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

Research Scientist

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

Faculty Members

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]
Abdelkader Lahmadi [Associate Professor, ENSEM - Lorraine National Polytechnic Institute]
Emmanuel Nataf [Associate Professor, Nancy 2 University]
André Schaff [Professor, ESIAL,Henri Poincaré - Nancy 1 University, HdR]

Technical Staff

Frédéric Beck [Engineer, Industrial grant (-11/2010)]
Alexandre Boeglin [Engineer, Industrial grant]
Jérôme Fran cois [Research Engineer, Industrial grant (-03/2010)]
Mohamed Nassar [Research Engineer, Industrial grant]
Humberto Abdelnur [Research Engineer, Industrial grant (-09/2010)]
Cyril Auburtin [Engineer, Industrial grant]

PhD Students

Sheila Becker [Co-tutelle with University of Luxembourg (10/2008-)]
Thibault Cholez [Industrial grant with regional co-sponsoship (10/2007-)]
Oussema Dabbebi [Industrial grant (10/2009-)]
Tom Leclerc [Industrial grant with regional co-sponsoship (10/2007-)]
Julien Siebert [MADYNES-MAIA cooperation. Industrial grant with regional co-sponsoship (10/2007-)]
Juan Pablo Timpanaro [Industrial grant with regional co-sponsoship (01/2010-)]
Gérard Wagener [Co-tutelle with University of Luxembourg (10/2007-)]

Administrative Assistant

Céline Simon [Project Assistant, INRIA]

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.

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

In addition to the great scietnific achievements thatw ill be presented in the results section of this report, we had two major highlights this year.

The first one is the official inauguration of the High Security Laboratory in the INRIA Nancy Grand Est premises. The team was highly involved in the setup of this lab for which we did design, deploy and now operate the whole network probes and data collection infrastructure [28]. The lab is now running for about a year collecting more than 14.000 malwares a day, hosting several long term experiments (MAPE project P2P monitoring, High-interaction honeypots in cooperation with the university of Luxemburg, Voice-over-IP probes with the VAMPIRE project).

The second major achievement of 2010 is the successful completion of the EMANICS Network of Excellence in may 2010. EMANICS which we managed over the last four years was, for the fourth year in a row awarded by the european commission as an outstanding project and put forward as an example of what a network of excellence should be. The network made numerous achievements in joint research, integration, dissemination and setup of joint testbeds.

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[1] acronym are associated to these standards.

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.

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

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: an advanced protocol fuzzing framework

Participants: Laurent Andrey, Humberto Abdelnur [contact], Olivier Festor, Abdelkader Lahmadi.

KiF[2] 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.

[2] http://kif.gforge.inria.fr/

The tool is entirely developed in Python. The current distribution is provided as a fully pre-installed and running framework packaged in a VMware image.

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].

In 2010, we added several capabilities to KiF including new protocols support : HTTP, DNS and DHCP. We have also enriched the feedback loop by remote instrumentation : mtrace and Javascript-aware mtracing. The GUI of KIF was also heavily improved.

Despite the large availability of Open source fuzzers and fuzzing frameworks and despite the recent announce made by the CERT regarding the Open Source distribution of a fuzzing framework, our request to make KIF freely available was refused by the industrial relationships department of INRIA. This decision to prevent us from distributing the software in the same conditions as the competitors had two direct impacts: (1) the community of developers we built around KiF decided to suspend their contribution and (2) some industrial partners in joint projects decided to move to 3rd party open source frameworks, despite the power gap between KiF and its competition. KiF remains today the most powerful fuzzer on the market but given the distribution constraints imposed by our administration, we had to suspend the developments on the framework until further notice.

5.2. Voip bots

Participants: Mohamed Nassar [contact], Olivier Festor.

VoIPbot 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 [4] 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

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

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.

In 2010 we have finalized the development of the framework. We have extended the execution engine and the language and have built a complete management interface to the environment. This interface offers both NETCONF and Web-based configuration of the service.

5.4. NDPMon

Participants: Frédéric Beck [contact], Isabelle Chrisment, Olivier Festor, 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 Auto-configuration (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 happened 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 distribution ...).

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 open source 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 distributions are also available for .deb and .rpm based Linux flavors.

5.5. 6Tea

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

6Tea[5] is a transition engine designed to help administrators of business networks to transition their network for IPv4 to IPv6. The tool implements the transition algorithms defined in our team, takes as input a network topology and network devices information (like firewall configurations, device types, access protocols for their configuration) and generates a safe Ipv6 configuration for that network. The tool is able to propagate the configuration to the networked devices under the condition of availability of specific plugins. 6tea provides plugins for CISCO routers and firewalls as well as plugins for all major Open Source routers and firewalls. An online version of the tool is also available for third party users interested in generating configurations and addressing plans for their network.

5.6. AA4M

Participant: Julien Siebert [contact].

[5] https://gforge.inria.fr/projects/v4-to-v6/

AA4MM (Agents and Artefacts for Multi-modeling and Multi-simulation) is a framework for coupling existing and heterogeneous models and simulators in order to model and simulate complex systems. This is the first implementation of the AA4MM meta-model proposed in Julien Siebert's PhD. AA4M is written in Java and relies upon Java Messaging Services (JMS).

AA4MM can be downloaded at http://www.loria.fr/~siebertj.

6. New Results

6.1. Advanced device fingerprinting

Participants: Olivier Festor [contact], Jérôme Fran cois.

The objective of device fingerprinting is to uniquely identify device types by looking at captured traffic from devices implementing that protocol. The main novelty of our approach consists in leveraging both temporal and behavioral features for this purpose. We have proposed a method that can automatically and passively extract these features. Our approach is based on a conceptual model for capturing behavior and related temporal information from devices that implement a given protocol. The key contribution is a fingerprinting scheme, where individual fingerprints are represented by tree-based temporal finite state machines. We have developed a fingerprinting scheme that leverages supervised learning approaches based on support vector machines for this purpose [26][12].

6.2. Smart protocol fuzzing

Participants: Humberto Abdelnur [contact], Sheila Becker, Olivier Festor.

The first extension we made to our fuzzing approach was to provide an extended feedback machanism to the KIF fuzzing framework and by building advanced models that exploit this feedback channel to improve the fuzzing strategies and impact. For the first target (improved feedback) we have finalized Mtrace, a fine-grained backtrace-oriented application tracer, able to trace the propagation of injected data into the target application. Mtrace was build for linux-executable code as well as for Javascript tracing. To optimize the fuzzing strategy, we have proposed a game theoretical model for fuzz testing, consisting in generating unexpected input to search for software vulnerabilities. As of today, no performance guarantees or assessment frameworks for fuzzing were reported in the litterature. We have addressed this issue by building a simple model that can be used to assess and identify optimal fuzzing strategies, by leveraging game theory. In this context, payoff functions are obtained using a tainted data analysis and instrumentation of a target application to assess the impact of different fuzzing strategies [4].

A second direction in our research on fuzzing, was to target new network level protocols. In 2010, we designed a fuzzing framework for IPv6 protocols. Our approach follows a machine learning approach, that leverages reinforcement based fuzzing method. We built a reinforcement learning algorithm to allow the framework to autonomically learn the best fuzzing mechanisms and to automatically test stability and reliability of IPv6 [6].

6.3. Anomaly and attack detection in SIP

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

We have pursued our efforts in SIP/VoIP intrusion detection. We have mainly provided two main contributions:

- a labeled data-set for intrusion detection evaluation. Given the lack of a common labeled data-set similar to what is available in TCP/IP network-based intrusion detection, the different algorithms proposed in the litterature for SIP-based intrustion detection cannot be jointly evaluated and compared on a common basis.

VoIP providers are not able to publicly share their data essentially because of privacy constraints. To overcome this limitation, we designed and built a framework for customizing and generating VoIP traffic in controlled environments. Using this framework we did generate a labeled data-set covering multiple features (Normal, Flood, SPIT, etc.). The data-set was generated in accordance with two different SIP network technologies (Asterisk-based and SER-based). Our data-set is composed of signaling and supporting protocol traces, Call Detail Records (CDRs) and server logs. This dataset is openly available and can be used by the community to evalute its anomaly and intrusion detection algorithms [19].

