1 Equipe VASCO - Axe Génie des Logiciels et des Systèmes d'Information

1.1 Scientific Presentation

Permanent research group members: Lydie du Bousquet (PR, UJF), Roland Groz (PR, GINP), Yliès Falcone (MCF, UJF), Akram Idani (MCF, GINP), Yves Ledru (PR, UJF, team leader), Catherine Oriat (MCF, GINP), Jean-Luc Richier (CR, CNRS), German Vega (IR, CNRS, shared 50% with the ADELE team). Paul Jacquet (PR, GINP) and Farid Ouabdesselam (PR, UJF) are also members of the team, but don't participate in its scientific activity.

This team composition has evolved since 2009: Yliès Falcone was recruited in 2011. Michel Delaunay (IR, CNRS) has retired in 2011. Paul Jacquet has retired in 2014.

From 2009 till june 2014, the VASCO team has counted 10 PhD students, 4 post-docs, and 2 academic visitors.

Research description - themes The evolution of Software Systems towards more openness, interconnection and integration has significantly raised the stakes for security issues as well as safety. Safety analysis and testing must deal with systems with high levels of interactions with other systems and external resources and components. The fast changing and adaptive nature of threats and attacks on information systems that have become more pervasive raises new challenges, because existing techniques can become obsolescent in such a context. The security challenges have motivated most research activities of the VASCO team during the past period. These research efforts focus on security testing and modelling.

Testing plays a central role in our research, which must face several challenges of testing, especially in the context of open environments: difficulty to control the environment's behaviour, incomplete models of the environment and of the application under test. Since less can be assumed on the environment, it becomes necessary to perform more tests to increase confidence. This leads to classical challenges of testing: automating test generation, controlling the size of the test suite, and automation of the test oracle. During the past period, the VASCO team was active on each of these challenges. We used fuzzing techniques and combinatorial testing for test generation. We proposed several reduction techniques to control the size of the test suite. We took advantage of monitoring rechniques to automate the test oracle, and studied trace analysis to perform fault localisation.

Models also play a significant role in our research. Models can provide an oracle for tests, or can be the basis for test generation. They also provide an abstraction of the system under validation, which can be explored to find security breaches and potential attacks. Therefore, our models address both functional/behavioural and security aspects of the system under validation. In the past period, we have conducted research on model inference to construct a model from an existing system, which will then be explored by model-checking. We also studied the use of simulation and testing to validate a security policy described as a B specification.

During the past five years, the team has participated to 2 european projects (ITEA/Diamonds and FP7/SPaCIoS) and 2 national (ANR) projects (Selkis and TASCCC), all dedicated to various facets of security. Our skills in security testing and modelling are also applicable to address safety, as demonstrated in the FUI IO32 project, where passive testing was associated to techniques for understanding traces. Our expertise in monitoring techniques gave rise to the Weave Droid project, which performs code injection in Android applications without source code.

These research efforts fit in the "Software and Information System Engineering" axis of the LIG, where we share with several teams of this axis the conviction that software engineering tools must be based on models. They are related to the "Security, safety, reliability", "Embedded Systems" challenges of LIG scientific programme and the PILSI project. They contribute to the "Sustainable ambiant computing" project of the LIG by its contributions to safety, security and software quality. Moreover the team is part of the SCCyPhy action of Persyval-lab, dedicated to various aspects of security.

1.2 Scientific and Technological Results

To achieve our goal of safe and secure systems through testing and modeling, our resarch can be organised along three major research themes: test generation, passive testing, model construction and inference. These themes denote an evolution of our research with respect to the previous period with the advent of new researches on passive testing, and less attention dedicated to test assessment activities (coverage measurement and testability). This evolution of themes took advantage of the recruitment of a young assistant professor bringing new ideas in the team, and giving the opportunity to expand our research on passive testing.

Test generation: fuzzing and combinatorial testing Two approaches have been followed by VASCO for test generation. Combinatorial testing is based on the Tobias tool, and raises the challenge of controlling combinatorial explosion. Fuzzing is dedicated to security testing.

Tobias was developed in 2000 during the RNTL COTE project, and reused later in the ANR POSE and ANR TASCCC projects. Tobias unfolds a test pattern into a large test suite, using combinations of input parameters and operations. The main challenge of using Tobias is to control combinatorial generation. Therefore, the tool was extended with selection and filtering mechanisms, and an incremental unfolding algorithm to guide test generation within a huge search space. In [49], we used the incremental algorithm and found 640 valid test cases hidden into a search space of 10^{23} test cases. By "valid" test cases, we mean sequences of operations which conform to pre-conditions, invariants or local assertions of a given formal specification. A case study of the TASCCC project led us to address a search space of 10^{100} test cases [47] (PhD Thesis). A limited version of the Tobias tool, including some of its selection mechanisms [32], is available as an on-line service at http://tobias.liglab.fr/. Moreover, the tool is integrated in the TASCCC Testing tool [7]. We also explored other ways to control the size of test suites: test case prioritisation [30] and test suite reduction [48].

Fuzz testing is the major testing technique for detecting vulnerabilities (security flaws) in software systems especially when the source code is not available. We have investigated smart fuzzing techniques that enhance the capabilities of detection by being state aware (model based), identifying the input (taint) flows, and adaptive to bypass sanitizing filters or other input transformations. We have worked in two directions. On the one hand, we developed in cooperation with our industrial partner and Verimag scalable smart fuzzing techniques to analyze large binaries [5]. On the other hand, we developed a smart fuzzer for detecting Cross Site Scripting (XSS) vulnerabilities in web applications. This has been implemented in the KameleonFuzz tool which combines smart crawling techniques (with some kind of model inference), static and dynamic taint flow analysis and genetic algorithms [9]. We have shown that KameleonFuzz clearly outperforms state of the art opensource fuzzers for the detection of XSS vulnerabilities, which was presented at "hacking" conferences such as NoSuchCon or BlackHat [8].

