INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Madynes

Management of Dynamic Networks and Services

Nancy - Grand Est

Theme : Networks and Telecommunications

Table of contents

1. Team **1**
2. Overall Objectives **1**
2.1. Introduction 1
2.2. Highlights of the year 2
3. Scientific Foundations **2**
3.1. Evolutionary needs in network and service management 2
3.2. Autonomous management 3
3.2.1. Models and methods for a self-management plane 3
3.2.2. Design and evaluation of P2P-based management architectures 3
3.2.3. Integration of management information 4
3.2.4. Modeling and benchmarking of management infrastructures and activities 4
3.3. Functional areas 4
3.3.1. Security management 4
3.3.2. Configuration: automation of service configuration and provisioning 5
3.3.3. Performance and availability monitoring 5
4. Application Domains **6**
4.1. Mobile, ad-hoc and constrained networks 6
4.2. Dynamic service infrastructures 6
5. Software **6**
5.1. KiF 6
5.2. Voip bots 7
5.3. SecSIP 7
5.4. NDPMon 8
6. New Results **8**
6.1. Protocol fuzzing 8
6.2. Fingerprinting 9
6.3. Vulnerabilities preventions techniques in SIP networks 9
6.4. Risk management 10
6.5. Monitoring of MESH networks 10
6.6. Pervasive computing 11
6.7. Voice over IP monitoring 12
6.8. Monitoring content cccess in peer-to-peer networks 13
6.9. IPv6 transition 14
7. Contracts and Grants with Industry **15**
7.1. VAMPIRE 15
7.2. EMANICS 15
7.3. INRIA-ALU joint lab 16
7.4. AIRNET 16
7.5. SARAH 17
7.6. MAPE 17
7.7. CISCO CARD 18
7.8. FIREFLIES RTLS 18
8. Other Grants and Activities **18**
8.1. International relationships and cooperations 18
8.2. National initiatives 19
8.3. Mobility 19
9. Dissemination **19**
9.1. Program committees and conference organization 19
9.2. Teaching 19

9.3. Tutorials, invited talks, panels, presentations 20
9.4. Commissions 20
10. Bibliography **21**

MADYNES is a project group of the LORIA (UMR 7503) laboratory, joint lab of CNRS, INRIA, Henri Poincaré University - Nancy 1, Nancy 2 University and the Lorraine National Polytechnic Institute (INPL).

This report covers the group activity and publications from January, 1st 2009 to December 31th, 2009.

1. Team

Research Scientist

Olivier Festor [Team Leader, Research Director (DR), INRIA, HdR]

Faculty Member

Isabelle Chrisment [Professor, ESIAL, Henri Poincaré - Nancy 1 University, HdR]
Laurent Andrey [Associate Professor, Nancy 2 University]
Rémi Badonnel [Associate Professor, ESIAL, Henri Poincaré - Nancy 1 University]
Laurent Ciarletta [Associate Professor, ENSMN - Lorraine National Polytechnic Institute]
Abelkader Lahmadi [Associate Professor, ENSEM - Lorraine National Polytechnic Institute (10/2009-)]
Emmanuel Nataf [Associate Professor, Nancy 2 University]
André Schaff [Professor[1], ESIAL,Henri Poincaré - Nancy 1 University, HdR]

Technical Staff

Frédéric Beck [Engineer, Industrial grant]
Mohamed Nassar [Research Engineer, Industrial grant]
Humberto Jorge Abdelnur [Research Engineer, Industrial grant]

PhD Student

Jérôme François [CNRS BDI grant with regional co-sponsorship (10/2006-)]
Cristian Popi [Industrial grant with regional co-sponsorship (10/2006-)]
Thibault Cholez [Industrial grant with regional co-sponsoship (10/2007-)]
Julien Siebert [MADYNES-MAIA cooperation. Industrial grant with regional co-sponsoship (10/2007-)]
Tom Leclerc [Industrial grant with regional co-sponsoship (10/2007-)]
Gérard Wagener [Co-tutelle with University of Luxembourg (10/2007-)]

Administrative Assistant

Christelle Wagner [Project Assistant, INRIA (-10/2009)]

Other

Oussema Dabbebi [Ms Degree Internship, (02/2009-07/2009)]
Laurent Debricon [Ms Degree Internship, Nancy University (02/2009-07/2009)]
Jorge Lucangeli Obes [Ms Degree Internship, University of Buenos Aires, Argentina (02/2009-07/2009)]
Juan Pablo Timpanaro [Ms Degree Internship, (02/2009-07/2009)]
Thomas Buehring [Bachelor, University of Federal Armed Forces, Munich Germany (02/2009-07/2009)]

2. Overall Objectives

2.1. Introduction

The goal of the MADYNES research group is to design, to validate and to deploy novel management and security paradigms together with supporting software architectures and solutions that are able to cope with the growing dynamicity and the scalability issues induced by the ubiquitous Internet.

[1] Due to its administrative duties at the University, André Schaff could not contribute to the activity of the team in 2009

The project develops applied research activities in the following areas :

- **Autonomous Management**:
  - the design of models and methods enabling **self organization and self-management** of networked entities and services,
  - the evaluation of management architectures based on **peer-to-peer and overlay principles**,
  - the investigation of novel approaches to the representation of **management information**,
  - the modeling and **performance evaluation** of management infrastructures and activities.
- **Functional Areas** instanciate autonomous management functions :
  - the **security plane** where we focus on buidling closed-loop approaches to protect networking assets,
  - the **service configuration** where we aim at providing solutions covering the delivery chain from discovery to delivery in dynamic networks,
  - **monitoring** where we aim at building solutions to characterize and detect unwanted service behaviour.

The next generation Internet is the main application field of our research. Its architecture and the services that it is planned to support offer all dynamic and scalability features that we address in the complementary research directions of the project.

2.2. Highlights of the year

The first highlights of the year were the three Ph.D. defenses within the team (Humberto Abdelnur, Jérôme François) and Mohamed Nassar) and the Habilitation Degree diploma of our former team member Radu State.

2009 has also seen three scientific highlights in our contributions to the security of Voice over IP systems. There the first highlight is the design and implementation of a novel protection approach against known vulnerabilities. This approach includes a protection policy specification language called VeTo and an execution engine entitled SecSIP. We also publicly released our first Android SPIT protection application entitled Hinky. The second highlight is the novel backtrace model we did integrate in our fuzzing scheme. This has brough excellent feedback and helps improved fuzzing selection and fuzzers evalution.

A third highlight of 2009 is the outstanding evaluation received for its third year activity by the EMANICS network of excellence from the European Commission. Like in 2008, the project that we manage received the highest mark a project can get out of a review. We also received the best paper award at AIMS for our contribution on flow monitoring schemes in wireless MESH networks.

3. Scientific Foundations

3.1. Evolutionary needs in network and service management

The foundation of the MADYNES research activity is the ever increasing need for automated monitoring and control within networked environments. This need is mainly due to the increasing dependency of both people and goods towards communication infrastructures as well as the growing demand towards services of higher quality. Because of its strategic importance and crucial requirements for interoperability, the management models were constructed in the context of strong standardization activities by many different organizations over the last 15 years. This has led to the design of most of the paradigms used in today's deployed approaches. These paradigms are the Manager/Agent interaction model, the Information Model paradigm and its container, together with a naming infrastructure called the Management Information Base. In addition to this structure, five functional areas known under the FCAPS[2] acronym are associated to these standards.

[2]Fault, Configuration, Accounting, Performance and Security

While these models were well suited for the specific application domains for which they were designed (telecommunication networks or dedicated protocol stacks), they all show the same limits. Especially they are unable:

1. to deal with any form of dynamicity in the managed environment,
2. to master the complexity, the operating mode and the heterogeneity of the emerging services,
3. to scale to new networks and service environments.

These three limits are observed in all five functional areas of the management domain (fault, configuration, accounting, performance and security) and represent the major challenges when it comes to enable effective automated management and control of devices, networks and services in the next decade.

MADYNES addresses these challenges by focusing on the design of management models that rely on inherently dynamic and evolving environments. The project is centered around two core activities. These activities are, as mentioned in the previous section, the design of an autonomous management framework and its application to three of the standard functional areas namely security, configuration and performance.

3.2. Autonomous management

3.2.1. Models and methods for a self-management plane

Self organization and automation are fundamental requirements within the management plane in today's dynamic environments. It is necessary to automate the management processes and enable management frameworks to operate in time sensitive evolving networks and service environments. The automation of the organization of devices, software components, networks and services is investigated in many research projects and has already led to several solution proposals. While these proposals are successful at several layers, like IP auto-configuration or service discovery and binding facilities, they did not enhance the management plane at all. For example, while self-configuration of IP devices is commonplace, no solution exists that provides strong support to the management plane to configure itself (e.g. finding the manager to which an agent has to send traps or organizing the access control based on locality or any other context information). So, this area represents a major challenge in extending current management approaches so that they become self-organized.

Our approach is bottom-up and consists in identifying those parameters and framework elements (manager data, information model sharing, agent parameters, protocol settings, ...) that need dynamic configuration and self-organization (like the address of a trap sink). For these parameters and their instantiation in various management frameworks (SNMP, Netconf, WBEM, ...), we investigate and elaborate novel approaches enabling fully automated setup and operation in the management plane.

3.2.2. Design and evaluation of P2P-based management architectures

Over the last years, several models have emerged and gained wide acceptance in the networking and service world. Among them, the overlay networks together with the P2P paradigms appear to be very promising. Since they rely mainly on fully decentralized models, they offer excellent fault tolerance and have a real potential to achieve high scalability. Mainly deployed in the content delivery and the cooperation and distributed computation disciplines, they seem to offer all features required by a management framework that needs to operate in a dynamic world. This potential however needs an in depth investigation because these models have also many characteristics that are unusual in management (e.g. a fast and uncontrolled evolution of the topology or the existence of a distributed trust relationship framework rather than a standard centralized security framework).

