INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team Madynes

Management of Dynamic Networks and Services

Nancy - Grand Est

THEME COM

Table of contents

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

This report covers the group activity and publications from January, 1st 2008 to December 31th, 2008.

1. Team

Research Scientist

Olivier Festor [Team Leader, Research Director (DR), INRIA, HdR]
Radu State [Researcher Associate (CR) INRIA (-09/2008)]

Faculty Member

Isabelle Chrisment [Professor, ESIAL, Henri Poincaré - Nancy 1 University, HdR]
Laurent Andrey [Associate Professor, Nancy 2 University]
Rémi Badonnel [[Associate Professor, ESIAL, Henri Poincaré - Nancy 1 University]
Laurent Ciarletta [Associate Professor, ENSMN - Lorraine National Polytechnic Institute]
Jacques Guyard [Professor[1], ESIAL, Henri Poincaré - Nancy 1 University, HdR]
Abelkader Lahmadi [ATER, ENSMN - Lorraine National Polytechnic Institute (-08/2008)]
Emmanuel Nataf [Associate Professor, Nancy 2 University]
André Schaff [Professor[2], ESIAL,Henri Poincaré - Nancy 1 University, HdR]

Technical Staff

Frédéric Beck [Engineer, Industrial grant]
Balamurugan Karpagavinayagam [Engineer,INRIA associate engineer program (-08/2008)]

PhD Student

Mohamed Nassar [MEN grant, since 10/2005]
Humberto Jorge Abdelnur [Industrial grant with regional co-sponsorship (01/2006-)]
Jérôme François [CNRS BDI grant with regional co-sponsorship (10/2006-)]
Cristian Popi [Industrial grant with regional co-sponsorship (10/2006-)]
Thibault Cholez [Industrial grant with regional co-sponsoship (10/2007-)]
Julien Siebert [MADYNES-MAIA cooperation. Industrial grant with regional co-sponsoship (10/2007-)]
Tom Leclerc [Industrial grant with regional co-sponsoship (10/2007-)]
GÃ©rard Wagener [Co-tutelle with University of Luxembourg (10/2007-)]

Administrative Assistant

Caroline Suter [Project Assistant, INRIA (-02/2008)]
Isabelle Slota [Project Assistant, INRIA (02/2008-03/2008)]
Maria Plancy [Project Assistant, INRIA (04/2008-07/2008)]
Isabelle Blanchard [Project Assistant, INRIA(07/2008-08/2008]
Christelle Wagner [Project Assistant, INRIA (08/2008-)]

Other

Sheila Becker [Ms Degree Internship, Nancy University (02/2008-07/2008), co-tutelle Ph.D. since 10/2008]

2. Overall Objectives

2.1. Introduction

Keywords: *automated management*, *benchmarking*, *dynamic environments*, *management frameworks*, *mobile device management*, *monitoring*, *network management*, *provisioning*, *security*, *service configuration*, *service management*, *telecommunications*.

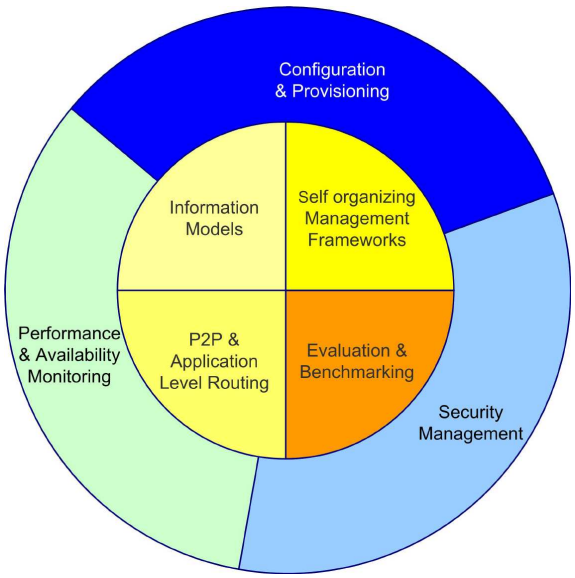

Figure 1. The MADYNES research themes

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 research activities in the following areas (see Figure 1):

- **Autonomous Management** (inner circle of Figure 1):
  - 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 modelling and **performance evaluation** of management infrastructures and activities.
- **Functional Areas** instanciate autonomous management functions (outer circle of Figure 1):
  - 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.

[1] Due to its administrative duties at the University, Jacques Guyard could not contribute to the activity of the team in 2008
[2] Due to its administrative duties at the University, AndrÃ© Schaff could not contribute to the activity of the team in 2008

2.2. Highlights of the year

2008 has seen two scientific highlights in our contributions to the security of Voice over IP systems.

The first highlight is the design and implementation of a novel approach to perform fingerprinting of devices into a network. The approach is based on the analysis of the structure of messages rather than relying only on the content of the data fields. A patent has been filled on this new approach and a demonstrator has been built. In late 2008, the approach and it evaluations were presented at RAID'2008.

The second highlight of 2008 is the design of a novel approach to detect unusual and attack traffic in the Voice over IP signaling plane. We built a very efficient algorithm based on Support Vector Machines operating over 38 features of a SIP service slice. This model was succesfully tested against large SIP traces and has demonstrated real-time capabilities. The algorithm has also been presented at the RAID'2008 conference.

A third highlight of 2008 is the outstanding evaluation received for this second year activity by the EMANICS network of excellence from the European Commission. This project that we manage received the highest mark a project can get out of a review. Along the same track, we have scored high in the new collaborative project proposals we were involved in, having all accepted in the various calls we submitted to.

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[3] 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.

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] Fault, Configuration, Accounting, Performance and Security

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 establish 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 configuration and constraints while we study XML-based protocols for coordinating distribution and synchronization. Off and online validation of configuration data is also part of this effort.

