived as a set of security actions pertaining to different layers of the security architecture as defined by the International Telecommunication Union (ITU): application layer (network-based applications), service layer (basic connectivity, transport and added value services) and infrastructure layer (physical network nodes and communication links) [11].

We provide a definition of security context based on a non-exhaustive categorization of security context items (such as user location, device capabilities, access network type) and we adopt contextual graphs to model the decision process for defining multi-layer security polices adapting to changing context.

A significant contribution of this paper is the integration and composition of multiple context categories into contextual graphs in order to specify multi-layer security policies in the NGN scenario. With respect to the related research work, our aim is to propose a more general and extensible approach to face the complex security challenges envisaged by the NGN architectures. A possible implementation of the model into a NGN architecture is then proposed, by identifying proper functionalities to achieve the contextual-graph-based adaptation of security policies.

The paper is organized as follows: Section 2 discusses related work in context-aware security; in Section 3 we describe the main elements of the Context-aware Security Framework, namely the security context model, the security actions (by providing some examples for each security layer) and the use of contextual graphs for modeling context-based multi-layer security policies; Section 4 proposes an architectural model of the context-aware security framework; Section 5 concludes the paper and gives further research directions.

2 Related Work

While several works exist in the research field of context-aware computing and context-aware services in several application domains [7][17], only a few works have investigated the use of context aware computing models for designing adaptive security mechanisms.

Covington et al. [5] proposes a Context-Aware Security Architecture (CASA) enabling the design of security services which use security-relevant “context” knowledge to provide flexible access control and policy enforcement. CASA has been used to implement a Role-Based Access Control model based on the concept of “environment role” (i.e. environmental conditions that are relevant to access control).

Masone [12] proposes a Role Definition Language to describe roles in terms of context information. Other works present context-aware authentication and authorization policies for augmenting network security in Intranet environments [20] and in ubiquitous computing environments [1].

In [14] a model for context-based security policies specification based on the use of contextual graphs is proposed. The model has been applied for deducing context-aware authorization policies to be enforced in a pervasive environment.

Some recent works are beginning to investigate mechanisms to address security issues in mobile environments with such a broader perspective. In the IST MAGNET Project, a Context-aware Security Manager (CASM) is responsible for adapting security policies based on a security level determined according to two context categories (user location/scenario and device constraints) [13]. In [21] a context-aware security policy agent activates new security actions according to a change of context parameters (i.e. user preferences, power and location of the mobile platform).

With respect to these contributions, our security context model mainly refers to [14], and takes into account a wider range of context parameters, as described in Section 3.3. This contextual knowledge is exploited in order to define the most appropriate approach for enforcing security at the infrastructure, service and application layer.

3 Context-Aware Security Framework

The proposed Contex-Aware security framework aims at providing extensible mechanisms for defining and enforcing security policies in NGN environments. Extensibility is here intended as the capability of the system to cope with new security requirements which may be determined by new application domains, information services to be secured, available sources of context information and/or new security actions which can be enforced thanks to technological advancement and standards evolution. Extensibility of the proposed framework is mainly supported by the contextual graph-based modeling approach as discussed in [2].

Hereafter we describe the main elements of the Context-aware Security Framework: the Security Context, a classification of security actions and the approach for context-aware security policy definition based on contextual graphs.

3.1 Security Context

In the domain of context-aware security, a definition of security context is the one provided in [14]:

"A security context is a set of information collected from the user's environment and the application environment and that is relevant to the security infrastructure of both the user and the application."

Referring to communication environment, as the set of users, devices, applications, data and communication links that characterize the communication, we propose the following definition:

"A security context is any information that can be used to characterize the security situation of a communication environment. The security situation can be characterized in terms of possible security threats, user status and requirements with respect to information protection, available communication and computing resources which can

be exploited by a system in order to specify and enforce proper actions to guarantee end-to-end security".