Our approach envisions how a complete redesign of a management framework is done given the characteristics of the underlying P2P and overlay services. Among the topics of interest we study the concept of management information and operations routing within a management overlay as well as the distribution of management functions in a multi-manager/agent P2P environment. The functional areas targeted in our approach by the P2P model are network and service configuration and distributed monitoring. The models are to be evaluated against highly dynamic frameworks such as ad-hoc environments (network or application level) and mobile devices.

3.2.3. Integration of management information

Representation, specification and integration of management information models form a foundation for network and service management and remains an open research domain. The design and specification of new models is mainly driven by the appearance of new protocols, services and usage patterns. These need to be managed and exposed through well designed management information models. Integration activities are driven by the multiplication of various management approaches. To enable automated management, these approaches need to inter-operate which is not the case today.

The MADYNES approach to this problem of modelling and representation of management information aims at:

1. enabling application developers to establish their management interface in the same workspace, with the same notations and concepts as the ones used to develop their application,
2. fostering the use of standard models (at least the structure and semantics of well defined models),
3. designing a naming structure that allows the routing of management information in an overlay management plane, and
4. evaluating new approaches for management information integration especially based on management ontologies and semantic information models.

3.2.4. Modeling and benchmarking of management infrastructures and activities

The impact of a management approach on the efficiency of the managed service is highly dependent on three factors:

- the distribution of the considered service and their associated management tasks,
- the management patterns used (e.g. monitoring frequency, granularity of the management information considered),
- the cost in terms of resources these considered functions have on the managed element (e.g. method call overhead, management memory footprint).

While the first factor was investigated in several research projects so far, none of the other two were investigated at all. The lack of such benchmarking data and models simply makes the objective evaluation of the operational costs of a management approach impossible. This may be acceptable in backbone networks where processing and communication resources can be tuned very easily (albeit sometimes at a non negligible cost). This is not true in constrained environments like devices constrained by battery or processing power as found in wireless networks for which the lack of management cost models is a serious concern.

MADYNES addresses this problem from multiple viewpoints: communication patterns, processing and memory resources consumption. Our goal is to provide management patterns combining several management technologies if needed so as to optimize the resources consumed by the management activity imposed by the operating environment.

Therefore, we establish *abacuses* for management frameworks and in parallel we collect data on current management practice. These data will form the core of the "Constraints-based management tuning activity" that we are working on and can be used for rigorous comparison among distribution and processing of management activities.

3.3. Functional areas

3.3.1. Security management

Securing the management plane is vital. While several proposals are already integrated in the existing management frameworks, they are rarely used. This is due to the fact that these approaches are completely detached from the enterprise security framework. As a consequence, the management framework is "managed" separately with different models; this represents a huge overhead. Moreover the current approaches to security in the management plane are not inter-operable at all, multiplying the operational costs in a heterogeneous management framework.

The primary goal of the research in this activity is the design and the validation of a security framework for the management plane that will be open and capable to integrate the security services provided in today's management architectures. Management security interoperability is of major importance in this activity.

Our activity in this area aims at designing a generic security model in the context of multi-party / multi-technology management interactions. Therefore, we develop research on the following directions:

1. Abstraction of the various access control mechanisms that exist in today's management frameworks. We are particularly interested in extending these models so that they support event-driven management, which is not the case for most of them today.
2. Extension of policy and trust models to ease and to ensure coordination among managers towards one agent or a subset of the management tree. Provisional policies are of great interest to us in this context.
3. Evaluation of the adequacy of key distribution architectures to the needs of the management plane as well as selecting reputation models to be used in the management of highly dynamic environments (e.g. multicast groups, ad-hoc networks).

A strong requirement towards the future generic model is that it needs to be instantiated (with potential restrictions) into standard management platforms like SNMP, WBEM or Netconf and to allow interoperability in environments where these approaches coexist and even cooperate. A typical example of this is the security of an integration agent which is located in two management worlds.

Since 2006 we have also started an activity on security assessment. The objective is to investigate new methods and models for validating the security of large scale dynamic networks and services. The first targeted service is VoIP.

3.3.2. Configuration: automation of service configuration and provisioning

Configuration covers many processes which are all important to enable dynamic networks. Within our research activity, we focus on the operation of tuning the parameters of a service in an automated way. This is done together with the activation topics of configuration management and the monitoring information collected from the underlying infrastructure. Some approaches exist today to automate part of the configuration process (download of a configuration file at boot time within a router, on demand code deployment in service platforms). While these approaches are interesting they all suffer from the same limits, namely:

1. they rely on specific service life cycle models,
2. they use proprietary interfaces and protocols.

These two basic limits have high impacts on service dynamics in a heterogeneous environment.

We follow two research directions in the topic of configuration management. The first one aims at establishing an abstract life-cycle model for either a service, a device or a network configuration and to associate with this model a generic command and programming interface. This is done in a way similar to what is proposed in the area of call control in initiatives such as Parlay or OSA.

In addition to the investigation of the life-cycle model, we work on technology support for distributing and exchanging configuration management information. Especially, we investigate policy-driven approaches for representing configurations and constraints while we study XML-based protocols for coordinating distribution and synchronization. Off and online validation of configuration data is also part of this effort.

3.3.3. Performance and availability monitoring

Performance management is one of the most important and deployed management function. It is crucial for any service which is bound to an agreement about the expected delivery level. Performance management needs models, metrics, associated instrumentation, data collection and aggregation infrastructures and advanced data analysis algorithms.

Today, a programmable approach for end-to-end service performance measurement in a client server environment exists. This approach, called Application Response Measurement (ARM) defines a model including an abstract definition of a unit of work and related performance records; it offers an API to application developers which allows easy integration of measurement within their distributed application. While this approach is interesting, it is only a first step toward the automation of performance management.

We are investigating two specific aspects. First we are working on the coupling and possible automation of performance measurement models with the upper service level agreement and specification levels. Second we are working on the mapping of these high level requirements to the lower level of instrumentation and actual data collection processes available in the network. More specifically we are interested in providing automated mapping of service level parameters to monitoring and measurement capabilities. We also envision automated deployment and/or activation of performance measurement sensors based on the mapped parameters. This activity also incorporates self-instrumentation (and when possible on the fly instrumentation) of software components for performance monitoring purpose.

4. Application Domains

4.1. Mobile, ad-hoc and constrained networks

The results coming out from MADYNES can be applied to any dynamic infrastructure that contributes to the delivery of value added services. While this is a potentially huge application domain, we focus on the following environments at the network level:

1. multicast services,
2. ad-hoc networks,
3. mobile devices and IPv6 networks,
4. voice over IP infrastructure.

All these selected application areas exhibit different dynamicity features. In the context of multicast services, we focus on distribution, monitoring and accounting of key distribution protocols. On *ad -hoc* and dynamic networks we are investigating the provisioning, monitoring, configuration and performance management issues.

Concerning mobile devices, we are interested in their configuration, provisioning and monitoring. IPv6 work goes on in Information Models and, combined with SNMPv3, on self-configuration of the agents.

4.2. Dynamic service infrastructures

At the service level, dynamics is also increasing very fast. We apply the results of our work on autonomous management on infrastructures which support dynamic composition and for which self-instrumentation and management automation is required.

The target service environments are:

- Voice over IP networks,
- peer-to-peer infrastructures,
- ambiant environments.

5. Software

5.1. KiF

Participants: Humberto Abdelnur [contact], Olivier Festor, Radu State.

KiF is an advance protocol fuzzer developed by the team. The tool builds on novel algorithms to make stateful, in depth fuzzing of remote devices. In its current version, it offers stateful fuzzing for Voice Over IP systems using the SIP signalling protocol. It offers smart fuzzing using either on the fly data generation or using pre-generated test suites to enable performant fuzzed messages issuance. The environment also enables easy specification, addition and execution of new fuzzing scenarios.

The tool is entirely developed in Python and is freely available to third party users. The current distribution is provided as a fully pre-installed and running framework packaged in a VMware image.

Although being distributed under an Open Source model, availability requires prior signature of a non-disclosure agreement to prevent its usage in malicious activities like the attack of operational third party voice over IP infrastructures. As of today, a dozen companies and universities signed the NDA and are actively using the KiF framework. More details on KIF can be found on the environment's web site[3].

5.2. Voip bots

Participants: Mohamed Nassar [contact], Olivier Festor, Radu State.

VoIP bot is a VoIP security tool created as a demonstrator of how attacks can be launched against VoIP/SIP services and users in a remotely and distributed manner. The environment contains bots that can be remotely managed over an Internet Relay Chat (IRC) channel from a cental manager. Our bots are currently able to perform the following tasks :

- send SPAM over IP Telephony (SPIT),
- distributed denial of service through intensive generation of invite messages to a target device,
- active scanning of users through incremental options messages issuance to servers and response analysis,
- cracking through brute-force testing of passwords against an identified user account,
- simple device scanning and fingerprinting,
- target aware device fuzzing.

The tool is developed using the Java programming language. It uses the JAIN-SIP, JMF and PIRCBOT libraries. The tool is distributed under a GPL2 Open Source license. Reports show its use mainly in the testing business so far.

5.3. SecSIP

Participants: Abdelkader Lahmadi [contact], Olivier Festor.