Passive testing: monitoring and trace analysis Test cases need to be complemented with effective test oracles that detect failures or analyze the execution of the system (when for instance the system under test is in production and should be monitored). For this reason, our team has explored different approaches. First, in [1, 3, 2], execution traces of embedded applications in micro-controller are analyzed for fault localization. Several algorithms for compression and fault localization have been adapted and implemented in a tool called Comet (APP in progress). J-Cyclitur, a part of this tool (compression of traces) is available on line. Second, in [14, 12, 13], we characterize the set of properties that can be monitored and tested during the execution of a system. In [4, 11], we considered the generation of decentralized test oracles or monitors from logic and automata-based specifications. These approaches have been implemented in decentmon1 and decentmon2, two open-source tools. Third, for specifications where physical time needs to be taken into account, we proposed in [41, 40, 39] synthesis techniques for enforcement monitors, i.e., monitors that have the ability to correct the execution of the system under test to meet the desired specification. Fourth, when the system is built using component-based design, we proposed in [16, 15] dedicated monitors expressed as components.

Model construction and inference Models provide an abstraction of the system under validation. This abstraction can be used to search for defects, vulnerabilities or potential attacks, or to generate abstract test cases. Once reified these test cases are run against the actual system to confirm the existence of defects. In this area, the researches of VASCO have followed two directions: the integration

of graphical and formal languages for the construction of validated models, and the inference of a model from an existing system.

The integration of graphical and formal languages has been studied for a long time in the VASCO team. The RoZ tool [1] developed earlier combined the UML class diagram with formal annotations, and generated an animatable Z specification. Since 2009, we have extended this approach to take into account SecureUML diagrams, i.e. class diagrams completed with access control information. This combination was initially studied in Z [31, 43, 44] and [42] (PhD Thesis). These works showed that authorization constraints associated to an access control permission could lead to unexpected internal attacks where insiders perform legal actions to modify the system state, and are granted unwanted permissions. This approach was adapted to the B formal method, and a tool (B4MSecure) [22] was built to support the generation of the B specification. The choice of B is motivated by the availability of the ProB model-checker which can support animation, model exploration and test generation. These results were reported in [28, 29]. The B4MSecure tool is distributed at http://b4msecure.forge.imag.fr/.

VASCO has developed its activities on active inference techniques, to retrieve models from black box systems (no access to source or binary code) by sending input sequences and observing outputs. We have worked on improvements of algorithms initially designed for inference of automata so as to address software engineering issues:

- abstraction and concretization between model events and real interactions with a system
- inputs and outputs with parameters having infinite domain sets
- non-determinism
- assessing and updating models

We developed generic algorithms, and we also worked more specifically on the application and adaptation of inference in the context of security modelling and testing, especially in the context of web applications. To address non-determinism, we extended existing algorithms [10] and developed methods to identify non-deterministic parameters that are crucial in security applications (such as nonces and session-ids or cookies) [6]. We have used extended finite state machines models (with parameterized inputs and outputs and local variables) and proposed algorithms that can infer variable values and guards on transitions. We also worked on other improvements for dealing with large input sets [26, 19]. To interface with real systems, we developed algorithms and heuristics for the detection of relevant parameters and automatic generation of test drivers [20]. And we have developed a novel inference approach based on quotient automata that allows to build increasingly precise quotients of the system, by making abstractions on the possible inputs [38]. Other techniques have also been investigated to cover the assessment of models and comparison with the systems [25, 19, 27] [24]. All major algorithms are implemented in the SIMPA tool, which is integrated in the SPaCIoS platform.

Additional research themes: Home automation, Embedded systems validation We briefly describe two additional research directions followed during the last five years, and which led to PhD thesis. These lines of research are currently stopped in the VASCO team, and are not part of our research project for the next five years.

In collaboration with Ioannis Parissis from the LCIS lab, we investigated during the PhD thesis of Yves Grasland [17] the test of hybrid systems, such as used in cyber-physical control of home environments, with a special focus on the use of resources such as energy. This led to an approach to define metrics to assess the coverage of tests for hybrid systems and associated test selection methods, dealing with discretization and imprecision in measurement of continous values [18].

For embedded systems validation, we have considered a synchronous approach as a continuation of our previous research activities. In particular, we have studied the coverage assessment of Lustre programs and extended the definition of structural coverage criteria towards the use of multiple clocks as well as the integration testing (LUSTRUCTU). We also led further developments of our test generator LUTESS, in order to consider programs with numerical inputs/outputs [36, 35, 34, 37] and [33, 45] (Phd thesis).

[1] http://vasco.imag.fr/RoZ/

Publications summary These researches have led to a total of 131 publications between 2009 and 2014, with a significant increase in international journal articles compared to the previous term (2005-2008).

	2005-2008	2009	2010	2011	2012	2013	2014	Total 2009-2014
International peer reviewed journal [ACL]	5	3	1	2	3	2	1	12
International peer-reviewed conference proceedings [ACT]	60	9	8	9	13	12	5	56
Short communications [COM] and posters [AFF] in conferences and workshops	14	3	2	2	6	7	2	22
Scientific books and chapter [OS]	2	2	0	0	0	2	0	4
National peer reviewed journal [ACLN]	7	1	1	0	1	0	0	3
National peer-reviewed conference proceedings [ACTN]	11	2	2	0	3	1	0	8
Book or Proceedings editing [DO]	4	1	1	1	1	1	0	5
Doctoral Dissertations and Habilitations Theses [TH]	14	3	2	1	1	4	0	11
Other Publications [AP]	3	0	2	0	3	5	0	10
Total	120	24	19	15	31	34	8	131

1.3 Visibility and attractivity

Distinctions Farid Ouabdesselam was promoted to the rank of officer in the academic palms order (2012)

Best paper awards

- Yliès Falcone and Andreas Bauer (NICTA, Canberra, Australia) received the Best Paper Award at FM 2012 (Paris, 2012)
- Lydie du Bousquet received the Best Paper Award at ICSEA 2009 (Porto, Portugal, 2009)

Direction of research structures Paul Jacquet was administrateur général of Grenoble INP from 2008 till 2012. Farid Ouabdesselam was president of the Université Joseph Fourier from 2007 till 2012. Since 2012, he is the director of the Institut Carnot Logiciels et Systèmes Intelligents, and the president of Floralis, sister company of the Université Joseph Fourier.

