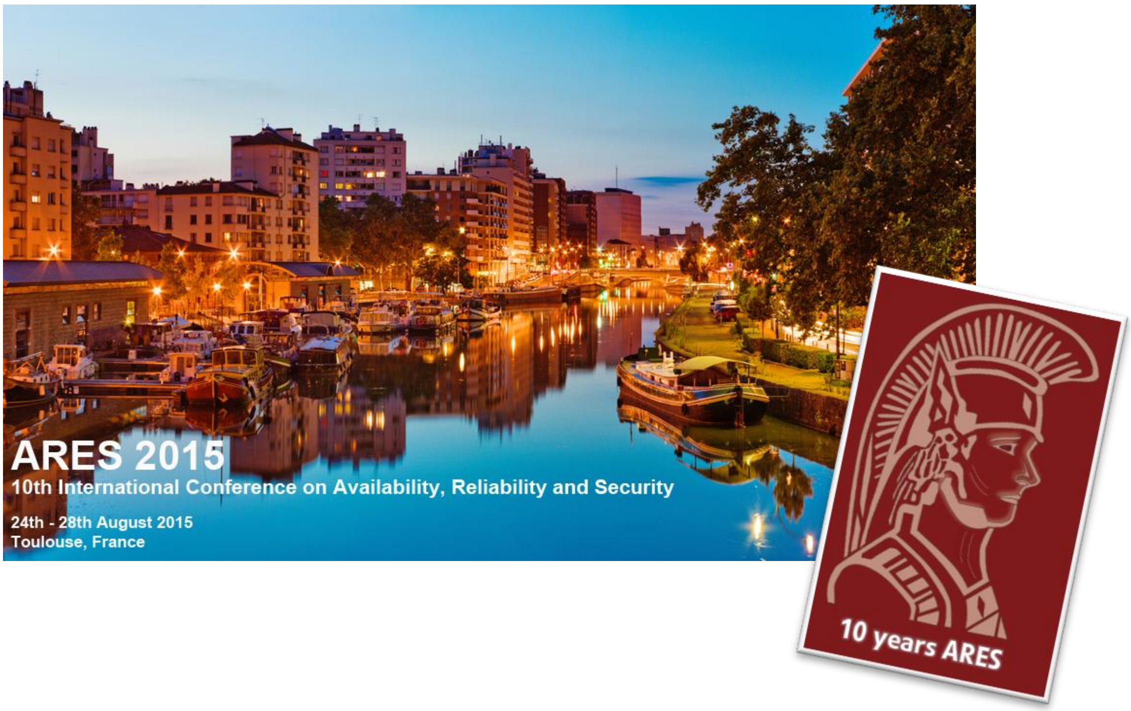
ARES Conference
International Conference on Availability, Reliability and Security

ARES 2015

10th International Conference on Availability, Reliability and Security

24-28 August 2015
Toulouse, France


ARES 2015
10th International Conference on Availability, Reliability and Security
24th - 28th August 2015
Toulouse, France
10 years ARES

Organized by....

SBA Research

Université Toulouse III Paul Sabatier

IRIT CNRS - INPT - UPS - UT1 - UTM

Supported by....

ICT Knowledge Transfer Society

Technische Universität Wien
Vienna University of Technology

Table of Content

Welcome to ARES 2015

It is our great pleasure to welcome you to the Tenth International Conference on Availability, Reliability and Security (ARES 2015).

The Tenth International Conference on Availability, Reliability and Security (ARES 2015) brings together researchers and practitioners in the field of dependability and information assurance. ARES 2015 highlights the various aspects of dependability, following the tradition of previous ARES conferences, again with a special focus on the crucial linkage between availability, reliability, security and privacy. ARES 2015 is dedicated to expanding collaborations between different sub-disciplines and to strengthening the community for further research which, previous ARES conferences have started to build.

This year we are very happy to welcome three well-known keynote speakers: Peter Eckersley (*EFF Technology Projects Director),* Rainer Böhme (*University of Innsbruck, Austria) and* Pierangela Samarati (*Università degli Studi di Milano, Italy).* Further we are happy to welcome Afonso Ferreira *(Trust & Security Unit, European Commission)* who will give an invited talk.

From the many submissions we have selected the **17** best for a presentation as full paper. The quality of submissions has steadily improved over the last years and the conference officers sometimes faced a difficult decision when selecting which papers should be accepted. This year's acceptance rate for full papers only is **29%**. In addition, several workshops and short papers are included in the program and show intermediate results of ongoing research projects and offer interesting starting points for discussions. The ARES EU Projects Symposium is held for the first time in conjunction with the ARES Conference. The goal is to disseminate the results of EU research projects, meet potential project partners and exchange ideas within the scientific community.
ARES celebrates its 10th anniversary in Toulouse - and we are proud to present a truly diverse program at ARES 2015, consisting not only of ARES sessions but also a variety of interesting workshop sessions, the ARES EU Symposium, three keynote speeches and one invited talk as well as a social program, which will give you the opportunity to share ideas with other researchers and practitioners from institutions around the world and see all the beautiful sights of Toulouse and surroundings.

Putting together ARES 2015 was a team effort. We first thank the authors for providing the content of the program. We are grateful to the program committee, who worked very hard in reviewing papers and providing feedback for authors. Finally, we thank all workshop chairs for their efforts in organizing interesting workshop sessions.