With respect to the first definition our definition does not mention any possible context source and/or context information category (e.g. user and application environment), as most appropriate context information and related sources can vary according to application purposes and the available technological infrastructure. Moreover, as the focus is on end-to-end security, the context should consider not only the situation concerning the environment of a target end-user, but also the situation of the destination peer (i.e. the host delivering information services, or another user interacting via communication services with the first one). Based on the security context definition proposed above, we provide an enumeration of categories for organizing security context items. The enumeration does not aim at being exhaustive. Indeed, our attempt has been to select first those context items that can be considered of general value for securing information exchange and, possibly, can be acquired by common and easily deployable sensing infrastructure. In section 3.3 we also provide an example of how these context categories can be applied to define context-aware security policy in an application scenario.

We first defined the following basic context information categories:

- **User.** This category includes information items representing current user personal sphere, surrounding environment attributes, preferences and attitudes. For instance, the user environment can be characterized by multiple mobile and fixed devices available for accessing different kind of communication services. The following items can be included in this category:
  - *User Location*: symbolic position of the user. Possible values are: "public" (the user is located in a public environment, where possible eavesdroppers may be close to the user accessing the network), "private" (the user is located in private environment – e.g., a house, an office, where eavesdropping may be feasible only within the core network or via side-lobes of the private wireless network).
  - *User Status*: user's current activity and/or availability to interact with communication and information services. It can be associated to the "user status" typical of messaging services. Possible values are: "not available", "available", "only textual interaction", "only voice interaction".
  - *Available Devices*: devices that are associated to the target users and can be used to access network-based services. Examples of user devices are: mobile phones, Personal Digital Assistants (PDA), notebooks, desktop PCs, fixed phones.
  - *Required Security Level*: security level which is required by the end-user. Possible values are: "high" (the user is asking for a high security communication, this may be the case for a remote access to very critical data), "medium" (the user is asking for a medium security communication, this may be required for an access to personal, but not critical data), "low" (the user is not particularly asking for a specific security level, this may be the case for entertainment online services).

Many of the above mentioned items can be directly acquired by user manual input. However, different mechanisms can be put in place in order to automate the process of context information acquisition. For instance, positioning techniques can be

integrated in user devices in order to localize users (e.g. GPS, RFID readers, etc.). Typically, localization mechanisms can acquire information on user's physical position (e.g. latitude and longitude coordinates). Proper physical-symbolic positions association can be defined for frequently visited locations (e.g. "home" and "work" locations). In order to estimate user required security level from available contextual information, several mechanisms could be alternatively or jointly applied, such as machine learning and rule-based inference mechanisms (for instance, a rule may state that the required security level is low when the user location is of type "private").

- **Device.** This context category aims at representing most relevant technical characteristics of the user "active" device, i.e. the device that the user is currently using to access network-based services to be secured. We selected the following basic context information:
  - *Device type*: possible types of end-user devices are, for instance: mobile phone, Personal Digital Assistant (PDA), notebook, desktop PC.
  - *Device capabilities*: it refers to the capabilities of the end-user devices, in terms of hardware, software and configuration settings. These capabilities can be classified as follows: hardware (es. CPU, memory), display (es. size, resolution), protocols (es. HTTP, SIP, SMTP), networking (es. Bluetooth, WI-FI, GPRS, UMTS), application platform (es. JVM).
  - *Security settings*: This includes parameters such as antivirus signature version, personal firewall availability and rules setting, routing tables, and file-system permissions settings.
  - *Available Energy Supply*: this parameter takes into account device resources which are relevant to energy management. It can be represented as a combination of two components: a flag variable accounting if the system is powered by an external AC (alternating current) input; a second parameter representing the remaining battery life.

This information on the active device can be useful in order to estimate security risks (for instance if the antivirus version is not up-to-date) and to evaluate if a desirable security action can be enforced on the target device, according to its capabilities. For instance, on a mobile device characterized by limited computational resources and high energy consumption, the system cannot enforce the activation of a VPN to secure the communication channel. Context items characterizing the device category can be represented by means of the composite capability/preference profile (CC/PP) representation scheme [19].

