A Security Analysis for Home Gateway Architectures

Pierre Parrend, Stephane Frenot

***Abstract*— Providing Services at Home has become over the last few years a very dynamic and promising technological domain. It is likely to enable wide dissemination of secure and automated living environments. We propose a methodology for identifying threats to Services at Home Delivery systems, as well as a threat analysis of a multi-provider Home Gateway architecture. This methodology is based on a dichotomous positive/preventive study of the target system: it aims at identifying both what the system must do, and what it must not do. This approach completes existing methods with a synthetic view of potential security flaws, thus enabling suitable measures to be taken into account. Security implications of the evolution of a given system become easier to deal with. A prototype is built based on the conclusions of this analysis.**

***Keywords*— Security requirements, Connected Home, OSGi, Sofware Components.**

I. Introduction

Personal Internet connections now commonly provide most users with broadband connectivity and advanced multimedia services. On the other hand, more and more personal services are proposed that enable people to maximize comfort and home automation: elderly people care, protection against burglars, centralized control of home equipments. A strong movement has developed during the few last years that aims at merging the two worlds. Personalization of services can then meet large communication resources and existing infrastructure, so as to make a large dissemination of such services not only possible but also affordable for a broader population. We use the term Services at Home to name these advanced services.

In particular, several industrial consortia and academic projects targeting at specifying Home Network systems have an important research and specification activity: Echonet in Japan [2], Home Gateway Initiative (HGI) [6] or the Muse Consortium [10] in Europe, DLNA [1] in the USA support interoperability and specification efforts of firms that are active in this domain.

The key element in the Services at Home architecture is the Home Gateway, or residential Gateway, because it both provide Internet connectivity and support for advanced services [13]. It is defined as the "high tech device ensuring continuity between the home network(s) and the in home connected devices and the external world represented by a wide area network (WAN)" [6]. The Home Gateway must support high-level service delivery over Internet broadband access, it must be suitable for generic service software deployment and upgrade, compatible with network monitoring utilities, and it needs to be able to support remote control of ambient systems, assisted living, home automation appliances, energy management and control or security (in the sense of fire and crime prevention).

Architecture and use cases of Home Gateway based systems has been specified, but surprisingly little work has been published to promote understanding of security implications of such systems. As far as most gateways can be expected to be vendor specific, it is not realistic - and even less useful - to propose a frozen secured gateway. However, knowledge about generic behavior of Home Gateways systems in a multi-provider context as well as a systematic approach to threats will enable each designer and vendor not to overlook potential risks bound to the system. They will thus be able to take them into account while building a specific Home Gateway.

In this paper, we define and exploit a suitable method for identifying Home Gateway Systems characteristics. It is based on the first hand on EBIOS[1] [14], a method that has been defined by the french DCSSI (Central Direction for Security of Information Systems) and several firms and administration of the European Community, and on the other hand on ISO Common Criteria [8], which is the standard process for designing secure systems. It aims at providing tools that support the expression of security characteristics of Home Gateways. These tools are a generic Role Based Access model (RBac) model [3] for Services at Home Systems, as well as attack trees for the various weak points of the architecture. Our method thus defines a dichotomous positive/preventive approach, that is to say analyzes on the first hand what the system must do, and on the other hand what he must not do. This approach completes existing methods with a synthetic view of potential security flaws, thus enabling suitable measures to be taken. The security implications of the evolution of a system become easier to deal with. Such knowledge will become increasingly important as advanced Home Gateways will find their way along to the home of the users.

The paper is organized as follows. Next section defines what a Services at Home delivery system is. Section III presents the positive analysis of the architecture. Section IV the preventive one. Section VI presents related works, and section VII concludes this paper and highlights identified needs for future work.

[0]Authors are with INRIA Ares team, CITI Laboratory, 21 Avenue J. Capelle, INSA Lyon, France (phone: +33 (0) 04 72 43 71 29; e-mail: pierre.parrend,stephane.frenot@insa-lyon.fr).
This work has been done in the frame of IST FP6 Projects Muse 026442.

[1]http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html

II. Definition of the Analyzed System

The first step for running a proper security analysis of a system is to define it precisely. We established the following generic definition of multi-provider Home Gateway systems specifically so as to make subsequent security analysis possible.