In 2008, Yves Ledru has created the GDR CNRS Génie de la Programmation et du Logiciel, and was its director from 2008 till 2011. Since 2012, he is member of its committee. Akram Idani and Lydie du Bousquet are responsible for the Special Interest Groups MFDL and MTV2 of this GDR. Moreover, Lydie du Bousquet co-chairs the work on "challenges for software engineering and programming at horizon 2025".

At the regional level, Yves Ledru is scientific leader of the ARC6 of the Rhône-Alpes region since 2012. ARC6 is a research network grouping 1363 academics from 42 laboratories of the region. Before ARC6, Yves Ledru was the scientific leader of the regional research cluster on "informatics, signal and embedded software".

Editorial boards and programme committees, Expert reviews, membership of committees

	Steering committee*, Editorial board°, co-editor‡, Programme (co-)chair†, Organizing commitee•	Programme committees	Others
Lydie du Bousquet	Mutation (2010, 2011)†, SCENARIOS (2011)†	ICFI, ICSEA, ICST, ICSOFT, VALID	member of CNU (2009-2011), recruitement committees at University Paris Sud, INSA Lyon, and the University of Nantes.
Yliès Falcone	MAROC 2013†, CSRV 2014†, special issue of Springer's STTT‡, proc. 1st RV‡, RV 2014•, ETAPS 2014•, MAROC 2013•, Summer School on Cyber-Physical Systems 2013•, IsoLA'12•, AFADL'12•, RV'10•, CAV'09•, VVPS'09•	SecTest, CSRV, FORTE, RV, MSR, Isola, SERP	reviewer for the ANRT Ph.D. Grant (2013) and ANR Grants 2013.
Roland Groz	Testcom(until 2012)*, Annals of Telecommunications (Springer)°	AFADL, AMOST, CFIP, ICST, ICTSS, MDV, QSIC, SARSSI, SECTEST, TestCom	
Akram Idani	B workshop (2011)•, Journées MFDL (2012, 2014)•, AFADL 2012•, SEFM 2014†	AFADL, ICCES, FBIT, ICEIS, MEDI, VOLT	
Yves Ledru	ASE (until 2013), TSI (Hermès, 2008-11)°	AFADL, ASE, ASWEC, CAL, ERTS2, FHIES/SEHC, FM, FormaliSE JLDP, LMO, MEDI, SCENARIOS, WETICE/FVSBS, WISSE	scientific committee of IMAGINOVE cluster since 2007. Reviews of international programmes (PHC) of MESR (2008-2010) Expert for ANR, Digiteo labs, Institut Telecom, LABRI Laboratory (Bordeaux), Aquitaine region. scientific committee of DIOM laboratory (St Etienne) (2009). scientific committee of the PRF IDEAS of ONERA/Centre de Toulouse. (2010) recruitment committees at the U. Lorraine, and U. Paris 12.
Jean-Luc Richier		ICFI, SARSSI	reviewer for an ITEA2 project (2012).

Jean-Luc Richier, Catherine Oriat, Akram Idani, Lydie du Bousquet, and Yves Ledru have participated to local recruitment committees in Grenoble.

International collaborations The VASCO team has a long lasting cooperation with Prof. Alexandre Petrenko (CRIM, Montréal, Canada). In 2012, he was invited and spent two months in our group. This cooperation has led to joint publications [30, 38]. We also welcomed Prof. Pierre-Yves Schobbens from the Univ. of Namur for 5 months in 2009, which led to a joint publication [23].

The team was also involved in two european projects (ITEA Diamonds and FP7 SPaCIoS), and we developed relationships with T.U. München, ETH Zurich, T.U. Graz, and Univ. of Oulu.

Yliès Falcone is in charge of international relations of UJF with ENSA Tétouan (Marocco), Pontificia Universidad Javeriana (Colombia), Galatasaray University (Turkey). He has also developed numerous research collaborations, leading to joint publications, with researchers from U. of Manchester (UK), NICTA (Australia), fortiss (Germany), NASA JPL (USA), American University of Beirut (Lebanon), Hanoi University of Sciences and Technology (Vietnam), U of Illinois at Chicago (USA).

Akram Idani has initiated collaborations with Tunisia and Morocco: a PhD student (Amira Radhouani) is currently co-directed by Narjes Ben Rajeb (INSAT Tunis), Akram Idani and Yves Ledru. We also attracted several master's students from INSAT and ENSI Tunis during the last five years. Moreover, research work in progress with ENSIAS Rabat (Morocco) led to a joint publication [21].

Lydie du Bousquet has set up a collaboration with several norvegian groups, including Simula Labs (Norway), supported by a PHC AURORA project (2009-2010). This cooperation has led to a joint publication [46].

Yves Ledru was invited to report on two PhD theses in Denmark, at the Universities of Copenhagne (2010) and Aarhus (2013).

1.4 Social, economical, and cultural impact

With the pervasive advent of ICT in our society, security and safety issues have become essential for everyday's life. The researches of VASCO contribute to these goals, and our participation to research projects contribute to spread our results to the society, through our industrial partners.

During the last term, VASCO has participated to numerous research projects, with international, national and local funding.