- **Communication**: here we include the characteristics of the end-user device communication link.
  Most relevant attributes are:
  - *Current access network type*: possible values are GPRS, UMTS, Wi-Fi, etc.
  - *Available bandwidth*: bandwidth available for information transmission. Possible symbolic values are: "high" (e.g. more than 2Mbps) "medium" (e.g. between 2 Mbps - 56 Kbps) "low" (e.g. 56 Kbps as traditional modem).
  - *Signal quality*: in case of wireless access network, this parameter represents the quality of the transmission signal. Possible values are "high, medium, "low". Mapping with physical values is dependent on the technological infrastructure and application domain.

  - *Access network security*: security settings of the access network in use (e.g. encryption available/not available). This information may be useful for determining possible security risks (e.g. if the communication channel is not encrypted) and for selecting the set of possible security actions that can be reliably supported.
- **Application:** this context category includes parameters describing end-user applications' characteristics, such as:
  - *Content Sensitiveness*: content to be exchanged can be "sensitive" (e.g. user personal data) or "not-sensitive" (e.g. broadcast news).
  - *Content Size*: size of content to be exchanged. Possible symbolic values are "high", "medium", and "low". Mapping with physical values (e.g. kB) is dependent on the application domain.
  - *Active Application*: type of network-based application to be secured. Applications can be distinguished in user-to-user interaction (e.g. voice over IP, instant messaging, etc.) and access to information services (e.g. Web browsing).
  - *Currently Executing Applications*: currently executing applications that can have conflicts of interest with the target active application.
  - *User Application Profile*: it represents the user's role in a service application domain (e.g. patient, nurse, general practitioner in a e-health scenario). At lower-level, it can also be represented by a profile of permissions for accessing application services. In such case, possible values are "read only" (e.g. only "get" operations), "read & write" (e.g. only "get" and "post" operations), "superuser" (e.g. any operation)..

3.2 Security Actions

The objective of the proposed security framework is to exploit system's knowledge of context to select appropriate security actions to be enforced in order to guarantee an expected security level.

With respect to the state of the art [1],[14],[20], our work aims at providing a flexible framework which can encompass heterogeneous security actions (not just encryption, authentication and authorization), and, in principle, all the available tools and technologies capable of improving the protection of the exchanged data.

More precisely, our objective is to adopt a multi-layered approach, i.e. to exploit contextual knowledge in order to adapt security policies. Such policies are defined as a combination of actions at the different layers of the security architecture for systems providing end-to-end communications, as defined by the International Telecommunication Union (ITU).

The Security Layers are hereafter defined [11]:

- **Application Layer:** this layer focuses on security of the network-based applications accessed by end-users. Examples are: file transport and web browsing applications, voice messaging and email, as well as vertical applications (e.g., customer relationship management, electronic/mobile-commerce).
- **Service Layer:** this layer addresses security of services provided by service providers. Examples are: basic transport and connectivity services (e.g., AAA

services and domain name services), value-added services (QoS, VPN, location services).

Infrastructure Layer: This security layer focuses on the hardware resources at both network and end users' sites. Examples are: routers, switches and servers, communication links, end-user devices.