SecSip [20] is developed by the team to defend SIP-based (The Session Initiation Protocol) services from known vulnerabilities. It presents a proactive point of defense between a SIP-based network of devices (servers, proxies, user agents) and the open Internet. Therefore, all SIP traffic is inspected and analyzed against authored Veto specification before it is forwarded to these devices. When initializing, the SecSIP runtime starts loading and parsing authored VeTo blocks to identify different variables, event patterns, operations and actions from each rule. It implements an input and output layer, to capture, inject, send and receive SIP packets from and to the network. Intercepted packets are moved to the SIP Packet parser module. The main function of this module is to extract different fields within a SIP message and trigger events specified within the definition blocks. During each execution cycle when a SIP message arrives, the SecSIP runtime uses a data flow acyclic graph network to find definition matching rules and triggers defined events.

The paired events in each operator node are propagated over the graph until a pattern is satisfied. When the pattern is satisfied, the respective rule is fired and the set of actions is executed. More details on SecSIP can be found on the web site of the tool[4].

[3] http://kif.gforge.inria.fr
[4] http://secsip.gforge.inria.fr

5.4. NDPMon

Participants: Frédéric Beck [contact], Isabelle Chrisment, Olivier Festor, Thomas Buehring, Thibault Cholez.

The Neighbor Discovery Protocol Monitor (NDPMon) is an IPv6 implemention of the well-known ArpWatch tool. NDPMon monitors the pairing between IPv6 and Ethernet addresses (NDP activities: new station, changed Ethernet address, flip flop...). NDPMon also detects attacks on the NDP protocol, as defined in RFC 3756 (bogon, fake Router Advertisements...). New attacks based on the Neighbor Discovery Protocol and Address Autoconfiguration (RFC 2461 and RFC 2462) have been identified and integrated in the tool. An XML file describes the default behavior of the network, with the authorized routers and prefixes, and a second XML document containing the neighbors database is used. This second file can be filled during a learning phase. All NDP activities are logged in the syslog utility, and so the attacks, but these ones are also reported by mail to the administrator. Finally, NDPMon can detect stack vulnerabilities, like the assignment of an Ethernet broadcast address on an interface.

NDPMon comes along with a WEB interface acting as a GUI to display the informations gathered by the tool, and give an overview of all alerts and reports. Thanks to color codes, the WEB interface makes possible for the administrator to have an history of what happenned on his network and identify quickly problems. All the XML files used or produced by the daemon (neighbor cache, configuration file and alerts list) are translated in HTML via XSL for better readability. A statistic module is also integrated and gives informations about the discovery of the nodes and their type (MAC manufacturer repartition...).

The software package and its source code is freely distributed under an opensource license (LGPL). It is implemented in C, and is available through a SourceForge project at http://ndpmon.sf.net. An opensource community is now established for the tool which has distributions for several Operating Systems (Linux, FreeBSD, OpenBSD, NetBSD and Mac OS X). It is also integrated in FreeBSD ports at http://www.freebsd.org/cgi/cvsweb.cgi/ports/net-mgmt/ndpmon/. Binary distribution is also available for ..deb and .rpm based Linux distributions.

Developments continue in the team on the software so as to (1) increase the robustness of the environment and (2) add support for the detection of new attacks.

6. New Results

6.1. Protocol fuzzing

Participants: Humberto Abdelnur [contact], Olivier Festor.

Fuzz testing is an abnormal testing technique which focuses in finding unexpected behavior (vulnerable code) rather than checking the functional behavior of the equipment under test. The main problem encountered in the software testing area, is in fact, the quantity of tests required to build in order to completely enssure the quality of a piece of code. This year, we circumvented this problem by building a dynamic monitor capable of recollect information from the tested equipment, called mtrace. Mtrace is a tracer that can be used to follow the system and dynamic library calls made by a program. Using this information, mtrace can follow from the received data (e.g from the network sockets or files) the tainted data propagation and therefore build the tainted data tree associated to the input execution. Thus, for each of the messages generated by our fuzzer, the tracer immediately transmit back the tainted data information. This tainted information allows us to identify the traces of the program executed. Thus, we build a platform for comparing how different fuzzing strategies work (therefore, comparing how the impact of different fuzzer frameworks are), identify the code coverage exposed by each technique and finally, define stopping criteria when no new code is been tested. In a second phase, we also make the link between tainted data and the syntax tree build by our initial fuzzer. The syntax tree is a tree representation of the input data based on the grammar of the protocol. Since each syntax node contains full specification of the composition for the fields, we are able to generate malicious data only in fields known to be used in the execution at the target program. Concluding, this close-loop technique reported a higher code execution coverage with a higher impact in a considerable lower set of malicious inputs.

We also submitted a draft to the IETF SIPPING group describing one standard vulnerability together with a solution to avoid it.

6.2. Fingerprinting

Participants: Olivier Festor [contact], Humberto Abdelnur, Jérôme François.

The goal of this work is to propose new methods to identify automatically the type of a device (hardware or software). This challenging task is related to network management as it can help to build an inventory of the different active devices. Besides, security domain is also covered by device fingerprinting as for instance to detect potential victims of a new attacks, in order to rapidly provide them a patch, or to track abnormal devices like attackers. In this way, a reinforced authentication mechanism can be based on fingerprinting to identify the devices.

The first method we propose aims to infer the type of a device without strong knowledge about the employed protocol by only considering the types of the exchanged messages. Hence, a first step of protocol reverse engineering needs to be applied. We propose a novel method based only on network traces which benefits from recent classification techniques (Support Vector Clustering) [16]. Regarding other similar techniques, our main advantage is a limited complexity. The first fingerprinting method introduces a new formalization: "Random Tree Parameterized Extended Finite State Machine" (TR-FSM) which represents the behavior of the devices. The behavior is a set of sequences of exchanged messages from one device with other ones. In order to apply the support vector machines multi-class classification algorithm, a new kernel function was introduced providing very good results [39] with the SIP protocol, a widely used protocol by VoIP operators today for which many threats exist.

The second fingerprinting techniques assumes the grammar protocol knowledge to build the syntactic tree of a message. Indeed, most of other current approaches are very specific by studying some fields of a protocol. Our approach is not related to a specific protocol and don't focus on the semantic of certain fields but more on the hierarchical organization of the message content. A new similarity function is defined to compare two syntactic trees. The results on the SIP protocol are very encouraging (90%). Besides, we extend the ROCK classification algorithm to propose an unsupervised method for identifying devices without any learning process [38].

6.3. Vulnerabilities preventions techniques in SIP networks

Participants: Abdelkader Lahmadi [contact], Olivier Festor.

The fuzzing activity carried in the Madynes team reveals the large number of vulnerabilities related to the SIP. The sources of these vulnerabilities are mainly the weakness of its implementations and sometimes even its specification semantics. A primary way to counter SIP implementations vulnerabilities is through patching. However, patching time is often important or unknown and until that happens a SIP network is kept on leash by attackers. A defense system can start with network level firewalls, where packets are filtered without a deep understand of the SIP protocol semantics. Another way, is to use detection engines like Snort. These solutions are inefficient to prevent from SIP protocol existing vulnerabilities since they are stateless and they are unable to provide all necessary protection scheme against those vulnerabilities.

To overcome such scourge, we have developed a defense tool, called SecSIP [20] to protect a SIP network from SIP protocol related vulnerabilities. The SecSIP tool is fed with vulnerabilities specifications and their counter measures. It screens the SIP traffic, identifies the vulnerabilities and applies preventions actions. The preventions schemes within the SecSIP tools are authored using our developed domain-specific language, called VeTo. The VeTo language relies on an event-driven and rule-based approach to specify in a flexible, and a scalable manner preventions schemes from existing vulnerabilities within a SIP network. The language combines context, definition and events blocks extracted from vulnerabilities properties to provide the ability to prevent against its exploitation. The context block exhibits the vulnerability surrounding environment properties. The definition block provides the vulnerability related assumptions on its behavior such as the involved SIP messages and their respective fields. The pr evention block describes the vulnerable behavior within its context and includes a response action. We have shown through real discovered vulnerabilities the usage of VeTo specifications to protect different deployed SIP devices on a target testbed.

6.4. Risk management

Participants: Rémi Badonnel [contact], Laurent Debricon, Oussema Dabbebi, Olivier Festor.

The main research challenges addressed in our work focused on applying and automating risk management in VoIP networks and services. Telephony over IP is a critical service exposed to multiple security attacks. A large variety of detection and protection mechanisms have been developed for identifying and blocking these attacks. However detection methods have rapidly shown their limits in terms of sensitivity and specificity. Moreover protection mechanisms may have a significant impact on IP telephony performances in terms of operational continuity and quality of service. In that context we have designed a runtime risk management solution for automatically and continuously adapting the exposure of VoIP equipments to the quantified risk level [48]. This exposure is controlled by the application of graduated security safeguards driven by a dedicated risk model. This solution permits to prevent potential risks while maintaining the VoIP network performances. For that purpose we have extended the Rheostat formal risk model to VoIP infrastructures and have identified a set of adequate security safeguards. We have shown how the restriction and relaxation algorithms can provide a progressive response to risks by activating or deactivating these security safeguards at runtime. The activation of a security safeguard permits to reduce the exposure when the potentiality of an attack is increasing, while its deactivation permits to reduce security costs when this potentiality is decreasing. We have evaluated the performances of our solution through a set of experimental results obtained in the case scenario of SPIT attacks [47]. We have determined the impact of the two algorithms on the risk level and have quantified their benefits and limits in comparison with traditional approaches. We have also experimented different temporal behaviours of SPIT attacks. The integration of risk models to detection and prevention systems clearly contributes to a more appropriate response to attacks for such critical services. We are interested in extending our risk management solution to a larger scope of VoIP threats and in developing autonomic mechanisms for dynamically refining the risk model parameters.

6.5. Monitoring of MESH networks

Participants: Olivier Festor, Emmanuel Nataf [contact], Cristian Popi.