- a novel monitoring framework for SIP enterprise networks. In this work, we aimed to foster security within SIP enterprise domains by providing monitoring capabilities at three levels: the network traffic, the server logs and the billing records. We proposed an anomaly detection approach based on appropriate feature extraction/selection and one-class Support Vector Machines (SVM). We proposed methods for anomaly/attack type classification and attack source identification. Our approach was validated through experiments on a controlled test-bed using a customized normal traffic generation model and synthesized attacks. The results showed promising performances in terms of accuracy, efficiency and usability [18].

We were also developing a VoIP honeypot software named Artemisa. The honeypot is designed to connect to a VoIP enterprise domain as a back-end user-agent in order to detect malicious activity at an early stage. The honeypot can play an efficient role in the real-time adjustment of the security policies of the enterprise domain where it is deployed. We aimed, by this contribution, to encourage the deployment of such honeypots at large scale and the collection of attack traces. We tested the capacity of the honeypot to handle a series of known SIP script-kiddies attacks and presented results from diverse scenarios [11].

6.4. High security lab telescope and network experimentation facility

Participants: Frédéric Beck [contact], Alexandre Boeglin, Olivier Festor.

The objective of the High Security Lab at INRIA Nancy Grant Est is to provide both the infrastructure and the legal envelope to researchers to perform sensitive security oriented experimentations. We do contribute to this laboratory by (1) designing and operating a large network telescope and (2) performing vulnerability assessment research, network data and malware collection and analysis.

In 2010, in the scope of the inauguration of the High Security Lab in July, we moved the telescope to a dedicated, secured and isolated room built in the basement. This room includes a servers' room, an open space office and a room dedicated to access control and electrical management. All DSL lines have been moved alongside to the infrastructure itself. Both sub-projects are now coexisting within this new room.

Moreover, we also performed a full software upgrade of the telescope. The new version is now able to support various honeypots of different kinds, all logging in the same centralized collector. This operation allowed us to diversify the emulated vulnerabilities (known vulnerabilities for usual services) and deploy a new type of honeypot logging brute force attacks on SSH servers, and log the shell session after successful login (the session is limited to a small set of emulated commands on a virtual file system, no further attacks can be performed). Due to that upgrade, the SDSL connection has saturated, which is why we initiated the upgrade from the existing 1Mbit/sec connection to the maximum bandwidth allowed on the line, 2Mbit/sec. In order to diversify even more the data collected, we also join the leurrecom.org Honeypot Project by deploying an instance of their honeypot in the telescope. We keep on collecting networks flows and traces on all these honeypots and are initiating their analysis.

We continued the experimentations on the dedicated cluster with experiments on the Tor network (anonymisation through onion routing, experiments suspended as we already collected enough data), Peer-to-Peer monitoring on KAD and Bit-torrent networks in the scope of the MAPE ANR Project and VoIP honeypots (several honeypots deployed and compared) in the scope of the Vampire ANR project.

The full specification of the telescope is publicly available. The details of the infrastructure updates made in 2010 can be found in [28].

As of today, we have deployed more than 80 sensors based on 4 different honeypots. Almost 1.5M of malwares (146 000 unique binaries) and 1.1T Bytes of network traces have been collected (including 20GB of network flows). After the upgrade, the telescope undergoes around 200 000 attacks leading to around 18 000 malwares downloaded daily.

6.5. Collaborative SPAM filtering on smart-phones

Participants: Abdelkader Lahmadi [contact], Olivier Festor.

Text-based messaging services are highly popular and heavily used today. These services are widely provided by emerging social networks like Twitter, Facebook or simply by the the most known SMS service on mobile phones. Nowadays, the cost of SMS is decreasing and many providers offer unlimited texting plans. These costs cut make mobile-phone users a more attractive target for spammers. In addition, modern SmartPhones offer more capabilities than traditional mobile phones. They are able to compute and communicate using different communication means. By focusing on these communication capabilities, spammers are interested in delivering abusive or malicious SMS content to smartphone users.

Our team has developed a model implemented in a tool called Hinky available for Android-based mobiles, to help users to filter SMS and call spams using a local black list. The filtering method behind Hinky is user centric, i.e. the user himself tags the SMS messages as spam. The next time an SMS is received from this sender, it is automatically treated as spam and the SMS is discarded. This preliminary approach was limited since each user does not benefit from other users black lists.

We have extended our method to filter spam on smartPhones with a collaborative approach. When a user tags an SMS as spam, then this human effort is shared among other users. When a message is identified as spam by somebody elsewhere, other users of the collaborative platform are protected from this undesired message. Our collaborative filtering solution relies on a mixture of distributed Bloom filters and hashing based lists to store, query and publish SMS spam content between users using a simple friendship mechanism. We evaluated the efficiency of our solution regarding the storage space and the rate of false positive which is an important metric due to the criticality of an SMS [36].

6.6. SecSIP: a SIP exploit prevention engine

Participants: Alexandre Boeglin, Olivier Festor, Abdelkader Lahmadi [contact].

SECSIP [32] is developed by the team to defend SIP-based 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. The preventions schemes within the SecSIP tool are authored using our developed domain-specific language, called VeTo [13]. 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 prevention 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.

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 specifications to identify different variables, event patterns, operations and actions from each rule.

Manually writing and generating these prevention specifications is tedious and error-prone. Therefore, we have developed a method which automatically infers these specifications by analyzing exploit SIP protocol messages and then provide them to the detection engine. Our approach relies on a genetic algorithm applied to regular expressions to characterize malformed messages. We automatically generate a set of candidate regular expressions to match a malformed pattern within a SIP message, and evaluate their quality to ensure that

their are specific enough to only match exploit messages. The genetic algorithm is used to optimize the set of candidate regular expressions. The algorithm considers each candidate regular expression as a chromosome which is evaluated using an appropriate fitness function. A selection algorithm is then applied to select the best regular expression. Finally, we apply a set of recombination and mutation rules on the selected regular expressions to produce a new generation. The evolution cycle is repeated until a defined number of evolution is reached.

While the genetic process terminates and we obtain the best set of regular expressions which only matches exploit messages, the tool generates a set of VeTo specifications over these regular expressions.

6.7. Netconf-based Configuration Management

Participants: Emmanuel Nataf [contact], Olivier Festor, Abdelkader Lahmadi.

The work on configuration data modeling language that was finalized last year and that led to the implementation of a new YANG parser (jYang) has been used to improve the open source EnSuite configuration management framework supported by MADYNES. Previous version of EnSuite didn't make use of YANG but just has an XML based interface. The work that has been done was on the two sides of the NETCONF protocol, first at the server side it was necessary to enhance a message in order to annonce which YANG data models are implemented within the server. Second at the client side we have build a visualization tools based on YANG data models. The framework is now enable to show the data model of a configuration either with a static view, like a specification browser, either on real network devices [20], like an usual MIB browser in the network supervision domain.

YANG is now an IETF Request For Comment (RFC6020) and will probably be very much used by network devices vendors to specify their configuration data model. We are working on a YANG oriented editor in the Eclipse environement through the creation of a plug-in that will help YANG data modellers in their work. [43]. MADYNES is in relationship with the IETF working group on YANG and will probably have to evaluate several YANG data models that will be proposed to the Internet standardization.