Table 1. Security Layers and Related Actions

Security Layer	Security Action	Security Dimension	Security Action strength
Infrastructure Layer	Device switching (vertical handover)	Availability, Communication Security	Cellular phone, PDA, notebook, desktop PC
Services Layer	MAC layer Encryption activation	Confidentiality	WEP, WPA (shorter key), WPA (longer key)
	VPN IPSec activation	Confidentiality, Authentication, Data Integrity	3DES, AES-128bit, AES-256bit, etc.
	Blocking of other concurrent session potentially harming the desired session	Communication Security	
Application Layer	SSL session activation.	Confidentiality, Authentication, Data Integrity	Plain SSL with not-trusted certificates, SSL with trusted certificates.
	User alerting	Privacy	Textual alert, audio alert, Video alert
	Data encryption	Confidentiality	Encryption algorithm (e.g. AES) with different key sizes and rounds number)
	Adaptive authentication	Authentication	Anonymous, Pseudonymous (weak auth), strong authentication

For each security layer, Table 1 shows a set of possible security actions (selected as most meaningful for the considered NGN scenarios). These actions can be enforced with different strength, depending on implementation choices. A possible, non exhaustive, list of implementation options is shown for each selected action.

With respect to the ITU-T X.805 standard specification, the security actions considered in this section address the following security dimensions: Authentication, Data Confidentiality, Communication Security, Data Integrity, Availability, and Privacy. The other Security Dimensions (Access Control, Non repudiation) have not been taken into account. As a matter of fact, such dimensions are already addressed by other works [14], which can complement or extend the functionalities offered by the proposed Context-aware Security Framework.

3.3 Context-Based Security Policies

As described in Section 2, our work is based on the approach proposed in [14]. In particular, [14] specifies that rule-based formalism is often adopted for modeling context-based decision processes, but it suffers from the following main limitations: the difficulty to maintain such formalisms in case of complex systems to secure, to

identify all the needed contextual information from the rule-based formalism, and to understand the followed strategy of the policy. Therefore, we also adopted the contextual graph approach, which can be used to represent a set of practices to perform in order to solve a given problem. A path, from the input to the output of the contextual graph, represents a practice with the contextual elements explicitly considered.

A contextual graph is an acyclic graph with a unique input, a unique output and a serial-parallel organization of nodes connected by oriented arcs. A node can be an action to be enforced, a contextual node, or a recombination node. A contextual node represents the instantiation of a context item, which is evaluated in order to direct the process through one path among all the possible alternatives. A recombination node allows to represent the convergence of different paths into a single node. An action node represents a security action to be enforced.

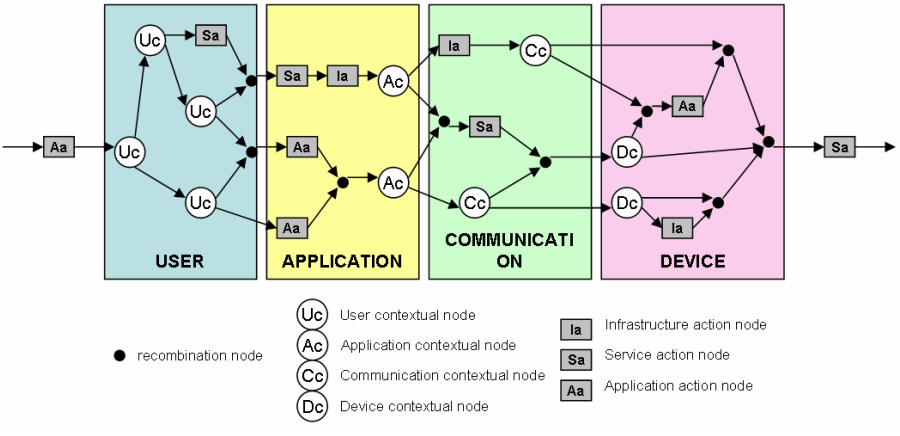

Fig. 1. An example of Contextual Graph

With respect to the Moustefaui proposal in [14] that has the aim to specify authentication and authorization policies, we extend the contextual graph theory, in order to cope with both the security categorization and the multi-layer approach of the security policy. As shown in Fig. 1, the decision process is based on the evaluation of the four categories of the security context and it is represented by a sequence of User, Application, Communication, or Device contextual nodes. Furthermore, a more complete end-to-end security policy is here represented by the instantiation of three different action node types (Infrastructure, Service and Application action nodes), in order to model a multi-layer security policy. Security context items which have been acquired by the system are evaluated in the graph at the corresponding contextual node, to select proper security actions, which are represented by action nodes. The contextual graph is thus a sequence of context evaluation nodes representing the most relevant attributes of the communication environment, and security enforcement nodes defining the security policy to be implemented in that specific communication environment.