Related to monitoring aspects in wireless mesh networks, we have proposed, evaluated and implemented a prototype of WiMFlow, a distributed and self-organized flow monitoring framework for wireless mesh networks. Since flows entering/exiting a wireless mesh network, usually take multiple hops inside the backbone of the mesh network to reach the destination, a naive approach could have all backbone nodes (mesh routers) monitor the flows and export the collected flow information to a collector. This results in redundant flow information being sent by multiple mesh nodes, which entails a high export network overhead.

In our work we searched for mechanisms to distribute the flow monitoring charge accross the network, in such a way that minimizes the number of times a flow is monitored, while adapting the monitoring service availability to the dynamicity of the network's backbone due to link instability or node shut-down inherent in wireless mesh networks.

All routers behave as possible probes. In order for the probes to make decisions on which one monitors a flow, a global vision of the routing entries of all the nodes in the backbone is required on every node. This allows a probe that sees a flow passing through its interfaces to trace the flow's path. A prerequisite for monitoring a flow is that a probe P that sees a flow F on one of its interfaces has to know the flow's entry and exit points in the backbone, as well as the next hop towards the exit point for each node on the path of the flow.

In accordance with this, we proposed a multi-layered functional architecture of the monitoring system. The routing plane builds up the routing table of the mesh nodes (with the help of a pro-active routing protocol). It then provides the routing table entries of all nodes to the monitoring overlay, which uses this information to organize the nodes into monitoring or non-monitoring probes.

Two components come into the decision making process when organizing the nodes for monitoring: the routing information received from the routing plane to locally build the path of a flow on a node, and the metrics that allow to differentiate between nodes located on the path of the flow. These metrics are distance (in number of hops) of the node from the collector (to which the node is configured to send flow records), connectivity degree and up link quality. Nodes with better distance, higher connectivity or up link quality are the ones elected to monitor the flow.

In order to reduce the number of control messages we use the concept of Multi Point Relay (MPR) employed by the OLSR routing protocol to flood topology control messages. The MPR Set selection scheme is that of OLSR. Hello messages are used to convey neighbourhood information. For flooding the network with routing entries, routing control message (RC) are sent by every node and broadcast via the MPRs, containing the entire routing table of the sender. In a second phase we have proposed a mechanism to adapt the emission times of the Hello and RC messages to the dynamicity of the topology, with the goal of keeping the cost of the monitoring overlay low.

A modular implementation prototype of WiMFlow has been implemented based on nprobe for flow information packaging into v5 and v9 export formats, which was tested on a small-scale wireless mesh network set-up in the premises of the team's offices.

In the area of configuration management, we have also worked on the semaless integration of Netconf-based XML oriented management with the new data-modeling language under standardization within the IETF: YANG. We were the first to offer a full Yang-based operational manager demonstrating the usefulness of this approach.

6.6. Pervasive computing

Participants: Laurent Ciarletta [contact], Vincent Chevrier [MAIA Team], Tom Leclerc, Julien Siebert, Cyril Auburtin.

In Pervasive or Ubiquitous Computing, a growing number of communicating/computing devices are collaborating to provide users with enhanced and ubiquitous services in a seamless way. This is a domain that we are exploring in general and that can be considered at the convergence of several Computer Science fields such as Networking, Embedded Systems, Software engineering, and CHI/AI. Madynes is focussing on Ubiquitous networks and services, where there is a lot of different requirements and research topics that can be both generic or specific to our domain of expertise. But we are collaborating with other research teams (mainly INRIA - Maia) to be able to encompass issues and research questions pertaining to this domain in a wider way. The following lists those speciï¬cally related to the work done within Madynes:

- An adaptable yet high level of safety and security is needed. These computing devices should be working in such a way that common users can trust and rely on them,
- Pervasive Computing is high-technology seamlessly woven into our everyday life: therefore it requires autoconfiguration and reconfiguration of its elements and networks,
- The technologies need to be evaluated not only per domain, but on a larger scale, where end-user concerns and interactions should also taken into account. We are still pursuing our investigations on this domain and have been working more specifically on 3 prospects:
  - Multi-models of these Pervasive computing environments (including the users in the modelisation and the simulations). We have been focusing on the collaborative simulations of dynamic networks/elements, namely P2P (to be extended to adhoc networks) using agents to drive those simulations. This work is done in collaboration with the MAIA team.
  - State of the art on Service Discovery protocols, contextual metrics in adhoc networks, and Service Discovery in adhoc networks using an hybrid between cluster-like (WCPD) and MPR-based (OLSR) broadcasting [8] .
  - Geolocation of wireless devices: a research collaboration with Fireflies RTLS was started in March 2009.

Pervasive Computing is built around a user-centric model. In distributed, dynamic networks, services and applications, such as Peer-to-Peer (P2P) networks or Mobile Ad hoc NETworks (MANET), the users behaviour has a strong influence on the quality of service (QoS) and reciprocally.

We've first proposed to use models and simulators from both internetworking and AI (human behaviour) fields and then to make them interact rather than building one as an extension of the other.

Pervasive Computing is built around a user-centric model. In distributed, dynamic networks, services and applications, such as Peer-to-Peer (P2P) networks or Mobile Ad hoc NETworks (MANET), the users behaviour has a strong influence on the quality of service (QoS) and reciprocally.

We've first proposed to use models and simulators from both fields (internetworking and AI (human behaviour) and then to make them interact rather than building one as an extension of the other.

At first, an existing simulator (Peerfactsim) has been extended, with a strong coupling approach to study the influence of the rate of cooperation of user and the rate of pollution of data on the functioning of the P2P network. Results [11] showed the limits of such a strongly tied and centralized approach. A coupling of models and simulators has been proposed and we've first tackled the coordination issues (synchronization, compatibility and coherence) by using the Agent and Artefact paradigm. We have developped a decentralized coordination framework called AA4MM. The aim of this framework is to make heterogeneous simulators interact in such a way that coordination and integration issues are transparent for the people involved in the simulation process. When someone wants to include an existing simulator within the AA4MM framework, only few changes are needed. Moreover, the framework is based upon a decentralised coordination model that has been formalised (in Event-B) [45] in collaboration with Joris Rehm, in order to prove that coordination occurs with a finite number of simulators and that no deadlock is possible. Source code and JMS implementation have been developped in collaboration with Virginie Galtier Ciarletta from Supelec, Metz. Examples, demonstrations and the first realase of the framework are available[5].his framework is currently used in oder to study the impact of the user mobility on the performances of MANET.

In order to build a stable yet adaptable architecture for context-aware service discovery with multimedia capabilities, we've looked into 2 ways of organising and communicating between mobile nodes. Previous work around the study of properties of clustering and adhoc protocols applied to contextual service discovery has been invited for an extended version in [8] where the number of cluster reorganisation has been improved in mix-mode mobility (similar proportion of highly moving nodes and more static ones). Following these results, a new protocol called SLSF (Stable Linked Structured Flooding) has been developed and is currently under submission for ICC 2010. It is based on clustering (WCPD) to allow for a quick toplogy building with an OLSR-like protocol for inter-cluster communication. It is enriched with a fault-recovery mechanisms. Overall, this solution gives a high-reachability with a low bandwidth usage. An architecture for advanced service discovery has been proposed [46] in the context of the ANR SARAH. In this project, the core of the hybrid network is a MANET, but a cloud of fixed servers and access-point surrounds this unstable core but can't be relied on. Our solution allows for an autonomous service discovery that is improved when the fixed services are available, and is currently being developed and tested wit our mulit-simulations and will hopefully be tested in real-scale at the Museum des Télécoms.

The collaboration with the University of Luxembourg has been extended to Collaborative Filtering in adhoc networks [17], with P. Gratz. This is a technique to share and rate (multimedia) content in adhoc networks in a way that avoids flooding with information and requests, by filtering the "pertinence" of the exchanged data with regards to user profiles.

6.7. Voice over IP monitoring

Participants: Rémi Badonnel, Mohamed Nassar, Olivier Festor [contact].

[5] http://www.loria.fr/~siebertj/aa4mm/aa4mm.html

We focus on designing solutions for the protection, detection and prevention of attacks against the IP multimedia communications (often referred to as VoIP). The security risks are quite numerous. In particular we address SPIT (Spam over Internet Telephony), flooding and fraud. We have proposed to monitor inbound/outbound traffic. We have developed a package for feature extraction from traces and mixed traces. We have also proposed to monitor the VoIP service infrastructure. Our approach is to reveal the state of a server (basically: normal vs. Alert status) using a number of probes or statistics that are provided in several cases by the server command interface or its management interface. The mathematical foundation of our approach is the theory of Support Vector Machines (SVM). We have also compared with other machine learning techniques such as Naive Bayesian Trees (Chapter 8- http://tel.archives-ouvertes.fr/tel-00376831/fr/). A script to monitor OpenSIPS using one-class SVM has been developped[6]. We have implemented this approach in several exemplary VoIP enterprise networks (e.g. based on Asterisk, or the triple OpenSIPS+MediaProxy+RADIUS). The normal traffic is provided by a number of VoIP bots that send and receive calls while respecting a statistical distribution (Poisson) and a social model. The malicious traffic is ensured by hacking tools[7] or also by unexpected behavior of bots (Chapter 7 - http://tel.archives-ouvertes.fr/tel-00376831/fr/). The experiments show that effective and real-time monitoring of servers is entirely possible. The selection and the visualization of statistics that contribute the most to the detection is necessary to reveal the real sources of the attack and to remove them. We tested several techniques of feature selection. Experiments demonstrate that the selection is important to increase the detection accuracy and performance. At the same time it is useful for attack characterization and classification. A quite manageable framework (tools and deployment models) is useful for researchers in this field in order to implement, test and compare their approaches, especially because the VoIP enterprises do not give access to their data and network traces for privacy reasons.

6.8. Monitoring content cccess in peer-to-peer networks

Participants: Thibault Cholez, Isabelle Chrisment [contact], Olivier Festor.