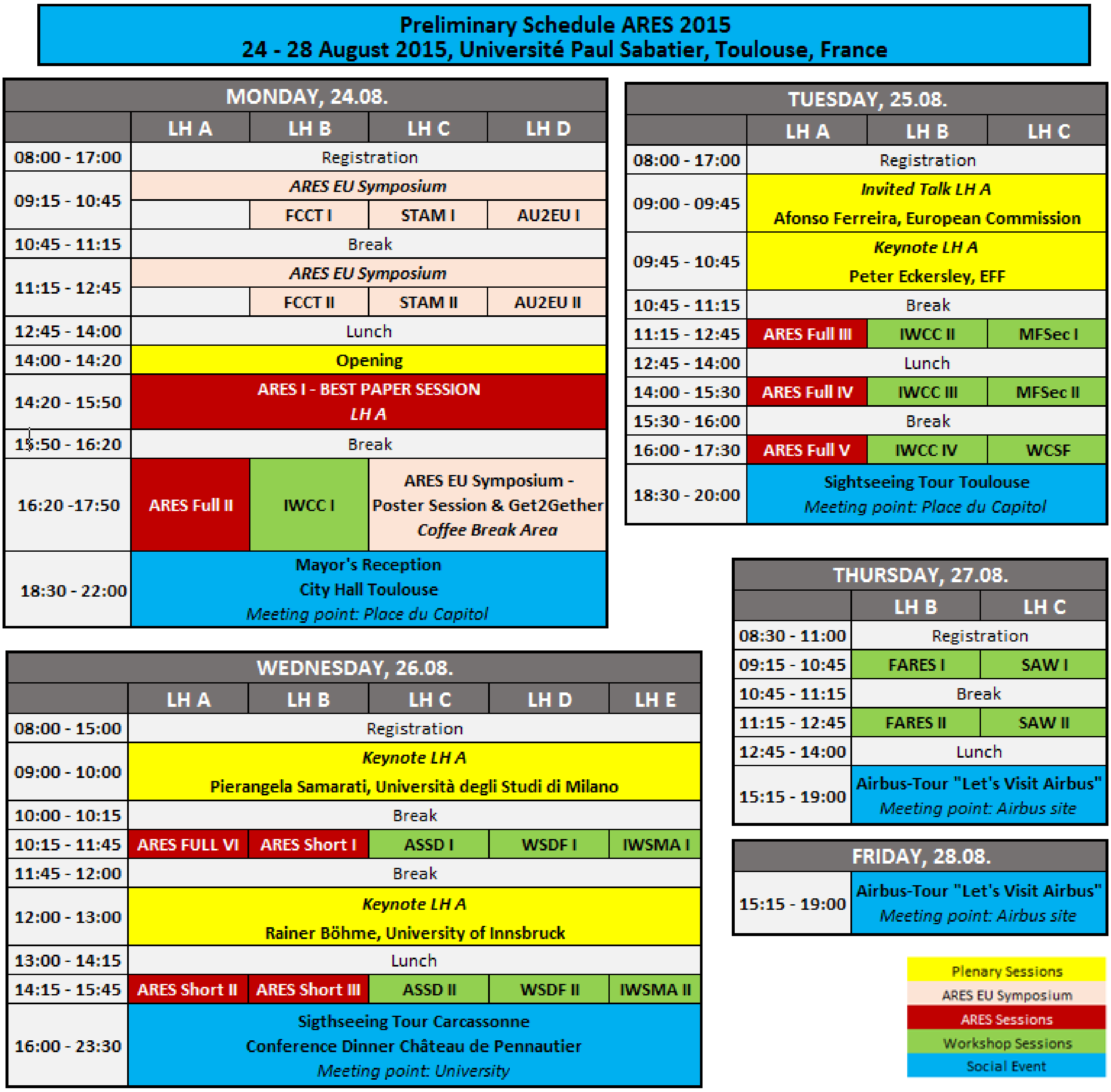
A different country hosts the conference every year. The 2015 edition takes place in Toulouse, France at the Université Paul Sabatier. We would like to thank the Université Paul Sabatier and the Institut de Recherche en Informatique de Toulouse for hosting ARES 2015!

We hope that you will find this program interesting and thought-provoking.
Enjoy ARES 2015 and Toulouse!

Stefan Katzenbeisser
ARES 2015 Program Chair
TU Darmstadt & CASED, Germany

Abdelmalek Benzekri
ARES 2015 General Chair
Université Paul Sabatier, France

Program Overview



Preliminary Schedule ARES 2015
24 - 28 August 2015, Université Paul Sabatier, Toulouse, France

MONDAY, 24.08.				
	LH A	LH B	LH C	LH D
08:00 - 17:00	Registration			
09:15 - 10:45	*ARES EU Symposium*			
		FCCT I	STAM I	AU2EU I
10:45 - 11:15	Break			
11:15 - 12:45	*ARES EU Symposium*			
		FCCT II	STAM II	AU2EU II
12:45 - 14:00	Lunch			
14:00 - 14:20	Opening			
14:20 - 15:50	ARES I - BEST PAPER SESSION *LH A*			
15:50 - 16:20	Break			
16:20 -17:50	ARES Full II	IWCC I	ARES EU Symposium - Poster Session & Get2Gether *Coffee Break Area*	
18:30 - 22:00	Mayor's Reception City Hall Toulouse *Meeting point: Place du Capitol*			

TUESDAY, 25.08.			
	LH A	LH B	LH C
08:00 - 17:00	Registration		
09:00 - 09:45	*Invited Talk LH A* Afonso Ferreira, European Commission		
09:45 - 10:45	*Keynote LH A* Peter Eckersley, EFF		
10:45 - 11:15	Break		
11:15 - 12:45	ARES Full III	IWCC II	MFSec I
12:45 - 14:00	Lunch		
14:00 - 15:30	ARES Full IV	IWCC III	MFSec II
15:30 - 16:00	Break		
16:00 - 17:30	ARES Full V	IWCC IV	WCSF
18:30 - 20:00	Sightseeing Tour Toulouse *Meeting point: Place du Capitol*		

WEDNESDAY, 26.08.					
	LH A	LH B	LH C	LH D	LH E
08:00 - 15:00	Registration				
09:00 - 10:00	*Keynote LH A* Pierangela Samarati, Università degli Studi di Milano				
10:00 - 10:15	Break				
10:15 - 11:45	ARES FULL VI	ARES Short I	ASSD I	WSDF I	IWSMA I
11:45 - 12:00	Break				
12:00 - 13:00	*Keynote LH A* Rainer Böhme, University of Innsbruck				
13:00 - 14:15	Lunch				
14:15 - 15:45	ARES Short II	ARES Short III	ASSD II	WSDF II	IWSMA II
16:00 - 23:30	Sigthseeing Tour Carcassonne Conference Dinner Château de Pennautier *Meeting point: University*				

THURSDAY, 27.08.		
	LH B	LH C
08:30 - 11:00	Registration	
09:15 - 10:45	FARES I	SAW I
10:45 - 11:15	Break	
11:15 - 12:45	FARES II	SAW II
12:45 - 14:00	Lunch	
15:15 - 19:00	Airbus-Tour "Let's Visit Airbus" *Meeting point: Airbus site*	

FRIDAY, 28.08.	
15:15 - 19:00	Airbus-Tour "Let's Visit Airbus" *Meeting point: Airbus site*

Plenary Sessions
ARES EU Symposium
ARES Sessions
Workshop Sessions
Social Event

Monday 24th August 2015

08:00 – 17:00 Registration desk open

09:15 – 10:45 Parallel Sessions – ARES EU Symposium

ARES EU Symposium – AU2EU I

Session Chair: John Zic (CSIRO, Australia)

Location: Lecture Hall D

Time: 09:15 – 10:45

1. Invited Talk: Anonymous Authentication in a Cloud Context

Jan Camenisch (IBM Research, Switzerland)

Abstract: The cloud provides a new model for the deployment and development of services and applications. This model that makes deployment and development significantly easier. However, it also means that some or all components of an application run somewhere in the cloud and thus also potentially process user data in the cloud, i.e., in a domain that is not necessarily controlled by the owner of the data. In this talk we look at the case of how the different components of an anonymous authentication system can be used in conjunction with the cloud model, identify potential issues and discuss how they can be addressed.

2. AU2EU: Integrated eAuthentication and eAuthorization platform for Collaborative Services (presentation only)

Milan Petkovic (Philips Research / Eindhoven University of Technology, Netherlands)

3. A secure integrated platform for rapidly formed multiorganisation collaboration

John Zic, Nerolie Oakes, Dongxi Liu, Jane Li, Chen Wang, Shiping Chen (CSIRO, Australia)

Abstract: Establishing secure collaborations between multiple organisations, potentially who are in competitors, requires substantial careful attention to how information is exchanged during the collaboration, from the formulation of policies and agreements between the organisations that govern the collaboration at the most abstract level, through to authentication and authorisation services and down to secure network and storage infrastructure. This paper presents a high level description of the secure integrated collaboration platform for distributed groups that has been developed and deployed as a part of a pilot for the AU2EU project. This secure platform utilises advanced eAuthentication and eAuthorisation services integrated into an advanced real-time collaborative system offering high definition telepresence combined with a secure common shared workspace that gives capability based collaborative access to specialised instruments, data sets and images.