3.3.3. Performance and availability monitoring

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

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

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

4. Application Domains

4.1. Mobile, ad-hoc and constrained networks

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

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

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

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

4.2. Dynamic service infrastructures

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

The target service environments are:

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

5. Software

5.1. KiF

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

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

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

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

5.2. Voip Bots

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

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

- send SPAM over IP Telephony (SPIT),
- distributed denial of service through intensive issuance 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. 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 Autoconfiguration (RFC 2461 and RFC 2462) have been identified and integrated in the tool. An XML file describes the default behavior of the network, with the authorized routers and prefixes, and a second XML document containing the neighbors database is used. This second file can be filled during a learning phase. All NDP activities are logged in the syslog utility, and so the attacks, but these ones are also reported by mail to the administrator. Finally, NDPMon can detect stack vulnerabilities, like the assignment of an Ethernet broadcast address on an interface.

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

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

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

6. New Results

6.1. Protocol fuzzing and fingerprinting

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

Fuzzing refers to the generation and injection of random and malicious data into applications in oder to discover vulnerabilities in their implementations. We were the first to develop a stateful technique capable of revealing vulnerabilities in deep states of a protocol implementation. In 2008, we have extended our stateful fuzzing model with a modular scenario support engine. This enables the fuzzing process to be easily extended with new scenarios written in Python. Another direction we have followed is the use of the fuzzer for intensive fuzzing activities, i.e. fuzzing activities that require high number of messages to be sent over short periods of time to a given device. To enable such scenarios we have developed a scenario definition language and the corresponding processing engine that enables the pre-generation of large set of tests which can be assembled in a very efficient way to send fuzzing messages at a very high rate. Using the framework, we continued our search for/and discover ed multiples vulnerabilities. Related publications are [14], [9].

A second activity which complements fuzzing in security assement models is fingerprinting. In the context of structured text-based protocols, we have designed a new fingerprinting approach which is able to learn a device fingerprint from analysis of its traces independently of the actual content of the data fields. This is done by focusing exclusively on the structure of the message itself. Having such a set of signatures from a device, the system is able to build a discrimination database to identify on a network those devices for which it knows the signature. Large evaluations have shown excellent results in terms of both accuracy and efficiency. A patent for this model has been filled and a prototype is operational [51]. It uses large grid infrastructures to build the signature database. Once this database is ready, the actual fingerprint is done on a single message. The approach was intensively tested on SIP signalling to identify VoIP devices. The model and underlying algorithms were presented at the RAID'2008 conference [13].

Starting from vulnerabilities identified at the SIP protocol specification level during the fuzzing process on VoIP devices, we cooperate with the CASSIS team at INRIA to formally verify the thruthfulness of these vulnerabilities and assess the efficiency of the counter measures we propose. We did this exercice on one authentication stealing vulnerability we discovered in the "on-hold" sub-protocol. We have shown through the formal specification in HPSL and the validation with AVISPA that the vulnerability is real and part of the specification. We have also been able to proove that the proposed change we introduce, i.e. the creation of a dedicated `RE-INVITE` service primitive to avoid usage ambiguities, enables the resolution of the problem and avoids any further occurrence of the discovered vulnerability. The results were published in [12].

6.2. Risk management

Participants: RÃ©mi Badonnel [contact], Sheila Becker, Olivier Festor, Radu State.

The main research challenge addressed in our work consisted in measuring the risk and assessing defensive techniques in P2P communication infrastructures. We consider a variant of a gossip like P2P communication protocol that is implemented in current malware (Slapper worm) and show how risk analysis can be applied in this context.The main result consists in casting the communication mechanism in a game theoretical framework and assessing defensive/offensive strategies with the well known Nash equillibrum concept. We proposed two measures for assessing P2P communication infrastructures. These measures have correspondent in the classical telecommunication networks and represent the blocking probability and respectively delay related characteristics. We have proposed a game theoretical approach for the study of both defensive and attack strategies against such network, where the payoff function is based on the blocking probability. We have computed the Nash equilibriums for several scenarios and were capable to derive optimal attack and defensive strategies. Our framework is instanciated for the specifics of an existing P2P communication paradigm used by the Slapper worm. This work has been published in [34].

Our work can be extended to multiple other target infrastructures, like for instance in critical ad-hoc and P2P communication environments. We plan to address also other P2P communication architectures, where P2P SIP will of major importance due to the ongoing evolution of the current Voice/IP communication paradigms.

6.3. Management models and architectures

Participants: Laurent Andrey [contact], Abdelkader Lahmadi, Olivier Festor, Cristian Popi.

Since its start in 2004, the team maintains an activity on the design of new management models and architecture. While less important in terms of efforts in 2008, this activity continued in three directions. One of them is related to performance evaluation of management systems on building performance model for management applications. We worked on a model to adequately characterize delays in management requests [26]. We did also design and evaluate a queuing theory-based network model of an agent-manager system.

The second investigation targets management architectures for wireless ad-hoc and wireless MESH networks. The first architecture we built enables the monitoring and collection of topology (in terms of neighborhood) among nodes participating in an ad-hoc network. The data collection architecture uses a distributed hash table to store in a distributed way the topology information and a retrieval service has been built on top [30], [21]. In configuration management, we investigated the use of a combined Netconf/CIM/Ldap chain to configure in a centralized way wireless mesh networks. A prototype for router configuration has been developed in the context of the AirNet project. Finally, we did invetigate stochastic models to monitor flow data in wireless mesh networks. We studied several models ranging from random decision of per flow monitoring to coordinated decision among probes with both accuracy and efficiency objectives. This final activity is still in an early stage.

6.4. Autonomic management

Participants: Rémi Badonnel [contact], Olivier Festor.

Autonomic management has become a major paradigm for dealing with the growing complexity of systems and networks, and simplifying their maintenance. Autonomic servers are capable of managing themselves based on closed control loops in order to: (1) configure their components, (2) detect and correct their failures, (3) monitor and control their own resources in an optimal manner, (4) identify and protect themselves against attacks. These servers can typically be deployed in data centers and provide multi-tier applications and services on a voluntary manner. Their autonomic property poses new challenges with respect to the support and composition of services.