Peer-to-peer (P2P) networks are now commonly used to share files within the Internet. They offer lots of advantages compared to the client-server scheme by giving possibility to gather and share a large amount of resources with the collaboration of many individual peers. However, peer-to-peer networks also provide support for harmful and malicious activities that can voluntarily propagate strongly undesirable contents.

As peer-to-peer systems are self-organized, dynamic and do not have a centralized infrastructure, it is not obvious to collect information to measure them and to observe the behavior of malicious users. With passive monitoring we can observe, from one point, the P2P traffic without sending additional data into the network. However, these approaches do not allow to study specific contents at the network scale. Active monitoring removes this drawback but is more intrusive in the sense that some traffic (queries, files) is injected in the network to gather more information concerning the P2P system. Many crawlers have been used to study the different P2P protocols like Gnutella, Napster, e-Donkey and KAD. Alone, a crawler can just observe the network without acting on it. In the case of KAD, a crawler just discovers the peers but not the shared contents. To have a better view of the network and to control it, a crawler has been associated to a Sybil attack which consists in creating a very large number ($\sim 2^{16}$) of fake peers, controlled by one computer, and placing them actively in the part of the DHT to observe.

We showed that recent protection mechanisms have been introduced in KAD to make this intrusive approach inefficient [13]. We assessed the protection mechanisms entered into recent clients to fight against the Sybil attack in KAD, a widely deployed Distributed Hash Table. We studied three main mechanisms: a protection against flooding through packet tracking, an IP address limitation and a verification of identities. We evaluated their efficiency by designing and adapting an attack for several KAD clients with different levels of protection. Our results showed that the new security rules mitigate the Sybil attacks previously launched. However, we proved that it is still possible to control a small part of the network despite the new inserted defenses with a distributed eclipse attack and limited resources.

[6] http://www.loria.fr/~nassar/opensips_monitoring_scripts/monitoring_script_1.bash
[7] http://www.hackingvoip.com/sec_tools.html

We proposed then a new P2P Honeynet architecture called HAMACK [30], [15] that bypasses the Sybil attack protection mechanisms introduced recently in KAD. HAMACK is composed of distributed Honeypeers in charge of monitoring and acting on specific malicious contents in KAD through keywords and files. Those Honeypeers are set very close to malicious references of the DHT and are able to take control over them. Our approach does not rely on the injection of Sybils and is absolutely non-intrusive for the network besides the targeted contents. Quiet monitoring of all the incoming requests and eclipsing the malicious contents are some interesting features of HAMACK, to study and protect the network. The most accomplished feature is the possibility to announce many files for a given keyword with realistic and attractive attributes, in particular the number of sources. Through the announcement of fake files, HAMACK is able to attract and capture all the requests of a malicious peer: from the search of a keyword, to the final download request, assessing the actions of malicious users.

To achieve these features, HAMACK exploits the weakness of KAD [25] allowing to freely choose the KADID of a peer and relies on the very efficient search process of the KAD DHT. As described in our model, a search launched on a target of HAMACK will be captured by the Honeypeers with a very high probability ($\geq 93\%$). Our work highlights a new dilemna of KAD which has to choose between its routing efficiency and the safety of its indexed contents. HAMACK is implemented by a lightweight architecture and fully functional. It uses modified aMuled clients deployed on PlanetLab nodes, and coupled with a secured database. The first experiments run on the real KAD network helped to set the parameters of the architecture. They showed 3 important results: 1- the coordination between Honeypeers increases the efficiency of HAMACK, 2- the architecture has to fit with the latest constraints inserted in KAD and 3- a low upper bound of needed Honeypeers. Then, several experiments were run and showed that HAMACK is extremely efficient to attract all the requests of the target IDs, resulting in the total control of the contents. Finally, our final experiment poisoning a real content confirmed the great importance of controlling the number of sources to make an efficient honeypot.

HAMACK has been designed to study and fight against pedocriminal contents in P2P networks, and was deployed in this purpose [14].

6.9. IPv6 transition

Participants: Frédéric Beck, Isabelle Chrisment [contact], Olivier Festor.

IP networks are widely spread and used in many different applications and domains. Their growth continues at an amazing rate sustained by its high penetration in both the Home networks and the mobile markets. Although often postponed thanks to hacks like NAT, the exhaustion of available addresses, and other scale issues like routing tables explosion will occur in a near future. The IPv6 protocol was defined [RFC2460] with a bigger address space (128 bits) and comes along with new built-in services (address auto-configuration [RFC2462], native IPSec and other functionalities, routes aggregation, simplified header...). It is a fact that IPv6 deployment is slower than foreseen. Many reasons are valid to explain this: economic, political, technological, and human. In this project we are interested in the scientific part of the technological problems that highly impact human acceptance. Many network administrators are indeed reluctant to deploy IPv6 because (1) they do not well know the protocol itself and (2) they do not have sufficiently rich software support to manage seamlessly the transition from their Ipv4 to Ipv6 networks. To address this later issue, we propose to investigate, design and later implement a transition framework with the objective of making it self-managed. As the IPv4-IPv6 transition is a very complex operation, and can lead to the death of the network, there is a real need for a transition engine to ease the network administrators task; the ideal being a "one click" transition.

The first step of our work was to establish a data model representing the network on which the transition will be applied. The addressing mechanism is based on a logic representation of the network to transition. This means that, for example, Virtual LANs will be seen as different links in the graph, even if physically they are multiplexed on the same link. The network will thus be represented as a graph with the border router (interconnected with the ISP) as root. In case of multi-homing, we would have one logical view of the network per border router. We defined a specification of the different network topologies (for example, simple networks

as lines or trees, bus, mesh, rings) that can be transitioned from IPv4 to IPv6 [27]. We also described all the procedures for IPv4-IPv6 numbering like they were listed for renumbering an IPv6 network in the RFC4192.

Then, we identified the pre-requisites to the transition of an IPv4 network to IPv6 and we built the specification of a transition engine and the associated algorithms given an addressing scheme for the site, using the minimal number of /64 prefixes possible and optimizing the aggregation [28].

7. Contracts and Grants with Industry

7.1. VAMPIRE

Participants: Olivier Festor [contact], Jérôme Francois.

Dates January 2009 - December 2011

Partners INRIA, EURECOM, Symantec Labs, Orange Labs

VAMPIRE is a collaborative project which aims at providing the conceptual approaches and the practical solutions to detect and manage vulnerabilities in the current and future Internet.

The project targets the development of advanced vulnerability discovery methods based on :

- smart fault injection -fuzzing-
- stateful and automated fuzzing and
- passive host-level attack detection.

The project particularly targets IMS and VoIP services and infrastructures. The major research activities undertaken in the VAMPIRE project will be to build a theory of fuzzing and vulnerability monitoring capable to provide both quantitative and qualitative indicators, as well as to provide a structured approach capable to deal efficiently with unknown applications/services.

VAMPIRE is funded by the French National Research Agency (ANR) under contract no. ANR-08-VERS-017. INRIA is leading the project. In the first year, the project did make major progress on identification of unknown protocols, feedback-based fuzzing as well as on IMS and VoIP fuzzing. Several vulnerabilities have been discovered in multiple implementations tested within the project.

7.2. EMANICS

Participant: Olivier Festor [contact].

Dates January 2006 - April 2010

Partners 12 european universities and one financial institute

EMANICS is an FP6 Network of Excellence which brings together most of the best european research teams on management. It is built around 13 research teams and one financial coordination entity and led by Olivier Festor. The network aims at shaping the European research in the area of device, network and service management to provide the necessary coordination and integration so as to enable the participants, while maintaining and enhancing their excellence in their respective field, to contribute in a unified way to the design of management solutions covering all of the challenges arising in this field.

EMANICS is now running for four years and has reached many great successes in the area of researchers and community integration, joint research results, outstanding publications quality and score, standard contributions, operational testbeds, visibility and recognition. Details on the networks and its achievements can be found on the networks Web site at: http://www.emanics.org. Evaluated in march 2009, the network received for the third time in a row, the highest mark a project can get in an evaluation stating that it did fully achieve its objectives and technical goals for the period and that it has even exceeded expectations.

In addition to the management and animation of the network [32], [35], [34], [33], [36], we did contribute in 2009 in the activities related to the EMANICS virtual laboratory, Open Source developments coordination and support [37], scalable management as well as autonomic management.

7.3. INRIA-ALU joint lab

Participants: Humberto Abdelnur, Laurent Andrey, Rémi Badonnel, Olivier Festor [Contact].

Dates July 2008 - December 2011

Partners Alcatel Lucent, INRIA.

This joint lab brings together research teams from INRIA and Alcatel Lucent Bell Labs for addressing the key challenges of autonomous networking in three critical areas: semantic networking, high manageability and self-organized networks. Our activity is part of the joint initiative dedicated to high manageability, and focuses on security management aspects with the Alcatel-Lucent Bell Labs teams on network security. Our work in this joint lab concerns the automation of security management. It includes a first activity related to fuzzing, which includes the improvement of the KiF framework as well as the design of novel fuzzing models for Alcatel-Lucent specific protocols. A second activity of the joint lab aims at investigating to what extent risk management strategies can be applied to VoIP infrastructures. The objective is to design and experiment dynamic risk management methods and techniques for voice oriented critical services.