4. Attribute Based Authentication and Authorization for Collaborative Services

Stefan Thaler, Jerry den Hartog (Technical University of Eindhoven, Netherlands), Dhouha Ayed (Theresis Lab - Thales, France), Dieter Sommer (IBM Research, Switzerland), Michael Hitchens (Macquarie University, Australia)

Abstract: In bio-security emergencies, such as an outbreak of an exotic animal disease, it is essential that the organizations involved in combating this outbreak collaborate effectively and efficiently. To achieve such a collaboration potentially confidential infrastructure and resources need to be shared amongst members of the participating organizations. In AU2EU we demonstrate the combination of existing data minimizing authentication, attribute-based authorization technologies to dynamically enable collaborations between these organizations. However, a key problem that occurs during the establishment of such collaboration is different terminologies for similar authorization attributes. To overcome these differences and to minimize the overhead for new organizations to join an existing consortium we propose an ontology-based solution for converting attributes from one domain vocabulary to another. Additionally, we propose a methodology to construct a shared domain vocabulary. Using a shared domain vocabulary in the conversion process decreases the amount of alignments required for collaborating. We integrate and demonstrate the feasibility of this approach in a real-life scenario within the scope of AU2EU. This paper presents preliminary work, which is currently being deployed and will be evaluated in the upcoming months.

ARES EU Symposium – FCCT I

Session Chair: Peter Kieseberg (SBA Research, Austria)

Location: Lecture Hall B

Time: 09:15 – 10:45

1. Welcome & Presentation of the CyberRoad project

David Ariu (University of Cagliari, Italy)

2. Keynote: Risk-centric threat modelling of cybercrime threats targeting the financial sector

Marco Morana (Managing Director Minded Security, UK)

3. 0-Day Vulnerabilities and Cybercrime

Jart Armin, Paolo Foti (CyberDefcon, UK)

Abstract: This study analyses 0-day vulnerabilities in the broader context of cybercrime and economic markets. The work is based on the interviews of several leading experts and on a field research of the authors. In particular, cybercrime is considered when involving traditional criminal activities or when military operations are involved. A description of different 0-day vulnerability markets - White, Black and Government markets - is provided, as well as the characteristics of malware factories and their major customers are discussed.

4. Integrating Human Behavior into the Development of Future Cyberterrorism Scenarios

Max Kilger (University of Texas at San Antonio, USA)

Abstract: The development of future cyberterrorism scenarios is a key component in building a more comprehensive understanding of cyber threats that are likely to emerge in the near- to mid-term future. While developing concepts of likely new, emerging digital technologies is an important part of this process, this article suggests that understanding the psychological and social forces involved in cyberterrorism is also a key component in the analysis and that the synergy of these two dimensions may produce more accurate and detailed future cyber threat scenarios than either analytical element alone.

ARES EU Symposium – STAM I – Security Testing and Monitoring Solutions

Session Chair: Ana Cavalli (Montimage, France)

Location: Lecture Hall C

Time: 09:15 – 10:45

1. Security Monitoring in the Cloud: an SLA-based approach

Valentina Casola, Alessandra De Benedictis (University of Napoli Federico II, Italy), Massimiliano Rak (University of Napoli Federico II, Italy)

Abstract: In this paper we present a monitoring architecture that is automatically configured and activated based on a signed Security SLA. Such monitoring architecture integrates different security-related monitoring tools (either developed ad-hoc or already available as open-source or commercial products) to collect measurements related to specific metrics associated with the set of security Service Level Objectives (SLOs) that have been specified in the Security SLA. To demonstrate our approach, we discuss a case study related to detection and management of vulnerabilities and illustrate the integration of the popular open source monitoring system OpenVAS into our monitoring architecture. We show how the system is configured and activated by means of available Cloud automation technologies and provide a concrete example of related SLOs and metrics.

2. An Active Testing Tool for Security Testing of Distributed Systems

Mohamed H. E AOUADI, Khalifa TOUMI, Ana Cavalli (TELECOM SudParis, France)

Abstract: This paper describes the TestGen-IF tool that allows the automatic generation of test cases based on model based active testing techniques. This paper describes the overall functionality and architecture of the tool, discusses its strengths and weaknesses, and reports our experience with using the tool on a case study, the Dynamic Route Planning (DRP) service of Vehicular Networks. This case study demonstrates how to use our testing tool to verify the system implementation against its security requirements. This paper also proposes improvements to this tool in the form of a GUI interface to facilitate its use and an approach which permits a gain in time and efficiency by generating test objectives.

3. TEAR: a Multi-purpose Formal Language Specification for TEsting At Runtime

Jorge López, Stephane Maag (Institut Mines Telecom, Telecom SudParis, France), Gerardo Morales (Universidad Galileo, Guatemala)

Abstract: Collaborative systems are growing in use and in popularity. The need to boost the methods concerning the interoperability is growing as well; therefore, trustworthy interactions of the different systems are a priority. We have proposed a formal distributed network monitoring approach to analyse the packets exchanged by the entities, in order to prove a system is acting in a trustworthy manner. Using this approach, some limitations regarding the tester's resources have been found. In this paper, we identify the constraints and propose and new language suited for testing at runtime in different environments.

10:45 – 11:15 Coffee Break

11:15 – 12:45 Parallel Sessions – ARES EU Symposium

ARES EU Symposium – AU2EU II

Session Chair: Milan Petkovic (Philips Research / Eindhoven University of Technology, Netherlands)
Location: Lecture Hall D
Time: 11:15 – 12:45

1. Virtual Machine Introspection: Techniques and Applications

Yacine Hebbal (Ecole des Mines de Nantes, France), Sylvie Laniepce (Orange Labs, France), Jean-Marc Menaud (Ecole des Mines de Nantes, France)

Abstract: Virtual Machine Introspection (VMI) is a technique that enables monitoring virtual machines at the hypervisor layer. This monitoring concept has gained recently a considerable focus in computer security research due to its complete but semantic less visibility on virtual machines activities and isolation from them. VMI works range from addressing the semantic gap problem to leveraging explored VMI techniques in order to provide novel hypervisor-based services that belong to different fields. This paper aims to survey and classify existing VMI techniques and their applications.

2. The Measurement of Data Locations in the Cloud

Ulrich Waldmann, Annika Selzer (Fraunhofer Institute for Secure Information Technology, Germany), Sebastian Luhn (Westfaelische Wilhelms-Universitaet Muenster, Germany), Reiner Kraft (Fraunhofer Institute for Secure Information Technology, Germany), Bernd Jaeger (COLT Technology Services, Germany)

Abstract: If a company uses cloud computing services to process their employees' or their customers' personal data, they need to ensure that the cloud provider complies with the relevant privacy statues. One of the things that need to be ensured is that all personal data are processed only in lawful locations. Data sources that can be used to automatically determine the current location of data processing could help cloud users to fulfil their duty and to strengthen the confidence in a privacy friendly processing of their personal data. For that, data location metrics need to be defined, appropriate data sources need to be determined and the measured data need to be combined reasonable. This paper describes the procedure and system architecture of such data location metrics.

