IN PARTNERSHIP WITH:
CNRS

Université de Lorraine

Activity Report 2011

Project-Team MADYNES

Management of dynamic networks and services

IN COLLABORATION WITH: Laboratoire lorrain de recherche en informatique et ses applications (LORIA)

RESEARCH CENTER
Nancy - Grand Est

THEME
Networks and Telecommunications

Table of contents

Project-Team MADYNES

Keywords: Ambient Computing, Monitoring, Network Protocols, Peer-to-Peer, Security, Self-Management

1. Members

Research Scientist

Olivier Festor [Team Leader, Research Director (DR) 20% of his time since November 1st, 2011, 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

Alexandre Boeglin [Engineer, Industrial grant]
Mohamed Nassar [Research Engineer, Industrial grant (-08/2011)]
Cyril Auburtin [Engineer, Industrial grant (-11/2011)]
Andrea Oroseanu [Engineer, Industrial grant (-06/2011)]

PhD Students

Sheila Becker [Co-tutelle with University of Luxembourg (10/2008-)]
Martin Barrere [Industrial grant (01/2011-)]
Oussema Dabbebi [Industrial grant (10/2009-)]
Tom Leclerc [Industrial grant with regional co-sponsoship (-09/2011)]
Julien Siebert [MADYNES-MAIA cooperation. Industrial grant with regional co-sponsoship (-09/2011)]
Juan Pablo Timpanaro [Industrial grant with regional co-sponsoship (01/2010-)]
Gérard Wagener [Co-tutelle with University of Luxembourg (-09/2011)]

Administrative Assistant

Céline Simon [INRIA]

2. Overall Objectives

2.1. Overall Objectives

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.

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.

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.

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

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 modeling 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. 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.

5.2. SecSIP

Participants: Abdelkader Lahmadi [contact], Olivier Festor.

SecSip [2] is developed by the team to defend SIP-based (The Session Initiation Protocol) services from known vulnerabilities. It presents a proactive point of defense between a SIP-based network of devices (servers, proxies, user agents) and the open Internet. Therefore, all SIP traffic is inspected and analyzed against authored Veto specification before it is forwarded to these devices. When initializing, the SecSIP runtime starts loading and parsing authored VeTo blocks to identify different variables, event patterns, operations and actions from each rule. It implements an input and output layer, to capture, inject, send and receive SIP packets from and to the network. Intercepted packets are moved to the SIP Packet parser module. The main function of this module is to extract different fields within a SIP message and trigger events specified within the definition blocks. During each execution cycle when a SIP message arrives, the SecSIP runtime uses a data flow acyclic graph network to find definition matching rules and triggers defined events. The paired events in each operator node are propagated over the graph until a pattern is satisfied. When the pattern is satisfied, the respective rule is fired and the set of actions is executed.

SecSIP is freely available on the Internet and has been demonstrated in various High Security Labs exhibits in 2011.

5.3. NDPMon

Participants: Isabelle Chrisment, Olivier Festor [contact].

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.

[2] http://secsip.gforge.inria.fr/doku.php

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.

5.4. AA4MM

Participants: Laurent Ciarletta, Julien Siebert [main developer].

This work has been undertaken in a joint Phd Thesis between the Madynes and MAIA Teams. Vincent Chevrier (MAIA team, LORIA) has been the co-advisor of this PhD and correspondant for this software.

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. It is written in Java and relies upon Java Messaging Services (JMS) for its distributed version.

AA4MM can be downloaded at http://www.loria.fr/~siebertj/aa4mm/index.html.

5.5. MASDYNE

Participants: Laurent Ciarletta, Julien Siebert [main developer].

This work is undertaken in a joint Phd Thesis between the Madynes and MAIA Teams. Vincent Chevrier (MAIA team, LORIA) has been co-advisor of this PhD and correspondant for this software.

Other contributors to this software are: Tom Leclerc (Madynes), Francois Klein, Christophe Torin, Marcel Lamenu, Guillaume Favre and Amir Toly.

MASDYNE (Multi-Agent Simulator of DYnamic Networks usErs) is a multi-agent simulator for modeling and simulating users behaviors in mobile ad hoc network. This software is part of joint work with MAIA team, on modeling and simulation of ubiquitous networks.

It has been notably coupled with a network simulator (JANE : Java Adhoc Network Development Environment) to advanced behavior capabilities to standard network simulations.

6. New Results

6.1. Behavioral Fingerprinting

Participant: Olivier Festor [contact].

Device fingerprinting aims to automatically determine the types (name and version of software, brand name and series of hardware) of remote devices for a given protocol. Hence, keeping an up-to-date inventory database of devices in use on a network is possible and helpful as for example to check remotely if unauthorized applications have been installed. Some types of devices for which vulnerabilities are known can be easily detected in order to patch them or at least send alerts to the owners. From a security point of view, attackers use specific tools to perform their attack which may also be detected rapidly thanks to fingerprinting. Most current systems rely only on signatures of differences in implementation of a given protocol stack and signatures are often outdated.

We have designed a new fingerprinting scheme that is accurate even on protocol stacks that are completely identical, but which run on hardware having different capabilities (CPU power, memory resources, etc). Our fingerprinting scheme can learn distinctive patterns in the state machine of a particular implementation. We see such a pattern as a restricted tree finite state machine that provides additional time-related information about the transitions performed [15]. The captured identification models were then used to automatically build attack prevention rules [19].

This work was done in cooperation with Jérôme Francois, Radu State and Thomas Engel from the Univeristy of Luxembourg.

6.2. Management and monitoring of P2P networks

Participants: Isabelle Chrisment [contact], Olivier Festor, Juan Pablo Timpanaro.

Content pollution is one of the major issues affecting P2P file sharing networks. However, since early studies on FastTrack and Overnet, no recent investigation has reported its impact on current P2P networks. In [21], we presented a method and the supporting architecture to quantify the pollution of contents in the KAD network. We first collected information on many popular files shared in this network. Then, we proposed a new way to detect content pollution by analyzing all filenames linked to a content with a metric based on the Tversky index and which gives very low error rates. By analyzing a large number of popular files, we showed that 2/3 of the contents are polluted, one part by index poisoning but the majority by a new, more dangerous, form of pollution that we call index falsification. This work was done, in collaboration with the University of Technology of Troyes, within the context of the ACDA-P2P[3] Project funded by GIS- 3SGS[4].

BitTorrent is a widely deployed P2P file sharing protocol, extensively used to distribute digital content and software updates, among others. Recent actions against torrent and tracker repositories have fostered the move towards a fully distributed solution based on a distributed hash table to support both torrent search and tracker implementation. We conducted an analysis on one of the BitTorrent's DHT (Mainline DHT) and developed a monitoring architecture, so as to measure and discover security flaws on the network. In [23] we compared KAD DHT against BitTorrent DHT in terms of security by deploying different attacks on the network. We showed that the lack of security in Mainline DHT allows very efficient attacks that can easily impact the operation of the whole network. We also provided a peer-ID distribution analysis of the network, so as to adapt previous protection schemes to the Mainline DHT. The mechanisms are assessed through large-scale experiments on the real DHT-based BitTorrent tracker.