Services at Home systems are composed of the users' equipments (Home Gateway and Devices), of various Services Providers, and of authorized managers. Devices, or Home equipments, are the elements that provide the actual service: a television connected to a Video-On-Demand facility, a device for fire detection, a beeper connected to a medical emergency facility, and so on. The Home Gateway contains two elements: the Access Gateway, providing the connection to the Internet, and the Service Gateway that plays the role of an applicative server. Both elements can share the same hardware support - or not, depending on the policy of the Access Gateway provider. The second configuration (Access and Service Gateway on different hardware parts) implies some legal constraints as far as the Access Gateway is often considered to be part of the telecommunication network. This is not the case for other set-top boxes, that are considered as Home Equipments. But it does not imply real technological difference. In the following, we will consider that the Home Gateway play both roles of Access and Service Gateways.

Managers are network entities, or persons, that have rights to control the Gateway. Their role is to enable new Services Providers or Services to be proposed to the user. Each entity of the Gateway has its specific manager (see fig 1). For multi-provider support, each Service Provider must have a separate access to the gateway. A Service Provider can typically be a Home Equipment builder, which provides specific services for its devices, or a third party Provider which provides services for a class of devices (for instance all devices related to energy consumption). Data and Service providers are considered separately, so as to enable delegation in the service realization.

Home Gateways have recently evolved from telecommunications network terminals to high-level servers connected to ambient home equipments. They serves at the same time as ingress router to the home network, as a firewall limiting intrusions, as a wireless gateway, and as a server [13]. The first three characteristics relate to classical network level properties. Last facility is becoming more and more central to Home Gateway as proposed services become more complex and personalized.

A prototypical Home Gateway is presented by [11]. It is based on OSGi and uses UPnP technology for service discovery. However those technologies are not mandatory in themselves, they reach an ever broader acceptance in the Home Gateway community, as far as they provide robust tools for supporting identified characteristics. Such an architecture has many advantages over other configurations: it enables the insertion of new Home Equipments (also named Devices, or Terminals) with UPnP, and can support new services and new service providers with OSGi. OSGi also provides service management facilities and the possibility to add and remove software components, and thus services. [19] proposes a similar environment, using the SIP protocol for session management.

A technical solution for enabling multi-provider support is to create Virtual OSGi Gateways [12]. A Virtual Gateway is namely an instance of OSGi platform running inside another OSGi platform, so as to appear to the user (here the Service Manager or Provider) as a full-fledged Gateway. This architecture enables full transparency of access. Dynamic extension of services is realized through installation of components at runtime in Virtual Gateways.

Figure 1 shows the global architecture for service delivery over Home Gateways, with the various elements of the Gateway, Providers, Managers, along with the interactions between them. These interactions are governed by services contracts between the different parties that intervene in Service at Home delivery scenarios.

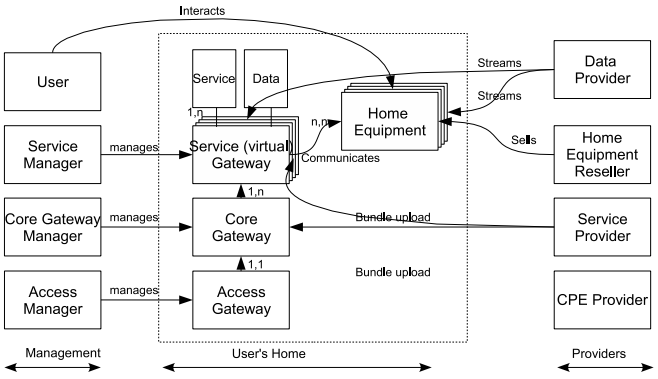

Fig. 1. The Global Architecture for Services at Home Delivery

III. Positive Analysis of the System

The positive analysis of a given system is a systematic view on the actions the system must perform. It makes it possible for the system designers to forbid all actions that does not correspond to identified required operations. The behavior of the system is expressed as scenarios and formalized as UML Sequence Diagrams. Authorized interactions are presented under the form of RBac (Role-Based Access Control) Model, identifying entities and interactions between them. The life cycle of the system must be fully covered, as well as the runtime behavior.