6.8. Risk Management in VoIP Architectures

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

IP telephony has known a large scale deployment since the standardization of dedicated signalling protocols. This telephony service is less confined than traditional PSTN. It is therefore more exposed to security attacks. These ones can be specific to VoIP protocols such as SPIT, or can be inherited from the IP layer such as ARP poisoning. A large variety of protection mechanisms is available, but their activation may seriously impact on the quality of service of such critical environments [10]. Our work focuses on exploiting and automating risk management methods and techniques for VoIP infrastructures, in order to protect them while maintaining their usability [9]. In this context, we have extended our runtime risk modelling to cover a larger spectrum of security attacks [46]. We have then evaluated how the observability properties of these attacks influence the performance of our solution, in particular in the case of low attack signature size. Our approach relies on a set of security safeguards that can be activated or deactivated with respect to threat potentiality. We have quantified the impact of these safeguards and their characteristics on our runtime risk management. We have also observed how the parametrization of such a risk modelling can be difficult to maintain. As a consequence, we have proposed a self-configuration strategy based on an econometric feedback mechanism. The objective is to simplify the configuration of our risk management modelling by dynamically refining the model parameters at runtime. We have defined this econometric feedback mechanism in a theoretical manner and have shown how it can be integrated into our solution [47]. Finally, we have investigated the coupling with anomaly detection techniques based on support vector machines (SVM). SVM has already been proven to be efficient and accurate in monitoring VoIP signalling traffic. We have determined to what extent the detection sensitivity and specificity affect our risk management [17].

6.9. Safe Configuration in Autonomic Networks

Participants: Martin Barrere, Rémi Badonnel, Olivier Festor [contact].

The main research challenge addressed in this work has focused on integrating configuration vulnerability descriptions into the management plane of autonomic networks and systems. The continuous growth of networks and their services significantly increases the complexity of their management and requires the delegation of management functionalities to the networks themselves. Networks and systems have therefore to take in charge their own management, by optimizing their parameters, adapting their configurations and ensuring their protection against security attacks. Operations and changes executed by autonomic networks during these activities may however generate vulnerable configurations. In this context, we have proposed a new prevention strategy for dealing with configuration vulnerabilities in autonomic networks and systems [45]. We have considered the Open Vulnerability Assessment Language (OVAL) which has known a strong standardization effort. This language permits to specify in a standardized manner the description of configuration vulnerabilities, seen as a set of forbidden combinations of configuration parameters. We have shown how these standardized descriptions can be integrated into an autonomic environment in order to ensure a safer self-configuration. In particular, we have formalized the translation of OVAL vulnerability descriptions into policies and policy rules, which are interpretable by an autonomic configuration tool (Cfengine). We have proposed a functional architecture for supporting this vulnerability prevention mechanism into an autonomic infrastructure, and have experimented and evaluated this approach through a first implementation prototype focusing on the case of IOS vulnerability descriptions.

6.10. Safe IPv6 transition

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

Despite its slow start, IPv6 is the most mature network protocol for the future Internet. To foster its acceptance and deployment, it has however to offer capabilities reducing and often eliminating the man in the loop.We are convinced that such features are also required for the evolutionary aspects of an IP network, the transition from IPv4to IPv6 being an essential one. Many network administrators are indeed reluctant to deploy IPv6 because they do not fully master the protocol itself and because they do not have sufficiently rich algorithmic support to seamlessly manage the transition from their IPv4 networks to IPv6. To address this issue, we worked on the design of a transition framework with the objective of making this network function self-managed. The results of this work are :

1. a set of algorithms that automate the generation of the IPv6 addressing scheme for an IPv4 enterprise network that can be enriched with on-the fly administrator constraints;
2. an algorithm that generates the security configuration of firewalls for the newly created IPv6 addressing plan,
3. a fully operational, openly available and extensively tested in real environments transition engine that also propagates on-demand the configuration to the devices.

The algorithms have been published in CNSM'2010 [3], the most selective conference in network and service management having an acceptance rate below 14%. The monitoring components were published in [1].

6.11. Pervasive computing

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

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. Madynes is focussing on the networking aspects of ubiquitous systems. We cooperate with with the Maia to be able to encompass issues and research questions that combine both networking and cognitive aspects.

In 2010 we worked on the following research topics :

- Multi-models of these Pervasive computing environments (including the users in the modeling and the simulations). We have been focusing on the collaborative simulations of dynamic networks/elements, namely P2P and adhoc networks using agents to drive those simulations. This work is done in collaboration with the MAIA team. The results have been published in [16], [22] and [23]. In parallel we are exploring how the behavior and other factors such as spatial and temporal dimensions are mutually influencing and the impact of parameters variability of our models [24] in environment where collective behaviors can emerge.
- Specification of core-engine requirements for co-simulation and how it can be applied to cooperation of applications in general. Our goal is to provide a usable framework that would serve as a reference implementation and would scale up to complex settings.
- Study of 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. The SLSF (Stable Linked Structured Flooding) protocol and its improved version with error correction have been published in [14] and [15].
- Energy-constraint geolocalization of wireless devices: a research collaboration with Fireflies RTLS was started in March 2009 and is ongoing. The work will be extended to routing and energy-cost function with a joint work with the TRIO Team.

Multi-modeling and multi-simulation

Pervasive Computing Systems and Ambiant Networks can be studied as Complex systems. They are 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 behavior has a strong influence on the quality of service (QoS) and reciprocally.

Complex systems generally require to use different points of view (abstraction levels) at the same time on the system in order to capture and to understand all the dynamics and the complexity. Being made of different interacting parts, a model of a complex systems also requires simultaneously modeling and simulation (M&S) tools from different scientific fields.

Building a model and a simulation of a complex system from the interaction of the different existing M&S tools present in each scientific field involved, is also a complex task. To represent a complex system, we need to couple several models (multi-modeling) that each represent a part of the whole system. Each model has been designed by and for a specific scientific domain. And making different models interact raise hard issues on model interoperability (semantic coherence, formalism compatibility). As many simulators exist in the scientific fields evolved, a good approach to make a simulation of a complex system is to reuse and make interact these existing simulators. Also, each simulator has been developed for specific purposes and making them interact raise hard issues (interoperability, synchronization). The multiagent paradigm allows the designers to model a complex system as a set of autonomous, proactive and heterogeneous entities, called the agents, that interact and self-organize in an environment.

The contribution of this work is to propose an homogeneous multiagent meta-model (called AA4MM) that provides solutions both for multi-modeling and multi-simulation of complex systems by reusing existing and heterogeneous M&S tools. AA4MM has been implemented and used both for proof of concept and a real case study. A proof of concept has been made by coupling different simulators together to develop a multi-model of prey-predator model. This has permitted us to show both conceptual and operational properties of AA4MM such as interaction of heterogeneous models, modularity, interoperability. This multiagent meta-model for multi-modeling and multi-simulation by reusing existing and heterogeneous M&S tools has been applied to model complex systems integrating user behavior, node mobility, radio propagation in ubiquitous networks.

From co-simulation to collaborative applications

While AA4MM is conceptually decentralized, the actual implementation is centralized and is a proof of concept. A Master student from ENSG (Ecole Nationale Supérieure de Geography) has explored the requirements of the the core engine and applied his results to a computer vision chain of applications [35].

The co-simulations and their current architectures do not provide sufficient flexibility and modularity. Because of their important centralization, they are difficult to use on a larger scale. The emergence or the improvement of technologies like multi-agents systems or web services allow to propose networks of independent applications, supervised by an artificial intelligence. Complex systems could be built by assembling basic modules driven by agents. This work uses results obtained in the field of co-simulations to validate choices made to define our co-simulation platform. Among different possible technological solutions we have chosen a combination of them that answer to our scope statement. We extend this solution for co-simulations to a cooperation of applications. Moreover, in order to fulfill the need of developing a chain of image processing and to prove the feasibility of such architecture, we have proposed a platform that allows to heterogenous applications to collaborate. The chain of image processing, that we studied, rebuilds a 3D environment using images provided by a camera. The created data are shared with other customer applications that increased this way their knowledge. This chain uses applications of computer vision able to process the informations very quickly, allowing thus a (almost) real time reactivity.

Service discovery

The objective of this work is to design and implemented a set of tools and solutions regarding service discovery in mobile ad hoc networks. Improvements are on the information dissemination throughout the network, by proposing a stable and robust connected dissemination structure and on the service discovery, especially the end user experience, by considering node and user context. As a matter of fact, dynamicity in ad hoc network is mainly induced by the human factor of those network. Human behavior, network and node information together represent the context to be considered in order to obtain relevant service discovery and improved overall performances.