If BitTorrent's Mainline DHT is exposed to several identified security issues, in parallel, the KAD DHT has been the core of intense research and was improved over years. We presented a study that motivates the integration of both worlds. We provided a performance comparison of both DHTs in terms of publishing efficiency. We investigated the security threats and showed that the current BitTorrent's Mainline DHT is more vulnerable to attacks than KAD while the download service of BitTorrent has much better performance. Given the strengths and weaknesses of both DHTs, we designed a hybrid architecture [24], which is based on KAD's indexation mechanism and BitTorrent download protocol. On the one hand, the client is able to index its files in the well-known KAD DHT, taking advantage of KAD's security mechanism and its double-indexation scheme. On the other hand, the client uses the BitTorrent download protocol so as to download a given file, which has been proven to surpass KAD's. We implemented this hybrid architecture, that we called `hMule`, as a unified KAD-BitTorrent file-sharing application , which is compatible with both P2P file sharing networks and provides the KAD advantages on indexation and the BitTorrent speed for transfer without losing backward compatibility.

We started our research about being anonymous when downloading from BitTorrent. We conducted a set of measurements from High Security Lab aiming to characterize the usage of the I2P network, a low-latency anonymous network based on garlic routing [35]. Our goal was to answer the following questions: what is the network used for? when is it used the most? which kind of applications the network designers should pay

[3] Approche Collaborative pour la Détection d'Attaques dans les réseaux Pair à Pair

[4] Groupement d'Intérêt Scientifique - Surveillance, Suretê et Sécurité des grands Systêmes

more attention to? We designed a distributed monitoring architecture for the I2P network and we showed that, through three one-week long experiments, we were able to identify 32% of all running applications, among web servers and file-sharing clients. Additionally, we identified 37% of published I2P applications, which turned out to be unreachable after their publication on the I2P distributed database.

In parallel, we built-up a model of I2P encryption/decryption approach and using the Avispa tool, we able to find a possible attack on the network. Further work will be focused on probing right and on developing a proof-of-concept of this.

6.3. Configuration security automation

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

The main research challenge addressed in this work has focused on enabling configuration security automation in autonomic networks and services. In particular our objective has been to increase vulnerability awareness in the autonomic management plane in order to prevent configuration vulnerabilities. The continuous growth of networking significantly increases the complexity of management. It requires autonomic networks and services, which are capable of taking in charge their own management by optimizing their parameters, adapting their configurations and ensuring their protection against security attacks. However, the operations and changes they execute during these management activities may generate vulnerable configurations. A first part of our work has therefore consisted in consolidating a security automation strategy for preventing vulnerabilities and maintaining safe configurations in autonomic infrastructures [7]. This solution relies on the integration of configuration vulnerability descriptions into the management plane [8]. The OVAL language, part of the SCAP protocol, has become the de-facto standard for specifying configuration vulnerabilities in a technical viewpoint. We have refined a mathematical modeling for mapping OVAL descriptions into policy rules which can be interpreted by the autonomic Cfengine configuration system. These policies enable the Cfengine system to assess and detect vulnerabilities. We have designed a functional architecture and formalized a translation algorithm for supporting this security automation. We have also prototyped an OVAL-to-Cfengine translation module, called Ovalyzer, and analyzed its interactions with the components of the Cfengine system. Based on vulnerability descriptions extracted from the official OVAL repository, we have performed an extensive set of experiments to quantify the performance and coverage of the Ovalyzer module. A second part of our work has consisted in investigating how our security automation solution can be extended to distributed configuration vulnerabilities. In SCAP-based traditional approaches, a distributed vulnerability is typically understood as the aggregation of individual configuration vulnerabilities which are spread in the network and might allow a multi-step attack. We have shown through the analysis of a case study that this definition does not offer a complete outlook of the problem. In particular, each network device can individually present a secure configuration, but when combined across the network, a global vulnerable configuration may be produced. In that context, we have introduced in [27] a mathematical definition for distributed vulnerabilities and have specified the DOVAL language (Distributed OVAL), on top of OVAL, as a means for describing these vulnerabilities in a machine readable manner. A case study in the area of VoIP networks and services has been considered for demonstrating the instantiation of DOVAL main constructs. The DOVAL descriptions constitute useful security definitions that in turn can be exploited for security automation. We have built a framework for supporting these distributed configuration vulnerabilities based on the Cfengine system. In particular, we have proposed and evaluated collaborative strategies and optimized algorithms for performing the assessment of DOVAL descriptions.

6.4. Online Risk Management

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

Telephony over IP has known a large scale deployment and has been supported by the standardization of dedicated signaling protocols. This service is however exposed to multiple attacks due to a lower confinement in comparison to traditional PSTN networks. While a large variety of methods and techniques has been proposed for protecting VoIP networks, their activation may seriously impact on the quality of such a critical service. Risk management provides new opportunities for addressing this challenge. In particular, our work aims at performing online risk management for VoIP networks and services. The purpose is to adapt the service exposure with respect to the threat potentiality, while maintaining a low security overhead. Based on the classification of VoIP attacks and the analysis of their properties, we have refined in [11] an extended risk modeling for IP telephony infrastructures. This modeling permits to cover a large spectrum of security attacks. It supports our online risk management strategy which is capable of dynamically activating or deactivating security safeguards in the VoIP infrastructure. The mitigation is based on the control of the service exposure using these safeguards. We have compared our solution to other traditional strategies, and have quantified the benefits and limits according to multiple performance criteria. We have also analyzed the impact of the risk model parameters on our mitigation, and showed to what extent the parameterization can be partially automated in [12]. An important part of our efforts has focused in the year 2011 on extending our online risk management strategy to more distributed configurations [32]. While our initial work was centered around Asterisk-based enterprise networks, we have taken a particular interest in P2PSIP networks. They constitute an open decentralized solution where the registration and location servers are implemented by a distributed hash table responsible for storing the bindings between the address-of-record SIP-URI and the contact SIP-URI. We have identified different attack sources and attack scenarios in these P2PSIP networks, considering the functional roles that are played by the SIP peers. The security threats are specific to the P2PSIP protocol or are the result of inheritance from the SIP layer and the peer-to-peer area. In that context, we have analyzed the instantiation of our online risk modeling by taking into account the properties and components of the P2PSIP architecture, and have established a portfolio of dedicated countermeasures, including replication-based an certification-based techniques. We have evaluated the strategy performance and scalability through an extensive set of experiments performed with the OMNET++ simulator. We also have quantified the complementarity of our solution with the RELOAD security framework which relies on a central certificate enrolment server.