A. Behavior of Home Gateway Systems

Life cycle of Home Gateway systems includes all stages from Internet access subscription to service runtime. Network-level connection follows a well-know process that is nowadays widely commercialized. However, Home Equipments as well as multi-provider support is still realized on ad hoc manners and will require further specifications for providing detailed knowledge and mastered security properties.

Following use scenarios must be defined:

- Access subscription, for Internet broadband access,
- Connection establishment, when the Internet access is established,

- Home equipment buy time, when the user buys a new Home Equipment,
- Home equipment plug time (initial provisioning), when the user plugs its new Home Equipment in its home network,
- Service subscription, for additional services,
- Service use, when the user uses services he has subscribed to.

Available place in this paper do not let us present systematically each of these scenarios. We will therefore give as example a single scenario, initial provisioning, which is central to service delivery in a multi-provider environment. Initial provisioning occurs when the user plugs its newly bought Device in the home network. Suitable services must then be loaded onto the Home Gateway so as to enable proper connection and configuration of the Device, as well as the possibility of subscription to new services.

Figure 2 shows as example the process of initial provisioning for a new Device for Services at Home delivery.

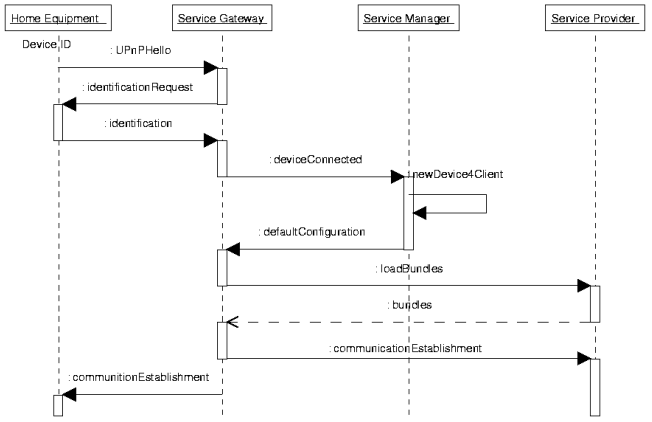

Fig. 2. Initial Provisioning of Services at Home

B. Distributed RBac Model

Classical RBac Model controls access to a given centralized system according to the role that the user plays in this system. In the case of Service at Home delivery, numerous actors intervene in the process (see part II). They are bound together through service contracts, but can not be considered as hierarchically dependent on a single party. Consequently, no unique authorization mechanism is possible. Each of the actors acts for its own benefit, and can not have control rights over other actors that are potentially competitors. The RBac model must therefore be seen as distributed. A global view can be given in order to make service delivery possible, but each part is responsible for ensuring that its partners provide afforded services. Each party is thus responsible for enforcing correct matching between role and authorized actions, as well as to perform authentication of third party entities it communicates to. Consequences of the distributed aspects of this RBac model are not visible at global system design time. Nevertheless, this approach implies that each entity must contain replicated security features, especially authentication facilities and an applicative firewall for ensuring that only authorized users execute actions they are allowed to.

Figure 3 shows the resulting RBac model for Services at Home Delivery.

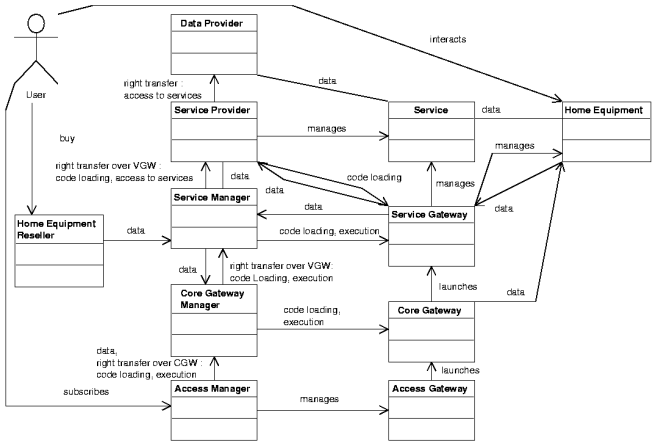

Fig. 3. RBac Model for Services at Home Delivery

Distributed RBac model is derived from scenarios. A global table summarizing all entities and their mutual communications has been established for guaranteeing exhaustivity. In particular, the type of communication (data exchange, management, code loading) are identified. Particular attention is to be paid about interactions inside the Gateway: Access Gateway launches a Core Service Gateway, which launches a set of Service (Virtual) Gateways. Each Service Virtual Gateway may contain services from different providers. The Manager of one of these entities needs to have sufficient access for creating entities of level n+1, but without having runtime access to the created parts. Suitable policies are to be defined to prevent conflicts. Access Rights delegation is managed at the Managers and Providers stack. Again, a careful design is necessary so as to make management and access conflicts impossible.