In the following we describe a reference application scenario, used to provide an example of application of the contextual graph for the enforcement of multi-layer security policies.

At 8.00 am John, a doctor, is at the railway station, on the way to visit a patient (Mr Smith), who has been visited last week by a colleague. John decides to discuss Mr Smith's health record with his colleague. By accessing the open public WLAN available at the railway station, John uses his PDA to call the colleague (Situation A). During the conversation, John shares with the colleague the patient health record's information. John goes directly to the patient's home to visit him; then he accesses the information services of the hospital and update the patient record (Situation B).

In Fig. 2 we provide an example of how user, application, communication and device-related context can be taken into account for the definition of multi-layer security policies. For the sake of brevity, the example has the objective of presenting some relevant decision steps, not a complete decision path. Situation A is characterized by the following decision path, that represents the security context of the communication environment. First, John accesses the service network through a public access point at the railway station; due to his public location, he is exposed to greater threats then other locations. Second, the service is about transmitting sensitive content (the patient health record) and can be characterized as an interaction with another person. The access network is an "open" WLAN (i.e. link without encryption). As encryption is enabled on the user device (and also decryption is enabled at destination side) the content is encrypted before transmission. In Situation B, the user is accessing a service, which implies the access to sensitive content. As VPN is enabled at both user and destination site, the security action to be enforced is the VPN setup.

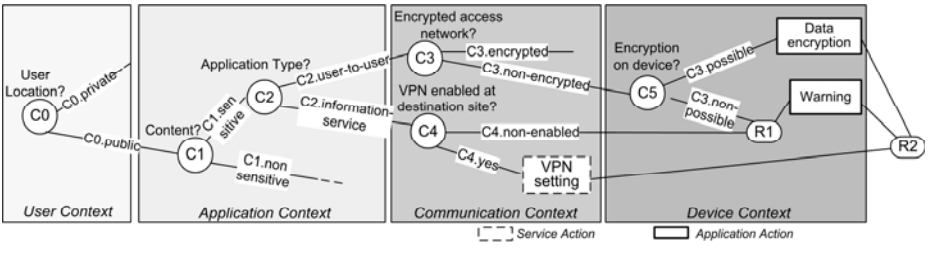

Fig. 2. Example of context-aware security policies

4 Architectural Model

This section describes how the considered security-context aware system can fit into a high-level architecture for adaptive security in Next Generation Networks. In Figure 3 we depict the main functional blocks of the architecture.

Context Data Acquisition: This block collects context information about the communication environment, related to users, devices, applications, data and communication links. Context data are acquired by heterogeneous context providers,

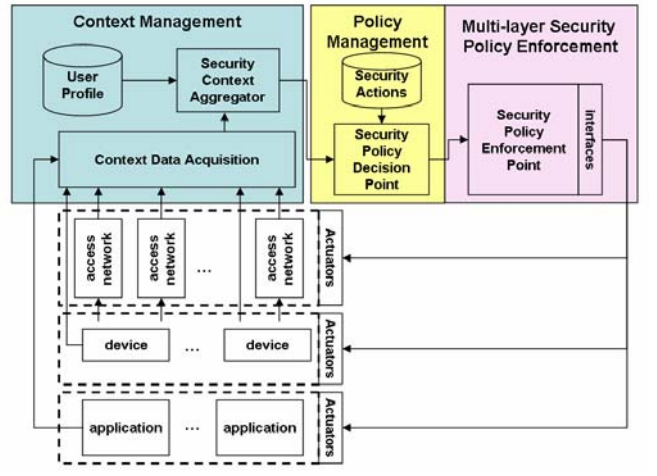

Fig. 3. Architecture of the Security Context Aware Framework

by exposing an interface, or, more precisely, a composition of different interfaces for push/pull data acquisition. For instance, device information may be gathered by the device Management Information Base via SNMP, or CC/PP messages. Information related to the end user may be collected either from the user profiles managed by the network infrastructure, via network signaling protocols, or by application-dependent profile information, through remote interface invocations (e.g. via Web Service interfaces).