6.5. VoIP Security

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

In previous work, we have proposed the prevention system SecSIP [5] for SIP-based networks which uses a rule-based approach to build prevention specifications on SIP protocol activities that stop attacks exploiting an existing vulnerability before reaching their targets. We have pursued our efforts in VoIP security which led to two new contributions:

- Building and maintaining prevention rules using the VeTo language can become a time consuming and error prone task, especially when addressing an important number of vulnerabilities discovered using a fuzzing tool. The discovered vulnerabilities using such process are usually based on a single exploit message with a malformed field or sequence of vulnerable messages. To reduce this effort, we have designed a generation method to produce VeTo specifications targeting those vulnerable messages. The method mainly characterizes a malformed field within an exploit message or the vulnerable sequence of messages and generates a set of VeTo rules specifications to prevent their exploit. The generated VeTo rules are then deployed and maintained on the SecSIP engine to be applied against the SIP traffic. The solution [19] relies on generating rules using genetic algorithms operating on a a set of candidate regular expressions to match a malformed pattern within a SIP message, and evaluate their quality using a well defined fitness function to ensure that their are specific enough to only match exploit messages.
- SecSIP uses a plain text configuration file in which VeTo specifications are authored and managed manually. While extending the deployment of the framework beyond our own lab, support for remote configuration was required. Given the promise of Netconf, we naturally turned our investigations towards this protocol and embraced the YANG data-modeling framework. In [20] we have presented the Yang model built for VeTo policies and the Netconf framework put in place.

We have developed a flexible SIP honeypot. It is flexible in the sense that a behavior can be externally and easily defined. The goal of such a honeypot is to be able to be quickly customized in response to an observation made on a more generic and large scale honeypot. If the initial observation is likely to be an attack the customized honeypot would eventually get deeper and more informative interactions with the attacker. The realization is a module of the Dionaea general framework for honeypot (successor of the well-known nepenthes framework) and we use the SIPP test tool as an engine to animate SIP interactions provided as automata in some XML file. More detail on the implementation can be found in [26].

6.6. VoIP Fraud

Participants: Olivier Festor [Contact], Mohamed Nassar.

In the context of a cooperation with the University of Liege, we have addressed the problem of SPIT from a new perspective [22]. Based on end-user feedback, we have proposed a scheme for generating SPIT signatures from the SIP INVITE messages. Hence it is possible to filter the next SPIT calls before ringing their destinations. The generated SPIT signatures are adaptive to the benign signaling traffic in the sense that they do not conflict with it. The generation of signatures is based on supervised machine learning techniques. We namely investigated decision trees with categorical at- tributes obtained by parsing the SIP messages.

Our system works in two modes: a batch and an online mode. The batch mode consists on training the decision tree over a labeled (spit, normal) data-set and then trans- forming the tree into an if-else rule-set. In online mode, the successive learnt signatures are aggregated and the possible conflicts are resolved. Experimentation on off-the-shelf SPIT tools showed the efficiency of our approach to find the good signatures. However, experiments show that the J48 decision tree is easily defeated using some obfuscation techniques. We therefore proposed a generalisation approach to translate the tree into an if-else rule-set shows instead good robustness against such attacks. The overall framework provides suitable performance for operational deployment in terms of learning time, required memory, size of 18the rule-set and the call setup delay. The different parameters of the system (i.e. size of the different buffers and windows) are easily configurable.Different SPIT signatures may imply different SPIT capabilities. For example, a spitter may break a Captcha test by bruteforcing a DTMF guess. Another spitter may start talking by a human-like congratulation in order to bypass a Turing test. One of the goals of our approach is to provide a framework for applying reinforcement learning techniques and hence increasing the efficiency of the filtering process. The reinforcement learning aims at selecting the best challenge to be used when a given SPIT signature is detected. Basically the re-inforcement learning maintains a table matching each signature with the best challenge response discovered so far. The table is continuously updated using a trial and error scheme.

We did validate the approach on multiple data-sets otbained from Voice over IP operators members of the SCAMSTOP project.

6.7. Pervasive computing

Participants: Laurent Ciarletta [contact], Tom Leclerc, Julien Siebert, Olivier Festor, André Schaff.

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 focusing on the networking aspects of ubiquitous systems. We cooperate with the Maia (and Trio) team(s) to be able to encompass issues and research questions that combine both networking and cognitive aspects.

Pervasive Computing is about interconnected and situated computing resources providing us(ers) with contextual services. These systems, embedded in the fabric of our daily lives, are complex: numerous interconnected and heterogeneous entities are exhibiting a global behavior impossible to forecast by merely observing individual properties. Firstly, users physical interactions and behaviors have to be considered. They are influenced and influence the environment. Secondly, the potential multiplicity and heterogeneity of devices, services, communication protocols, and the constant mobility and reorganization also need to be addressed. Our research on this field as detailed in [10] is going towards both closing the loop between humans and systems and taming the complexity, using multi-modeling (to combine the best of each domain specific model) and co-simulation (to design, develop and evaluate) as part of a global conceptual and practical toolbox.

In 2011 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 extensively described in the PhD thesis of Julien Siebert [3].
- Study of service discovery protocols, contextual metrics in adhoc networks, and Service Discovery in adhoc networks using an hybrid model between cluster-like (WCPD) and MPR-based (OLSR) broadcasting. The results have been extensively described in the PhD thesis (Contributions for Advanced Service Discovery in Ad hoc Networks) of Tom Leclerc [2]. In this thesis, we consider service discovery in MANETs, that are a collection of devices that communicate with each other over a wireless medium. Such networks are formed spontaneously whenever devices are in transmission range without any preexisting infrastructure. The main characteristic of MANETs is the high dynamics of nodes (induced by the users moving around), the volatile wireless transmissions, the user behavior, the services and their usage. We've proposed a complete solution for service discovery in ad hoc networks, from the underlying network up to the service discovery itself. A first contribution, is the Stable Linked Structure Flooding (SLSF) protocol that creates stable based cluster structure and thereby provides scalable and efficient message dissemination. The second contribution is the Stable Linked Structure Routing (SLSR) protocol that uses the SLSF dissemination structure to enable routing capabilities. Using those protocols as basis, we propose to improve service discovery by additionally considering context awareness and adaptation.
- Context awareness and mobility/usage models

  We contributed on improving simulations by coupling simulators and models that, together, can model and simulate the variety and richness of ad hoc related usage scenarios and their human characteristic. A guideline for all of our contributions was to be able to integrate and/or consider context and context awareness in both the proposed protocols and the related research tools and models. On one hand, The proposed protocols all have the capacity to adapt their efforts according to certain metrics, that represent the context. The simulator coupling architecture, on the other hand, permits to model and design scenarios in which the context, such as the service usages or the human behavior, has an impact and matters.
- Energy-constraint geolocalization, addressing, routing and management of wireless devices: a research collaboration with Fireflies RTLS was started in March 2009 and is ongoing. The initial work has been extended in a joint work with the TRIO Team and leads towards finding a global energy-cost function, and life expectancy of the wireless sensor system.

In the future work, we plan to apply those results to Cyper Physical Systems, within the Aetournos (Airborne Embedded auTonomOUs Robust Network of Objects and Sensors) platform at Loria. We aim at developing cross-layer solutions to robust routing between flying drones.

We are also working inside a CPER project towards management solutions of wireless network sensors (project ECOSUR) used to control Smart Spaces.

6.8. Co-Simulation and multi-modeling

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

Vincent Chevrier (MAIA team, LORIA) and Tomas Navarette are external collaborators.

6.8.1. Multiagent approach for multimodeling and simulation coupling.

Participants: Laurent Ciarletta [contact], Julien Siebert.