In that context, we have investigated the issue of supporting services amongst autonomic servers by exploring the benefits of a voluntary load-balancing strategy. This work is part of a strong cooperation with the research team of Mark Burgess at the Oslo University College. We have shown how this strategy can transfer the authoritative decision from the load-balancer to the servers in the system [15]. This approach is particularly appropriate for autonomic servers such as servers implementing the Cfengine maintenance tool developed by Mark Burgess. We have modeled this strategy using the promise theory framework and have specified how to implement it based on two architectural solutions. We have quantified the performances of our approach through an extensive set of experiments. We have compared these results to traditional strategies in various scenarios with homogeneous and heterogeneous servers [16]. We have also evaluated its scalability when adding extra servers in the system, experimentally and theoretically (analysis of promise graphs). Khereiddine Messai has also experimented an alternative hybrid load balancing strategy [48] and has shown the convergence to similar results in the case of autonomic servers.

Another major issue we have addressed is the orchestration of services in such environments. We have presented with Ustun Yildiz (INRIA ECOO Team) a new service orchestration model conceived for uncertained infrastructures [23]. The most innovative aspect of the proposed model is that it bridges the gap between two orthogonal dimensions of management. The contribution consists of the consideration of two main layers. The first layer provides information about the behavior of autonomic servers in the infrastructure. The second layer quantifies the interested aspects of a process specification with respect to service selection criteria.

Two outcomes of respective layers are used to characterize the adequacy of nodes for the orchestration. We have evaluated the extent to which the uncertainty model is useful in evaluating the availability of composed services where they subject different behavior in service repositories.

Autonomic management systems require that the autonoic plane is fed with accurate data about the underlying managed network and supported services. We are contributing to this activity by investigating the applicability of several known algorithms to automatically discover service dependencies in an enterprise network while looking only at flow information collected from standard flow probes like Netflow. We have shown that a dynamic adaptation of the discovery engine switching from a start-time only discovery algorithm to a flow containment one depending on network load highly increases the discovery accuracy while working fine with flows and thus avoiding any issue related to payload inspection of pre-required knowledge [47].

6.5. Pervasive computing

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

Pervasive Computing, where a growing number of computing devices are collaborating to provide users with enhanced and ubiquitous services, is a domain that we are currently exploring. It has a lot of different requirements. The following ones are specifically related to the work done within Madynes:

- an adaptable yet high level of security is needed since these computing devices should be working in such a way common users trust themselves,
- pervasive computing is high technology seamlessly woven into our everyday life: therefore it requires autoconfiguration and reconfiguration of its elements and networks,
- the technologies need to be evaluated not only per domain, but on a larger scale, where end-user concerns are also taken into account. We are still pursuing our investigations on this domain and have been working more specifically on two prospects:
- multi-models of these Pervasive computing environments (including the users in the modelisation and the simulations). We have been focusing on the collaborative simulations of dynamic networks/elements, namely P2P (soon to be extended to adhoc networks) using agents to drive those simulations [22], [27], [31], this work is done in collaboration with the MAIA team,
- State of the art on Service Discovery protocols, contextual metrics in adhoc networks, and Service Discovery in adhoc networks using an hybrid between cluster-like (WCPD) and MPR-based (OLSR) broadcasting [19].

6.6. Voice over IP Security

Participants: Humberto Abdelnur, RÃ©mi Badonnel, Mohamed Nassar, Olivier Festor, Radu State.

VoIP inherits the adjacent security problems associated with the IP as well as new VoIP specific ones. Attackers can profit from the vulnerabilities of the VoIP protocols and architectures. Both signaling protocols such as SIP (Session Initiation Protocol) and H.323 and media transport protocols such as RTP and RTCP could be the target of a wide set of attacks, ranging from eavesdropping, denial of service, fraudulent usage and SPIT (Spam over internet telephony).

Important work in both host and network intrusion detection has already been done by the industrial and academic research community, focused in scope towards network intrusion detection for transport, routing and application level protocols. Security assessment techniques and approaches have been deployed in the operational landscape and had been the subject of the research community. However, specific approaches for VoIP are still an incipient stage and our work was motivated to leverage existing conceptual solutions for the VoIP specific application domain.

Our research work addressed three main directions. The first is concerned with automated security assessment and penetration testing for SIP implementations. There we mainly worked on VoIP fuzzing as described in the protocol fuzzing and fingerprinting section.

The second direction of our research on Voice over IP security did target intrusion detection systems for this service. We proposed a novel online monitoring approach able to distinguish between attacks and normal activity in SIP based Voice over IP environments. The solution builds on the monitoring of 38 features in VoIP flows and on Support Vector Machines for the classiÃcation part. We did validate our proposal through large online experiments performed over a mix of real world traces from a large VoIP provider and attacks locally generated on our own testbed. Results show high accuracy to detect SPIT and flooding attacks even in the presence of very limited data sets for the learning phase. The solution has shown promising performance for an online deployment [20].

The third is oriented towards protecting customers from unsollicited profiling. Monitoring methods and techniques can be applied to VoIP traffic in order to profile and track network users. We have proposed in [44] a counter-measure approach for preventing this VoIP profiling. We have described the underlying architecture and defined several noise generation functions capable to dynamically generate fake VoIP messages in order to deteriorate the profiling performances. We have evaluated the benefits and limits of this approach through experimental results obtained in the case scenario of PCA (Principal Component Analysis) profiling methods.

6.7. Distributed and adaptive revocation mechanism for Peer-to-Peer networks

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

With the increasing deployment of P2P networks, supervising the malicious behaviours of participants, which degrade the quality and performance of the overall delivered service, is a real challenge. We proposed a fully distributed and adaptive revocation mechanism based on the reputation of the peers [24] (best paper award) and [17]. The originality of our approach is that the revocation is integrated in the core of the P2P protocol and does not need complex consensus and cryptographic mechanisms, hardly scalable. The reputation criteria evolve with the contribution of a peer to the network in order to highlight and help fight against selfish or malicious behaviours.

We have also implemented our revocation mechanism within the KAD network. KAD is a part of the popular eMule and aMule file-sharing applications. It is based on the Kademlia protocol and is one of the widest deployed structured P2P network with millions of simultaneous users. To do that, we have introduced different modifications in the KAD client.

This prototype was deployed on several nodes in EmanicsLab in order to evaluate the performances and the feasibility of our solution. The experiment consisted in measuring the time needed to retrieve a reputation according to the number of replications.