Metrics are proposed to capture the context of nodes in their environment. Metrics can be of different nature at different levels. For example they can measure the available bandwidth of a link at the network level or capture information about the goals of the user (e.g. destination) at the user level. Moreover levels can influence each other, human relations (e.g. groups, friends) can become network connections (e.g. neighbor nodes). If the network is bad human relation might become less stable (e.g. user moving to find better network connectivity) which in turn worsen the network. On the other hand, a good network connectivity might attract more user thus improving ad hoc network performances and robustness.

To be able to study those elements and their specific aspects different tools from various domains are combined and/or adapted to the specific service discovery in ad hoc network case. Therefore, additional to a classic network simulation, tools capable of modeling and simulating user interactions, user behaviors and service usage are required. Simulating, using one or more coupled simulators or tools, a complete scenario from the network protocol to the high level user behavior permits to study and further analyze protocol performances.

A first part of this work has been to build a stable structure on top of spontaneously created ad hoc networks. A major challenge is to reach a satisfactory stability by keeping the bandwidth low to create this stable structure. An out of the box definition of stability for ad hoc networks doesn't exist, even worse the definition of stability is closely related to the usage or application of the ad hoc network.

Another peculiarity of MANETs is the human part. Devices are humanly operated on the application level but also the mobility is directly dependent on the human behavior. Most research done in MANETs tend to forget about this human part. We take this into account using the multiagent paradigm to couple simulators and to represent rich users' behavior in our simulations.

6.12. Monitoring content access in Peer-to-Peer networks

Participants: Thibault Cholez, Isabelle Chrisment [contact], Juan Pablo Timpanaro, 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.

P2P honeypots are another way of monitoring contents in P2P networks. The common solutions consist in advertising fake files as normal peers in order to log the download queries received for these files, but without any guarantee that these files will attract all peers looking for the studied content.

MADYNES proposed a new monitoring approach, called HAMACK (Honeynet Architecture for Monitoring content ACcess in KAD), to control content access in a distributed hash table (DHT) and more specifically in a real P2P network called KAD.

In 2010, we pursued our work on HAMACK. Our solution is based on distributed honeypots that passively monitor, with few resources (around 20 nodes), all the requests issued by the peers for a specific content (keyword or file). We showed that we can control the DHT at a local level with a new strategy bypassing the Sybil attack protections inserted in KAD. For the targeted DHT entries, we monitor all requests emitted by the peers, from the initial content publication or search, to the final download request of fake files, assessing accurately peers interest to access it. We demonstrated the efficiency of our approach through large scale experiments performed on the worldwide KAD network [8].

In parallel, we designed a new solution to protect the widely deployed KAD DHT against localized attacks which can take control over DHT entries [7]. We showed through measurements that the IDs distribution of the best peers found after a lookup process follows a geometric distribution. We then used this result to detect DHT attacks by comparing real peers'ID distributions to the theoretical one thanks to the Kullback-Leibler divergence. Our method detects the most efficient attacks with a very small false negative rate, while countermeasures successfully filter almost all malicious peers involved in an attack. Besides, our solution introduces no networkd overhead, it can be applied to any P2P network based on a DHT and is fully backward compatible with older clients.

This solution was implemented in a KAD client and was able to successfully protect the emitted requests from attackers that we inserted on few DHT entries. We also used our method which analyzes peers' ID distribution to detect the contents under attack in the KAD network. First, we developed a crawler able to discover with a high accuracy all peers participating to KAD P2P network [40]. Then, we analyzed the distribution of the peers' identifiers close to a set of keywords related to popular contents (provided by a database from a e-business site) and we searched for the discovered suspcious peers in the rest of the DHT. We estimate that around 1500 contents are either monitored or attacked in this network.

7. Contracts and Grants with Industry

7.1. EMANICS

Participants: Rémi Badonnel, 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 has been running for four and a half 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 network Web site at: http://www.emanics.org. The final evaluation took place in april 2010. For the fourth time in a row, the network received 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 largely exceeded expectations.

In addition to the management and animation of the network , we did contribute in 2010 as in previous years, in the activities related to the EMANICS virtual laboratory, Open Source developments coordination and support, scalable management as well as autonomic management.

7.2. 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.

The project was successfully completed in february 2010. All deliverables were delivered on time and a final demo including co-simulation and service discovery is available. In addition, we spend quite some resources to finalize a demo in a telecom museum building on our service discovery techniques.

7.3. CISCO CARD

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

Dates January 2008 - June 2010

Partners CISCO, INRIA Nancy Grand-Est (MADYNES)

This project is follow-up to a previous CISCO CARD project related to the monitoring and management of IPv6 network renumbering. In this continuation, we propose to revisit and investigate the self-management capabilities in the root scenario of IPv6 deployment, namely transition. This project initially planned to end in december 2009 was extended by 6 months in 2010.

During this period, we finalized a novel algorithm that enables fully automated and safe IPv6 transition for enterprise networks. This algorithm takes as input the network topology and the IPv6 prefix the network inherits. Given these informations, the algorithm generates the adressing scheme together with the security policies (in terms of firewall policies) to apply to automate the network renumbering.

The algorithm has been implemented in a tool entitled 6Tea. 6Tea is distributed in Open Source and an online transition engine service is also available. The transition algorithm and its implementation have been published in [1].

7.4. INRIA-ALBLF HIMA

Participants: Humberto Abdelnur, Rémi Badonnel, Oussema Dabbebi, 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 2010, we have built a specific branch of both KIF and the feedback engine working on specific Alcatel-Lucent Linux environments. This environment was succesfully transfered to the industrial partner and a training session was organized in the Alcatel-Lucent premises to sutstain the transfer. This activity was succesfully completed.

A second achievement within the cooperation is the amount of results obtained in the area of risk management models applied to Voice over IP services (see related results section for the details). Our efforts on risk management concerned the generalization of our risk modelling to cover a larger variety of attacks, the specification of a self-configuration strategy for dynamically refining parameters based on an econometric feedback mechanism, and the integration of anomaly detection techniques using support vector machines. These results were published in the most selective conference in network and service management.

7.5. FIREFLIES RTLS

Participants: Cyril Auburtin, Laurent Ciarletta [contact], Olivier Festor.

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.

In 2010, the work led to the design of improved algorithms for location computing of sensors. These algorithms were implemented and tested in both indoor and outdoor conditions and the associated implementation was transfered to the industrial partner [25].

A second achievement of 2010 in this cooperation is the design and implementation of a full-fledged SNMP-based management framework for the Fireflies sensor networks. This includes a complete information model, a tunable SNMP proxy implmeneting the model and aninstantiation with standard monitoring tools.

7.6. VAMPIRE

Participants: Olivier Festor [contact], Humberto Abdelnur, Laurent Andrey.

Dates March 2000 - February 2012

Partners EURECOM, INRIA Nancy Grand-Est (MADYNES), Orange Labs, Symantec

VAMPIRE is a research project funded by the French Research Agency (ANR, VERSO ANR-08-VERS-017) coordinated by the team. The goal of the project to investigate new thread security issues induced by Voice Over IP (VoIP) protocols and web2.0. Madynes has the lead on this project.

In this project we have delivered a framework for protocol fuzzing (test by fault injection) with a better feedback than the simple ping usually used in the domain. A grey-box approach is proposed which uses tainted data analysis to observe the impact on memory of an injection of one or several protocol message. More informations are extracted to build graph where node a tainted memory states and edges sequences of system calls that leads to the states. On these informations some metrics can be calculated and they allows comparisons of sequences of injections generated by several fuzzers (sequences generators). These informations also gives feedback to the generation process in order to get a better test coverage for a given quantity of injections.

All the proposed mechanisms have been implemented in the Madynes KIF fuzzing framework and used on some open source SIP implementations.. One publication describing this work is submitted and all details are given in a research report [27].