Main contracts

Name: SPACIOS EC FP7/STREP (Europe) 2010-2014
Partners: U. di Verona (lead), U. di Genova, ETH Zűrich, IeAT, T.U. Műnchen, SAP, Siemens
Description: Methods and tools to detect vulnerabilities in deployable services over the Internet.

Name: Diamonds Eureka/ITEA2 (Europe) 2010-2013
Partners: Fraunhofer FOKUS (lead). 22 partners in 6 countries.
Description: Techniques and tools for security testing in industry.

Name: IO32 FUI/Minalogic (France) 2010-2013
Partners: AIM, EASii IC, STMicrolectronics, Trilogie
Description: Instrumentation and tools for micro-controlers.

Name: CIFRE Thesis Contract with Vupen (France) 2010-2013
Description: Smart fuzzing for x86 binary code.

Name: SELKIS ANR/ARPEGE 2008-2012
Partners: MEDECOM, SWID, CHU Brest, IFREMMONT, CEDRIC/CNAM, LACL (lead), Télécom Bretagne
Description: Model-Driven Engineering approach for the analysis and design of Secure Information Systems, with focus on medical information systems.

Name: TASCCC ANR/ARPEGE 2009-2012
Partners: Gemalto, Trusted Labs, Smartesting, Serma Technologies, LIFC (lead), Supélec
Description: Automated testing based on scenarios and Common Criteria.

Name: SIESTA ANR/RNTL 2008-2011
Partners: Airbus France, Astrium Space Transportation, Hispano-Suiza, Turbomeca, Esterel Technologies, CEA-LIST, LCIS, LIG (lead), LRI, ONERA
Description: Automation for test of embedded systems in SCADE and SIMULINK.

Name: IPOTEST Université Joseph Fourier/pôle MSTIC 2008-2009
Partners: ADELE and VASCO teams of LIG
Description: Test of home automation systems based on a service oriented architecture.

Name: Vulcain Université Joseph Fourier/pôle MSTIC 2009-2010
Partners: Vérimag
Description: Automated techniques for detection of security vulnerabilities in a "classical" environment.

Name: ARC6 and ISLE Rhône-Alpes region 2009-2010
Partners: 42 laboratories in the Rhône-Alpes region
Description: These projects correspond to the scientific responsibility for regional research networks in the fields of ICT.

Software distribution The nature of VASCO's research leads us to develop tools and research prototypes. One of the goals identified in 2009 was to improve the distribution of our research tools. As a result, the following actions have been performed:

- SIMPA, the model inference tool is integrated with associated documentation as a module in *SPaCIos Tool* and the Nessos platform: http://www.spacios.eu/tutorialsimpa.php
- The Tobias combinatorial generator is available as a service through a web page http://tobias.liglab.fr/. Written and video documentation are provided and the service has been experimented during master's courses.
- B4MSecure, which integrates SecureUML and B, is distributed as an instantiation of the Eclipse/Topcased environment from http://b4msecure.forge.imag.fr/. Written and video documentation are also provided.
- JCyclitur, compression tool for execution traces, is distributed as a runnable standalone Java archive from http://io32.forge.imag.fr/jcyclitur.html
- DecentMon, an OCaml benchmark for Decentralized Monitoring of LTL formulae is available as open-source from http://decentmonitor.forge.imag.fr/
- Efforts are currently on-going to industrialize Weave Droid with support of GRAVIT (Grenoble's innovation accelerator) and the LSI Carnot Institute.

1.5 Team Organization and life

Variability of subgroups The team offers a variety of expert collaborators in the areas of testing, modeling, and security. This allows us to combine adequate skills on each research project. In most cases, several members of the team cooperate on a given research work. Moreover, all PhD theses are co-directed by members of the team. As a result, there is a good cohesion in the group: there are no fixed sub-groups in the team, and information about work in progress spreads within the team.

Contributions to the LIG organisation Lydie du Bousquet is, with Dominique Rieu (SIGMA team), in charge of the "Software and Information System Engineering" axis of the LIG. Jean-Luc Richier chairs the LIG users commission for ICT infrastructure, and has responsibilities for the security of LIG Information System. Yliès Falcone is in charge of Valorisation in the LIG, and member of the educational board of Persyval-lab.

Answer to the remarks of the previous evaluation : impact of resarch funding on scientific directions One of the major risks identified by the previous evaluation was the influence of research contracts on the scientific directions. This risk was taken into account, and we tried, as much as we could, to align our contributions to the projects with our major research objectives.

Scientific themes such as model inference, integration of graphical and formal languages, combinatorial testing were already present during the 2004-2008 period. They were inserted into the Spacios, Selkis, and TASCCC projects to ensure research continuity. We also tried recently to take more leadership in the submission of research projects, and hence ensure their compatibility with our main topics of interest. Nevertheless, the team remains dependent on the choices of selection committees.

1.6 Training through research, educational involvment

Doctors and post-docs 10 PhD thesis and one habilitation thesis have been defended by members of the team between 2009 and 2014. Two PhD thesis will be defended in the first semester of 2014. One student has stopped his thesis due to health problems. One PhD thesis is currently in its first year. The VASCO team also appointed four post-docs.

The Habilitation thesis was defended by Lydie du Bousquet who has now a Professor position in VASCO.

Regarding the doctors, Yliès Falcone is now member of the VASCO team. Besnik Seljimi is assistant professor at the South East European University (Macedonia). Nafees Qamar has a post-doc position at

Vanderbilt University (Tennessee). Muhammad Rabee Shaheen has a teaching position in Syria. Sofia Bekrar, Taha Triki, and Virginia Papailiopoulou have taken engineering positions in software companies. Muhammad Naeem Irfan and Yves Grasland are creating their companies. Azzedine Amiar is student in a management school.