Context Data Aggregator: It integrates and correlates raw context data collected by the Context Data Acquisition in order to obtain context data at the level of abstraction needed in the decision process and to maintain data consistency and quality. Several data processing and reasoning techniques can be adopted for this purpose: a programmatic approach, rule-based reasoning, ontology-based reasoning, self-learning techniques, etc.

Security Policy Decision Point (PDP)**:** This block defines the proper multi-layer security policy according to the current context. This component builds the above-described contextual graph and searches for a path matching with available context items' values. Security actions that are selected along the path are communicated to the Security Policy Enforcement Point for their actuation.

Security Policy Enforcement Point (PEP)**:** This block takes as input the context-based security actions to drive their enforcement, by communicating with the appropriate actuators situated in the network nodes and/or in the end-user device. As security actions may involve different layers (as depicted in Fig. 2) the Security PEP interacts via proper interfaces with different actuators.

Actuators: The actuators are active entities listening for commands sent by the Policy Enforcement Point and communicating with software and hardware resources for the realization of security actions. While the decision process can be conceived as a

centralized module in the considered architecture, the security policy actuation is typically distributed, due to the extreme heterogeneity of the possible enforcing points and actuators (e.g., current device, alternative devices, network access point, etc).

Since it is expected that the NGN also will use the enhanced IP Multimedia Subsystem (IMS) to integrate IP-based multimedia services over the Internet, wireline telecommunications networks, and diverse wireless networks [16], in the following a possible implementation of the context-aware security framework in IMS is proposed. It should, indeed, be noted that the above-mentioned functional blocks are basically standard components that are already embedded in the whole IMS architecture.

The NGN architecture, according to the access independent principle, is characterized by multiple access networks converging into a common IP based core network. In such scenario, IMS provides specific gateways to the control plane for each access technology (e.g., GPRS, xDSL, WLAN, etc.), through specific Proxy Call State Control Function (P-CSCF). Furthermore, the suitability of the IMS as the environment in which our model can be implemented, results from the use of a wide set of Internet Engineering Task Force (IETF) protocols, in order to harmonize with Internet services. Specifically, IMS uses the Session Initiation Protocol (SIP) [10] for signaling and session management; Diameter [5] protocol and common open policy service (COPS) [8] for operations and management. Each of these protocols can represent a possible, although not complete, implementation of functionalities of our proposed model. Session Description Protocol (SDP [9]), which is used for describing multimedia sessions in order to support a suitable resources reservation, contains parameters (e.g., required bandwidth, service type, connection parameters, etc.) that are also useful during the decision process of our model and that can be used by Context Acquisition and Aggregation functions in order to derive many security context attributes. The user presence attributes can be derived from the IETF presence model [6], which is integrated in IMS through the use of an extension of the SIP protocol, called SIP/SIMPLE (SIP for Instant Messaging and Presence Leveraging Extensions) [3]. Other user attributes, such as the addressing of the available devices, and access state parameters can be derived directly from the Home Subscriber Server (HSS) of the the IMS architecture. The main data stored in HSS include, indeed, user identities (the private one, and the public ones), registration information, access parameters and service-triggering information [16].

Also regarding the enforcement functions, their implementation could be driven by exploiting proper mechanisms native in NGN architecture, such as session mobility between different devices. According to our approach, the device switching, supported by the control plane of NGN architecture for QoS requirements [15], should be driven also by security issues. Further, relating to the enforcement of security actions, COPS protocol provides the suitable communication in a PDP-PEP mechanism, in order to manage the resource allocation for the current communication.