IV. Preventive Analysis of the System

The preventive analysis of a given system is a systematic view on the attacks that the system is likely to encounter during its lifetime. It requires the identification of both weaknesses inherent to the system and existing risks involved by the users or by the environment. Weaknesses are potential security holes opened in each entity. Risks are made up of various actors or events whose behavior may negatively impact the behavior of the system. Negative impacts can be short or long term unauthorized modifications to the availability of the system, to the identity of actors, to confidentiality or to integrity. They are often implied by malicious actions, but can also originate in accidental events.

Weaknesses and risks can be expressed as attack trees, which represent various attack possibilities for a set of attack classes. An attack class is a particular set of attacks that all intend to make similar damages to the system, but using different strategies.

A. Weaknesses and risks

Weaknesses of the system are derived from the characteristics of the entities, and from existing interactions defined in the scenarios we introduced. The main weakness in identified scenarios is the possibility of impersonation - that is to say the theft of identity - of the different Managers and Providers, all the more as they may be numerous. A weakness specific to the Home Gateways is the possible management of Service Virtual Gateways by its creator, and not restricted to official Service Providers. Other kinds of elevation of privileges are also to be prevented: Service Managers, Service Providers and Data Managers should not have more rights than intended. Managers of the entities have also strong rights over the system. They should not be allowed to take initiatives that go against the system guidelines. Lastly, Service at Home should be 'user proof', that is to say that deliberate or accidental manipulation should not bring the system in an insecure state.

Generic existing risks have already been identified in the definition of the analysis method. It consists mainly in the STRIDE model attacks (spoofing, tampering, repudiation, information disclosure, denial of services and elevation of privileges) [7]. Additional risks exist, that can potentially damage the system or make it unavailable: electrical shutdown, issue of illegal requests through authorized entities, third party as single point of failure. Moreover, data protection needs to be suitable according to data sensitivity. For instance, a clear separation between different communication channels can prevent unauthorized access to private data. Three of these communication channels can be identified: streaming channels for multimedia services, basic data and services channels for services that require message-based communications, and management channels for supporting insertion of new equipments and services.

The combination of weaknesses and risks enables to visualize possible attacks, by determining the weaknesses that are exploited to achieve a given attack type. Attack trees represent this approach in a systematic way.

B. Attack Trees

Protecting a system makes necessary to have a deep knowledge over potential attacks. Attack trees make it possible to summarize in an intuitive way all identified attacks that can be used in order to harm the system in a certain way. Technical characteristics of the attack as well as concerned assets are detailed. All these elements make possible to determine security requirements for the system that is being analyzed, and to choose security objectives according to the assurance requirements.

Identified attack trees for Service at Home delivery systems based on Home Gateway are closely related to attack classes identified in [7]. They are namely:

- malicious code execution (cracking and phreaking),
- use of services without proper billing (phreaking),
- malicious actions related to management (cracking),
- denial of service (DoS).

Available place does not allow us to present each attack tree in a detailed manner. Rather, we will present those that are specific to the environments of Service at Home delivery. The main risk, as in every payed-for system, is that services are used without proper billing. The second important risk is the execution of malicious code. It is specific to platforms supporting dynamic extension through code loading, and is still poorly studied in spite of important impact on every component-based architectures and even application deployment environments.

Figure 4 shows the attack tree for use of services without proper billing. Two strategies can be taken: code theft, without direct service use, and unauthorized service use. Code theft can occur through eavesdropping on the bundle during its loading onto a Service Gateway. It can also be done by a regular platform if this latter can load code bundles without registering to matching services. Access to services without registration can be achieved through classical identity theft, through the creation of fake registration proof (in case that the system is based on a Mandatory Access Control, that is to say the user of a service has to prove he has the rights to access this service), through server corruption, or through eavesdropping on service content delivery (for instance on a stream used to transfer a video to the home of another user).