The last task started in september 2010 relates to the deployment of various VoIP honypots on the Loria-Inria Grand Est's High Security Lab infrastructure. A first round of network traces collection has been achieved and some improvements on the honeypots interactions have been identified for the next collection round.

7.7. MAPE

Participants: Isabelle Chrisment [contact], Thibault Cholez.

Dates January 2008 - Mars 2011

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

MAPE (Measurement and Analysis of Peer-to-peer Exchanges for pedocriminality fighting and traffic profiling) 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 are related to the active measurements and 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. 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 2010, we focused on the deployment of HAMACK, a distributed architecture that aims to investigate and control the spread of contents in the real KAD network. We launched an large-scale experiment to collect data related to the paedophile contents. We monitored the activity (files shared and requested) of 72 keywords (half of them being related to paedophilia) over two weeks. This experiment was done within the context of the High Security Laboratory at INRIA Nancy Grand Est. The ongoing analysis of the collected data aims to characterize paedophiles' sharing behavior in P2P networks.

7.8. Univerself

Participants: Martin Barrere, Rémi Badonnel, Olivier Festor, Emmanuel Nataf.

Dates September 2010 - August 2013

Partners 18 Industrial or Academic Partners, Project Leader : Alcatel Lucent Bell Labs

This FP7 european integrated project aims at consolidating the autonomic methods and techniques supporting the management of the future Internet, and at integrating these methods into a unified management framework. The objective of this framework is to address the management issues of the evolving Internet through the self-organisation of the control plane and the empowerment of the management plane with cognition. Our work in the Univerself project mainly concerns the security and safety challenges posed by the unified management framework, in particular the prevention of configuration vulnerabilities. Since the beginning of the project, we have analysed through a state of the art different vulnerability management strategies for supporting the self-configuration of autonomic networks and systems. We have distinguished methods for identifying known vulnerabilities (based on knowledge repositories) and methods for discovering unknown vulnerabilities (performed at an earlier stage). We are particularly interested in the recent standardization efforts done for specifying the description of configuration vulnerabilities (Open Vulnerability Assessment Language). We have also considered the large variety of techniques already proposed in the area of change management, such as techniques for evaluating the impact of a change or for assessing the risks associated to that change.

7.9. ACDA-P2P

Participants: Isabelle Chrisment [contact], Thibault Cholez, Andreea Orosanu.

Dates Avril 2010 - Décembre 2011

Partners UTT , LORIA (MADYNES)

ACDA P2P (Approche collaborative pour la détection d'attaques dans les réseaux pair à pair) is a research project funded by the GIS 3SGS which aims at strengthening and developing a multidisciplinary community in the field of the surveillance, of the safety and of the safety(security) of the big systems.

The goal of this project is to propose a new monitoring architecture, which is able to observe the peers behavior and to collect measurements relevant to detect attacks while not being intrusive and detectable. KAD and BitTorrent will be studied as target P2P networks. We focus more specifically on collaboration between distributed probes in charge of directly detecting attacks if possible, or collecting data for a further analyzis. This collaboration induces new challenges:

- coordination of collected measurements in order to have a global view of the network;
- design of indicators revealing a malicious behavior;
- optimization of data collection through learning methods;
- security issues to avoid vulnerabilities and weaknesses.

In 2010, we established a state of the art related to the monitoring architectures and approaches for P2P networks, the related security issues and some existing collaborative approaches for attack detection [34]. We also studied attacks and monitoring actions on the KAD DHT to determine the origin of these suspicious peers and their operating mode [40]. As the popular files and the associated keywords are generally the main target of these attacks, in a first time, we performed experiments that aims to establish a correlation between content popularity and attacks.

7.10. SCAMSTOP

Participants: Olivier Festor [contact], Mohamed Nassar.

Dates Avril 2010 - Décembre 2011

Partners INRIA Nancy Grand Est (MADYNES)

In traditional telecommunication, various experts estimate that fraud accounts for annual losses at an average of 5% of the operators revenue and still increasing at a rate of more than 10% yearly. Hence, with the openness and low cost structure of voice over IP (VoIP) service one can expect an even higher threat of fraud and higher losses of revenue making fraud and misuse of services one of the main challenges to VoIP providers. Fraud detection has been an active research and development area in the world of banking and credit card industry. In the VoIP area, there is still hardly any research or products that can assist providers in detecting anomalous behaviour. To fill in this gap, SCAMSTOP will provide a complete framework/solution for automatic fraud detection that alarms providers when suspicious behaviour is detected. The design of the SCAMSTOP fraud detection tools will be based on two aspects. On the one side, SCAMSTOP will use well known methods for statistical behavioural modelling and anomaly detection that have proven their efficiency in the area of credit card, banking and telecommunication and apply them to Internet telephony services. Of special interest here is characterizing the normal usage behaviour while taking into consideration the offered service plans and service structure. On the other side, innovative approaches based on multi-protocol event correlation that takes into account the specific nature of VoIP protocols and components will be developed. This solution will not only be designed to achieve a high detection rate but it will also be optimized to be resource efficient as well. To assess the efficiency and usability of the developed tools and mechanisms, the SCAMSTOP fraud detection system will be intensively tested and probed throughout the project. The consortium is a healthy mixture of SMEs including VoIP service provider, VoIP security and signalling products manufacturers as well as reputed research organizations.

In 2010 we have designed the full functional and physical architecture of the fraud protection framework [44].

8. Other Grants and Activities

8.1. Regional Initiatives

The TEAM is involved in several actions of the regional CPER (Contrat Plan Etat Region) initiative on networked security and more recently security of industrial networked systems. We are also involved in the smart living intiative of the CPER where we provide our expertise on embedded operating systems and sensors.

8.2. National Initiatives

The team is participating in several national research projects : ANR MAPE, ANR SARAH and coordinator of the ANR VAMPIRE project. In addition the team is involved in one P2P project with the University of Troyes (GIS 3S).

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 alliance on digital science (ALLISTENE) commission on future networks.

8.3. European Initiatives

EMANICS, the europea network of excellence managed by the team, was completed in May 2010. The network of excellence was awared by the review team aof the european commission s an outstanding project and for the third year in a row, as an example of integration and joint executed research activites.

A follow-up to EMANICS called MOOSE was submitted in call 5. The proposal passed the evaluation but was ranked 2nd out of 10 proposals while ony one got funded.

MADYNES has an ongoing collaboration with the university of Luxembourg on network security. Two joint thesis are part of this collaboration : the thesis of Gerard Wagener on high interaction honeypot models and the thesis of Sheila Becker on game theory-based protocol fuzzing.

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.

8.4. International Initiatives

We actively participate to the Internet Research Task Force (IRTF) Network Management Research Group (NMRG).

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 the context of a cooperation between the MADYNES EPI and the MASECNESS team, Emmanuel Nataf spent one week at the Polytechnical Superior National School (PSNS) of the Yaoundé University in august 2010. During this period he worked with phD and master students and animated a tutorial on network supervision. The goal of this stay was to carry on with the last comming in september 2009 of Mr Thomas Djotio, assistant professor at PSNS. One objective was to prepare the arrival in Nancy of two phD an one master students for one month in october 2010 and for Mr Djotio that cames from october to december 2010.

This collaboration has permitted the finalization of a common research project. Two main researches directions are considered, one is on the configuration management and the other is on intrusion detection system. These topics are both in the wireless sensors networks (WSN) scope and are focused to the widespread technology 6LowPan. One phD student from the PSNS is working for each research subject.

The research on configuration management aims to study the integration between the Internet standardized configuration management and the configuration of WSN. The main motivation is that WSN in general and particuarly 6LowPan based WSN extend the Internet and so should be managed like it. The main difficulty envisioned is that WSN are very resources restricted networks more than the Internet and so Internet standards solutions could not be implemented without specific adaptation. A first step will be to identify what is a configuration of a WSN and to propose a data model and associated semantic. The standard YANG data model language will be the modeling tool because of its expressivity and data constraints specification capabilities (and because it is the Internet standard for configuration data modeling). Following will be the study of a rigth sized architecture for configuration management that can support both the Internet standard NETCONF protocol and its use on WSN.