3. Nomad: A Framework for Developing Mission-Critical Cloud-based Applications

Mamadou Diallo, Michael August, Roger Hallman, Megan Kline, Henry Au, Vic Beach (US Department of Defense, USA)

Abstract: The practicality of existing techniques for processing encrypted data stored in untrusted cloud environments is a limiting factor in the adoption of cloud-based applications. Both public and private sector organizations are reluctant to push their data to the cloud due to strong requirements for security and privacy of their data. In particular, mission-critical defence applications used by governments do not tolerate any leakage of sensitive data. In this paper, we propose Nomad, a framework for developing mission-critical cloud-based applications. The framework is comprised of: 1) a homomorphic encryption-based service for processing encrypted data directly within the untrusted cloud infrastructure, and 2) a client service for encrypting and decrypting data within the trusted environment, and storing and retrieving these data to and from the cloud. Both services

are equipped with GPU-based parallelization to accelerate the expensive homomorphic encryption operations. To evaluate the Nomad framework, we developed CallForFire, a mission-critical application which enables defence personnel to call for fire on targets. Due to the nature of the mission, this application requires guaranteed security. The experimental results highlight the performance enhancements of the GPUbased acceleration mechanism and the feasibility of the Nomad framework.

ARES EU Symposium – FCCT II

Session Chair: Peter Kieseberg (SBA Research, Austria)
Location: Lecture Hall B
Time: 11:15 – 12:45

1. 2020 Cybercrime Economic Costs: No measure No solution

Giorgio Giacinto, Davide Ariu, Fabio Roli (UNICA, Italy), Piotr Kijewski (CERT. Polska/NASK, Poland), Bryn Thompson, Jart Armin (CyberDefcon.com/HostExploit.com, UK)

Abstract: Governments needs reliable data on crime in order to both devise adequate policies, and allocate the correct revenues so that the measures are cost-effective, i.e., the money spent in prevention, detection, and handling of security incidents is balanced with a decrease in losses from offences. The analysis of the actual scenario of government actions in cyber security shows that the availability of multiple contrasting figures on the impact of cyber-attacks is holding back the adoption of policies for cyber space as their cost-effectiveness cannot be clearly assessed. The most relevant literature on the topic is reviewed to highlight the research gaps and to determine the related future research issues that need addressing to provide a solid ground for future legislative and regulatory actions at national and international levels.

2. Comprehensive Approach to Increase Cyber Security and Resilience

Michal Choras, Rafal Kozik (University of Science and Technology in Bydgoszcz, Poland), Maria Pilar Torres Bruna (Everis Aeroespacial y Defensa sl, Spain), Artsiom Yautsiukhin (Consiglio Nazionale delle Ricerche, Italy), Andrew Churchill (CBRNE Ltd, UK), Iwona Maciejewska (DFRC AG, Switzerland), Irene Eguinoa (S21sec, Spain), Adel Jomni (Université de Montpellier, France)

Abstract: In this paper the initial results of the European project CAMINO in terms of the realistic roadmap to counter cybercrime and cyber terrorism are presented. The roadmap is built in accordance to so called CAMINO THOR approach, where cyber security is perceived comprehensively in 4 dimensions: Technical, Human, Organisational, and Regulatory.

3. Yet Another Cybersecurity Roadmapping Methodology

Davide Ariu, Luca Didaci, Giorgio Fumera (University of Cagliari, Italy), Enrico Frumento, Federica Freschi (CEFRIEL - ICT Institute Politecnico di Milano, Italy), Giorgio Giacinto, Fabio Roli (University of Cagliari, Italy)

Abstract: In this paper we describe the road mapping methodology we developed in the context of the CyberROAD EU FP7 project, whose aim is to develop a research roadmap for cybercrime and cyber terrorism. To this aim we built on state-of-the-art methodologies and available guidelines, including related projects, and adapted them to the peculiarities of our road mapping subject. In particular, its distinctive feature is that cybercrime and cyber terrorism co-evolve with their contextual environment (i.e., technology, society, politics and economy), which poses specific challenges to a road mapping effort. Our approach can become a best practice in the field of cybersecurity, and can be also generalised to phenomena that exhibit a similar, strong co-evolution with their contextual environment. We aim to describe here the road mapping methodology that will lead to the roadmap but not the roadmap itself (this one being, incidentally, still under construction at the time of writing this paper).

ARES EU Symposium – STAM II – Security in Virtualized and Cloud environments

Session Chair: Wissam Mallouli (Montimage, France)

Location: Lecture Hall C

Time: 11:15 – 12:45

1. Monitoring and Securing New Functions Deployed in a Virtualized Networking Environment

Bertrand Mathieu (Orange Labs, France), Guillaume Doyen (Charles Delaunay Institute, France), Wissam Mallouli (Montimage, France), Thomas Silverston (Loria, France), Olivier Bettan, François-Xavier Aguessy (Thales Services, France), Thibault Cholez, Abdelkader Lahmadi (Loria, France), Patrick Truong (Orange Labs, France), Edgardo Montes de Oca (Montimage, France)

Abstract: Network operators are currently very cautious before deploying a new network equipment. This is done only if the new networking solution is fully monitored, secured and can provide rapid revenues (short Return of Investment). For example, the NDN (Named Data Networking) solution is admitted as promising but still uncertain, thus making network operators reluctant to deploy it. Having a flexible environment would allow network operators to initiate the deployment of new network solutions at low cost and low risk. The virtualization techniques, appeared a few years ago, can help to provide such a flexible networking architecture. However, with it, emerge monitoring and security issues which should be solved. In this paper, we present our secure virtualized networking environment to deploy new functions and protocol stacks in the network, with a specific focus on the NDN use-case as one of the potential Future Internet technology. As strong requirements for a network operator, we then focus on monitoring and security components, highlighting where and how they can be deployed and used. Finally, we introduce our preliminary evaluation, with a focus on security, before presenting the testbed, involving end-users consuming real contents, that we will set up for the assessment of our approach.