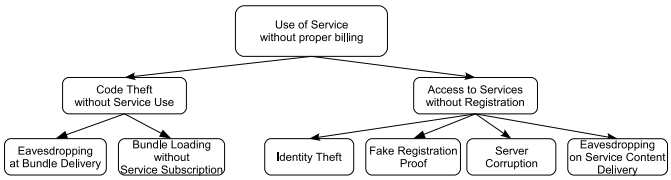

Fig. 4. The Attack Tree for service use without proper billing

Figure 5 shows the attack tree for malicious code execution. The two main strategies are to force the platform to misbehave, or to force the loaded services to misbehave. The platform is the execution environment of the services. In our study, the platform is OSGi. Its misbehavior is not specific to Service at Home or component-based environments. It can be realized through diffusion of bugged or malicious original code, or by substitution of platform code during deployment. Misbehavior of services can be achieved by insertion of misbehaving code at the publisher's, substitution of code in the bundle repository, or upload of unauthorized services directly on the platform. We invite the reader to refer to the diagram for further precisions.

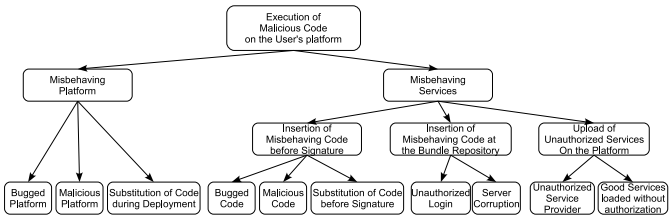

Fig. 5. The Attack Tree for malicious Code Execution

This analysis of multi-provider Service at Home delivery systems provide system designers with necessary informations about potential attacks their system may suffer from. This analysis makes it possible to take suitable security measures by inserting suitable functionalities in the system. The possibility also exists to extend these attack trees to cope with particular

configurations and/or environments. They can also be used as a firm basis for establishing assurance evaluation, for instance in conformance with Common Criteria process.

V. SFelix: A Secure Implementation of OSGi

A. First Protection Strategies

In building our own Home Gateway system prototype, following security features have been elected as being the more urgent ones. First, secure communications are required as in every multi-party system that communicates over a public network such as the Internet. The second measure is the validation of software bundles at install time, in order to ensure authentication of the issuer and their integrity.

B. Implementation

In order to provide a secure Home Gateway, we are working on a secure version of Apache Felix OSGi implementation. First step (aside from providing secure communication channels that are widely available technologies) is to support bundle validation. Current OSGi specifications only propose to sign bundles. This approach has two major limitations: potential performance losses when compared to secured communication channels, and no confidentiality in bundle loading. Moreover, current state of various Open Source OSGi implementations such as Felix or Knopflerfish do not provide such facilities. We therefore implement SFelix (http://sfelix.gforge.inria.fr/), that supports bundle verification on the client at install time. Moreover, we developed JarSigner, a tool for signing bundles. Signed archives include a specific file that follow IETF RFC 3369 CMS proposed standard. This format could also be used in the future to include encrypted content in the signature. However, one needs to be conscious that encryption requires that the OSGi platform loading the bundle is able to decrypt it. That is to say this mechanism would break existing transparency of bundle validation through signature: security unaware system can use them as well as security-aware ones.

Figure 6 (A) shows the process of signed bundle deployment that is supported by SFelix and the JarSigner tool. Bundles are signed by their issuer. Bundle loading from client side is based on existing OBR (OSGi Bundle Repository). After loading them, and before installation, the validity of bundle signature is checked, and bundles are decrypted if relevant.

Figure 6 (B) shows the process of deploying signed bundles through a secure communication channel, here SSH. This is an alternative to the mechanism of deployment proposed by OSGi specification. It has the drawback not to support security unaware clients, but brings with it several advantages. It guarantees the confidentiality of the component transfer over the network, which can be required in many commercial system whose managers do not want to offer the code. Moreover, it is very probable that communication over SSH proposes performances that are far better than OSGi bundle validation.