Vincent Chevrier (MAIA team, LORIA) is an external collaborator.

this work has been extensively detailed in Julien Siebert's PhD thesis [3] and partially in Tom Leclerc's , with an application to ubiquitous adhoc networks and services.

This work has been done between the fields of ubiquitous networks and multi-agent based simulation. The main context is to study mutual influences existing between ubiquitous network performances and their users behaviours. We have highlighted the need for reusing and coupling modelling and simulation softwares together in order to simultaneously integrate several abstraction levels in the study. We target those needs by a multiagent approach and we propose a metamodel : AA4MM. The core idea in AA4MM is to build a society of models, simulators and simulation softwares that solves the core challenges of multimodelling and simulation coupling in an homogeneous perspective. AA4MM major contributions are the possibility to easily reuse, to make interoperable and modular existing heterogeneous models and softwares, to manage scale changes and a simulation algorithm fully decentralized. We apply this metamodel to the field of ubiquitous networks in order to target the question of mutual influences between networks performances and users behaviours.

6.8.2. Adaptive control of a complex system based on its multi-agent model

Participants: Laurent Ciarletta [contact], Julien Siebert.

Vincent Chevrier (MAIA team, LORIA) and Tomas Navarette are external collaborators and main investigators of this theme.

As a starting point, 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 in environment where collective behaviors can emerge [6]. We did comparison of five different models. These models are built upon the same individual behavior hypothesis of a collective phenomenon present in peer-to-peer file exchange networks: "free-riding". We studied a global analytical model and four multi-agent models. Multi-agent models include the space and time dimensions rarely seen in the literature discussing aggregated models of the collective phenomenon in question. We have demonstrated that one individual decision algorithm can lead to contradictory information.

Using these results, we want to build a control mechanism for a complex/dynamic system. Specifically, we want to evaluate the effectiveness of creating a control mechanism based on a multi-agent model of the system.

Multi-agent models can be adapted to that purpose since usual approaches using analytical models as a basis can be intractable when dealing with such systems; and if we consider that the available control actions are meant to be applied locally, a multi-agent model is necessary. We are currently working on a case study within the dynamic networks domain, namely the free-riding phenomenon present in peer-to-peer networks.

We propose an architecture that gathers information from the system and uses it to parametrize and tune a set of multi-agent models. The outcome of simulations is used to decide which control actions have to be applied to the system, in order to achieve a predefined control objective. We consider that we do not have complete information to characterize the state of the system.

6.9. Sensor networks management

Participants: Cyril Auburtin, Alexandre Boeglin, Olivier Festor, Abdelkader Lahmadi, Emmanuel Nataf [contact].

6LowPAN networks denotes many embedded devices interconnected by a variety of links ranging from wireless technologies such as 802.15.4, bluetooth, Low Power Wifi to wired technologies such as low power PLC. The common property of such networks is the limited resources of their nodes in terms of power, computing, memory and communication. The network could be described with thousands of devices with very limited internal and external resources and their communication channels are low-bandwith, high loss rate and volatile links subject to failure over time. These networks rely on the 6LowPAN protocol defined by the IETF as an adaptation layer for the IPv6 protocol to address their low power and lossy properties.

During the year 2011, we have started a research activity around the monitoring and security assessment of 6LowPAN networks. Our contributions are mainly as follows:

- We are developing a novel approach to assign monitoring roles in 6LowPAN networks using available local information provided by the routing layer. The resulting monitoring architecture is adaptive taking benefit from the reactivity of the routing protocol when dynamic changes occur due to connectivity or nodes mobility. Our first simulations results reveal that our assignment approach is more efficient, less aggressive and less resources consuming than its competitors.
- We have also designed and implemented a piggybacking technique to deliver monitoring report into existing packets traveling through 6LowPAN networks. In our solution, we have extended the IPv6 Hop-by-Hop extension header with a new option which contains status data of monitored nodes. This technique can reduce the number of packets and bytes sent across the network since there is no specific monitoring packets competing with existing traffic. Monitoring data shares the routing path of application data packets until it reaches a management node. We have applied our piggybacking technique to discover coap-enabled management agents. Each agent in the deployed wireless sensor network piggybacks its identifier into the RPL routing protocol messages until it reaches a manager node.
- Regarding security management of these networks, we have developed a stateless fuzzing tool for the 6LowPAN protocol [28]. The tool is build upon the Scapy packets manipulation library. It provides different mutation algorithms to be applied on 6LowPAN messages. These messages are defined by interaction scenarios described in an XML format.
- Related also to security, we have modelled an ontology for intrusion detection system in sensor networks [17]. The model exposes family of intrusions depending on their objectives. The service provided by the network, the communication channels and the security mechanisms are the main classes of the model.

6.10. High Security Lab

Participants: Alexandre Boeglin [contact], Olivier Festor, Mohamed Nassar.

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.

During the year 2011, some maintenance tasks have been carried out on the High Security lab:

- the SDSL line, which previously had a capacity of 1Mbps, has been upgraded to a 2Mbps line, and traffic shaping rules have been added to the router, that allow honeypots to run alongside experiments, without impacting them,
- the storage capacity of our database server, which was starting to get full, has been multiplied by four, and existing data has been migrated to the new equipment.

A set of new experiments have also been deployed:

- a server has been dedicated to a new variant of SGNet, for the VAMPIRE project. This one specifically targets attacks on SIP services, which the other one cannot do,
- in collaboration with the INRIA Nancy Grant Est IT service, we started to log public (thus anonymous) DNS queries and responses made by the research center's recursive DNS servers, to use the collected data as input set for experiments.

In 2011 we worked also on the automated analysis of malware taces to extract flow-level signatures of malware. We obtained early results regarding network flow-graphs and tested several clustering techniques to separate malware traffic.

6.11. Sensas

Participants: Cyril Auburtin, Alexandre Boeglin [contact], Olivier Festor.

The goal of the SensAS ADT, which started in 2011, is to propose applications based on wireless sensor networks, building upon work that has been done through the SensLab and SensTools projects.

The Madynes team is responsible of the SensMGT part of the SensAS project, which focuses on sensor network management and configuration applications.

First, we adapted the existing contiki-snmp implementation to the SensLab WSN430 nodes. We did so by (1) reducing the memory footprint of the code and (2) by implementing several SNMP MIBs.

To reduce the memory footprint, we had to disable some optional features and unused drivers of the Contiki OS.

The MIBs that we chose to implement were:

- the SNMPv2-MIB that provides generic system information,
- the IF-MIB that provides information ans stasistics about the network interface of the sensor,
- and the ENTITY-SENSOR-MIB, that provides access to the actual sensors data.

Then, we were facing a problem, as the Contiki versions provided by the SensTools project were only stable releases, and we found it difficult to track the development version of Contiki with them. We then decided to create our own WSN430 drivers and platform definition for Contiki, well integrated with the development repository, and reusing as much as possible of already existing code. Our next step in this direction will be to have our contribution officially integrated in the Contiki OS.

And finally, we devised and implemented a COAP server discovery protocol using the piggybacking technique, which allows every node that offers COAP resources to announce itself to the grounded root of the sensor network, without requiring the transmission of additional packets.