2. MUSA: MUlti-cloud Secure Applications – Objectives and challenges (presentation only)

Erkuden Rios (TECNALIA, Spain)

3. CLARUS: A framework for user centred privacy and security in the cloud (presentation only)

Frederic Brouille (AKKA, France)

12:45 – 14:00 Lunch

14:00 – 15:50 Plenary Session

14:00 – 14:20 Opening

ARES Full I – Best Paper Session

Session Chair: Stefan Katzenbeisser (TU Darmstadt, Germany)

Location: Lecture Hall A

Time: 14:20 – 15:50

1. A Novel Security-Enhanced Agile Software Development Process Applied in an Industrial Setting

Dejan Baca (Ericsson AB, Sweden), Martin Boldt, Bengt Carlsson (Blekinge Institute of Technology, Sweden), Andreas Jacobsson (Malmö University, Sweden)

Abstract: A security-enhanced agile software development process, SEAP, is introduced in the development of a mobile money transfer system at Ericsson Corp. A specific characteristic of SEAP is that it includes a security group consisting of four different competences, i.e., security manager, security architect, security master and penetration tester. Another significant feature of SEAP is an integrated risk analysis process. In analysing risks in the development of the mobile money transfer system, a general finding was that SEAP either solves risks that were previously postponed or solves a larger proportion of the risks in a timely manner. The previous software development process, i.e., the baseline process of the comparison outlined in this paper, required 2.7 employee hours spent for every risk identified in the analysis process compared to, on the average, 1.5 hours for

the SEAP. The baseline development process left 50% of the risks unattended in the software version being developed, while SEAP reduced that figure to 22%. Furthermore, SEAP increased the proportion of risks that were corrected from 12.5% to 67.1%, i.e., more than a five times increment. This is important, since an early correction may avoid severe attacks in the future. The security competence in SEAP accounts for 5% of the personnel cost in the mobile money transfer system project. As a comparison, the corresponding figure, i.e., for security, was 1% in the previous development process.

2. Optimizing IT Service Costs With Respect to the Availability Service Level Objective

Sascha Bosse, Matthias Splieth, Klaus Turowski (Otto von Guericke University Magdeburg, Germany)

Abstract: Meeting the availability service level objective while minimizing the costs of the IT service provision is a major challenge for IT service designers. In order to optimize component choices and redundancy mechanisms, the redundancy allocation problem (RAP) was defined. RAP solution algorithms support decision makers with (sub) optimal design configurations that trade-off availability and costs. However, the existing RAP definitions are not suitable for IT service design since they do not include inter-component dependencies such as common mode failures. Therefore, a RAP definition is provided in this paper in which the characteristics of modern IT systems such as standby mechanisms, performance degradation and generic dependencies are integrated. The RAP definition and an adapted genetic algorithm are applied to optimize the costs of an excerpt of an application service provider's IT system landscape. The results demonstrate that the developed approach is applicable and suitable to minimize IT service costs while fulfilling the availability guarantees that are documented in service level agreements.

3. Structural Weaknesses in the Open Smart Grid Protocol

Klaus Kursawe, Christiane Peters (European Network for Cyber Security The Hague, Netherlands)

Abstract: The Open Smart Grid Protocol (OSGP) is currently deployed in various countries in large-scale Smart Metering projects. The protocol was developed by the OSGP Alliance and published as a standard by the European Telecommunications Standards Institute (ETSI). We identify several security issues in the OSG Protocol, primarily the use of a weak digest function and the way the protocol utilizes the RC4 algorithm for encryption. A straight-forward oracle attack triggers the leakage of key material of the digest function. We outline how an attacker can make use of the simple protocol structure to send maliciously altered messages with valid authentication tags to the meters.

15:50 – 16:20 Coffee Break

16:20 – 17:50 Parallel Sessions

ARES EU Symposium - Get2Gether and Poster Session

Location: Coffee Break Area
Time: 16:20 – 17:50

During the ARES EU Symposium Get2Gether, representatives from EU funded projects will present their latest advances (following the EU project workshops). Projects will be presented in the dedicated poster session, which serves as networking platform and should help to find new project partners for upcoming calls.

ARES Full II – Identity and Privacy

Session Chair: Edgar Weippl (SBA Research, Austria)
Location: Lecture Hall A
Time: 16:20 – 17:50

1. Advanced Identity and Access Policy Management using Contextual Data

Matthias Hummer, Michael Kunz (University of Regensburg, Germany), Michael Netter, Ludwig Fuchs (Nexis GmbH, Germany), Günther Pernul (University of Regensburg, Germany)

Abstract: Due to compliance and IT security requirements, company-wide Identity and Access Management within organizations has gained significant importance in research and practice over the last years. Companies aim at standardizing user management policies in order to reduce administrative overhead and strengthen IT security. Despite of its relevance, hardly any supportive means for the automated detection and refinement as well as management of policies are available. As a result, policies outdate over time, leading to security vulnerabilities and inefficiencies. Existing research mainly focuses on policy detection without providing the required guidance for policy management. This paper closes the existing gap by proposing a Dynamic Policy Management Process which structures the activities required for policy management in Identity and Access Management environments. In contrast to current approaches it fosters the consideration of contextual user management data for policy detection and refinement and offers result visualization techniques that foster human understanding. In order to underline its applicability, this paper provides a naturalistic evaluation based on real-life data from a large industrial company.

2. Publicly Verifiable Private Aggregation of Time-Series Data

Bence Gábor Bakondi, Andreas Peter (University of Twente, Netherlands), Maarten Everts (TNO, Netherlands Organisation for Applied Scientific Research, Netherlands), Pieter Hartel, Willem Jonker (University of Twente, Netherlands)

Abstract: Aggregation of time-series data offers the possibility to learn certain statistics over data periodically uploaded by different sources. In case of privacy sensitive data, it is desired to hide every data provider's individual values from the other participants (including the data aggregator). Existing privacy preserving time-series data aggregation schemes focus on the sum as aggregation means, since it is the most essential statistics used in many applications such as smart metering, participatory sensing, or appointment scheduling. However, all existing schemes have an important drawback: they do not provide verifiable outputs, thus users have to trust the data aggregator that it does not output fake values. We propose a publicly verifiable data aggregation scheme for privacy preserving time-series data summation. We prove its security and verifiability under the XDH assumption and a widely used, strong variant of the Co-CDH assumption. Moreover, our scheme offers low computation complex.

3. PALPAS – PAsswordLess PAssword Synchronization

Moritz Horsch (TU Darmstadt, Germany), Andreas Hülsing (Technische Universität Eindhoven, Netherlands), Johannes Buchmann (TU Darmstadt, Germany)

Abstract: Tools that synchronize passwords over several user devices typically store the encrypted passwords in a central online database. For encryption, a low-entropy, password-based key is used. Such a database may be subject to unauthorized access which can lead to the disclosure of all passwords by an offline brute-force attack. In this paper, we present PALPAS, a secure and user-friendly tool that synchronizes passwords between user devices without storing information about them centrally. The idea of PALPAS is to generate a password from a high entropy secret shared by all devices and a random salt value for each service. Only the salt values are stored on a server but not the secret. The salt enables the user devices to generate the same password but is statistically independent of the password. In order for PALPAS to generate passwords according to different password policies, we also present a mechanism that automatically retrieves and processes the password requirements of services. PALPAS users need to only memorize a single password and the setup of PALPAS on a further device demands only a one-time transfer of few static data.