The research on Intrusion Detection System (IDS) in WSN aims to study a new model for intrusion detection in WSN. IDS systems have already been widely invesitgated in the last five years, especially on WSN, but there is no result on the 6LowPan technology. So there is an important gap to fill because WSN will be an easy starting point for intruder to abuse, corrupt, destroy either the WSN either the part of the Internet that is connected with it. WSN are usually resources to much restricted to have robust security mechanisms (like an RSA key) and the first work to do is to stand a model to detect an intrusion from alterations on the WSN it involves with the less number of false positive (an intrusion that is not an intrusion but an usual behavior deviation). The main second part of the work will be to define and deploy an IDS architecture generic enough to be used by any 6LowPan based WSN and applications.

8.5. Mobility

Italo Da Costa from Georgia Tech, spent 3 months in the team, working on PhP-based applications fuzzing.

Jérôme François spent three weeks at the University of Twente to work with the team of Aiko Pras on intrusion detection based on flow analysis.

Thomas Djotio from the Polytecnic Institute of Yaoundé, Cameroun spent two months in the team together with three of his students, working sensor networks configuration and monitoring.

9. Dissemination

9.1. Animation of the scientific community

Olivier Festor is the Co-Chair together with Aiko Pras from University of Twente of the IFIP Working-Group 6.6 on Network and systems management. This working group is actively involved the animation of most major conferences in this research area and organizes frequent meetings and workshops on the domain.

Olivier Festor chaired sessions at the following conferences: IFIP/IEEE NOMS'2010 (session on Routing), Mobiquitous'2010 (session on Energy efficiency and awareness), IEEE/IFIP CNSM'2010 (session on Energy Management).

Olivier Festor served as a TPC Member of the following 2010 events: IFIP Autonomous Infrastructures Management and Security (AIMS'2010), IEEE/IFIP International Conference on Network and Service Management (CNSM'2010), IEEE/IFIP Network Operations and Management Symposium (NOMS'2010), IEEE Globecom, Communications Software, Services and Multimedia Applications Symposium (CSSMA), Malware 2010, IEEE/IFIP IEEE/IFIP International Workshop on Network Embedded Management and Applications(NEMA'2010), Francophone COnference on Network and Service Management (GRES'2010), CloudMan 2010, EUNICE'2010, 2010 IEEE Wireless Communications and Networking Conference.

Olivier Festor has been appointed General Chair for IFIP AIMS'2011 and TPC Co-Chair for IEEE/IFIP CNSM'2011.

Olivier Festor is member of the board of editors of the Springer Journal of Network and Systems Management. In october 2010, he was appointed as a member of the editorial board of the IEEE Transactions on Network and Service Management.

Isabelle Chrisment was member of the following technical program committees : ACM/IEEE/IFIP AIMS'2010 (International Conference on Autonomous Infrastructure, Management and Security), NOTERE 2010. She was also member of the steering committee of SARSSI 2010.

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, SSR (Services, Security and Networks) specialization, Isabelle Chrisment is in charge of the course entitled *Advanced Networking*. This course is one of the five foundation courses given to the students that follow a research and professional cursus in Networking in Nancy.

André Schaff is the Director of the ESIAL Engineering School. Isabelle Chrisment is co-directing the school and is in charge of the students recruitement process. Remi Badonnel is heading the Telecommunications and Networks specialization of the 2nd and 3rd years at the ESIAL engineering school. They teach the networking related courses in this cursus.

Laurent Ciarletta is heading the specialization Safe Systems Architecture of the Computer Science and IT department of the Ecole des Mines de Nancy ("Grande Ecole", Engineering School, Master degree level). He is most notably in charge of Advanced Networking, Middleware, Component-based software development, Pervasive Computing, Networking and Systems courses at the Ecole des Mines de Nancy. He is also co-responsible for the IPISO Master (Ecole des Mines de Paris - Nancy - Saint Etienne) and specifically the Software Architecture class. Notably, he is co-responsible for the "Businesses: the digital challenge *Entreprises : le défi numérique*, a class within the ARTEM alliance (ICN - Business School, Ecole des Mines de Nancy, Ecole d'Art / School of Art).

In 2010, the team was involved in the setup of new courses on : Android programming (Abdelkader Lahmadi and Laurent Ciarletta) and Distributed Algorithms (Abdelkader Lahmadi and Olivier Festor).

9.3. Tutorials, invited talks, panels, presentations

In addition to the presentation of all papers published in conferences in 2010, the team members made the following public talks:

- Olivier Festor was a panelist at IEEE/IFIP NOMS'2010 is Osaka in the panel on Programmable Networks;
- Olivier Festor and Humberto Abdlenur gave a talk on fuzzing-based vulnerability at a joint INRIA-Safe River workshop.
- Olivier Festor presented the LHS architecture and performed experiments at the LHS inaugural event in july 2010.
- Remi Badonnel gave a talk on the challenges of risk management in VoIP networks at the ONR FCNS conference in June in Prague, Czech Republic.
- Laurent Andrey presented the progress of the Vampire project at the ANR days in december 2010 in Rennes, France.
- Olivier Festor participated to a public panel on Cybercrime and Internet fear at the Café des Sciences in Metz in december 2010 and gave several interviews to journals and TV channels on the research in Internet Security.
- Isabelle Chrisment and Olivier Festor presented MADYNES work on monitoring and controlling paedophile contents in the KAD P2P network. Journée d'échange entre spécialistes en informatique et Gendarmerie Nationale, Police Judiciaire et Douane Judiciaire organisée par le LERTI et INRIA Grenoble. Septembre 2010.

9.4. Commissions

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

- Patrick GRAATZ, Ph.D. in Computer Science from the University of Luxemburg. Title: *: Approaches for Collaborative Filtering in distributed environments*, february 2010. (Laurent Ciarletta)
- Tiago FIOREZE, Ph.D. in Computer Science from the University of Twente, The Netherlands. Title: *Self-management of hybrid optical and packet switching networks*, february 2010. (Olivier Festor)
- Shahab GASHTI , Ph.D. in Computer Science from Université Pierre et Marie Curie, France. Title: *Architecture de la découverte de services pour les réseaux de domicile communautaires* , Mars 2010, (Isabelle CHRISMENT).
- Ion ALBERDI, Ph.D. in Computer Science from INSA Toulouse. Title: *Malicious trafic observation using a framework toparallelize and compose midpoint inspection devices*, april 2010. (Olivier Festor)
- Stere PREDA, Ph.D. in Computer Science from Institut Telecom - Telecom Bretagne . Title: *Reliable Context Aware Security Policy Deployment with Applications to IPv6 Environments*, april 2010. (Olivier Festor)

- Stephane WEISS, Ph.D. in Computer Science from Henri Poincaré - Nancy 1 University. Title: *Edition collaborative massive sur réseaux Pair-a-Pair*, october 2010. (Olivier Festor)
- Venkatesan BALAKRISHNAN Ph.D. in Computer Science from Macquarie University, Australia, Title: *Trust enhanced security framework for mobile ad hoc wireless networks*, November 2010, (Isabelle CHRISMENT).
- Charbel RAHHAL, Ph.D. in Computer Science from Henri Poincaré - Nancy 1 University. Title: *Wikis sémantiques distribués sur réseaux pair-à-pair*, november 2010. (Isabelle Chrisment, Olivier Festor)

Team members participated to the following Habilitation Degree defense committees:

- Yacine GHAMRI DOUDANE, Hailitation Degree in Computer Science from Paris-Est University. Title: *Contributions a l'amélioration de l'utilisation des ressources dans les réseaux de paquets sans fil*, december 2010. (Olivier Festor)

10. Bibliography

Publications of the year

Articles in International Peer-Reviewed Journal

[1] F. BECK, I. CHRISMENT, R. DROMS, O. FESTOR. *Autonomic Renumbering in the Future Internet*, in "IEEE Communications Magazine", 07 2010, vol. 48, p. 86-92, http://hal.inria.fr/inria-00531215/PDF/renumbering_cameraReadyv2.pdf.