In 2009, we have pursued our activity on fuzzing methods by completing the deployment testbed and by specifying more elaborated testing scenarios. In particular we have removed the SIP-specific features of our fuzzing tool so that we can specify testing scenarios with several different protocols. In the meantime we have developed new techniques allowing our fuzzing tool to generate a behaviour learnt from captured traces. Our efforts also focused on a runtime risk management strategy for preventing risks in VoIP networks and services. This strategy aims at dynamically altering the network exposure in a graduated manner in order to limit the impact of security safeguards on the VoIP service performances. Risk management provides new perspectives with respect to that issue. Risk is typically defined as the combination of the probability that a given threat exercises a vulnerability and the resulting impact of that adverse events on the network infrastructure. Risk management is the process consisting of identifying risks, assessing and evaluating them, and taking steps (security safeguards) to reduce risks to an acceptable level. In that context, we have extended a risk model, have specified a dedicated architecture and have evaluated the solution through a set of experiments in the case scenario of SPIT attacks. To ease the tracking of VoIP activity on heterogeneous environments, we have worked with Vijay Gurbani from Bell-labs on the design and early prototyping of a common log format for SIP entities. This format is now in its second release as an IETF draft [50], [49]. We pursue the standardization activity on this item.

7.4. AIRNET

Participants: Olivier Festor [contact], Cristian Popi.

Dates June 2006 - November 2009

Partners LSR-IMAG (Leader), LIP6, Université Pierre et Marie Curie, Eurécom, LSIIT, INRIA (MADYNES), Division R&D de France Télécom, Thales Communications, Ozone.

Airnet is a French collaborative research project funded by the RNRT-ANR. The objective of this project is to study the design, deployment and operation of a full wireless interconnection infrastructure over a public frequency.

The MADYNES contributions to this project are the investigation of distributed monitoring for mobile ad-hoc mesh-networks.

In 2009, we worked on the implementation of the flow-monitoring algorithms we defined for mesh networks. The project was completed in november 2009 and successfully evaluated by the ANR.

7.5. SARAH

Participants: Laurent Ciarletta [contact], Tom Leclerc, Julien Siebert.

Dates February 2007 - February 2010

Partners INRIA Lorraine (MADYNES), INRIA Rocquencourt (HIPERCOM) , LRI, LIP6, INT Ucopia, Orange Labs

SARAH is an ANR (Agence Nationale pour la Recherche, French National Research Agency) collaborative research project, in the area of Pervasive Computing and Ubiquitous Networks. It has been researching, implementing, experimenting and evaluating (a) novel hybrid ad hoc architecture(s) for the deployment of advanced multimedia services.

These services will be secured and use geo-localized context-aware information provided by Service Discovery protocols and follow some Pervasive Computing requirements :

- Ubiquitous availability,
- Context awareness,
- Self-adaptation to the users needs (the technology adapts and is available to provide services to the user and not the other way around)
- Disappearing computing (discreetly, almost naturally embedded in our daily environment)
- Ease of use.

Therefore it is not only necessary to extend the reach, the availability and the functionality of applications and services but also to ubiquitously offer them in the most secure and easy (natural) possible way. We contribute to the following activities of the project :

- Context aware service discovery for advanced services in ad hoc network. There, we are investigating the technologies and metrics needed in the project for service discovery protocols and the subsequent needs in the management plane. We are focusing on (geo)-location information. This has resulted in the proposition of a generic service discovery architecture.
- Simulation, prototypes, demo and evaluation of proof of concepts services and environment : in order to develop, evaluate and validate the overall project solutions, we are working both on simulations and on real-world implementations using the JANE simulation tool.

The work done within this project is part of both the Information models, configuration management and self-organization of the management plane activities of the MADYNES team.

7.6. MAPE

Participants: Isabelle Chrisment [contact], Thibault Cholez.

Dates January 2008 - December 2010

Partners LIP6-CNRS UPMC Paris 6, INRIA Nancy Grand-Est (MADYNES)

MAPE is a research project funded by the French Research Agency (ANR). The goal of the project is to measure and analyze peer-to-peer exchanges for paedocriminality fighting and traffic profiling.

The main MADYNES contributions to this project will be put in active measurements and in the analysis at the application level.

The active measurement requires the design of a distributed measurement infrastructure, in order to achieve the best complementarity among the different measurement clients. We will have to improve our measurement client based on a honeypot approach.

The issues in the analysis at the application level raises some research questions about how communities are structured and how this can be observed both active and passive measurements.

In 2009, we focused on the design of new attacks on KAD, attacks that bypass the existing protection schemes agaisnt sybill attacks. These were succesfully implemented and their effciency has been demonstrated on a large testbed. The project received a successful mid-term evaluation from the ANR in november 2009.

7.7. CISCO CARD

Participants: Frédéric Beck, Isabelle Chrisment [contact], Olivier Festor.

Dates January 2008 - December 2009

Partners CISCO, INRIA Nancy Grand-Est (MADYNES)

In this project, which is follow-up to a previous CISCO CARD project related to the monitoring and management of IPv6 network renumbering, we propose to revisit and investigate the self-management capabilities in the root scenario of IPv6 deployment, namely transition. More specifically, we want to reanalyze the available transition mechanisms available and through a combined extension and orchestration approach build a proof of concept that enables fully automated transition while ensuring both security and availability of assets and services during the transition phase

7.8. FIREFLIES RTLS

Participants: Laurent Ciarletta [contact], Cyril Auburtin.

Dates March 2009 - December 2013

Partners FIREFLIES RTLS

As part of our effort in Pervasive Computing research, we've started to work with Firelies RTLS, a French startup specialized in advanced geolocation services. They aim at providing long-term and resilient location service for high value assets using active RFID tags. This work has built on previous work driven by Laurent Ciarletta at the Ecole des Mines de Nancy in the wireless-based geolocation techniques. It has been initatied by a 6 months research project around the fundamentals of geolocation using wireless technologies, in parallels with the discovery and use of dedicated hardware chosen by Fireflies. It has been extended by a 3 months engineer work until the end of 2009 to develop a working prototype and will be followed by a long term (3 years) research contract starting in january 2010. Due to intellectual properties issues, detailed information regarding this project will be given with a 1 year delay.

8. Other Grants and Activities

8.1. International relationships and cooperations

We maintain several international relationships, either through a formal cooperation or on an informal basis. The largest international cooperation is currenlty performed under the EMANICS network of excellence described earlier in this report.

In 2009, we did setup a close cooperation with the Univeristy of Luxembourg (R. State) on honeypots and protocol fuzzing. This has led to several joint publications and a joint Ph.D. (G. Wagener). An INRIA associate-team proposal has been setup and submitted.

We have also setup a cooperation with the Team of Th. Djotio at the Polytechnique Institute of Yaoundé, Camerou, on safe configuration management. A joint project was submitted to INRIA and has been labeled Jeune Equipe in november 2009.

In 2009, we were heavily involved in the setup of eight new cooperative research programs targetting either a bilateral basis (industrial partner + MADYNES), national level (ANR or DGA calls) or european level(FP7 call 5).

Olivier Festor is co-chair of the IFIP Technical Commitee 6 Working-Group 6.6.

We actively participate to the Internet Research Task Force (IRTF) Network Management Research Group (NMRG). We are also members of the EUNICE consortium. EUNICE has been established to foster the mobility of students, faculty members and research scientists working in the field of information and communication technologies and to promote educational and research cooperations between its member institutions. The major event of EUNICE is an annual summer school which brings together lecturers, researchers, students and people from the industry across Europe for one week of presentations, discussions and networking. Isabelle Chrisment is member of EUNICE technical committee.

8.2. National initiatives

In addition to the cooperation with the various partners within national ANR-RNRT projects, we also participate to the CNRS pluridisciplinary network (RTP) on communication networks. Olivier Festor is member of the board of this network.

Olivier Festor is member of the board of the Next Generation Internet RESCOM CNRS-INRIA summer school. The team is regularly contributing to the organization of the school and is a contributor to several tutorials given during the school week. Olivier Festor is member of the board of the INRIA-Alcatel cooperation as part of the Alcatel research partnership. He is also member of the french national research agency ANR-VERSO commission.

8.3. Mobility

Olivier Festor spent three weeks at the university of Twente, The Netherlands, in the team of Aiko Pras in july 2009.

Thomas Djotio from the Polytechnique institute of Yaoundé spent two months in the team, working on assurable configuration in the Netconf sphere.

Thomas Buehring from the University of Federal Armed Forces in Munich spent 2 months in the team, working on IPv6 network discovery protocol activity monitoring.

9. Dissemination

9.1. Program committees and conference organization

Isabelle Chrisment was member of the following technical program committees : ACM/IEEE/IFIP AIMS'2009 (International Conference on Autonomous Infrastructure, Management and Security), NOTERE 2009. She was also member of the steering committee of SARSSI 2009. In 2009, Olivier Festor was member of the following program committees: IFIP/IEEE International SYmposium on Integrated Network Management (IM) 2009, RAID'2009, IFIP/IEEE Distributed Systems Operations and Management (DSOM 2009), IFIP EUNICE'2009, IFIP AIMS'2009, RESCOM'2009.

Olivier Festor did co-chair and co-organize with Pr. Jean-Jacques Pansiot from the University of Strasbourg, the french conference on protocol engineering (CFIP'2009).

Olivier Festor is also member of the Board of Editors of the Journal of Systems and Network Management.

9.2. Teaching

There is a high demand on networking courses in the various universities in which LORIA is par. This puts high pressure on MADYNES members which are all in charge of numerous courses in this domain. Especially the team professors and associate professors ensure more than the required amount of teaching obligation in their respective institutions: IUT, bachelor, master, ESIAL and École des Mines de Nancy engineering schools. In this section, we only enumerate the courses that are directly related to our research activity.

Within the Master degree, SDR (Distributed Services and Networks) specialization, Isabelle Chrisment and Olivier Festor are in charge of the course entitled *Routing and Organization within Dynamic Networks*. This course is one of the three foundation courses given to the students that follow a research cursus in Networking in Nancy; Isabelle Chrisment is in charge of the course entitled *Security within Dynamic Networks* at the Masters in Computer Science level.