7. Contracts and Grants with Industry

7.1. INRIA-ALBLF HIMA

Participants: 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.

7.2. VAMPIRE

Participants: Olivier Festor [contact], 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 do work on VoIP fuzzing methods, fingerprinting algorithms and Programmable honeypots.

7.3. MAPE

Participants: Isabelle Chrisment [contact], Andrea Oroseanu.

Dates January 2008 - July 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.

7.4. ACDA-P2P

Participants: Isabelle Chrisment [contact], Andrea Oroseanu.

Dates April 2010 - December 2011

Partners UTT , LORIA (MADYNES)

ACDA P2P (Approche collaborative pour la detection d'attaques dans les reseaux pair a 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.

7.5. SCAMSTOP

Participants: Olivier Festor [contact], Mohamed Nassar.

Dates April 2010 - December 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.

We have developped an integrated environment that allows an operator to perform various clustering activities on call detail records and use profiles. In a cooperation with the University of Liege, we have also investigated alternative methods to detect fraud in Voice over IP systems. A decision tree approach was designed to automatically classify INVITE messages as SPIT or normal based only on the content and order of their fields. A supporting architecture enabling user reporting of SPIT was also designed in this work.

7.6. FIREFLIES RTLS

Participants: Laurent Ciarletta [contact], Olivier Festor.

Priyadarsi Nanda (University of Technology of Sydney), Ye-Qiong Song, Bilel Nefzi and Hugo Cruz Sanchez (TRIO research team, INRIA Nancy-Grand-Est) are contributing to this activity. Tom Leclerc and Alexandre Boeglin have been ponctually participating.

Dates	March 2009 - December 2012
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 2011, the project has been refocused towards energy-constraints addressing, routing and management. This explains the joint-work with the TRIO team, and the arrival and Pr. Nanda from the University of Sydney. We are in the process of conducting a thorough evaluation of the Fireflies framework against standards and state of the art solutions in those areas. We are both building a local testbed and an extended simulation environment with a set of usage scenarii that are to be fed by real experiments. We are also working in improving the depth (number of hops) and the overall life-span of the sensor network in line with their application needs.

8. Partnerships and Cooperations

8.1. Regional Initiatives

The TEAM is involved in several actions of the regional CPER (Contrat Plan Etat Region) initiative on networked security as well as in the security of industrial networked systems initiative. 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 and coordinator of the ANR VAMPIRE project. In addition the team is involved in one P2P project with the University of Troyes (GIS 3S).

8.3. European Initiatives

8.3.1. Think tanks and european institutes

Olivier Festor is member of the Future Media Internet think tank at the European Commission, part of the european Future Internet Assembly. In 2011, the think tank did contribute to the FIA events and issue one white paper on the Future Media Internet Architecture [37].

Since november 1st 2011, Olivier Festor is the Director of Research of the European Institute of Innovation and Technology EIT ICT Labs.

8.3.2. Academics cooperations

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.

8.3.3. FP7 Projects

8.3.3.1. Univerself

Title: Univerself

Type: COOPERATION (ICT)

Defi: The Network of the Future

Instrument: Integrated Project (IP)

Duration: September 2010 - August 2013

Coordinator: Alcatel Lucent Bellabs (France)

Others partners: Alcatel-Lucent Bell Labs (France), Alcatel Lucent Ireland Limited (Ireland), Alcatel-Lucent Deutschland AG (Germany), NEC Europe Ltd. (Germany), Thales Communications SA (France), France Telecom SA (France), Telecom Italia S.p.A (Italia), Telefonica Investigacion y Desarrollo (Spain), Fraunhofer-Gesellschaft Zur Foerderung Der Angewandten Forschung E.V (Germany), Interdisciplinary Institute for Broadband Technology (Belgium), Inria (France), VTT Technical Research Centre of Finland (Finland), University College London (UK), University of Surrey (UK), National and Kapodistrian University of Athens (Greece), University of Piraeus Research Centre (Greece), Universiteit Twente (The Netherlands)

See also: www.univerself-project.eu/

Abstract: 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.

8.3.3.2. FI-WARE

Title: Future Internet Core Platform

Type: COOPERATION (ICT)

Defi: PPP FI: Technology Foundation: Future Internet Core Platform

Instrument: Integrated Project (IP)

Duration: May 2011 - April 2014

Coordinator: Telefonica (Spain)

Others partners: Telefonica I+D (Spain), SAP AG (Germany), IBM, Thales (France), Telecom Italia (Italy), Orange Labs - France Telecom (France), Nokia Siemens Networks (Germany), Deutsche Telekom (Germany), Technicolor (France), Ericsson (Sweden), ATOS ORIGIN S.A.E (Space), Engineering Ingegneria Informatica S.p.A (Italy), Alcatel-Lucent Deutschland AG (Germany), Alcatel-Lucent Italia S.p.A (Italy), Siemens AG (Germany), Intel (Ireland), NEC Europe Ltd. (Germany), Fraunhofer Institute for Open Communication Systems FOKUS (Germany), Inria (France), Universidad Politecnica de Madrid (Spain), University of Duisburg-Essen (Germany), University of Rome - Sapienza (Italy), University of Surrey (UK),

See also: http://www.fi-ware.eu/

Abstract: The goal of the FI-WARE project is to advance the global competitiveness of the EU economy by introducing an innovative infrastructure for cost-effective creation and delivery of services, providing high QoS and security guarantees. FI-WARE is designed to meet the demands of key market stakeholders across many different sectors, e.g., healthcare, telecommunications, and environmental services. The project unites major European industrial actors in an unique effort never seen before.

The key deliverables of FI-WARE will deliver an open architecture and implementation of a novel service infrastructure, building upon generic and reusable building blocks developed in earlier research projects. This infrastructure will support emerging Future Internet (FI)ervices in multiple Usage Areas, and will exhibit significant and quantifiable improvements in the productivity, reliability and cost of service development and delivery - building a true foundation for the Future Internet.

The MADYNES contributions to the FI-WARE project are :

- a fuzzing framework for the Internet of Things part dimension of the FI-WARE platform. More specifically we will instanciate the KIF framework to a SCADA case study;
- a smartphone level flow monitoring appliance;
- integration facility of OVAL specifications into the FI-WARE ecosystem.

8.3.3.3. SCAMSTOP

Title: SCAMSTOP

Type: CAPACITIES (Research for SMEs)

Instrument: Research for the Benefit of SMEs (SME)

Duration: January 2010 - December 2011

Coordinator: Fraunhofer Institute for Open communication Systems FhG Fokus (Germany)

Others partners: TEI of Mesolonghi (Greece), Inria (France), Telio (Norway), Voz Telecom (Spain), PDM & FC (Portugal)

See also: http://www.sme-scamstop.eu/

> Abstract: SCAMSTOP will provide a complete framework/solution for automatic fraud detection that alarms providers when suspicious behaviour is detected. Thereby, SCAMTOP will make fraud detection not only simpler but much faster as well. The developed tools can be used by VoIP/ISP providers to protect their services against losses due to fraud and to identify previously uncollected revenue sources.

We do contribute to this project by the design and implementation of fraud detection mechanisms based on advanced clustering techniques.