[2] P. DE SAQUI-SANNES, T. VILLEMUR, B. FONTAN, S. MOTA, M. S. BOUASSIDA, N. CHRIDI, I. CHRISMENT, L. VIGNERON. *Formal Verification of Secure Group Communications Using AVISPA and TURTLE*, in "The Innovations in Systems and Software Engineering journal", 2010, p. 125-133, http://hal.inria.fr/hal-00447682.

International Peer-Reviewed Conference/Proceedings

[3] F. BECK, O. FESTOR, I. CHRISMENT, R. DROMS. *Automated and Secure IPv6 Configuration in Enterprise Networks*, in "6th International Conference on Network and Service Management - CNSM 2010", Niagara Falls Canada, 10 2010, http://hal.inria.fr/inria-00531212/PDF/PID1466223.pdf.

[4] S. BECKER, H. ABDELNUR, J. L. OBES, R. STATE, O. FESTOR. *Improving Fuzz Testing using Game Theory*, in "NSS'2010", Mebourne Suisse, 2010, http://hal.inria.fr/inria-00546174/en/.

[5] S. BECKER, H. ABDELNUR, R. STATE, T. ENGEL. *An Autonomic Testing Framework for IPv6 Configuration Protocols*, in "IFIP AIMS'2010", Zurich Suisse, Springer LNCS, 2010, http://hal.inria.fr/inria-00546171/PDF/fulltext.pdf.

[6] S. BECKER, H. ABDELNUR, R. STATE, T. ENGEL. *An Autonomic Testing Framework for IPv6 Configuration Protocols*, in "IFIP AIMS'2010", Zurich Suisse, Springer LNCS, 2010, vol. 6155/2010, p. 65-76 [*DOI :* 10.1007/978-3-642-13986-4_7], http://hal.inria.fr/inria-00546171/en/.

[7] T. CHOLEZ, I. CHRISMENT, O. FESTOR. *Efficient DHT attack mitigation through peers' ID distribution*, in "Seventh International Workshop on Hot Topics in Peer-to-Peer Systems - HotP2P 2010", Atlanta États-Unis, IEEE International Parallel & Distributed Processing Symposium, 04 2010, http://hal.inria.fr/inria-00490509/PDF/HotP2P10-KAD_DHT_attack_mitigation-cholez.pdf.

[8] T. CHOLEZ, I. CHRISMENT, O. FESTOR. *Monitoring and Controlling Content Access in KAD*, in "International Conference on Communications - ICC 2010", Capetown Afrique Du Sud, IEEE, 05 2010, http://hal.inria.fr/inria-00490347/PDF/ICC10-Monitoring_KAD_Contents-Cholez.pdf.

[9] O. DABBEBI, R. BADONNEL, O. FESTOR. *Automated Runtime Risk Management for Voice over IP Networks and Services*, in "Network Operations and Management Symposium - Noms 2010", Osaka Japon, IEEE, 04 2010, p. 57 - 64, http://hal.inria.fr/inria-00538675/PDF/noms.pdf.

[10] O. DABBEBI, R. BADONNEL, O. FESTOR. *Managing Risks at Runtime in VoIP Networks and Services*, in "Autonomous Infrastructure, Management and Security (AIMS 2010)", Zurick Suisse, IFIP, 06 2010, p. 89-92, http://hal.inria.fr/inria-00538685/PDF/aims.pdf.

[11] R. DO CARMO, M. NASSAR, O. FESTOR. *A Honeypot Back-end to Support Security in VoIP Domains*, in "Principles, Systems and Applications of IP Telecommunications (IPTCOMM)", Munich Allemagne, 08 2010, Poster, http://hal.inria.fr/inria-00547461/en/.

[12] J. FRANÇOIS, R. STATE, O. FESTOR, T. ENGEL. *Online Device Fingerprinting*, in "3rd International Conference on Computational Intelligence in Security for Information Systems", Leon Espagne, 2010, http://hal.inria.fr/inria-00547367/en/.

[13] A. LAHMADI, O. FESTOR. *VeTo: An Exploit Prevention Language from Known Vulnerabilities in SIP Services*, in "IEEE/IFIP Network Operations and Management Symposium - NOMS 2010", Osaka Japon, IEEE, 04 2010, p. 216-223, ISBN :978-1-4244-5366-5 C.: Computer Systems Organization/C.2: COMPUTER-COMMUNICATION NETWORKS/C.2.3: Network Operations/C.2.3.0: Network management [*DOI :* 10.1109/NOMS.2010.5488464], http://hal.inria.fr/inria-00544976/en/.

[14] T. LECLERC, L. CIARLETTA, A. SCHAFF. *A Stable Linked Structure Flooding for Mobile Ad Hoc Networks with Fault Recovery*, in "8th International Conference on Wired/Wireless Internet Communications - WWIC 2010", Luleå Suède, T. M. B. EVGENY OSIPOV, X. MASIP-BRUIN (editors), Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 06 2010, vol. 6074, p. 204-215, The original publication is available at www.springerlink.com [*DOI :* 10.1007/978-3-642-13315-2], http://hal.inria.fr/inria-00490306/PDF/SLSFwRecovery-Leclerc.pdf.

[15] T. LECLERC, L. CIARLETTA, A. SCHAFF. *SLSF: Stable Linked Structure Flooding For Mobile Ad Hoc Networks*, in "IEEE International Symposium on Wireless Pervasive Computing - ISWPC 2010", Modena Italie, 05 2010, http://hal.inria.fr/inria-00488902/PDF/Leclerc.pdf.

[16] T. LECLERC, J. SIEBERT, V. CHEVRIER, L. CIARLETTA, O. FESTOR. *Multi-modeling and co-simulation-based mobile ubiquitous protocols and services development and assessment*, in "7th International ICST Conference on Mobile and Ubiquitous Systems - Mobiquitous 2010", Sydney Australie, 12 2010, http://hal.inria.fr/inria-00534575/PDF/mobiquitous2010.pdf.

[17] M. NASSAR, O. DABBEBI, R. BADONNEL, O. FESTOR. *Risk Management in VoIP Infrastructures using Support Vector Machines*, in "6th International Conference on Network and Services Management - CNSM 2010", Niagara Falls Canada, 10 2010, p. 48–55, http://hal.inria.fr/inria-00530167/PDF/73838.pdf.

[18] M. NASSAR, R. STATE, O. FESTOR. *A framework for monitoring SIP enterprise networks*, in "Fourth international conference on Network and System Security - NSS 2010", Melbourne Australie, IEEE, 09 2010, p. 1–8 [*DOI :* 10.1109/NSS.2010.79], http://hal.inria.fr/inria-00519728/PDF/nss10.pdf.

[19] M. NASSAR, R. STATE, O. FESTOR. *Labeled VoIP Data-set for Intrusion Detection Evaluation*, in "EUNICE 2010", Trondheim Norvège, 2010, p. 97-106, http://hal.inria.fr/inria-00497735/PDF/main.pdf.

[20] E. NATAF, O. FESTOR. *End-to-end YANG-based Configuration Management*, in "IEEE/IFIP Network Operations and Management Symposium - NOMS 2010", Osaka Japon, IEEE, 2010, p. 674–684, http://hal.inria.fr/inria-00534434/en/.

[21] C. POPI, O. FESTOR. *WiMFlow: a distributed, self-adaptive Architecture for Flow Monitoring in Wireless Mesh Networks*, in "2010 IEEE/IFIP Network Operations and Management Symposium", Osaka Japon, IEEE, 04 2010, C.: Computer Systems Organization/C.2: COMPUTER-COMMUNICATION NETWORKS, http://hal.inria.fr/inria-00526006/PDF/62539_1.pdf.