VI. Related Works

Not surprisingly due to the importance of the topic, several works have been done that foster the development of secure and dependable (that is to say secure and fault-resilient) Services at Home delivery system. However, existing analyses either target dependability, or provide protection profiles for prototypical Gateways without releasing the information necessary to re-use them. Moreover, most works in the field of security for Home Gateway systems provide useful tools, but without giving an associated global view.

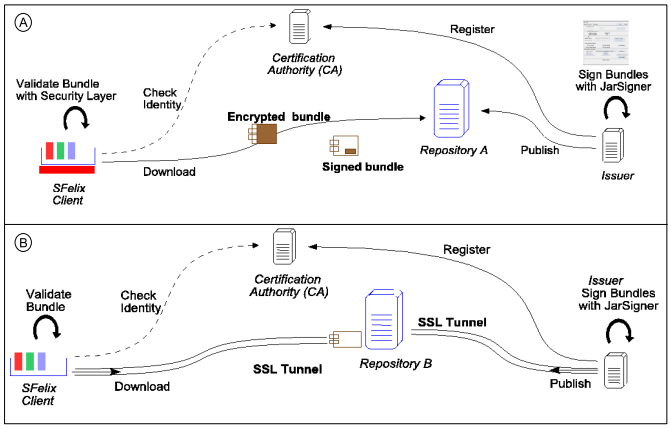

Fig. 6. Bundle Signing to Bundle Validation: Process supported by SFelix, and SSH Extension

A. Security Analyses of Home Gateway Systems

Several works aim at establishing a systematic analysis of the dependability properties of Services at Home and Home Gateway systems. They can be considered parallel to our work. However, they focus towards fault resilience rather that toward malicious behavior of internal or external actors.

A systematic analysis of the dependability of home automation system is provided by [5]. It is based on fault trees, and aims at identifying consequences of malfunctions with regard to the user's trust in the system. Analysis is done through a single monitoring tool, that already includes basic security features, and could easily be extended to monitor sensitive security elements. However, its goal is slightly different from ours: we intend to propose a design methodology, when this work provides a runtime tool that could be used with great benefit by the Service Providers. While similar in spirit and in method, both analyses have different targets, and thus different applications.

Analysis in [18] is based on an architecture that is very similar to ours, with Home Gateway and devices connected to it. It proposes a heart-beat mechanism for ensuring the continuity of the activity of the device. Particularity of this work is to use powerline to support the home network.

[16] provides an extensive analysis of security problems in Home Gateways. It has been realized in the frame of the E-Pasta IST project, and is based on Common Criteria (CC). Its goal is to specify CC protection profiles for the Home Gateway in different use contexts: dynamic service discovery, identification of right level of security, open platform. It is based on a trust value chain of providers. This work proposes a specification for secure Home Gateway system, but do not provides enough information so as to let designers adapt it to their own systems.

B. Existing Solutions

Several implementations of secure Home Gateways or secure functionalities for Services at Home delivery systems have been proposed.

A full Gateway specification along with several necessary facilities is proposed by the Theaha project [15]. The security in Theaha is obtained from conjunction of secure communication and of secure components. Secure components provide several functions. The first of these functions is a security manager that supports secure service discovery and business policies enforcement. The second element contains a module for secure storage of data, code and configuration, as well as a cryptographic engine. The work is limited to the specification of the Home Gateway, and do not consider in detail its interactions with the rest of the system.

Tools for supporting secure Service and Devices discovery are provided by the Universal Plug and Play (UPnP) protocol. Detailed study of security in UPnP is proposed by [9].

Once a service has been identified and found, it can be useful to protect it from third parties, including actors of the Services at Home system. [17] has built a prototype for a secure broker that protect messages exchanged between the client and the service from every potential intruder. [4] gives performances of this system and compares it to insecure communications. Use of dedicated per-message encryption proves to have significantly lower performances than the use of SSL. This shows than security solutions should use existing security tools as soon as possible. This is all the more true as ad-hoc solutions are more likely to have security flaws.

Ranging from dependability analysis to Gateway specification to service discovery and use, existing works cover a wide part of problems designers can meet while building a new Home Gateway based system. However, this short survey also highlights the need for an analysis specifically targeted at security of multi-provider Home Gateway systems, that seems not to be yet available, and that we propose in this work.