8.4. International Initiatives

We actively participate to the Internet Research Task Force (IRTF) Network Management Research Group (NMRG). Since march 1st 2011, Olivier Festor was named co-chair of this research group within IRTF. The group did organize one meeting in Quebec in july 2011. A workshop on flow-level management will be held in conjunction with the next IETF (march 2012) in Paris.

8.4.1. INRIA International Partners

We have established a strong cooperation with the team of Thomas Djotio at the Polytechnical Superior National School (PSNS) of the Yaoundé University. We curretnly have two joint Ph.D. students and regular exchanges of researchers.

8.4.2. Visits of International Scientists

8.4.2.1. Invited researchers and professors

Ramin Sadre from University of Twente, spent 3 weeks in the team, working on anomaly detection based on flow analysis.

Pr Priyadarsi Nanda fom the University fo technology, Sydney Australia spent 6 months on the team working on new naming schemes and advanded routing on wireless sensor networks.

8.4.2.2. Internships

Balkiss Souissi (from Feb 2011 until Aug 2011)

Subject: A self-monitoring approach for RPL-enabled wireless sensor networks

Institution: Ecole Nationale d'Ingénieurs de Tunis (ENIT) (Tunisia)

Cesar Bernardini (from Mar 2011 until Oct 2011)

Subject: An Offensive Security Tool for 6lowpan Networks

Institution: Universidad Nacional de Cordoba (Argentina)

Bilel Saadallah (from Mar 2011 until Aug 2011)

Subject: Passive Monitoring of 802.15.4/6LowPan-enabled Wireless Sensor Networks

Institution: Ecole Nationale des Sciences de l'Informatique (Tunisia)

Lucia Masola

Subject: Collaborative Sharing of Vulnerability Descriptions in Autonomic Networks

Institution: Universidad Nacional del Centro de la Provincia de Buenos Aires (Argentina)

Fran cois Despaux

Subject: Highly Modular SIP Honeypot

Institution: Universidad de la Republica (Uruguay)

Damian Vicino

Subject: Design and Implementation of a Multi-Protocol Peer-to-Peer Client

Institution: Universidad de Buenos Aires (Argentina)

Prabhjot Prabhjot Singh

Subject: NETCONF Friendly Firewall Configuration Models

Institution: IIT Bombay (India)

Imen Mahjri (from Mar 2011 until Aug 2011)

Subject: Exploring cognitive techniques for sensor networks management

Institution: Ecole Nationale des Sciences de l'Informatique (Tunisia)

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. He is also co-chair of the IRTF Network Management Research Group.

In march 2011, Olivier Festor has been appointed as the Co-chair together with Lisandro Zambenedetti Grandvile from the Federal University of Rio Grande do Sul (UFRGS) of the Internet Research Task Force (IRTF) Network Management Research Group.

Olivier Festor chaired sessions at the following conferences: IEEE ICC CSMA symposium.

Olivier Festor served as a TPC Member of the following 2011 events: 3rd ACM Workshop on Assurable and Usable Security Configuration (SafeConfig); Security track of the 4th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2011); Colloque Francophone sur l'IngÈnierie des protocoles (CFIP 2011); IEEE POLICY 2011 (International Conference), ISPS 2011; International Workshop on Networks and Services Security (NSS'2011); IEEE International Conference on Communications ICC 2011 (TPC member of CISS and CSMA tracks); IEEE ICDM 2011 Workshop on Data Mining in Networks (DAMNET).

Olivier Festor has been appointed General Chair for IFIP AIMS'2011 and TPC Co-Chair for IEEE/IFIP International Conference on Network and Service Management (CNSM'2011). He was also Tutorial co-chair for the 15th IFIP/IEEE International Conference on Integrated Management (IM'2011).

Olivier Festor is member of the board of editors of the Springer Journal of Network and Systems Management. He is member of the editorial board of the IEEE Transactions on Network and Service Management.

Olivier Festor served as an expert for the CIFRE Ph.D. programme at the ANRT. He also served as an expert for the european commission in the area of network and service management. In 2011, Olivier Festor served as an expert for the review of the french national research council. He also served on the 2011 committee for academic scientific excellence bonus allocation (+400 applications have been processed by this committee in 2011).

Isabelle Chrisment was TPC Co-chair of CFIP'2011 and of IFIP AIMS'2011. She was member of the TPC of 2th joint TC6 and TC11 International IFIP Conference on Communications and Multimedia Security (CMS'2011) and of NOTERE 2011. She was also member of the steering committee of SARSSI 2011.

Isabelle Chrisment served as an expert to evaluate projects for ANR and also for DIM Logiciel et systèmes complexes(LSC) from Île-de-France area.

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 2011, Olivier Festor and Abdelkader Lahmadi did setup a new course at the ENSEM engineering school on distributed systems and distributed algorithms.

9.3. Tutorials, invited talks, panels, presentations

In addition to the presentation of all papers published in conferences in 2011, the team members made the following public talks:

- Olivier Festor did participate to the Dagstuhl Seminar 11042 entitled: *Learning from the Past: Implications for the Future Internet and its Management ?* This seminar took place from January 27-30, 2011 in Schloss Dagstuhl, Germany.
- Alexandre Boeglin gave a presentation entitled at IETF 81 in Quebec City, Canada in the IRTF-NMRG session in july 2011.

9.4. Commissions

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

- Amélie Medem, Ph.D. in Computer Science from Université Pierre et Marie Curie - Sorbonne Universités. Title: *Conception de mécanismes d'amélioration de la gestion d'incidents dans les réseaux IP*, February 2011. (Olivier Festor)
- Patrick Battistello, Ph.D. in Computer Science from Telecom Bretagne. Title: *Protocole d'etablissement d'appels sécurisés limitant les risques de (D)DOS et de SPIT ‡ l'interconnexion entre opérateurs*, April 2011. (Olivier Festor)
- Sinan Hatahet, Ph.D. in Computer Science from University of Technology of Compiègne. Title: *Security in Unstructured P2P Systems*, April 2011. (Isabelle Chrisment)
- Gérard Wagener, joint Ph.D. in Computer Science from University of Luxembourg and INPL. Title *Self-Adaptive Honeypots Coercing and Assessing Attacker Behaviour*, June 2011. (Olivier Festor)