For other specific exchanges between user devices and network nodes inside a NGN architecture, extensions of the SIP protocol could be implemented [3].

Then, in such a NGN architecture, the decision process of our context aware security model is implemented by a dedicated service node of the control plane, or, referring to IMS architecture, by the Serving Call State Control Function (S-CSCF), which represents the central element of the signaling network. The adoption of the

IMS architecture as an enabling environment for the implementation of the proposed model is supported by the consideration of IMS as the reference platform for NGN control plane, however our context aware security model preserves his validity regardless of IMS, and allows possible implementation in other policy decision and enforcing systems.

Relating to a possible implementation of the Context-Aware Security in IMS, the sequence diagram proposed in Figure 4 refers, for example, to a session set-up, based on the request/response mechanism of a SIP architecture. With respect to a typical SIP interaction [10], the S-CSCF intercepts the communication between the SIP user agents, while activating the decision process and promoting the implementation of the consequent security policy, by exchanging "ACTION REQUEST" messages with enforcement points, here represented by the Control Plane Gateways (i.e., Proxies according to the user view) and by the SIP user agents on the user devices.

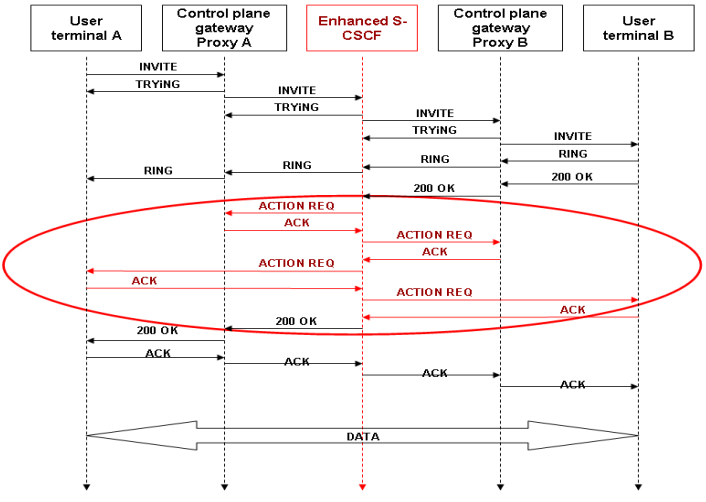

Fig. 4. Session set-up in a Context-Aware Security system in IMS

5 Conclusions

This work presented a context-aware security framework for addressing the problems of end-to-end security on behalf of end-users in a Next Generation Network scenario. We discussed the definition of context in the security domain and proposed a set of categories for organizing context items. The security framework uses contextual graphs to define security policies encompassing actions at different layers of communication systems' architecture (i.e. application, service and infrastructure layers of the ITU-T security architecture), while adapting to changing context. In order to demonstrate the feasibility of the proposed system, we also discussed a possible implementation in a generalized NGN architecture. Future research activities will be devoted to the design and development of a prototype for the Security Context Aware Framework in an e-health application scenario. The analysis of the target

scenario will also provide useful hints for refining the context items' and security actions' models. Furthermore we will investigate how the proposed approach could be extended in order to manage security policies at different levels of abstractions and/or priorities (e.g. by using sub-graphs and/or a hybrid approach integrating further reasoning techniques). This analysis will aim at defining high-level policies (e.g. matching with organizational and user requirements) and binding them with low-level implementation policies.