Workshop IWCC I – Cyber Crime Techniques & Prevention I

Session Chair: Krzysztof Szczypiorski (Warsaw University of Technology, Poland)
Location: Lecture Hall B
Time: 16:20 – 17:50

1. Intensifying state surveillance of electronic communications: a legal solution in addressing extremism or not?

Murdoch Watney (University of Johannesburg, South Africa)

Abstract: Extremism appears to be on the increase. Electronic communication reaches countless people across borders, canvassing support for radical views and/or inciting hatred and/or violence. This legal discussion deals with many inter-related questions that are of global relevance as electronic communication permeates our lives. Should a government tighten surveillance of electronic communication to combat and/or detect extremism or does such information gathering practices violate the user's right to freedom of expression and privacy? Should government agencies carry out the surveillance or should the ISP as provider of access and/or hosting of information gather information on extremist communication? Will the aftermath of the 2013 Snowden revelations of unwarranted, general and bulk state surveillance result in governments being wary to tighten state surveillance powers or has the level of extremism reached such a degree that it warrants governments to focus on monitoring as a surveillance method counteracting radicalism that may endanger the safety and security of a country. Tension between human rights protection and government use of surveillance powers is unavoidable as some argue that security and safety factors are exaggerated to justify extension of state surveillance powers, however the evidence of extremism unfortunately speaks for itself. This discussion provides an overview of the approach to surveillance a government may apply to online extremism.

2. Malicious Insiders with Ties to the Internet Underground Community

Jason Clark, Matt Collins and Jeremy Strozer (Carnegie Mellon University, USA)

Abstract: In this paper, we investigate insider threat cases in which the insider had relationships with the Internet underground community. To this end, we begin by explaining our insider threat corpus and the current state of Internet underground forums. Next, we provide a discussion of each of the 17 cases that blend insider threat with the use of malicious Internet underground forums. Based on those cases, we provide an in-depth analysis to include: 1) who the insiders are, 2) why they strike, 3) how they strike, 4) what sectors are most at risk, and 5) how the insiders were identified. Lastly, we describe our aggregated results and provide best practices to help mitigate the type of insider threat we describe.

3. An empirical study of click fraud in mobile advertising networks

Geumhwan Cho, Junsung Cho, Youngbae Song and Hyoungshick Kim (Sungkyunkwan University, Republic of Korea)

Abstract*:* Smartphone advertisement is increasingly used among many applications and allows developers to obtain revenue through in-app advertising. Our study aims at identifying potential security risks of a type of mobile advertisement where advertisers are charged for their advertisements only when a user clicks (or touches) on the advertisements in their applications. In the Android platform, we design an automated click generation attack and empirically evaluate eight popular advertising networks by performing real attacks on them. Our experimental results show that six advertising networks (75%) out of eight (Millennial Media, AppLovin, AdFit, MdotM, RevMob and Cauly Ads) are vulnerable to our attacks. We also discuss how to develop effective defence mechanisms to mitigate such automated click fraud attacks.

4. Network-based HTTPS Client Identification Using SSL/TLS Fingerprinting

Martin Husák, Milan Cermák, Tomáš Jirsík and Pavel Celeda (Masaryk University, Czech Republic)

Abstract: The growing share of encrypted network traffic complicates network traffic analysis and network forensics. In this paper, we present real-time lightweight identification of HTTPS clients based on network monitoring and SSL/TLS fingerprinting. Our experiment shows that it is possible to estimate the UserAgent of a client in HTTPS communication via the analysis of the SSL/TLS handshake. The fingerprints of SSL/TLS handshakes, including a list of supported cipher suites, differ among clients and correlate to User-Agent values from a HTTP header. We built up a dictionary of SSL/TLS cipher suite lists and HTTP UserAgents and assigned the User-Agents to the observed SSL/TLS connections to identify communicating clients. We discuss host based and network-based methods of dictionary retrieval and estimate the quality of the data. The usability of the proposed method is demonstrated on two case studies of network forensics.

18:30 – 22:00 Mayor’s Reception

The City of Toulouse invites us for a Mayor’s Reception, taking place shortly after the last session in the City Hall of Toulouse. We will meet directly in the City Hall of Toulouse.

Address:
Place du Capitole
31000 Toulouse

How to get from the conference venue to the Mayor´s Reception

Take the metro line “B” direction “Borderouge TOULOUSE” and change to metro line “A” at “Jean Jaurès” direction “Basso Cambo TOULOUSE”. Get out at the stop “Capitole”. The City Hall of Toulouse is about 150 metres away from the underground stop.

Tuesday, August 25th

08:00 – 17:00 Registration desk open

09:00 – 09:45 Plenary Session

Invited Talk

Location: Lecture Hall A
Time: 09:00 – 09:45

The European Strategic Agenda for Research and Innovation in Cybersecurity

Afonso Ferreira (European Commission, Brussels)

Abstract: This talk will present the European Strategic Research and Innovation Agenda (SRA) for cybersecurity as it is being released by the Working Group on Secure ICT Research and Innovation (aka WG3) of the Network and Information Security Platform, which is a public-private partnership put in place by the European Commission in 2013. Members of WG3 are close to two hundred. They address issues related to cybersecurity research and innovation in the context of the EU Strategy for Cyber Security and of the Network and Information Security Platform. WG3 identified the key challenges and corresponding desired outcomes in terms of innovation-focused, applied but also basic research in cybersecurity, privacy, and trust. The European SRA for cybersecurity designed by WG3 serves as main input for the drafting of Horizon 2020 Work Programmes by the European Commission and is source of inspiration for the coordination of, and collaboration between, research agendas across Europe, including industry research roadmaps and national research and innovation programmes of the Member States.

09:45 – 10:45 Plenary Session

Keynote

Location: Lecture Hall A
Time: 09:45 – 10:45

Let's Encrypt: Deploying free, secure, and automated HTTPS certificates for the entire Web

Peter Eckersley (EFF Technology, USA)

Abstract: EFF Technology Projects Director Peter Eckersley will discuss the obstacles that have prevented us from transitioning to a secure, encrypted Web that uses HTTPS by default. He will provide an overview of the Let's Encrypt CA which EFF is building with Mozilla, Cisco, Akamai and IdentTrust, to offer free and automated deployment of certificates for HTTPS/TLS/SSL, and of other standards initiatives that will be necessary to make Web communications safe by default against surveillance, censorship, and tampering on the network.

10:45 – 11:15 Coffee Break

11:15 – 12:45 Parallel Sessions

ARES Full III – Networks and Protocols

Session Chair: Mark Scanlon (University College Dublin, Ireland)
Location: Lecture Hall A
Time: 11:15 – 12:45

1. Accountable Redactable Signatures

Henrich C. Pöhls (University of Passau, Germany), Kai Samelin (University of Darmstadt, Germany)

Abstract: Redactable signature schemes (RSS) allow removing blocks from signed data. State-of-the-art schemes have public redactions, i.e., any party can remove parts from a signed message. This prohibits meaningful definitions of accountability. We address this gap by introducing the notion of accountable redact able signature schemes (ARSS). We present a generic construction which couples a sanitizable signature scheme (SSS) to profit from its accountability with an RSS to maintain the reduced malleability of RSSs. Depending on the building blocks, the resulting scheme offers transparency or public accountability. Transparency provides stronger privacy guarantees, while public accountability meets legal and application requirements.

2. Empirical Evaluation of the A3 Environment: Evaluating Defenses Against Zero-Day Attacks

Shane Clark, Aaron Paulos, Brett Benyo, Partha Pal, Rick Schantz (BBN Technologies, USA)

Abstract: A3 is an execution management environment that aims to make network-facing applications and services resilient against zero-day attacks. A3 recently underwent two adversarial evaluations of its defensive capabilities. In one, A3 defended an App Store used in a Capture the Flag (CTF) tournament, and in the other, a tactically relevant network service in a red team exercise. This paper describes the A3 defensive technologies evaluated, the evaluation results, and the broader lessons learned about evaluations for technologies that seek to protect critical systems from zero-day attacks.