VII. Conclusions and Future Works

Wide dissemination of Service at Home systems makes mandatory for designers to have an extensive knowledge of the characteristics of Home Gateways. In particular, security features are central to successful services, because they guarantee a high quality of service from the point of view of the user and ensure providers that they will get paid for the service they make available.

Proposed security analysis of Service at Home systems provides system designers and researchers that work over Home Gateway with precise knowledge about the positive characteristics of such system - what do my Gateway and associated providers must do - but also with a detailed preventive view - for each identified attack class, what are the potential attacks a malicious person can realize ? Moreover, by providing an intuitive method along with the results of the analysis, we enable everyone to take advantage of the result and to adapt them to their specific configuration. Strong integration of concepts coming from widely used methods allows to use these methods in conjunction with our methodology, for instance to define a Common Criteria assurance evaluation.

Based on the results of our study, we are developing a prototype for a secure Home Gateway system. This tool suite includes a modified version of Felix OSGi that supports the validation of integrity of the code bundles and the authentication of the issuer, as well as JarSigner for signing bundles.

Additional work is to be realized in order to provide a full-fledged infrastructure for supporting secure Service at Home delivery. Policies need to be defined for a proper key management mechanism, and for making it possible to enforce identified Role-based Access model is required. A specific security analysis of the Java/OSGi execution platform at the software level that takes into account language and platform characteristics will complete this work.

References

[1] Digital Living Network Alliance. Dlna overview and vision whitepaper 2006. DLNA Whitepaper, 2006.

[2] Echonet Consortium. Echonet specifications, version 2.11. http://www.echonet.gr.jp/english/8_kikaku/index.htm.

[3] D. Ferraiolo and R. Kuhn. Role-based access controls. In *15th NIST-NCSC National Computer Security Conference*, pages 554–563, 1992.

[4] W. Haerick and S. Van Hoecke. Secure brokering of web services. In *5th FTW PhD Symposium, Ghent, Belgium*, December 2004.

[5] A. Herzog and N. Shahmehri. Towards secure e-services: Risk analysis of a home automation service. In *6th Nordic Workshop on Secure IT-Systems (Nordsec)*, pages 18–26, November 2001.

[6] HGI. Home gateway initiative, vision and whitepaper, 2005.

[7] M. Howard and D. LeBlanc. *Writing Secure Code*. Microsoft Press, 2001.

[8] International Standard Organization. Common criteria. International Standard ISO 15408, 1999.

[9] M. D'Hooge (Trialog). Report on a secure home network architecture and related protection profiles specification. Deliverable DA.3.7, IST-MediaNet Project, February 2006.

[10] Muse Consortium. Muse project presentation. Muse Public Deliverable D A0.1, July 2004.

[11] Muse Consortium. Detailed description of residential gateway and advanced features. Muse Public Deliverables D TF3.2, December 2005.

[12] Y. Royon, S. Frenot, and F. LeMouel. Virtualization of service gateways in multi-provider environment. In *Component Based Software Engineering*, 2006.

[13] T. Saito, I. Tomoda, Y. Takabatake, K. Teramoto, and K. Fujimoto. Gateway technologies for home network and their implementations. In *IEEE Distributed Computing Systems Workshop,*, pages 175–180, April 2001.

[14] Secretariat general de la defense nationale, DCSSI. Expression of needs and identification of security objectives, February 2004.

[15] Theaha Project. Towards secure, zero-configuration seamless interworking - architecture overview. Project IST-2004-507-029 Whitepaper, November 2005.

[16] Trialog. e-protection of appliances through secure and trusted access. E-Pasta IST Project Final Report 2000-26086, December 2002.

[17] S. Van Hoecke, W. Haerick, G. D. Jans, F. D. Turck, E. Laermans, B. Dhoedt, and P. Demeester. Design and implementation of a secure media content delivery broker architecture. In *The 2005 International Symposium on Web Services and Applications (ISWS'05) in Las Vegas, USA*, 2005.

[18] Y.-M. Wang, W. Russell, A. Arora, J. Xu, and R. K. Jagannathan. Towards dependable home networking: An experience report. In *International Conference on Dependable Systems and Networks (DSN 2000)*, pages 43–48, 2000.

[19] D. Zhang, H. Lee, X. Ni, and S. Zheng. Open service residential gateway for smart homes. In *ISCE*, December 2003.