References

1. Al-Muhtadi, J., Ranganathan, A., Campbell, R., Mickunas, M.D.: Cerberus: a context-aware security scheme for smart spaces. In: Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, March 23-26, pp. 489–496 (2003)
2. Brezillon, P., Pasquier, L., Pomerol, J.C.: Reasoning with contextual graphs. European Journal of Operational Research 136(2), 290–298 (2002)
3. Brok, J., Kumar, B., Meeuwissen, E., Batteram, H.J.: Enabling New Services by Exploiting Presence and Context Information in IMS. Wiley Interscience, Hoboken (2006)
4. Calhoun, P., Loughney, J., Guttman, E., Zorn, G., Arkko, J.: Diameter Base Protocol. Request for Comments 3588 (September 2003), http://www.ietf.org/rfc/rfc3588.txt
5. Covington, M.J., Fogla, P., Zhan, Z., Ahamad, M.: A Context-Aware Security Architecture for Emerging Applications. In: Proceedings of the Annual Computer Security Applications Conference (ACSAC), Las Vegas, Nevada, USA (December 2002)
6. Day, M., Sugano, H., Rosenberg, J.: A Model for Presence and Instant Messaging. Request for Comments 2778 (February 2000), http://www.ietf.org/rfc/rfc2778.txt
7. Dey, A.K., Abowd, G.D.: Towards a Better Understanding of Context and Context-Awareness. In: Workshop on The What, Who, Where, When, and How of Context-Awareness, as part of the 2000 Conference on Human Factors in Computing Systems, CHI 2000 (2000)
8. Durham, D., Boyle, J., Cohen, R., Herzog, S., Rajan, R., Sastry, A.: The COPS Protocol. Request for Comments 2748 (January 2000), http://www.ietf.org/rfc/rfc2748.txt
9. Handley, M., Jacobson, V.: SDP: Session Description Protocol. Request for Comments: 2327 (April 1998), http://www.ietf.org/rfc/rfc2327.txt
10. Handley, M., Schulzrinne, H., Schooler, E., Rosenberg, J.: SIP: Session Initiation Protocol. Request For Comment 2543 (March 1999), http://www.ietf.org/rfc/rfc2543.txt
11. International Telecommunication Union. ITU-T X.805 Security architecture for systems providing end-to-end communications SERIES X: Data Networks and Open System Communications – Security (2003)
12. Masone, C.: Role definition language (rdl): A language to describe context-aware roles. Technical report, Dartmouth College, Computer Science, Hanover, NH (2002)
13. Mihovska, A., Prasad, N.R.: Adaptive Security Architecture based on EC-MQV Algorithm in Personal Network (PN). In: 4th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Philadelphia, USA (2007)

14. Mostefaoui, G.K., Brezillon, P.: Modeling context-based security policies with contextual graphs. In: The Proc. of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, pp. 28–32 (2004)
15. Nasser, N., Hasswa, A., Hassanein, H.: Handoffs in Fourth Generation Heterogeneous Networks. IEEE Communications Magazine (October 2006)
16. Poikselka, M., Mayer, G., Khartbil, H., Niemi, A.: The IMS – IP Multimedia Concepts and Services. Wiley, Chichester (2006)
17. Ranganathan, A., Campbell, R.H.: An Infrastructure for Context-Awareness based on First Order Logic. Personal and Ubiquitous Computing 7(6), 353–364 (2003)
18. Roberts, M.L., Temple, M.A., Mills, R.F., Raines, R.A.: Evolution of the air interface of cellular communications systems toward 4G realization. In: Communications Surveys & Tutorials, vol. 8(1), pp. 2–23. IEEE, Los Alamitos (First Quarter 2006)
19. World Wide Web Consortium, Composite Capability/Preference Profiles (CC/PP): Structure and Vocabularies 1.0 (January 2004)
20. Wullems, C., Looi, M., Clark, A.: Towards Context-aware Security: An Authorization Architecture for Intranet Environments. In: The Proc. of the Second IEEE Annual Conference on Pervasive Computing and Communications, pp. 132–137 (2004)
21. Yee, G., Korba, L.: Context-aware Security Policy Agent for Mobile Internet Services. In: Proc. of the 2005 IFIP International Conference on Intelligence in Communication Systems (2005)