- Thibault Cholez, Ph.D. in Computer Science from University Henri Poincaré, Nancy 1. Title *Supervision des réseaux P2P structurés appliquée à la sécurité des contenus*, June 2011. (Isabelle Chrisment et Olivier Festor)
- Guilherme Koslovski, Ph.D. in Computer Science from ENS Lyon. Title: *Dynamically provisioned Virtual Infrastructures: specification, allocation and execution*, June 2011. (Olivier Festor)
- Tigran Avanesov, Ph.D. in Computer Science from University Henri Poincaré, Nancy 1. Title *Résolution de contraintes de déductibilité. Application à la composition de services Web sécurisés*, September 2011. (Isabelle Chrisment)
- Houssein Wehbe, Ph.D. in Computer Science from University of Rennes 1. Title *Transmission de flux vidéo en direct sur les réseaux pair à pair : optimisation de l'overlay et de la retransmission*, September 2011. (Isabelle Chrisment)
- Tony Bourdier, Ph.D. in Computer Science from University Henri Poincaré, Nancy 1. Title *Méthodes algébriques pour la formalisation et l'analyse de politiques de sécurité*, October 2011. (Isabelle Chrisment)
- Jörn Franke, Ph.D. in Computer Science from University Henri Poincaré, Nancy 1. Title *Coordination of Distributed Activities in Dynamic Situations. The Case of Inter-organizational Crisis Management*, October 2011. (Isabelle Chrisment)
- Cristian Rosa, Ph.D. in Computer Science from University Henri Poincaré, Nancy 1. Title *Performance and Correctness Assessment of Distributed Systems*, October 2011. (Isabelle Chrisment)
- Abdelhamid Salah Brahim, Ph.D. in Computer Science from Université Pierre et Marie Curie - Sorbonne Universités. Title *Information diffusion and community structure in a blog network*, December 2011. (Isabelle Chrisment)
- Johan Mazel, Ph.D. in Computer Science from INSA Toulouse. Title: *Unsupervised Network Anomaly Detection*, December 2011. (Olivier Festor)

Team members participated in the following academic recruitment committees :

- Isabelle Chrisment did lead a Professor position in mathematics recruitment committee in Nancy University.
- Olivier Festor was member of a Professor position recruitment committee in computer science at the Joseph Fourier University in Grenoble.
- Laurent Ciarletta was member of an Associate Professor position recruitment committee in computer science in Nancy University.

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] T. Cholez. *Supervision des réseaux pair à pair structurés appliquée à la sécurité des contenus*, Université Henri Poincaré - Nancy I, June 2011, http://tel.archives-ouvertes.fr/tel-00608907/en/.

[2] T. Leclerc. *Contributions for Advanced Service Discovery in Ad hoc Networks*, Université Henri Poincaré - Nancy I, November 2011, http://tel.archives-ouvertes.fr/tel-00608907/en/.

[3] J. Siebert. *Approche multi-agent pour la multi-modélisation et le couplage de simulations. Application à l'étude des influences entre le fonctionnement des réseaux ambiants et le comportement de leurs utilisateurs.*, Université Henri Poincaré - Nancy I, September 2011, http://tel.archives-ouvertes.fr/tel-00642034/en/.

[4] G. Wagener. *Self-Adaptive Honeypots Coercing and Assessing Attacker Behaviour*, Institut National Polytechnique de Lorraine - INPL, June 2011, Thèse en co-tutelle entre l'INPL et l'Université du Luxembourg sous la direction Commune de Thomas Engel et Olivier Festor avec la participation de Radu State, http://tel.archives-ouvertes.fr/tel-00627981/en/.

Articles in National Peer-Reviewed Journal

[5] A. Lahmadi, O. Festor. *SecSIP : un environnement de protection pour la voix sur IP*, in "Techniques de l'Ingenieur", February 2011, n^{o} IN 130, http://hal.inria.fr/inria-00594861/en/.

[6] 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 "Revue d'Intelligence Artificielle", 2011, vol. 25, n^{o} 5, p. 625–651 [*DOI :* 10.3166/ria.25.625-651], http://hal.archives-ouvertes.fr/hal-00640079/en/.

International Conferences with Proceedings

[7] M. Barrere, R. Badonnel, O. Festor. *Supporting Vulnerability Awareness in Autonomic Networks and Systems with OVAL*, in "Network and Service Management -CNSM'11", Paris, France, October 2011, http://hal.archives-ouvertes.fr/hal-00614085/en/.

[8] M. Barrere, R. Badonnel, O. Festor. *Towards Vulnerability Prevention in Autonomic Networks and Systems*, in "Proceedings of the 5th International Conference on Autonomous Infrastructure, Management and Security - AIMS 2011", Nancy, France, June 2011, http://hal.archives-ouvertes.fr/hal-00580315/en/.

[9] T. Cholez, C. Hénard, I. Chrisment, O. Festor, G. Doyen, R. Khatoun. *Détection de pairs suspects dans le réseau pair à pair KAD*, in "SAR-SSI 2011: 6ème Conf. sur la Sécurité des Architectures Réseaux et Systèmes d'Information", La Rochelle, France, IEEE, May 2011, Financement GIS - 3SGS - Projet ACDAP2P, http://hal.inria.fr/inria-00596677/en/.

[10] L. Ciarletta. *Co-simulation and multi-models for Pervasive Computing as a complex system*, in "14th International Conference on Human-Computer Interaction - HCI International 2011", Orlando, États-Unis, Springer, July 2011, http://hal.inria.fr/inria-00584928/en/.

[11] O. Dabbebi, R. Badonnel, O. Festor. *A Broad-Spectrum Strategy for Runtime Risk Management in VoIP Enterprise Architectures*, in "Proceedings of the 12th IFIP/IEEE International Symposium on Integrated Network Management - IEEE IM'2011", Dublin, Irlande, IEEE, May 2011, 7, Laboratoire Commun Alcatel Lucent INRIA, http://hal.archives-ouvertes.fr/hal-00580317/en/.

[12] O. Dabbebi, R. Badonnel, O. Festor. *Econometric Feedback for Runtime Risk Management in VoIP Architectures*, in "Proceedings of the 5th International Conference on Autonomous Infrastructure, Management and Security - AIMS 2011", Nancy, France, June 2011, 12, Laboratoire Commun Alcatel Lucent INRIA, http://hal.archives-ouvertes.fr/hal-00580314/en/.

[13] R. Do Carmo, M. Nassar, O. Festor. *Artemisa: an Open-Source Honeypot Back-end to Support Security in VoIP Domains*, in "IFIP/IEEE International Symposium on Integrated Network Management - IM 2011", Dublin, Irlande, IEEE, May 2011, http://hal.inria.fr/inria-00594857/en/.

[14] J. François, A. Humberto, R. State, O. Festor. *PTF: Passive Temporal Fingerprinting*, in "IFIP/IEEE IM'2011", Dublin, Irlande, IEEE, May 2011, 8, http://hal.inria.fr/hal-00645299/en/.

[15] J. François, R. State, T. Engel, O. Festor. *Enforcing Security with Behavioral Fingerprinting*, in "7th International Conference on Network and Service Management - CNSM 2011", Paris, France, October 2011, http://hal.inria.fr/hal-00641831/en/.

[16] J. François, R. State, T. Engel, O. Festor. *Enforcing Security with Behavioral Fingerprinting*, in "IFIP/IEEE in cooperation wit ACM CNSM'2011", Paris, France, 2011, http://hal.inria.fr/hal-00644696/en/.

[17] H. N. Kenfack, T. Djotio Ndié, E. Nataf, O. Festor. *Une ontologie pour la description des intrusions dans les RCSFs.*, in "CFIP 2011 - Colloque Francophone sur l'Ingénierie des Protocoles", Sainte Maxime, France, UTC, May 2011, Session Sécurité Réseau, http://hal.inria.fr/inria-00586889/en/.

[18] A. Lahmadi, L. Delosière, O. Festor. *Hinky: Defending Against Text-based Message Spam on Smartphones*, in "IEEE International Conference on Communications ICC2011", Kyoto, Japon, June 2011, http://hal.inria.fr/inria-00594854/en/.