Regarding former post-docs, Ajitha Rajan is now a Chancellor's Fellow/Lecturer at the School of Informatics in the University of Edinburgh (since December 2012). Sanjay Rawat is assistant Professor at the IIIT Hyderabad (India). Laya Madani has taken an engineering position in a software company. Mickaël Delahaye is post-doctoral researcher at French Alternative Energies and Atomic Energy Commission (CEA) since february 2014.

Education responsibilities The professors of the team are teaching in bachelor and masters degrees at the Université Joseph Fourier or Grenoble INP. From a research and education point of view, they are involved in the Advanced Information Systems and Software Engineering option of the MOSIG Research Master. Yliès Falcone is a member of the educational board of Persyval-Lab, and has been member of the organisation committee of the CPS summer school in 2013 and 2014.

Moreover, the team members have the following responsibilities:

Roland Groz is deputy director of Ensimag since 2010 and chargé de mission "Culture" for Grenoble INP since 2013.

Lydie du Bousquet has been in charge of the Informatics School of UFR IM2AG (UJF) since 2011.

Yves Ledru has been the head of the HDR commission for Informatics and Applied Mathematics of UJF until 2013, and of the University of Grenoble since 2013. He has also been in charge of the software engineering option of the Professional Master Génie Informatique since 2006.

Roland Groz has been in charge of the special curriculum (X4A) at Ensimag for students from "École Polytechnique" since 2003, and he was in charge of the Master in Telecommunication (Ensimag-Phelma) from 2008 to 2013. He is also a member of the advisory committee to Ensimag since 2006.

Akram Idani has been in charge of the 1st year of Ensimag since 2013, and coordinator of the 2nd year thematic projects.

Catherine Oriat has been member of the pedagogical mission of Grenoble INP since 2010 .

1.7 Strategy and Research Project

VASCO's research project is aligned with the three major themes of Section 1.2: Test Generation, Passive Testing, Model Construction and Inference. These themes will enrich each other and transversal research works are foreseen for the next five years. All these researches aim at assessing safe and secure systems, using test and modeling techniques.

Test generation: fuzzing and combinatorial testing The results over the last period have shown that the combination of software engineering techniques (such as dataflow analysis, search based testing, test prioritization) provide significant improvement to fuzzing. Smart fuzzing has been based so far on rather crude models from crawling approaches or finite state models. This can be further improved with more accurate models: we consider developing more synergies between fuzzing and model inference and possibly machine learning techniques. The fuzzing patterns can be defined using a grammar that could also be derived from existing attack patterns, using other grammatical inference approaches than those used for regular languages. Coverage based approaches and diversity-based testing are other directions to be investigated.

Our researches on combinatorial testing have been concretized in the Tobias tool. Improvements of this tool will motivate new researches on this topic. The Tobias tool is mature enough to be applied to validation activities of the group such as test generation for access control policies or to express vulnerability detection patterns. Nevertheless the architecture of the tool may be improved: we intend to shift our test generation principle from the unfolding of bounded regular expressions to the traversal of a directed graph where every path corresponds to an abstract test case. This will impact the combinatorial generation engine, the architecture of the tool and its internal and output formats. This will also inspire the identification of new combinatorial primitives for the Tobias input language, and the definition of post-treatments such as test suite selection and reduction based on graph manipulations.

Passive testing: monitoring and trace analysis We will propose distributed monitoring algorithms that withstand more and more adversarial (and consequently realistic) environments for component-based systems. For example, we will relax the synchronous assumption on both communications and component processing (which were taken for granted in our previous approaches). Moreover, in practical settings, components may have to face faults, in particular the intermittent loss of messages in communication links. Hence, fault-tolerance should be addressed when dealing with distributed monitoring. For this purpose, we will propose solutions that handle unreliable links and component crashes. Moreover, we intend to continue our research work on how to elaborate oracles for dynamical or auto-adaptative systems.

Model construction and inference The B4MSecure platform provides a strong basis to study the validation of access control policies. Our short term project is to use tools associated to the B language (ProB, Genesyst) to automatically generate test cases and find attack scenarios. A PhD thesis has started in 2013 on this topic. Its goal is to characterize the notion of insider attack, and guide the ProB tool to find out such attacks. At longer term, we intend to use ProB, in combination with our Tobias combinatorial generator, in order to generate access control test suites. We also intend to use the B specification as oracle for conformance tests of a given implementation.

Regarding inference, our project aims at further developing the applicability of model inference in model-based software and system engineering. We consider several directions. As a first step, we need to address the issue of systems that cannot be reset, and inference from non initial states. This could lead us to investigate further the connection with probabilistic models. Timed systems and embedded contexts (learning a component inside an architecture) are also natural directions. As a more global goal, we would also like to develop the connection with adaptive computing, esp. with machine learning based on statistical models and the potential of having embedded learners "in the loop" within a system.

Transversal researches There is a huge potential for cross-fertilization of researches within the team.

Our research works on model inference, applied in the context of application crawling and component integration, might also be applied to infer a security policy model from an existing implementation, or to identify a test pattern from a series of existing test cases. And as mentioned earlier, there is a natural overlap betwen smart fuzzing (based on models) and inference.

Another transversal research combines our expertise in test generation and fault localization. Our current approach to fault localization is based on an existing execution trace exhibiting a failure, regardless of how the trace was generated. If the trace was generated using active testing, it is interesting to investigate which test generation technique leads to the most exploitable traces for fault localization, and how test generation can be guided to produce such traces.

1.8 Self assesment

The composition of the VASCO team remained rather constant during the last 5 years, with researches focused on testing, modeling and security.

Regarding publications, the scientific production of the team has increased qualitatively since the previous period. Between 2005 and 2008, we published 5 papers in international journals and 11 in national ones. Between 2009 and 2013, this number raised to 11 papers in international journals and 8 in national ones. There is thus a shift towards more international visibility of our publications. Regarding international conferences, the numbers remained rather constant, but it must be noted that a recent member of the team (Yliès Falcone) had the best paper award at the FM'2012 conference. So we believe that the team has consolidated its scientific production and improved its international visibility.