[22] J. SIEBERT, L. CIARLETTA, V. CHEVRIER. *Agents and artefacts for multiple models co-evolution. Building complex system simulation as a set of interacting models*, in "9th Int. Conf. on Autonomous Agents and Multiagent Systems - AAMAS 2010", Toronto Canada, 05 2010, p. 509-516, http://hal.archives-ouvertes.fr/hal-00452865/PDF/article-aamas2010_siebert_v2.pdf.

[23] J. SIEBERT, L. CIARLETTA, V. CHEVRIER. *Agents and Artefacts for Multiple Models coordination. Objective and decentralized coordination of simulators.*, in "SAC 2010 25th Symposium on Applied Computing - SAC 2010", Lausanne Suisse, ACM, 03 2010, ACM, http://hal.archives-ouvertes.fr/hal-00426601/PDF/sac2010_siebert_accept.pdf.

National Peer-Reviewed Conference/Proceedings

[24] T. NAVARRETE GUTIERREZ, J. SIEBERT, L. CIARLETTA, V. CHEVRIER. *Impact des dimensions spatiale et temporelle dans la modélisation d'un phénomène collectif de type "free-riding"*, in "18èmes Journées Francophones des Systèmes Multi-Agents - JFSMA'10", Mahdia Tunisie, 10 2010, http://hal.inria.fr/inria-00534600/PDF/main.pdf.

Workshops without Proceedings

[25] L. CIARLETTA, C. AUBURTIN. *Rssi Positioning Technics in Networks*, in "RESCOM 2010", GIENS France, 06 2010, http://hal.inria.fr/inria-00547474/en/.

Scientific Books (or Scientific Book chapters)

[26] J. FRANÇOIS, H. ABDELNUR, R. STATE, O. FESTOR. *Semi-Supervised Fingerprinting of Protocol Messages*, in "Computational Intelligence in Security for Information Systems 2010", Springer-Verlag, 11 2010, vol. 85, p. 107-115 [*DOI :* 10.1007/978-3-642-16626-6_12], http://hal.inria.fr/inria-00536067/PDF/cisis10.pdf.

Research Reports

[27] H. ABDELNUR, R. STATE, J. L. OBES, O. FESTOR. *Spectral Fuzzing: Evaluation & Feedback*, INRIA, Feb 2010, RR-7193, http://hal.inria.fr/inria-00452015.

[28] F. BECK, A. BOEGLIN, O. FESTOR. *High Security Laboratory - Network Telescope Infrastructure Upgrade*, INRIA, 11 2010, http://hal.inria.fr/inria-00538922/PDF/Technical_Report_LHS_Telescope_Upgrade.pdf.

[29] F. BECK, I. CHRISMENT, O. FESTOR. *Automatic IPv4 to IPv6 Transition - D2.1 Metric and Addressing Algorithm*, INRIA, 06 2010, http://hal.inria.fr/inria-00531207/PDF/deliverable-2.1.pdf.

[30] F. BECK, I. CHRISMENT, O. FESTOR. *Automatic IPv4 to IPv6 Transition D2.2 - Transition Engine Specification and Implementation*, INRIA, 06 2010, http://hal.inria.fr/inria-00531208/PDF/deliverable-2.2.pdf.

[31] F. BECK, I. CHRISMENT, O. FESTOR. *Automatic IPv4 to IPv6 Transition D3.1 - Secured Transition Engine*, INRIA, 06 2010, http://hal.inria.fr/inria-00531209/en/.

[32] A. BOEGLIN, A. LAHMADI, O. FESTOR. *SecSIP Technical Documentation*, INRIA, 10 2010, n^{o} RT-0393, http://hal.inria.fr/inria-00524247/PDF/RT-0393.pdf.

[33] A. BOEGLIN, A. LAHMADI, O. FESTOR. *SecSIP User Documentation*, INRIA, 07 2010, n^{o} RT-0394, http://hal.inria.fr/inria-00547831/en/.

[34] T. CHOLEZ, I. CHRISMENT, O. FESTOR, G. DOYEN, R. KHATOUN, J. DROMARD. *Etat de l'art : Réseaux pair à pair, supervision, sécurité et approches collaboratives*, INRIA, 10 2010, http://hal.inria.fr/inria-00533385/en/.

[35] L. CIARLETTA, S. GROSJEAN. *Co-simulation : étude et réalisation d'un prototype Application à la reconstruction 3D à partir d'imagerie vidéo*, INRIA, 09 2010, http://hal.inria.fr/inria-00547464/en/.

[36] L. DELOSIÈRES. *Filtrage collaboratif des Spams SMS*, INRIA, 06 2010, http://hal.inria.fr/inria-00547379/en/.

[37] 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 Ð April 30, 2010*, INRIA, 2010, http://hal.inria.fr/inria-00546369/en/.

[38] O. FESTOR, G. DREO, D. HAUSHEER, G. PAVLOU, A. PRAS, R. SADRE, J. SERRAT, J. SCHOENWAELDER, B. STILLER. *EMANICS Quarterly Management Report #16*, INRIA, 2010, http://hal.inria.fr/inria-00546398/en/.

[39] O. FESTOR, G. DREO, D. HAUSHEER, G. PAVLOU, A. PRAS, R. SADRE, J. SERRAT, J. SCHOENWAELDER, B. STILLER. *EMANICS Quarterly Management Report #17*, INRIA, 2010, http://hal.inria.fr/inria-00546402/en/.

[40] C. HÉNARD. *Détection des attaques sur le réseau pair-à-pair KAD*, INRIA, 08 2010, http://hal.inria.fr/inria-00546151/en/.

[41] T. LECLERC, L. CIARLETTA, L. REYNAUD, A. SCHAFF. *Prototype d'architecture de découverte de service avancée*, INRIA, 02 2010, http://hal.inria.fr/inria-00546977/en/.

[42] C. E. MESSAOUD. *Génération automatique des règles de protection VeTo pour les services voix sur IP*, INRIA, 06 2010, http://hal.inria.fr/inria-00547397/en/.

[43] E. NATAF, O. FESTOR, G. GÉRARD. *Réalisation d'un plug-in Eclipse pour supporter le langage YANG*, INRIA, 06 2010, http://hal.inria.fr/inria-00539966/en/.

[44] R. YACINE, M. NASSAR, D. TASOS, O. FESTOR, A. PANAYIOTIS, P. GEORGE, G. CHRISTOS. *SCAMSTOP : Scams and Fraud Detection in Voice over IP Networks FP7 contract number: 232458 D2.2 General anti-Fraud security framework for VoIP infrastructures*, INRIA, 11 2010, http://hal.inria.fr/inria-00537985/en/.

Other Publications

[45] M. BARRERE, R. BADONNEL, O. FESTOR. *Towards Vulnerability Prevention in Autonomic Environments*, 11 2010, Internal working document, http://hal.archives-ouvertes.fr/hal-00545594/en/.

[46] O. DABBEBI, R. BADONNEL, O. FESTOR. *A Generalized Modelling for Supporting Risk Management in VoIP Infrastructures*, 04 2011, Internal working document, http://hal.archives-ouvertes.fr/hal-00545588/en/.

[47] O. DABBEBI, R. BADONNEL, O. FESTOR. *Self-Configuring Risk Models in VoIP Architectures*, 07 2011, Internal working document, http://hal.archives-ouvertes.fr/hal-00545589/en/.

[48] V. GURBANI, E. BURGER, T. ANJALI, H. ABDELNUR, O. FESTOR. *The Common Log Format (CLF) for the Session Initiation Protocol (SIP) - draft-gurbani-sipclf-problem-statement-00*, 02 2010, Draft, http://hal.inria.fr/inria-00546445/en/.

[49] V. GURBANI, E. BURGER, T. ANJALI, H. ABDELNUR, O. FESTOR. *The Common Log Format (CLF) for the Session Initiation Protocol (SIP) - draft-gurbani-sipclf-problem-statement-01*, 01 2010, Draft, http://hal.inria.fr/inria-00546437/en/.