[19] A. Lahmadi, O. Festor. *Génération automatique de politiques de sécurité pour SecSIP*, in "CFIP 2011 - Colloque Francophone sur l Ingénierie des Protocoles", Sainte Maxime, France, UTC, 2011, Session Sécurité Réseau, http://hal.inria.fr/inria-00586832/en/.

[20] A. Lahmadi, E. Nataf, O. Festor. *YANG-Based Configuration Modeling - The SecSIP IPS Case Study*, in "IFIP/IEEE International Symposium on Integrated Network Management", Dublin, Irlande, May 2011, http://hal.inria.fr/inria-00595825/en/.

[21] G. Montassier, T. Cholez, G. Doyen, R. Khatoun, I. Chrisment, O. Festor. *Content Pollution Quantification in Large P2P networks : a Measurement Study on KAD*, in "11th IEEE International Conference on Peer-to-Peer Computing (IEEE P2P'11)", Kyoto, Japon, IEEE Communications Society, August 2011, p. 30-33, Projet GIS 3SGS ACDAP2P, http://hal.inria.fr/inria-00619965/en/.

[22] M. Nassar, S. Martin, G. Leduc, O. Festor. *Using Decision Trees for Generating Adaptive SPIT Signatures*, in "ACM SIN'2011", Sydney, Australie, ACM, November 2011, p. 13-20, http://hal.inria.fr/hal-00644821/en/.

[23] J. P. Timpanaro, T. Cholez, I. Chrisment, O. Festor. *BitTorrent's Mainline DHT Security Assessment*, in "4th IFIP International Conference on New Technologies, Mobility and Security - NTMS 2011", Paris, France, IEEE, February 2011, Projet GIS 3SGS ACDAP2P (Approche collaborative pour la détection d'attaques dans les réseaux pair à pair), http://hal.inria.fr/inria-00577043/en/.

[24] J. P. Timpanaro, T. Cholez, I. Chrisment, O. Festor. *When KAD meets BitTorrent - Building a Stronger P2P Network*, in "HotP2P 2011", Anchorage, ALASKA, États-Unis, May 2011, http://hal.inria.fr/inria-00595086/en/.

Scientific Books (or Scientific Book chapters)

[25] I. Chrisment, A. Couch, R. Badonnel, M. Waldburger. *Managing the Dynamics of Networks and Services, Proceedings of the 5th International Conference on Autonomous Infrastructure, Management and Security, AIMS 2011.*, Lecture Notes in Computer Science, Springer, June 2011, vol. 6734 [*DOI :* 10.1007/978-3-642-21484-4], http://hal.inria.fr/inria-00628157/en/.

Research Reports

[26] L. ANDREY, F. DESPAUX. *A flexible SIP honeypot*, Inria, November 2011, http://hal.inria.fr/hal-00646691/en/.

[27] M. BARRÈRE, R. BADONNEL, O. FESTOR. *Towards the Assessment of Distributed Vulnerabilities in Autonomic Networks and Systems*, Inria, September 2011, http://hal.inria.fr/hal-00646837/en/.

[28] C. BRANDINI, A. LAHMADI, O. FESTOR. *Development of a fuzzing tool for the 6LoWPAN protocol*, INRIA, November 2011, n^o RR-7817, http://hal.inria.fr/hal-00645948/en/.

[29] T. CHOLEZ, G. MONTASSIER, G. DOYEN, R. KHATOUN, I. CHRISMENT, O. FESTOR. *Détection et quantification de la pollution dans le réseau P2P KAD*, Inria, September 2011, http://hal.inria.fr/hal-00644174/en/.

[30] T. CHOLEZ, J. P. TIMPANARO, G. DOYEN, I. CHRISMENT, O. FESTOR, R. KHATOUN. *Vulnérabilités de la DHT de BitTorrent & Identification des comportements malveillants dans KAD*, Inria, August 2011, http://hal.inria.fr/hal-00644151/en/.

[31] O. DABBEBI, R. BADONNEL, O. FESTOR. *A trust approach for mitigating attacks in RELOAD*, Inria, October 2011, http://hal.inria.fr/hal-00646815/en/.

[32] O. DABBEBI, R. BADONNEL, O. FESTOR. *Managing Risks in P2PSIP Architectures*, Inria, September 2011, http://hal.inria.fr/hal-00646808/en/.

[33] A. LAHMADI, O. FESTOR. *VeTo: reference manual*, INRIA, November 2011, n^o RT-7816, http://hal.inria.fr/hal-00645913/en/.

[34] Y. REBAHI, N. CHATZIS, A. BORODIN, T. STEINICKE, B. GEORGIEVA, M. NASSAR, O. FESTOR, T. KAPOURNIOTIS, A. DAGIUKLAS, C. GOGOS, P. ALEFRAGIS. *SCAMSTOP - D4.1 Testing, integration and usage results*, November 2011, http://hal.inria.fr/hal-00655087/en/.

[35] J. P. TIMPANARO, I. CHRISMENT, O. FESTOR. *Monitoring the I2P network*, Inria, October 2011, http://hal.inria.fr/inria-00633574/en/.

[36] D. VICINO, J. PABLO TIMPANARO, I. CHRISMENT, O. FESTOR. *hMule: an unified KAD-BitTorrent file-sharing application*, INRIA, September 2011, n^o RR-7815, http://hal.inria.fr/hal-00645894/en/.

Other Publications

[37] M. ALDUAN, F. ALVAREZ, J. BOUWEN, G. CAMARILLO, P. CESAR, P. DARAS, O. FESTOR, E. IZQUIERDO, N. LAOUTARIS, A.-D. MEZAOUR, P. MOORE, G. PAU, G. PAVLOU, T. PIATRIK, S. SOURSOS, T. STEINER, C. TIMMERER, T. TSIODRAS, T. ZAHARIADIS. *Future Media Internet Architecture Reference Model (v1.0)*, March 2011, Future Media Internet Architecture Think Tank White Paper, http://hal.inria.fr/inria-00573841/en/.

[38] M. CLEMENTZ. *Classification de malware par traces réseau*, ESIAL, Nancy, October 2011, http://hal.inria.fr/hal-00655089/en/.

[39] A. MAYZAUD. *Analyse des vulnérabilités du réseau pair à pair anonymisé I2P*, ESIAL, Nancy, France, Villers-lès-Nancy, September 2011, http://hal.inria.fr/hal-00646336/en/.

[40] O. RUAS. *Analyse et visualisation de communautés dans les données P2P*, ENS Cachan, France, September 2011, http://hal.inria.fr/hal-00655084/en/.

[41] B. SAADALLAH, A. LAHMADI, O. FESTOR. *Mise en oeuvre d'une couche de communication CCN pour les réseaux de capteurs sans fil*, ENSI, Tunis, Tunisia, September 2011, http://hal.inria.fr/hal-00645949/en/.

[42] J. P. TIMPANARO, I. CHRISMENT, O. FESTOR. *Monitoring the I2P network*, October 2011, Research Report, http://hal.inria.fr/inria-00632259/en/.