3. The Role and Security of Firewalls in IaaS Cloud Computing

Jordan Cropper, Johanna Ullrich, Peter Frühwirt, Edgar Weippl (SBA Research, Austria)

Abstract: Cloud computing is playing an ever larger role in the IT infrastructure. The migration into the cloud means that we must rethink and adapt our security measures. Ultimately, both the cloud provider and the customer have to accept responsibilities to ensure security best practices are followed. Firewalls are one of the most critical security features. Most IaaS providers make firewalls available to their customers. In most cases, the customer assumes a best-case working scenario which is often not assured. In this paper, we studied the filtering behaviour of firewalls provided by five different cloud providers. We found that three providers have firewalls available within their infrastructure. Based on our findings, we developed an open-ended firewall monitoring tool which can be used by cloud customers to understand the firewall's filtering behaviour. This information can then be efficiently used for risk management and further security considerations. Measuring today's firewalls has shown that they perform well for the basics, although may not be fully featured considering fragmentation or stateful behaviour.

Workshop IWCC II – Cyber Crime Techniques & Prevention II

Session Chair: Krzysztof Szczypiorski (Warsaw University of Technology, Poland)
Location: Lecture Hall B
Time: 11:15 – 12:45

1. Deploying Honeypots and Honeynets: Issue of Privacy

Pavol Sokol (Pavol Jozef Safarik University in Kosice, Slovakia), Martin Husák (Masaryk University, Czech Republic) and František Lipták (Pavol Jozef Safarik University in Kosice, Slovakia

Abstract: Honeypots and honeynets are popular tools in the area of network security and network forensics. The deployment and usage of these tools are influenced by a number of technical and legal issues, which need to be carefully considered together. In this paper, we outline privacy issues of honeypots and honeynets with respect to technical aspects. The paper discusses the legal framework of privacy, legal ground to data processing, and data collection. The analysis of legal issues is based on EU law and is supported by discussions on privacy and related issues. This paper is one of the first papers which discuss in detail privacy issues of honeypots and honeynets in accordance with EU law.

2. Gradually Improving the Forensic Process

Sebastian Neuner, Martin Mulazzani (SBA Research, Austria), Sebastian Schrittwieser (FH St.Pölten, Austria) and Edgar Weippl (SBA Research, Austria)

Abstract: At the time of writing, one of the most pressing problems for forensic investigators is the huge amount of data to analyse per case. Not only the number of devices increases due to the advancing computerization of everydays life, but also the storage capacity of each and every device raises into multiterabyte storage requirements per case for forensic working images. In this paper we improve the standardized forensic process by proposing to use file deduplication across devices as well as file whitelisting rigorously in investigations, to reduce the amount of data that needs to be stored for analysis as early as during data acquisition. These improvements happen in an automatic fashion and completely transparent to the forensic investigator. They furthermore be added without negative effects to the chain of custody or artefact validity in court, and are evaluated in a realistic use case.

3. A Landmark Calibration Based IP Geolocation Approach

Jingning Chen, Fenlin Liu, Xiangyang Luo, Fan Zhao and Zhu Guang (Zhengzhou Science and Technology Institute, China)

Abstract: Aiming at the existing IP geolocation approaches does not consider the errors of landmarks, a new geolocation approach utilized landmark calibration is proposed in this paper. At first, by assigning a deviation, the location of the landmark with low reliability is regarded as a possible area; then geolocating the target IP can be converted into a constrained optimization problem; finding the location estimation of target IP by solving this problem, as well as the real deviation of landmark. The algorithm analysis and experimental results show that, when a landmark is not located in its claimed position, our geolocation approach can still give a location for the target IP.

4. Markov Process Based Retrieval for Encrypted JPEG Images

Hang Cheng (Shanghai University / Fuzhou University, China), Xinpeng Zhang, Jiang Yu (Shanghai University, China), Fengyong Li (Shanghai University of Electric Power, China)

Abstract: This work presents a retrieval scheme for encrypted JPEG images based on Markov process. In our scheme, the stream cipher and permutation encryption are combined to encrypt JPEG images, which are then uploaded to a database server. After that, the server without knowing the original content can extract features from the transition probability matrices of the AC coefficients of encrypted query image, in which those coefficients are modelled by Markov process. With the multi-class support vector machine (SVM), the features of encrypted query image can be converted into a vector with low dimensionality determined by the number of image categories. The encrypted database images are conducted similarly. After low-dimensional vector representation, the similarity between encrypted query image and database image may be measured by calculating the distance of their corresponding vectors. At the client side, the encrypted images returned by the server are decrypted to the plaintext images using encryption key. The proposed scheme can preserve file compliance and file size for encrypted JPEG images, while providing privacy-preserving image retrieval.

Workshop MFSec I – Web & social media data analytics for privacy awareness and terrorist-related content identification

Session Chair: Edgar Weippl (SBA Research, Austria)
Location: Lecture Hall C
Time: 11:15 – 12:45

1. A Framework for the Discovery, Analysis, and Retrieval of Multimedia Homemade Explosives Information on the Web

Theodora Tsikrika, George Kalpakis, Stefanos Vrochidis, Ioannis Kompatsiaris (Centre for Research and Technology Hellas, Greece), Iraklis Paraskakis, Isaak Kavasidis (The University of Sheffield, International Faculty, Greece), Jonathan Middleton, Una Williamson (Police Service Northern Ireland, UK)

Abstract: This work proposes a novel framework that integrates diverse state-of-the-art technologies for the discovery, analysis, retrieval, and recommendation of heterogeneous Web resources containing multimedia information about homemade explosives (HMEs), with particular focus on HME recipe information. The framework corresponds to a knowledge management platform that enables the interaction with HME information, and consists of three major components: (i) a discovery component that allows for the identification of HME resources on the Web, (ii) a content-based multimedia analysis component that detects HME-related concepts in multimedia content, and (iii) an indexing, retrieval, and recommendation component that processes the available HME information to enable its (semantic) search and provision of similar information. The proposed framework is being developed in a user-driven manner, based on the requirements of law enforcement and security agencies personnel, as well as HME domain experts. In addition, its development is guided by the characteristics of HME Web resources, as these have been observed in an empirical study conducted by HME domain experts. Overall, this framework is envisaged to increase the operational effectiveness and efficiency of law enforcement and security agencies in their quest to keep the citizen safe.

2. PScore: a framework for enhancing privacy awareness in online social networks

Georgios Petkos, Symeon Papadopoulos, Yiannis Kompatsiaris (Centre for Research and Technology Hellas, Greece)

Abstract: The phenomenal increase in the use of social media in recent years has raised a number of issues related to privacy. In this paper, we propose a framework for raising the awareness of Online Social Network (OSN) users with respect to the information about them that is disclosed and that can be inferred by OSN service operators as well as by third parties that can access their data. This framework takes the form of a semantic, hierarchical scoring structure that enables users to easily browse over different privacy-related aspects of their presence in a social network. Contrary to previous privacy scoring approaches, the proposed framework provides a finer and more intuitive organization of privacy information. Importantly, it also takes into account both information that is explicitly mentioned in users' shared content, as well as implicit information, that may be inferred from it. We make available an open source implementation of the framework1.