The team participated to numerous projects. While the previous term was mainly supported by national projects, in this term, we increased our participation to european projects. Both national and international projects involve industrial and academic participants, which helps the team to stay tuned to the challenges and advances of both communities, and helps spreading our research results.

The team has both national and international visibility. National visibility comes from the involvement of several members of the team in the GDR GPL. It also results from our participation to national projects and conferences. International visibility results of our participation to european projects (ITEA, FP7), and recurrent participation in steering, programme or organisation committees of international

conferences. It has been completed by cooperation with Morocco and Tunisia. Our cooperation with Tunisia has attracted PhD and masters students. Our national and international visibility helped attract post-docs from France and India. As a result, we have increased our international visibility but our longer term ambition remains to increase the international visibility of VASCO as a team, and not only as the result of the visibility of its individuals.

A large majority of the funding of VASCO (PhD grants, post-docs, travel budgets) comes from our contracts. This requires to submit projects on a regular basis, but also to dedicate most of our research efforts to these projects. We were very careful to align our participation to these projects with the research themes of the team, or to be at the origin of these projects. As a result, most of these projects contributed to our research goals.

Unfortunately, the current funding schemes of the French research make our team dependent on the success of project submissions. Since 2013, we are experiencing a significant drop of research funding although we multiplied project submissions (european, national, local).

Finally, we stated in the previous term that one of our objectives was to make our tools available to the research community. A significant effort was done to turn our internal research prototypes into distributable tools, asssociated to user documentation. Further efforts may include more integration between these tools, and to promote the visibility of some of these tools in the scientific community.

References

[1] Azzeddine Amiar, Mickaël Delahaye, Yliès Falcone, and Lydie Du Bousquet. CoMET: Compressing Microcontroller Execution Traces to Assist System Understanding. Technical Report RR-LIG-031, INRIA.

[2] Azzeddine Amiar, Mickaël Delahaye, Yliès Falcone, and Lydie Du Bousquet. Résumer les traces d'exécution des micro-contrôleurs. In *Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL 2012)*, Grenoble, France, 2012.

[3] Azzeddine Amiar, Mickaël Delahaye, Yliès Falcone, and Lydie Du Bousquet. Compressing Microcontroller Execution Traces to Assist System Analysis. In Gunar Schirner, Marcelo Marcelo Götz, Achim Achim Rettberg, Mauro C. Zanella, and Franz J. Rammig, editors, *IESS 2013 - 4th IFIP TC 10 International Embedded Systems Symposium*, volume 403 of *IFIP Advances in Information and Communication Technology*, pages 139–150, Paderborn, Allemagne, 2013. Springer.

[4] Andreas Bauer and Yliès Falcone. Decentralized LTL Monitoring. Technical report, March 2012. 31 pages.

[5] Sofia Bekrar, Chaouki Bekrar, Roland Groz, and Laurent Mounier. A Taint Based Approach for Smart Fuzzing. In *Proceedings of ICST 2012*, pages 818–825, Montreal, QC, Canada, April 2012. IEEE Computer Society. VUPEN Security and University of Grenoble.

[6] Matthias Büchler, Karim Hossen, Petru Florin Mihancea, Marius Minea, Roland Groz, and Catherine Oriat. Model Inference and Security Testing in the SPaCIoS Project. In *IEEE Working Conference on Reverse Engineering, CSMR-WCRE 2014*, pages 411–414, Antwerp, Belgique, 2014.

[7] Frédéric Dadeau, Kalou Cabrera Castillos, Yves Ledru, Taha Triki, German Vega, Julien Botella, and Safouan Taha. Test Generation and Evaluation from High-Level Properties for Common Criteria Evaluations - The TASCCC Testing Tool. In *ICST 2013, 6th Int. Conf. on Software Testing, Verification and Validation, Testing Tool track*, pages 431 – 438, Luxembourg, March 2013.

[8] Fabien Duchene, Sanjay Rawat, Jean-Luc Richier, and Roland Groz. A Hesitation Step into the BlackBox: Heuristic-Based Web Applications Reverse Engineering. In *NSC 2013 - NoSuchCon Conference*, Paris, France, May 2013.

[9] Fabien Duchene, Sanjay Rawat, Jean-Luc Richier, and Roland Groz. KameleonFuzz: Evolutionary Fuzzing for Black-Box XSS Detection. In *Fourth ACM Conference on Data and Application Security and Privacy (CODASPY 2014)*, pages 37–48, Unknown, Inconnu, 2014. ACM.

[10] Khaled El-Fakih, Roland Groz, Muhammad Naeem Irfan, and Muzammil Shahbaz. Learning Finite State Models of Observable Nondeterministic Systems in a Testing Context. In *22nd IFIP International Conference on Testing Software and Systems*, pages 97–102, Natal, Brésil, 2010.

[11] Yliès Falcone, Tom Cornebize, and Jean-Claude Fernandez. Efficient and Generalized Decentralized Monitoring of Regular Languages. July 2013.

[12] Yliès Falcone, Jean-Claude Fernandez, Thierry Jéron, Hervé Marchand, and Laurent Mounier. More Testable Properties. In *22nd IFIP International Conference on Testing Software and Systems*, volume 6435 of *Lectures notes in computer science*, pages 30–46, Natal, Brésil, August 2010. Springer.

[13] Yliès Falcone, Jean-Claude Fernandez, Thierry Jéron, Hervé Marchand, and Laurent Mounier. More testable properties. *International Journal on Software Tools for Technology Transfer*, 14(4):407–437, August 2012.