We showed that latencies are proportional to the number of accounts and as search time is limited (160s), all possible accounts are not found but only around 2/3. Our preliminary results have also confirmed that the user perceived latencies are not highly impacted.

We are currently focusing on the Sybil attack, where a node can create fake identifiers and take the control over the network. We study and evaluate the protection mechanisms against the Sybil attack that are implemented in KAD.

6.8. Malware models

Participants: Olivier Festor, Jérôme François [contact], Radu State.

The malware communication techniques are efficient and scalable. For instance, an attacker can control several thousands of machines by creating a botnet. In 2008 we continued to investigate the usability of this model for the management plane [18], [25]. The first major result that we obtained in this area was the characterization of robustness of botnets built on different communication models : IRC and P2P. We continue to work on the modeling of botnets and are investigating several methods to take them down. One of the approach we took in 2008 was built on fuzzing methods to attack botnets. We investigated this approach towards the Storm botnet and succeeded through this approach in stopping temporarely the activity of infected nodes while we failed in taking them down permanently. This activity also enabled us to collect useful traces of Storm activity as part of High Security Lab described in the next section.

A second direction we follow towards botnet modeling is based on protocol learning. The objective there is to be able to automated the learning of an unknown protocol to ease both its modeling and later fuzzing. To this end we are investigating the use of several classification methods to address the first part of a protocol learning process, namely message classification. Early results show good results using a combination of Support Vector Clustering and K-means clustering algorithms while Support Vector Machines are much less efficient when applied to an unencrypted protocol like SIP. The work based in Support Vector Machines is done in strong cooperation with Yann Guermeur, head of the ABC team at LORIA.

6.9. High Security Lab Telescope

Participants: FrÃ©dÃ©ric Beck [contact], Olivier Festor.

The objective of the High Security Lab at INRIA Nancy Grant Est is to provide both the infrastructure and the legal enveloppe 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 2008, we did design and set up the whole telescope. Build enterely around Open Source components, the telescope hosts more than 80 sensors continuously collecting data on several networks including ADSL lines. The telescope is extended with a small cluster that allows the deployment and execution of malware, thus the collection of operational traces. The full specification of the telescope is publicly available [33].

As of today, more than 100.000 malwares are collected by the telescope and we have large sets of network data available for analysis and investigation (62 GBytes of pcap traces and 872 MBytes of Netflow records). As part of the network traces, we isolated full Storm activities which, once anonymized were used by our industrial partners to evaluate their security solutions agains this specific worm.

7. Contracts and Grants with Industry

7.1. EMANICS

Participant: Olivier Festor [contact].

Dates January 2006 - December 2009

Partners 12 european universities and one financial institute

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

EMANICS is now running for three years and has reached many great successes in the area of researchers and community integration, joint research results, outstanding publications quality and score, standard contributions, operational testbeds, visibility and recognition. Details on the networks and its achievements can be found on the networks Web site at: http://www.emanics.org. Evaluated in march 2008, 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 even exceeded expectations.

In addition to the management and animation of the network [37], [36], [35], [40], [38], we did contribute in 2008 in the activities related to the EMANICS virtual laboratory [42], Open Source developments coordination and support [41], scalable management as well as autonomic management.

7.2. INRIA-ALU joint lab

Participants: Humberto Abdelnur, Laurent Andrey, RÃ©mi Badonnel, Olivier Festor [Contact].

Dates July 2008 - December 2011

Partners Alcatel Lucent, INRIA.

We have established a common laboratory with the Alcatel-Lucent team on network security. This activity is part of the broader joint initiative on Autonomic networks.

Our activity in this joint lab focuses on the automation of vulnerability management. It includes activites on fuzzing, concerned with 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 the link between vulnerability management and risk in the VoIP sphere. The objective there is to be able to design a rela time risk management model for voice oriented critical services.

In 2008, we focused our efforts on the extension of the fuzzing framework. This has resulted in the desing of a new function in KiF able to do intensive fuzzing through the use of pre-generated test cases. The environment has been installed on the Alcatel premises in november 2008.

7.3. AIRNET

Participants: Olivier Festor [contact], Cristian Popi.

Dates June 2006 - May 2009

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

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

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

In 2008, we designed a topology monitoring architecture able to log topology evolution over time in a fully distributed way. This monitoring architecture is also currently under investigation for flow monitoring in similar networks. We also did implement the basic building blocks to favour a YANG/Netconf-based configuration support in wireless mesh networks. These building blocks include : a YANG toolkit and the porting of YENCAP on a wireless mesh network. We also studied alternative configuration models based on CIM/LDAP schemes.

7.4. SARAH

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

Dates February 2007 - January 2010

Partners INRIA Lorraine (MADYNES), INRIA Rocquencourt (HIPERCOM) , LRI, LIP6, TELECOM SudParis (ex INT), Ucopia, Orange Labs (ex France TÃ©lÃ©com R&D)

SARAH is an ANR (Agence Nationale pour la Recherche, French National Research Agency) collaborative research project, in the area of Pervasive Computing. It aims at 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 information provided by service discovery protocols and follow Pervasive Computing requirements :

- ubiquitous availability,
- context awareness,
- self adaptation to the users' needs (the technology adapts and is available to provide services to the user and not the other way around)
- disappearing computing (discreetly, almost naturally embedded in our daily environment)
- ease of use.

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

We contribute to the following activities of the project :

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

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

7.5. MAPE

Participants: Isabelle Chrisment [contact], Thibault Cholez.

Dates January 2008 - December 2010

Partners LIP6-CNRS UPMC Paris 6, Mitsubishi Electric ITE-TCL, INRIA Nancy Grand-Est (MADYNES), France Télécom R&D

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

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

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

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

In 2008, we focused on the revocation mechanism within the KAD network and more specifically on the using of the sybil attack to achieve P2P active measurement.