Isabelle Chrisment is heading the Telecommunications and Networks specialization of the 3rd year at the ESIAL[8] engineering school and in charge of the students recruitement process. She also teaches the networking related courses in this cursus.

Olivier Festor and Emmanuel Nataf are in charge of the *Network and Service Management* course at the masters degree level.

André Schaff is the Director of the ESIAL Engineering School. Jacques Guyard is co-directing the school.

Laurent Ciarletta is heading the class specialization *Conception de logiciels et d'architectures pour les systémes sûrs/ Architectures and Software Design for Safe Systems* of the Computer Science department of the Ecole des Mines de Nancy (Master degree level). He is in charge of Advanced Networking, Middleware, Component-based software development, Pervasive Computing and Systems courses at the Ecole des Mines de Nancy. He is also responsible for the Software Architecture class in the IPISO Master (Ecole des Mines de Paris - Nancy - Saint Etienne), and co-responsible for the "Companies: the digital challenge"("Entreprises : le défi numérique") class of ARTEM.

Several MADYNES Ph.D. Students gave various courses in the area of networking, Voice over IP and security in most universities and engineering schools associated with LORIA.

9.3. Tutorials, invited talks, panels, presentations

In addition to the presentation of all papers published in conferences in 2008, the team members made the following presentations:

- Humberto Abdelnur and Abdelkader Lahmadi gave a demonstration on VoIP Fuzzing and protection with the SecSip protetion engine at the IPTCOMM 2009 event in Atlanta.
- Humberto Abdelnur and Jorge Obes gave, together with Radu State from the University of Luxembourg, a tutorial entiled *Owning the network with just a phone call* at the Hack.lu conference in october 2009.
- Olivier Festor gave together with Radu State from the University of Luxembourg a tutorial on VoIP vulnerabilities and fuzzing at the CRIMES conference in St Denis de la Réunion in november 2009.
- Isabelle Chrisment presented an invited paper entitled *Une architecture de honeypots distribués pour superviser le réseau P2P KAD* at the NOTERE conference in July 2009.

9.4. Commissions

Team members participated to the following Ph.D. defense committees :

- Radu DECA, Ph.D. in Computer Science from University of Québec, Montreal, Canada. Title: *Constraint-Based Models for Automated Network Service Provisioning*, august 2009. (Olivier Festor)
- Ha MANH TRAN, Ph.D. in Computer Science from Jacobs University Bremen, Bremen, Germany. Title: *Distributed Case-Based Reasoning for Fault Management*, august 2009. (Olivier Festor)
- Sylvie LANIEPCE , Ph.D. in Computer Science from Université de Compiègne, France. Title: *Routage par la disponibilitédans les réseaux ad-hoc hybrides* , July 2009. (Isabelle Chrisment as reviewer)

[8] *Ecole d'Ingénieurs en Informatique et ses Applications de Lorraine*

- Najah CHRIDI, Ph.D. in Computer Science from Université Henri Poincaré, Nancy 1, France. Title: *Contributions à la vérification automatique des protocoles de groupes*, September 2009. (Isabelle Chrisment as examiner)
- Pierre-Nicolas CLAUSS, Ph.D. in Computer Science from Université Henri Poincaré, Nancy 1, France. Title: *Algorithmes à front d'onde et accès transparent aux données*, November 2009. (Isabelle Chrisment as examiner)
- François LESUEUR, Ph.D. in Computer Science from Université de Rennes 1, France. Title: *Autorité de certification distribuée pour des réseaux pair-à-pair structurés: modèle, mise en œuvre et exemples d'application*, November 2009. (Isabelle Chrisment as examiner)
- Mohamad ALJNIDI, Ph.D. in Computer Science from Telecom ParisTech, École Nationale Supérieure des Télécommunications, France. Title: *Vers un système d'administration de la séÃ©curité pour les réseaux autonomes*. December 2009. (Isabelle Chrisment as reviewer)
- Salma KTARI, Ph.D. in Computer Science from Telecom ParisTech, École Nationale Supérieure des Télécommunications, France. Title: *Interconnexion et routage dans les systèmes pair-à-pair*. December 2009. (Isabelle Chrisment as reviewer)
- Uciel FRAGOSO-RODRIGUEZ, Ph.D. in Computer Science from Université Evry-Val d'Essone,Tél'ecom SudParis, France. Title: *Modèle de respect de la vie privée dans une architecture d'identité fédérée*. December 2009. (Isabelle Chrisment as reviewer)

Team members participated to the following Habilitation Degree defense committees:

- Hattem BETTAHAR, Ph.D. in Computer Science from Université de Technologie de Compiègne, France. Title: *Communications multicast : travaux sur la QoS et la sécurité*, Februrary 2009. (Isabelle Chrisment as reviewer)

10. Bibliography

Year Publications

Doctoral Dissertations and Habilitation Theses

[1] H. ABDELNUR. *Architecture de Sécurité sur la Voix sur IP*, Université Henri Poincaré - Nancy 1, 03 2009, http://tel.archives-ouvertes.fr/tel-00436270/en/, Ph. D. Thesis.

[2] J. FRANÇOIS. *Robustesse et Identification des Applications Communicantes*, Université Henri Poincaré - Nancy I, 12 2009, http://tel.archives-ouvertes.fr/tel-00442008/en/, Ph. D. Thesis.

[3] M. NASSAR. *Monitorage et Détection d'Intrusion dans les Réseaux Voix sur IP*, Université Henri Poincaré - Nancy I, 03 2009, http://tel.archives-ouvertes.fr/tel-00376831/en/, Ph. D. Thesis.

[4] R. STATE. *Audit et monitorage de la sécurité*, Université Henri Poincaré - Nancy I, 12 2009, http://tel.archives-ouvertes.fr/tel-00442530/en/, HDR.

Articles in International Peer-Reviewed Journal

[5] H. ABDELNUR, T. AVANESOV, M. RUSINOWITCH, R. STATE. *Abusing SIP authentication*, in "Journal of Information Assurance and Security", vol. 4, n^{o} 4, 2009, p. 311-318, http://hal.inria.fr/inria-00405356/en/LU.

[6] H. ABDELNUR, R. STATE, O. FESTOR. *Fuzzing for vulnerabilities in the VoIP space*, in "ACM International Journal of Computer Virology", 2009, http://hal.inria.fr/inria-00436373/en/.

[7] L. ANDREY, O. FESTOR, A. LAHMADI, A. PRAS, J. SCHOENWAELDER. *Survey of SNMP performance analysis studies*, in "International Journal of Network Management", vol. 19, n^{o} 6, 2009, p. 527-548, http://hal.inria.fr/inria-00432582/en/.

[8] T. LECLERC, A. ANDRONACHE, L. CIARLETTA, S. ROTHKUGEL. *Stabilizing cluster structures in mobile networks for OLSR and WCPD as Basis for Service Discovery*, in "International Journal on Advances in Internet Technologies", vol. 2, n^{o} 1, 2009, p. 206-214, http://hal.inria.fr/inria-00406472/en/LU.

Articles in National Peer-Reviewed Journal

[9] J. FRANÇOIS, R. STATE, O. FESTOR. *Botnets IRC et P2P pour une supervision à large échelle*, in "Technique et Science Informatiques", vol. 28, n^{o} 4, 2009, p. 433-458, http://hal.inria.fr/inria-00392573/en/.

[10] A. LAHMADI, L. ANDREY, O. FESTOR. *Caractéristiques des délais dans les applications de supervision de réseaux et de services*, in "Technique et Science Informatiques (TSI)", vol. 28, n^{o} 4/2009, 2009, p. 479 - 502, http://hal.inria.fr/inria-00404847/en/.

[11] J. SIEBERT, L. CIARLETTA, V. CHEVRIER. *De l'intérêt du couplage de modèles pour appréhender les interactions utilisateurs-réseaux dynamiques.*, in "Revue d'Intelligence Artificielle", 2009, http://hal.inria.fr/inria-00398679/en/.

International Peer-Reviewed Conference/Proceedings

[12] R. BADONNEL, O. FESTOR, K. HAMLAOUI. *Monitoring and Counter-Profiling for Voice over IP Networks and Services*, in "IEEE International Symposium on Integrated Network Management - IM'2009, USA, New York", I. PRESS (editor), IEEE Press, 2009-06-01, 8, http://hal.archives-ouvertes.fr/hal-00406537/en/.

[13] T. CHOLEZ, I. CHRISMENT, O. FESTOR. *Evaluation of Sybil Attacks Protection Schemes in KAD*, in "3rd International Conference on Autonomous Infrastructure, Management and Security - AIMS 2009, Pays-Bas Enschede", R. SADRE, A. PRAS (editors), vol. 5637, Springer, University of Twente, 2009, p. 70-82, http://hal.inria.fr/inria-00405381/en/.

[14] T. CHOLEZ, I. CHRISMENT, O. FESTOR. *Fighting against paedophile activities in the KAD P2P network*, in "Advances in the Analysis of Online Paedophile Activity, France Paris", Laboratoire d'Informatique de Paris 6, 2009, http://hal.inria.fr/inria-00405636/en/.

[15] T. CHOLEZ, I. CHRISMENT, O. FESTOR. *Une architecture de honeypots distribués pour superviser le réseau P2P KAD*, in "9e Conféence Internationale sur Les NOuvelles TEchnologies de la REpartition, Canada Montréal", A. OBAÃD (editor), Université du Québec à Montréal, 2009, p. 76-82, http://hal.inria.fr/inria-00405771/en/.

[16] J. FRANÇOIS, H. ABDELNUR, R. STATE, O. FESTOR. *Automated Behavioral Fingerprinting*, in "12th International Symposium on Recent Advances in Intrusion Detection - RAID 2009, France St Malo", E. KIRDA, S. J. D. BALZAROTTI (editors), vol. 5758, Springer Berlin / Heidelberg, 2009-09-30, http://hal.inria.fr/inria-00428972/en/LU.