[14] Yliès Falcone, Jean-Claude Fernandez, and Laurent Mounier. What can you verify and Enforce at Runtime? *Sotfware Tools for Technology Transfer*, page Online First, April 2011.

[15] Yliès Falcone, Mohamad Jaber, Thanh-Hung Nguyen, Dorel Marius Bozga, and Saddek Bensalem. Runtime Verification of Component-Based Systems in the BIP Framework with Formally-Proved Sound and Complete Instrumentation. *Journal on Software and System Modeling*, page 41 p., April 2013.

[16] Yliès Falcone, Mohamad Jaber, Thanh-Hung Nguyen, Marius Bozga, and Saddek Bensalem. Runtime Verification of Component-Based Systems. In Gerardo Schneider Gilles Barthe, Alberto Pardo, editor, *Software Engineering and Formal Methods (SEFM 2011)*, volume 7041 of *Lecture Notes in Computer Science (LNCS)*, pages 204–220, Montevideo, Uruguay, October 2011. Springer. FP7 IP ASCENS.

[17] Yves Grasland. *Test fonctionnel de propriétés hybrides.* These, Université de Grenoble, February 2013.

[18] Yves Grasland, Lydie Du Bousquet, Roland Groz, and Ioannis Parissis. A Functional Testing Approach for Hybrid Safety Properties with Incomplete Information. In *6th International Conference on Software Testing and Verification (ICST 2013)*, pages 104–113, Luxembourg, Luxembourg, March 2013.

[19] Roland Groz, Naeem Irfan, Muhammad, and Catherine Oriat. Algorithmic Improvements on Regular Inference of Software Models and Perspectives for Security Testing. In Tiziana Margaria and Bernhard Steffen, editors, *Leveraging Applications of Formal Methods, Verification and Validation. Technologies for Mastering Change*, volume 7609 of *Lecture Notes in Computer Science (LNCS)*, pages 444–457, Crete, Grèce, 2012. Springer.

[20] Karim Hossen, Roland Groz, Catherine Oriat, and Jean-Luc Richier. Automatic generation of test drivers for model inference of web applications. In *SECTEST 2013 - Fourth International Workshop on Security Testing (affiliated with ICST2013)*, pages 441–444, Luxembourg, Luxembourg, 2013. IEEE. Work funded by project SPaCIoS (n ° 257876, FP7-ICT-2009-5, ICT-2009.1.4: Trustworthy ICT).

[21] Akram Idani, Yves Ledru, and Adil Anwar. A rigorous reasoning about model transformations using the B method. In Selmin Nurcan et al., editor, *EMMSAD 2013 - International Conference on Exploring Modelling Methods for Systems Analysis and Design (held at CAiSE 2013)*, volume 147 of *Lecture Notes in Business Information Processing (LNBIP)*, pages 426–440, Valencia, Espagne, 2013. Springer.

[22] Akram Idani, Yves Ledru, and Mohamed-Amine Labiadh. B4MSecure : une plateforme IDM pour la modélisation et la validation de politiques de sécurité en Systèmes d'Information (démo). In Virginie Wiels Jeanine Souquières, editor, *AFADL 2013 - Journées Francophones sur les Approches Formelles dans l'Assistance au Développement de Logiciels*, pages 85–89, Nancy, France, 2013. LORIA et le centre Inria Nancy Grand-Est. Session 10 Projet ANR Selkis (ANR-08-SEGI-018) et Région Rhône-Alpes (ARC6).

[23] Akram Idani, Yves Ledru, and Pierre-Yves Schobbens. Approche formelle pour une Ingénierie des Modèles sûre. In *Atelier LMO/SafeModel*, Nancy, Inconnu, 2009.

[24] Muhammad Naeem Irfan. State Machine Inference in Testing Context with Long Counterexamples. In *Third International Conference on Software Testing, Verification and Validation, ICST 2010*, pages 508–511, Paris, France, 2010. IEEE Computer Society.

[25] Muhammad Naeem Irfan. *Analyse et optimisation d'algorithmes pour l'inférence de modèles de composants logiciels*. These, Université de Grenoble, September 2012.

[26] Muhammad Naeem Irfan, Roland Groz, and Catherine Oriat. Improving Model Inference of Black Box Components having Large Input Test Set. In *JMLR Workshop and Conference Proceedings*, volume 21, pages 133–138, College Park, MD, États-Unis, August 2012. http://jmlr.org/proceedings/papers/v21/.

[27] Muhammad Naeem Irfan, Catherine Oriat, and Roland Groz. Model Inference and Testing. In Atif Memon, editor, *Advances in Computers*, volume 89, pages 89–139. Elsevier, 2013. Chapter 3.

[28] Yves Ledru, Akram Idani, Jérémy Milhau, Muhammad Nafees Qamar, Régine Laleau, Jean-Luc Richier, and Mohamed-Amine Labiadh. Taking into Account Functional Models in the Validation of IS Security Policies. In Camille Salinesi and Oscar Pastor, editors, *Advanced Information Systems Engineering Workshops (CAiSE 2011)*, volume 83 of *Lecture Notes in Business Information Processing*, pages 592–606, London, Royaume-Uni, 2011. Springer. M.-A. Labiadh's work was partly supported by the ANR-08-SEGI-018 Selkis and ANR-09-SEGI-014 TASCCC projects.

[29] Yves Ledru, Akram Idani, Jérémy Milhau, Muhammad Nafees Qamar, Régine Laleau, Jean-Luc Richier, and Mohamed-Amine Labiadh. Validation of IS Security Policies featuring Authorisation Constraints. *International Journal of Information System Modeling and Design (IJISMD)*, 2014.

[30] Yves Ledru, Alexandre Petrenko, Sergiy Boroday, and Nadine Mandran. Prioritising Test Cases with String Distances. *Automated Software Engineering*, 19(1):65–95, March 2012. NSERC discovery grant OGP0194381.