8. Other Grants and Activities

8.1. International relationships and cooperations

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

In 2008, we were heavily involved in the setup of seven new cooperative research programs targetting either a bilateral basis (industrial partner + MADYNES), or seeking funding at the national level (ANR or DGA calls) or at the European level(FP7 calls). All six submissions succeeded but due to the leave of one team member, we had to cancel our participation from two of the selected projects and the french partners of the CELTIC project we were in, are the only ones not being funded. Two of the four projects we stayed in did already start in 2008 (the bilateral research project with Cisco and the one with Alcatel-Lucent). The other two (one ANR and one FP7 project) will start in early 2009.

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

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

8.2. National initiatives

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

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

Isabelle Chrisment participated in an evaluation commission as expert for the French Research Agency (ANR).

8.3. Mobility

In 2008, the team launched a supporting campaign to encourage its members to increase international cooperations. This has led to two mobilities in the team : Olivier Festor spent one month at the Univeristy of Twente in july 2008 and Radu State joined the University of Luxembourg in october 2008 for a long sabbatical.

Natenapa Sriharee, an ERCIM fellow from NTNU spent a week in october in the team working with Laurent Ciarletta on service discovery.

Ari Takanen, foudner of Codenomicon spend two days in the team exchanging on fuzzing.

9. Dissemination

9.1. Program committees and conference organization

In 2008, Radu State was technical program committee member for: IEEE/IFIP Network Operations and Management Symposium (NOMS 2008), IFIP/IEEE Distributed Systems Operations and Management (DSOM 2008), IEEE IPTCOMM 2008. He also served as publication chair for NOMS'2008 and TCP co-chair of IEEE IPTCOMM 2008.

Isabelle Chrisment was member of the following technical program committees : ACM/IEEE/IFIP AIMS'2008 (International Conference on Autonomous Infrastructure, Management and Security), MWNS'08 (International Workshop on Mobile and Wireless Networks Security) NOTERE 2008. She was also member of the steering committee of SARSSI 2008.

In 2008, Olivier Festor was member of the following program committees: IEEE/IFIP Network Operations and Management Symposium (NOMS 2008), IFIP/IEEE Distributed Systems Operations and Management (DSOM 2008), IFIP EUNICE'2008, ACM/IEEE/IFIP AIMS'2008, CFIP'2008, RESCOM'2008.

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

9.2. Teaching

There is a high demand on networking courses in the various universities to which the LORIA belongs. This puts high pressure on the 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, DEUG, bachelor, master, ESIAL and École des Mines de Nancy engineering schools or DEA (master research). In this section, we only enumerate the courses that are directly related to our research activity.

Within the Master degree, SDR (Distributed Services and Networks) specialization, Isabelle Chrisment and Olivier Festor are in charge of the course entitled *Routing and Organization within Dynamic Networks*. This course is one of the three foundation courses given to the students that follow a research cursus in Networking in Nancy; Isabelle Chrisment and Radu State are in charge of the course entitled *Security within Dynamic Networks* at the Masters in Computer Science level. Radu State is also giving three advanced courses on Network Security, one entitled *Systems and Network Security* given at the ESIAL Engineering School and at the Masters in Computer Science level, a second course entitled *Viral and Worm Epidemiology* given at the Masters in Computer Science level, and a course entitled *Introduction to Network Security* given at the Bachelor in Computer Science level.

Isabelle Chrisment is heading the Telecommunications and Networks specialization of the 3rd year at the ESIAL[4] engineering school and in charge of the students recruitement process. She also teaches the networking related courses in this cursus.

Olivier Festor and Emmanuel Nataf are in charge of the *Network and Service Management* course and Radu State teaches network security and wireless communications at the masters degree level.

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

Laurent Ciarletta is in charge of Advanced Networking, Middleware, Pervasive Computing and Systems courses at the Ecole des Mines de Nancy (Master degree level).

Several MADYNES Ph.D. Students gave various course in the area of networking, Java, Web-services and XML technologies, Service Oriented Architectures, Design patterns in most universities and engineering schools associated with the LORIA.

9.3. Tutorials, invited talks, panels, presentations

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

- Humberto Abdelnur and Radu State gave an talk on VoIP Fuzzing at the SCHMOCOON 2008 event in Washington in February 2008.
- Olivier Festor gave a tutorial on VoIP vulnerabilities at the University of Twente in July 2008.
- Olivier Festor gave a tutorial on the High Security Lab architecture at the University of Twente in July 2008.
- Olivier Festor gave a presentation on dynamic dependencies discovery using flow data at the October 30th IRTF-NMRG Meeting in Munich.
- Radu State gave a tutorial with labs on Web2.0 security at the EMANICS 2008 Summer School [11].

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

- Rémi Badonnel and Laurent Andrey gave a tutorial inluding labs on service monitoring using Nagios at the 2008 EMANICS Summer School [52].
- Olivier Festor is member of the panel on that will take place during the Future Internet Assembly in Madrid on december 9 and 10, 2008.
- Isabelle Chrisment gave a presentation on IPv6 renumbering monitoring at JTR 2008, Nancy, France, June 2008.
- Fredéric Beck gave a presentation on the NDPMon tool at JTR 2008, Nancy, France, June 2008.

9.4. Commissions

Team members participated to the following Ph.D. commissions:

- Nicolas BERNARD, Ph.D. in Computer Science from Université du Luxembourg, Luxemburg and Ph.D. in Computer Sicence from UniversitÃ© Joseph Fourrier de Grenoble, France. title: *Non-observabilitÃ© des communications Ã faible latence our Comment Alice peut-elle chatter avec Bob sans qu'Eve et Mallory le sachent*, september 2008. (Olivier FESTOR)
- Gonzales PIETRO, Ph.D. in Computer Science from KTH Royal Institute of Technology, Stockholm, Sweden. Title *Adaptative Real-time Monitoring for Large-scale Networked Systems*, November 2008. (Olivier FESTOR)
- Matthieu KACZMAREK Ph.D. in Computer Science from INPL, France. Title: *Des fondements de la virologie informatique vers une immiunologie formelle*, December 2008. (Olivier FESTOR)
- Anderson SANTANA DE OLIVEIRA, Ph.D. in Computer Science from Toulouse III University, Paul Sabatier, France. Title: *Méthodologie de conception de systèmes temps réel et distribués en contexte UML/SysML*, January 2008. (Isabelle CHRISMENT)
- Anderson SANTANA DE OLIVEIRA, Ph.D. in Computer Science from Nancy University, Henri Poincaré University, Nancy 1, France. Title: *Réécriture et modularité pour les politiques de sécurité*, March 2008. (Isabelle CHRISMENT)
- Khaled MASMOUDI, Ph.D. in Computer Science from Telecom Sud Paris, France. Title: *Gestion de la confiance dans les réseaux personnels*, April 2008. (Isabelle CHRISMENT)
- Maryna KOMAROVA, Ph.D. in Computer Science from Telecom Paris, Ecole Nationale des Télécommunications, France. Title: *Fast Authentication and Trust-Based Access Control in Heterogeneous Wireless Network*, May 2008. (Isabelle CHRISMENT)
- Sara del Socorro MOTA GONZALEZ, Ph.D. in Computer Science from Institut Polytechnique de Toulouse, France. Title: *Modélisation et vérification de protocoles pour des communications sécurisées de groupes*, June 2008. (Isabelle CHRISMENT)
- Ustun YILDIZ, Ph.D. in Computer Science from Nancy University, Henri Poincaré University, Nancy 1, France. Title: *Décentralisation des procédés métiers : qualité de services et confidentialité*, 8th September, 2008. (Isabelle CHRISMENT)
- Diala ABI HAIDAR, Ph.D. in Computer Science from Telecom Bretagne, Rennes 1 University, France. Title: *Web Service Access Negotiation*, 27th November 2008. (Isabelle CHRISMENT)

MADYNES members were members of the following Habilitation Degree commissions:

- FranÃ§ois CHAROY, Habilitation Degree in Computer Science from Nancy UniversitÃ©. Title: *Coordination explicite d'activitÃ©s coopÃ©ratives*, june 2008. (Olivier FESTOR)
- Marcello DIAS DE AMORIN, Habilitation Degree in Computer Science from Université Pierre et Marie Curie - Paris 6. Title: *Mobile multi-hop wireless networks: Conceptual and practical concerns*, october 2008. (Olivier FESTOR)
- Toufik AHMED, Habilitation Degree in Computer Science from UniversitÃ© Bordeaux 1. Title: *Transport Adaptatif et ContrÃ´le de la QualitÃ© de Services VidÃ©o sur les RÃ©seaux IP Filaires, Sans-fil et sur les Architectures P2P*, november 2008. (Olivier FESTOR)
- StÃ©phane FRÃ©NOT, Habilitation Degree in Computer Science from UnivesitÃ© Claude Bernard de Lyon. Title *Intergiciels systÃ¨mes pour passerelles de services ambiants*, december 2008. (Olivier FESTOR)

10. Bibliography

Major publications by the team in recent years

[1] R. BADONNEL, R. STATE, O. FESTOR. *Using Information Theoric Measures for Detecting Faulty Behavior in Ad-Hoc Networks*, Technical report, Jun 2005.

[2] M. S. BOUASSIDA, I. CHRISMENT, O. FESTOR. *An Enhanced Hybrid Key Management Protocol for Secure Multicast in Ad Hoc Networks*, in "Third International IFIP-TC6 Networking conference - NETWORKING 2004, Athenes, Greece", N. MITROU, K. KONTOVASILIS, N. ROUSKAS (editors), Lecture Notes in Computer Science, vol. 3042, Springer-Verlag, May 2004, p. 725-742.

[3] I. CHRISMENT. *Maîtrise de la dynamique dans l'Internet - de l'adaptation des protocoles à la sécurité des services*, Habilitation à Diriger des recherches, Université Henri Poincaré - Nancy I, Oct 2005.

[4] V. CRIDLIG, R. STATE, O. FESTOR. *Role-Based Access Control for XML Enabled Management Gateways*, in "15th IFIP/IEEE Distributed Systems: Operations and Management - DSOM 2004, Davis, CA, USA", A. SAHAI, F. WU (editors), Lecture notes in Computer Science, vol. 3278, Springer, UC Davis, Nov 2004, p. 183-195.

[5] G. DOYEN, E. NATAF, O. FESTOR. *A hierarchical architecture for a distributed management of P2P networks and services*, in "16th IFIP/IEEE Distributed Systems : Operation and Management - DSOM'05, Barcelona, Spain", Oct 2005.

[6] O. FESTOR. *Ingénierie de la gestion de réseaux et de services : du modèle OSI à la technologie active*, Habilitation à Diriger des recherches, UHP-Nancy 1, Dec 2001.

Year Publications

Articles in International Peer-Reviewed Journal

[7] R. BADONNEL, R. STATE, O. FESTOR. *Self-Configurable Fault Monitoring in Ad-Hoc Networks*, in "Ad-Hoc Networks", 2008, http://hal.inria.fr/inria-00153604/en/.

[8] M. S. BOUASSIDA, I. CHRISMENT, O. FESTOR. *Group Key Management in MANETs*, in "International Journal of Network Security", vol. Volume 6, 2008, p. pp. 67-79, http://hal.inria.fr/inria-00167843/en/.

Articles in National Peer-Reviewed Journal

[9] H. ABDELNUR, O. FESTOR, R. STATE. *Fuzzing dans la sphère VoIP*, in "MISC - Le journal de la sécurité informatique", 2008, http://hal.inria.fr/inria-00337663/en/.

Invited Conferences

[10] F. BECK. *Outils de supervision pour IPv6*, in "JTR 2008 - IPv6: Réalité et Perspectives, France Nancy", 2008, http://hal.inria.fr/inria-00323777/en/.

[11] R. STATE. *Hacking AJAX and WEB2.0*, in "EMANICS summer school, Suisse Zurich", 2008, http://hal.inria.fr/inria-00338143/en/.

International Peer-Reviewed Conference/Proceedings

[12] H. ABDELNUR, T. AVANESOV, M. RUSINOWITCH, R. STATE. *Abusing SIP Authentication*, in "Information Assurance and Security (ISIAS) Information Assurance and Security, 2008. ISIAS '08., Italie Naples", IEEE, 2008, p. 237-242, http://hal.inria.fr/inria-00326077/en/.