[17] P. GRATZ, T. LECLERC. *Delay-Tolerant Collaborative Filtering*, in "7th ACM International Symposium on Mobility Management and Wireless Access (MobiWac), Espagne Tenerife", ACM, 2009-10-26, p. Pages 109-113, http://hal.inria.fr/inria-00433769/en/LU.

[18] A. LAHMADI, L. ANDREY, O. FESTOR. *Design and Validation of an Analytical Model to Evaluate Monitoring Frameworks Limits*, in "The Eighth International Conference on Networks - ICN 2009, Mexique Cancun", 2009, http://hal.inria.fr/inria-00404862/en/.

[19] A. LAHMADI, L. ANDREY, O. FESTOR. *Performance of Network and Service Monitoring Frameworks*, in "11th IFIP/IEEE International Symposium on Integrated Network Management - IM 2009, USA, Long Island", 2009, http://hal.inria.fr/inria-00404856/en/.

[20] A. LAHMADI, O. FESTOR. *SecSip: A Stateful Firewall for SIP-based Networks*, in "11th IFIP/IEEE International Symposium on Integrated Network Management - IM 2009, USA, Long Island", 2009, http://hal.inria.fr/inria-00404853/en/.

[21] M. E. B. NASSAR, R. STATE, O. FESTOR. *VoIP Malware: Attack Tool & Attack Scenarios*, in "IEEE ICC 09, Allemagne Dresden", I. C. SOCIETY (editor), IEEE Communications Society, IEEE, 2009, http://hal.inria.fr/inria-00404837/en/.

[22] C. POPI, O. FESTOR. *Flow Monitoring in Wireless Mesh Networks*, in "International Conference on Autonomous Infrastructure, Management and Security - AIMS 2009, Pays-Bas Enschede", R. SADRE, A. PRAS (editors), vol. 5637, Springer, 2009, p. 134-146, http://hal.inria.fr/inria-00404956/en/.

[23] C. POPI, I. DIAZ, O. FESTOR, J. TOURINO, D. RAMON. *Ontological Configuration Management for Wireless Mesh Routers*, in "IEEE International Workshop on IP Operations and Management Volume 5843/2009, Venice Italie", S. B. /. HEIDELBERG (editor), Lecture Notes in Computer Science, 10 2009, http://hal.inria.fr/inria-00436280/en/.

[24] P. SAQUI-SANNES, T. VILLEMUR, B. FONTAN, S. MOTA, M. S. BOUASSIDA, N. CHRIDI, I. CHRISMENT, L. VIGNERON. *UML Modeling and Formal Verification of Secure Group Communication Protocols*, in "Second IEEE International workshop UML and Formal Methods - UML&FM'2009, Brésil Rio de Janeiro", 2009, http://hal.inria.fr/inria-00429747/en/.

Workshops without Proceedings

[25] T. CHOLEZ, I. CHRISMENT, O. FESTOR. *Exploiting KAD Vulnerabilities to Build an Efficient Honeypot Architecture*, in "2nd EMANICS Workshop on Peer-to-Peer Management, Royaume-Uni London", University College London, 2009, http://hal.inria.fr/inria-00405850/en/.

Scientific Books (or Scientific Book chapters)

[26] M. S. BOUASSIDA, I. CHRISMENT, O. FESTOR. *Key Management in Ad-Hoc Networks*, in "Wireless and Mobile Networks Security", H. CHAOUCHI, M. LAURENT-MAKNAVICIUS (editors), ISTE Ltd and John Wiley & Sons Inc, 2009-07, http://hal.inria.fr/inria-00434423/en/.

Research Reports

[27] F. BECK, I. CHRISMENT, O. FESTOR. *Automatic IPv4 to IPv6 Transition D1.1 - Network Topologies and Transition Procedures*, 2009, http://hal.inria.fr/inria-00407630/en/, Contrat.

[28] F. BECK, I. CHRISMENT, O. FESTOR. *Automatic IPv4 to IPv6 Transition D1.2 - Network representation and pre-requisites*, 2009, http://hal.inria.fr/inria-00407632/en/, Contrat.

[29] F. BECK, O. FESTOR. *Syscall Interception in Xen Hypervisor*, 2009, http://hal.inria.fr/inria-00431031/en/, Rapport Technique.

[30] T. CHOLEZ, I. CHRISMENT, O. FESTOR. *HAMACK: a Honeynet Architecture against MAlicious Contents in KAD*, 2009, http://hal.inria.fr/inria-00406477/en/, RR-6994, Rapport de recherche.

[31] O. FESTOR, G. DREO, D. HAUSHEER, G. PAVLOU, A. PRAS, R. SADRE, J. SERRAT, J. SCHOENWAELDER, B. STILLER. *EMANICS Periodic Activity Report January 1, 2008 - December 31, 2008*, 2009, http://hal.inria.fr/inria-00436060/en/, ContratDENLGBES.

[32] O. FESTOR, G. DREO, D. HAUSHEER, G. PAVLOU, A. PRAS, R. SADRE, J. SERRAT, J. SCHOENWAELDER, B. STILLER. *EMANICS Quarterly Management Report #12*, 2009, http://hal.inria.fr/inria-00436061/en/, ContratDENLGBES.

[33] O. FESTOR, G. DREO, D. HAUSHEER, G. PAVLOU, A. PRAS, R. SADRE, J. SERRAT, J. SCHOENWAELDER, B. STILLER. *EMANICS Quarterly Management Report #13*, 2009, http://hal.inria.fr/inria-00436054/en/, ContratDENLGBES.

[34] O. FESTOR, G. DREO, D. HAUSHEER, G. PAVLOU, A. PRAS, R. SADRE, J. SERRAT, J. SCHOENWAELDER, B. STILLER. *EMANICS Quarterly Management Report #14*, 2009, http://hal.inria.fr/inria-00436055/en/, ContratDENLGBES.

[35] O. FESTOR, G. DREO, D. HAUSHEER, G. PAVLOU, A. PRAS, R. SADRE, J. SERRAT, J. SCHOENWAELDER, B. STILLER. *EMANICS Quarterly Management Report #15*, 2009, http://hal.inria.fr/inria-00436056/en/, ContratDENLGBES.

[36] O. FESTOR, G. DREO, D. HAUSHEER, G. PAVLOU, A. PRAS, R. SADRE, J. SERRAT, J. SCHOENWAELDER, B. STILLER. *EMANICS Updated Joint Programme of Activities (Month 37-48)*, 2009, http://hal.inria.fr/inria-00436058/en/, ContratDENLGBES.

[37] O. FESTOR. *EMANICS D6.4 Open Source Support and Joint Software Development*, 2009, http://hal.inria.fr/inria-00436062/en/, Contrat.

[38] J. FRANÇOIS, H. ABDELNUR, R. STATE, O. FESTOR. *Advanced Fingerprinting For Inventory Management*, 2009, http://hal.inria.fr/inria-00419766/en/, RR-7044, Rapport de rechercheLU.

[39] J. FRANÇOIS, H. ABDELNUR, R. STATE, O. FESTOR. *Behavioral and Temporal Fingerprinting*, 2009, http://hal.inria.fr/inria-00406482/en/, RR-6995, Rapport de rechercheLU.

[40] C. JELGER, T. NOËL, I. DIAZ, C. POPI, O. FESTOR. *Wireless Mesh Network Configuration Platform Specification*, 2008, http://hal.inria.fr/inria-00338243/en/, Interne.

[41] E. NATAF, O. FESTOR. *jYang : A YANG parser in java*, 2009, http://hal.inria.fr/inria-00411261/en/, Rapport Technique.

[42] C. POPI, O. FESTOR. *Wireless Mesh Network Monitoring Management Platform Specification*, 2009, http://hal.inria.fr/inria-00436104/en/, Research Report.

[43] C. POPI, O. FESTOR, D.-E. MEDDOUR, H. AÏACHE, S. ROUSSEAU. *Prototypes de protocoles d'interopérabilité, de supervision et d'auto-organisation*, 2009, http://hal.inria.fr/inria-00436241/en/, Interne.

[44] S. RADU, F. OLIVIER, A. HUMBERTO, V. PASCUAL, J. KUTHAN, R. COEFFIC. *SIP digest authentication relay attack*, 2009, http://hal.inria.fr/inria-00441987/en/, Technical Report.

[45] J. SIEBERT, J. REHM, V. CHEVRIER, L. CIARLETTA, D. MÉRY. *AA4MM coordination model: Event-B specification*, 2009, http://hal.inria.fr/inria-00435569/en/, Rapport de recherche.

Other Publications

[46] L. CIARLETTA, T. LECLERC, L. REYNAUD. *Architecture pour la découverte de services avancée*, 2009, http://hal.inria.fr/inria-00417677/en/.

[47] O. DABBEBI. *Intégration d'un modèle de risques à un outil de gestion automatique*, 2009-07-15, http://hal.archives-ouvertes.fr/hal-00406543/en/.

[48] L. DEBRICON. *Gestion adaptative des risques dans les infrastructures voix sur IP*, 2009-07-01, http://hal.archives-ouvertes.fr/hal-00406540/en/.

[49] G. VIJAY, B. ERIC, A. T., H. ABDELNUR, O. FESTOR. *The Common Log File (CLF) format for the Session Initiation Protocol (SIP) - draft-gurbani-sipping-clf-01*, 2009, http://hal.inria.fr/inria-00436075/en/, Draft.

[50] G. VIJAY, B. ERIC, A. T., H. ABDELNUR, O. FESTOR. *The Common Log Format (CLF) for the Session Initiation Protocol (SIP) - draft-gurbani-sipclf-problem-statement-00*, 2009, http://hal.inria.fr/inria-00436073/en/, Draft.