[31] Yves Ledru, Muhammad Nafees Qamar, Akram Idani, Jean-Luc Richier, and Mohamed-Amine Labiadh. Validation of Security Policies by the Animation of Z Specifications. In Jorge Lobo Ruth Breu, Jason Crampton, editor, *Proceedings of the 16th ACM Symposium on Access control models and technologies (SACMAT 2011)*, pages 155–164, Innsbruck, Autriche, June 2011. ACM.

[32] Yves Ledru, German Eduardo Vega Baez, Taha Triki, and Lydie Du Bousquet. Test Suite Selection Based on Traceability Annotations. In *Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering (ASE 2012)*, pages 342–345, Essen, Allemagne, 2012. ACM. Session: Tool demonstration.

[33] Virginia Papailiopoulou. *Test automatique de programmes Lustre/SCADE*. These, Université Joseph-Fourier - Grenoble I, February 2010.

[34] Virginia Papailiopoulou, Ajitha Rajan, and Ioannis Parissis. Structural Test Coverage Criteria for Integration Testing of LUSTRE/SCADE Programs. In *Workshop on Formal Methods for Industrial Critical Systems (FMICS)*, pages 85–101, Trento, Italie, August 2011.

[35] Virginia Papailiopoulou, Besnik Seljimi, and Ioannis Parissis. Revisiting the Steam-Boiler Case Study with LUTESS : Modeling for Automatic Test Generation. In *Proceedings of the 12th European Workshop on Dependable Computing, EWDC 2009*, page 8 pages, Toulouse, France, May 2009. Helène WAESELYNCK.

[36] Virginia Papailiopoulou, Besnik Seljimi, and Ioannis Parissis. Automatic Test of Lustre/SCADE Programs. In *Model-Based Testing for Embedded Systems*, pages 171–194. CRC Press, September 2011.

[37] Ioannis Parissis, Laya Madani, and Virginia Papailiopoulou. Towards a testing methodology for reactive systems: a case study of a landing gear controller. In *Proceedings of the 3th International Conference on Software Testing and Verification (ICST 2010)*, pages 489 – 497, Paris, France, April 2010.

[38] Alexandre Petrenko, Keqin Li, Roland Groz, Karim Hossen, and Catherine Oriat. Inferring Approximated Models for Systems Engineering. In *15th IEEE International Symposium on High Assurance Systems Engineering (HASE 2014)*, pages 249–253, Miami, Florida, États-Unis, 2014.

[39] Srinivas Pinisetty, Yliès Falcone, Thierry Jéron, and Hervé Marchand. Runtime Enforcement of Parametric Timed Properties with Practical Applications. In *IEEE International Workshop on Discrete Event Systems*, cachan, France, 2014.

[40] Srinivas Pinisetty, Yliès Falcone, Thierry Jéron, and Hervé Marchand. Runtime Enforcement of Regular Timed Properties. In ACM, editor, *Software Verification and Testing, track of the Symposium on Applied Computing ACM-SAC 2014*, pages 1279–1286, Gyeongju, Corée, République De, 2014.

[41] Srinivas Pinisetty, Yliès Falcone, Thierry Jéron, Hervé Marchand, Antoine Rollet, and Omer Landry Nguena Timo. Runtime Enforcement of Timed Properties. In *3rd International Conference on Runtime Verification*, volume 7687 of *Lecture Notes in Computer Science (LNCS)*, pages 229–244, Istanbul, Turquie, 2013. Springer.

[42] Muhammad nafees Qamar. *Spécification et animation de modèles de conception de la sécurité avec Z.* These, Université de Grenoble, December 2011.

[43] Muhammad Nafees Qamar, Yves Ledru, and Akram Idani. Validation of Security-Design Models using Z. In Zongyan Qiu Shengchao Qin, editor, *Formal Methods and Software Engineering (ICFEM 2011)*, volume 6991 of *Lecture Notes in Computer Science (LNCS)*, pages 259–274, Durham, Royaume-Uni, October 2011. Springer. ANR Selkis and TASCCC Projects under grants ANR-08-SEGI-018 and ANR-09-SEGI-014.

[44] Nafees Qamar, Johannes Faber, Yves Ledru, and Zhiming Liu. Automated Reviewing of Healthcare Security Policies. In Isabelle Perseil Jens Weber, editor, *Foundations of Health Information Engineering and Systems*, volume 7789 of *Lecture Notes in Computer Science (LNCS)*, pages 176–193, Paris, France, 2013. Springer.

[45] Besnik Seljimi. *Test de logiciels synchrones avec la PLC.* These, Université Joseph-Fourier - Grenoble I, July 2009.

[46] Tor Stålhane, Guttorm Sindre, and Lydie Du Bousquet. Comparing Safety Analysis Based on Sequence Diagrams and Textual Use Cases. In *Advanced Information Systems Engineering, 22nd International Conference (CAiSE)*, volume 6051 of *Lecture Notes in Computer Science*, pages 165–179, Hammamet, Tunisie, 2010. Springer.

[47] Taha Triki. *Filtrage et réduction de tests combinatoires.* These, Université de Grenoble, October 2013.

[48] Taha Triki, Lydie Du Bousquet, and Yves Ledru. Réduction de suites de tests avec des critères d'équivalence basés sur la couverture structurelle. In *Actes de la Conférence AFADL 2012*, pages 120–134, Grenoble, France, January 2013. http://membres-liglab.imag.fr/idani/AFADL2012/programme.html.

[49] Taha Triki, Yves Ledru, Lydie Du Bousquet, Frédéric Dadeau, and Julien Botella. Model-Based Filtering of Combinatorial Test Suites. In *FASE'2012, 15th Int. Conf. on Fundamental Approaches to Software Engineering*, pages 439 – 454, Estonie, March 2012.