[13] H. ABDELNUR, R. STATE, O. FESTOR. *Advanced Network Fingerprinting*, in "Recent Advances in Intrusion Detection Lecture Notes in Computer Science Computer Science, États-Unis d'Amérique Boston", A. TRACHTENBERG (editor), vol. Volume 5230/2008, Springer Berlin / Heidelberg, MIT, 2008, p. 372-389, http://hal.inria.fr/inria-00326054/en/.

[14] H. ABDELNUR, R. STATE, O. FESTOR. *Fuzzing for vulnerabilities in the VoIP space*, in "17th EICAR Annual Conference 17th EICAR Annual Conference, France Laval", European Institute for Computer Antivirus Research, 2008, http://hal.inria.fr/inria-00326086/en/.

[15] R. BADONNEL, M. BURGESS. *Dynamic Pull-Based Load Balancing for Autonomic Servers*, in "International Network Operations and Management Symposium, 2008 (IEEE NOMS 2008), Brésil Salvador", C. WESTPHALL, M. BRUNNER (editors), IEEE Press, Mehmet Ulema and José Marcos Nogueira, 2008, http://hal.inria.fr/inria-00325237/en/.

[16] R. BADONNEL, M. BURGESS. *Service Load Balancing with Autonomic Servers: Reversing the Decision Making Process*, in "Second International Conference on Autonomous Infrastructure, Management and Security - AIMS 2008 Resilient Networks and Services Lecture Notes in Computer Science, Allemagne Bremen", D. HAUSHEER, J. SCHÖNWÄLDER (editors), vol. 5127, Springer, Jacobs University of Bremen, 2008, p. 92-104, http://hal.inria.fr/inria-00325232/en/.

[17] T. CHOLEZ, I. CHRISMENT, O. FESTOR. *A Distributed and Adaptive Revocation Mechanism for P2P networks*, in "ICN 2008, Mexique Cancun", 2008-04, p. pp. 290-295, http://hal.archives-ouvertes.fr/hal-00323990/en/.

[18] J. FRANÇOIS, R. STATE, O. FESTOR. *Towards malware inspired management frameworks*, in "Network Operations and Management Symposium IEEE/IFIP Network Operations and Management Symposium 2008, Brésil Salvador", 2008, p. 105-112, http://hal.inria.fr/inria-00310913/en/.

[19] T. LECLERC, L. CIARLETTA, A. ANDRONACHE, S. ROTHKUGEL. *OLSR and WCPD as Basis for Service Discovery in MANETs*, in "The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies - UBICOMM'08, Espagne Valencia", IEEE, 2008, p. 184-190, http://hal.inria.fr/inria-00334479/en/.

[20] M. E. B. NASSAR, R. STATE, O. FESTOR. *Monitoring SIP traffic using Support Vector Machines*, in "11th International Symposium on Recent advances in intrusion detection - RAID 2008 Recent Advances in Intrusion Detection Lecture Notes in Computer Science, États-Unis d'Amérique Boston", E. K. RICHARD LIPPMANN, A. TRACHTENBERG (editors), vol. 5230, Springer, 2008, p. 311-330, http://hal.inria.fr/inria-00325290/en/.

[21] C. POPI, O. FESTOR. *A Scheme for Dynamic Monitoring and Logging of Topology Information in Wireless Mesh Networks*, in "IEEE/IFIP Network Operations and Management Symposium, Brésil Salvador, Bahia", IEEE, 2008, p. 759 - 762, http://hal.inria.fr/inria-00326053/en/.

[22] J. SIEBERT, V. CHEVRIER, L. CIARLETTA. *Entwined influences of users'behaviour and QoS: a multi-model approach.*, in "Second International Conference on Autonomous Infrastructure, Management and Security - AIMS 2008, Allemagne Bremen", SPRINGER (editor), David Hausheer and Jürgen Schönwäl, 2008-07-04, p. 175-179, http://hal.archives-ouvertes.fr/hal-00326003/en/.

[23] U. YILDIZ, R. BADONNEL, C. GODART. *On service orchestration in mobile computing environments*, in "The 5th IEEE International Conference on Services Computing, SCC, États-Unis d'Amérique Honolulu", IEEE Computer Society, IEEE, 2008, p. 545-548, http://hal.inria.fr/inria-00304346/en/.

National Peer-Reviewed Conference/Proceedings

[24] T. CHOLEZ, I. CHRISMENT, O. FESTOR. *Un mécanisme de révocation distribué et adaptatif pour les réseaux pair-à-pair*, in "JDIR 2008, France Villeneuve d'Ascq", 2008-01-16, 87, http://hal.archives-ouvertes.fr/hal-00323940/en/.

[25] J. FRANÇOIS, R. STATE, O. FESTOR. *Les botnets et la supervision à large échelle*, in "9èmes Journées Doctorales en Informatique et Réseaux - JDIR 2008, France Lille", 2008, 10, http://hal.inria.fr/inria-00274977/en/.

[26] A. LAHMADI, L. ANDREY, O. FESTOR. *Caractérisation de la variation des délais dans les applications de supervision de réseaux et de services*, in "9èmes Journées Doctorales En Informatique et Réseaux - JDIR'08, France Villeneuve d'Ascq", 2008, http://hal.inria.fr/inria-00337569/en/.

[27] J. SIEBERT, V. CHEVRIER, L. CIARLETTA. *Modélisation multimodèle des réseaux dynamiques : cas des réseaux pair-à-pair*, in "9èmes Journées Doctorales en Informatique et Réseaux - JDIR'08, France Villeneuve d'Ascq", 2008-01-18, ?, http://hal.archives-ouvertes.fr/hal-00202453/en/.

Workshops without Proceedings

[28] F. BECK, I. CHRISMENT, O. FESTOR. *Supervision de la procédure de renumérotation IPv6*, in "JTR 2008 - IPv6: Réalité et Perspectives, France Nancy", 2008, http://hal.archives-ouvertes.fr/hal-00338200/en/.

[29] T. CHOLEZ, I. CHRISMENT, O. FESTOR. *Talk: A Distributed and Adaptive Revocation Mechanism for P2P Networks.*, in "1st EMANICS Workshop on Peer-to-Peer Management, Suisse Zurich", 2008, http://hal.inria.fr/inria-00338220/en/.

[30] C. POPI, O. FESTOR. *Monitorage et journalisation dynamiques des topologies dans les réseaux ad-hoc*, in "Colloque Francophone sur lIngénierie des Protocoles - CFIP 2008, France Les Arcs", 2008, http://hal.archives-ouvertes.fr/hal-00250235/en/.

[31] J. SIEBERT. *Agent-based modelization for p2p networks*, in "1st Emanics P2P Workshop, Suisse Zurich", 2008, http://hal.inria.fr/inria-00338217/en/.

Scientific Books (or Scientific Book chapters)

[32] H. SCHULZRINNE, R. STATE, S. NICCOLINI. *Principles, Systems and Applications of IP Telecommunications. Services and Security for Next Generation Networks / Second International Conference, IPTComm 2008 Heidelberg, Germany, July 1-2, 2008 Revised Selected Papers*, vol. 5310, Springer, 2008, http://hal.inria.fr/inria-00338144/en/.

Research Reports

[33] F. BECK, O. FESTOR, R. STATE. *High Security Laboratory - Network Telescope*, Rapport Technique, 2008, http://hal.inria.fr/inria-00337568/en/.

[34] S. BECKER. *Security Evaluation for P2P Communication Systems*, Stage, 2008, http://hal.inria.fr/inria-00338660/en/.

[35] O. FESTOR, G. DREO RODOSEK, G. PAVLOU, A. PRAS, J. SCHOENWAELDER, J. SERRAT, D. HAUSHEER, R. SADRE, B. STILLER. *D0.10 : Quarterly Management Report 10*, Contrat, 2008, http://hal.inria.fr/inria-00337626/en/.

[36] O. FESTOR, G. DREO RODOSEK, G. PAVLOU, A. PRAS, J. SCHOENWAELDER, J. SERRAT, D. HAUSHEER, B. STILLER. *D0.11 : Quarterly Management Report 11*, Contrat, 2008, http://hal.inria.fr/inria-00337630/en/.

[37] O. FESTOR, G. DREO RODOSEK, G. PAVLOU, A. PRAS, J. SCHOENWAELDER, J. SERRAT, R. STATE. *D0.8 : Quaterly Management Report 8*, Contrat, 2008, http://hal.inria.fr/inria-00337633/en/.

[38] O. FESTOR, G. DREO RODOSEK, G. PAVLOU, A. PRAS, J. SCHOENWAELDER, J. SERRAT, R. STATE, B. STILLER. *EMANICS Periodic Activity Report January 1, 2007 December 31, 2007*, Rapport de recherche, 2008, http://hal.inria.fr/inria-00337640/en/.

[39] O. FESTOR, G. DREO RODOSEK, G. PAVLOU, A. PRAS, J. SCHOENWAELDER, J. SERRAT, R. STATE, B. STILLER. *Joint Programme of Activities (month 25-42) for the EMANICS Network of Excellence*, Contrat, 2008, http://hal.inria.fr/inria-00337637/en/.

[40] O. FESTOR, G. PAVLOU, A. PRAS, J. SCHOENWAELDER, J. SERRAT, G. DREO, B. STILLER, R. SADRE, D. HAUSHEER. *D0.9 : Quaterly Management Report 9*, Contrat, 2008, http://hal.inria.fr/inria-00337624/en/.

[41] O. FESTOR, J. SCHOENWAELDER, F. BECK, D. HAUSHEER, C. MORARIU, T. BOCEK, F. HECHT, D. PERIC. *EMANICS Open Source Support and Joint Software Development Intermi Report*, Rapport de recherche, 2008, http://hal.inria.fr/inria-00337649/en/.

[42] O. FESTOR, J. SCHOENWAELDER, H. M. TRAN, C. MORARIU, F. EYERMANN, I. TUMAR, D. HAUSHEER, B. KARPAGAVINAYAGAM, T. BOCEK. *EMANICS Virtual Laboratory Integration Report*, Contrat, 2008, http://hal.inria.fr/inria-00337643/en/.

[43] O. FESTOR, R. STATE, H. M. TRAN, J. SCHOENWAELDER. *EMANICS Large scale Management Interim Report*, Contrat, 2008, http://hal.inria.fr/inria-00337650/en/.

[44] K. HAMLAOUI. *Mesures et Contre-Mesures Pour la Voix sur IP*, Stage, 2008, http://hal.inria.fr/inria-00337581/en/.

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

[46] A. LAHMADI, O. FESTOR. *Design and Development of a Stateful Firewall for SIP-based Networks*, Rapport de recherche, 2008, http://hal.inria.fr/inria-00337570/en/.

[47] S. MEHRI. *Découverte et analyse de dépendances dans les réseaux IP*, Stage, 2008, http://hal.inria.fr/inria-00338201/en/.

[48] K. MESSAI. *Supervision et Autonomie dans les Réseaux et Services*, Stage, 2008, http://hal.inria.fr/inria-00337595/en/.

[49] E. NATAF. *Data Link Layer Protocol Simulator User Guide*, RR-6417, Rapport Technique, 2008, http://hal.inria.fr/inria-00205027/en/.

[50] E. NATAF. *IP Simulator User Guide*, RR-6416, Rapport Technique, 2008, http://hal.inria.fr/inria-00205033/en/.

Other Publications

[51] H. ABDELNUR, O. FESTOR, R. STATE. *Moniteur de système de ommunication par messages amélioré*, n^{o} 07/08946, 2008-01-07, http://hal.inria.fr/inria-00338196/en/.

[52] L. ANDREY, R. BADONNEL. *An Introduction to Monitoring with Nagios*, 2008, http://hal.inria.fr/inria-00338224/en/.

[53] F. BECK, O. FESTOR, I. CHRISMENT. *NDPMon: ARPwatch pour IPv6*, 2008, http://hal.inria.fr/inria-00337578/en/.