3. AnonCall / Making Anonymous Cellular Phone Calls

Eric Chan-Tin (Oklahoma State University, USA)

Abstract: The threat of mass surveillance and the need for privacy have become mainstream recently. Most of the anonymity schemes have focused on Internet privacy. We propose an anonymity scheme for cellular phone calls. The cellular phones form an ad-hoc network relaying phone conversations through direct Wi-Fi connections. A proof-of concept implementation on an Android smartphone is completed and shown to work with minimal delay in communications.

12:45 – 14:00 Lunch

14:00 – 15:30 Parallel Sessions

ARES Full IV – Software Security

Session Chair: Martin Gilje Jaatun (SINTEF, Norway)
Location: Lecture Hall A
Time: 14:00 – 15:30

1. Fair fingerprinting protocol for attesting software misuses

Raphael Machado, Davidson Boccardo (Instituto Nacional de Metrologia, Qualidade e Tecnologia, Brazil), Vinícius de Sá, Jayme Szwarcfiter (Universidade Federal do Rio de Janeiro, Brazil)

Abstract: Digital watermarks embed information into a host artefact in such a way that the functionalities of the artefact remain unchanged. Allowing for the timely retrieval of authorship/ownership information, and ideally hard to be removed, watermarks discourage piracy and have thus been regarded as important tools to protect the intellectual property. A watermark aimed at uniquely identifying an artefact is referred to as a fingerprint. After presenting a formal definition of digital watermarks, we introduce an unbiased fingerprinting protocol—based on oblivious transfer—that lends no advantage to the prosecuting party in a dispute around intellectual property breach.

2. Uncovering Use-After-Free Conditions In Compiled Code

David Dewey (Georgie Institute of Technology, USA), Bradley Reaves, Patrick Traynor (University of Florida, USA)

Abstract: Use-after-free conditions occur when an execution path of a process accesses an incorrectly deallocated object. Such access is problematic because it may potentially allow for the execution of arbitrary code by an adversary. However, while increasingly common, such flaws are rarely detected by compilers in even the most obvious instances. In this paper, we design and implement a static analysis method for the detection of useafter-free conditions in binary code. Our new analysis is similar to available expression analysis and traverses all code paths to ensure that every object is defined before each use. Failure to achieve this property indicates that an object is improperly freed and potentially vulnerable to compromise. After discussing the details of our algorithm, we implement a tool and run it against a set of enterprise-grade, publicly available binaries. We show that our tool can not only catch textbook and recently released in-situ examples of this flaw, but that it has also identified 127 additional use-after-free conditions in a search of 652 compiled binaries in the Windows system32 directory. In so doing, we demonstrate not only the power of this approach in combating this increasingly common vulnerability, but also the ability to identify such problems in software for which the source code is not necessarily publicly available.

3. All-Solution Satisfiability Modulo Theories: applications, algorithms and benchmarks

Quoc-Sang Phan, Pasquale Malacaria (Queen Mary University of London, UK)

Abstract: Satisfiability Modulo Theories (SMT) is a decision problem for logical formulas over one or more first-order theories. In this paper, we study the problem of finding all solutions of an SMT problem with respect to a set of Boolean variables, henceforth All-SMT. First, we show how an All-SMT solver can benefit various domains of application: Bounded Model Checking, Automated Test Generation, Reliability analysis, and Quantitative Information Flow. Secondly, we then propose algorithms to design an All-SMT solver on top of an existing SMT solver, and implement it into a prototype tool, called aZ3. Thirdly, we create a set of benchmarks for All-SMT in the theory of linear integer arithmetic QF LIA and the theory of bit vectors with arrays and uninterpreted functions QF AUFBV. We compare aZ3 against MathSAT, the only existing All-SMT solver, on our benchmarks. Experimental results show that aZ3 is more precise than MathSAT.

Workshop IWCC III – Information Hiding I

Session Chair: Krzysztof Szczypiorski (Warsaw University of Technology, Poland)
Location: Lecture Hall B
Time: 14:00-15:30

1. Countermeasures for Covert Channel-internal Control Protocols

Jaspreet Kaur, Steffen Wendzel and Michael Meier (Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), Germany)

Abstract: Network covert channels have become a sophisticated means for transferring hidden information over the network, and thereby breaking the security policy of a system. Covert channel-internal control protocols, called micro protocols, have

been introduced in the recent years to enhance capabilities of network covert channels. Micro protocols are usually placed within the hidden bits of a covert channel's payload and enable features such as reliable data transfer, session management, and dynamic routing for network covert channels. These features provide adaptive and stealthy communication channels for malware, especially botnets. Although many techniques are available to counter network covert channels, these techniques are insufficient for countering micro protocols. In this paper, we present the first work to categorize and implement possible countermeasures for micro protocols that can ultimately break sophisticated covert channel communication. The key aspect of proposing these countermeasures is based on the interaction with the micro protocol. We implemented the countermeasures for two micro protocol-based tools: Ping Tunnel and Smart Covert Channel Tool. The results show that our techniques are able to counter micro protocols in an effective manner compared to current mechanisms, which do not target micro protocol-specific behaviour.

2. Novel Method of Hiding Information in IP Telephony Using Pitch Approximation

Artur Janicki (Warsaw University of Technology, Poland)

Abstract: In this paper a novel steganographic method, called HideF0, dedicated to IP telephony is proposed. It is based on the approximation of the parameter that describes the F0 frequency (the pitch) of the speaker's voice. We show that thanks to approximating some fragments of the „fine pitch" parameter in the Speex codec we can create efficient hidden transmission channels. We determined that for Speex working in mode 5 the HideF0 method can provide a hidden channel with a capacity of ca. 220 bps at the optimal operating point. We also demonstrated that the proposed method offers a significantly more advantageous trade-off between the steganographic bandwidth and steganographic cost than the classic least significant bit (LSB) approach.

3. StegBlocks: ensuring perfect undetectability of network steganography

Wojciech Frqczek and Krzysztof Szczypiorski (Warsaw University of Technology, Poland)

Abstract: The paper presents StegBlocks, which defines a new concept for performing undetectable hidden communication. StegBlocks is a general approach for constructing methods of network steganography. In StegBlocks, one has to determine objects with defined properties which will be used to transfer hidden messages. The objects are dependent on a specific network protocol (or application) used as a carrier for a given network steganography method. Moreover, the paper presents the approach to perfect undetectability of network steganography, which was developed based on the rules of undetectability for general steganography. The approach to undetectability of network steganography was used to show the possibility of developing perfectly undetectable network steganography methods using the StegBlocks concept.

4. Using Facebook for Image Steganography

Tejas Dakve, Jason Hiney (George Mason University, USA), Krzysztof Szczypiorski (Warsaw University of Technology, Poland) and Kris Gaj (George Mason University, USA)

Abstract: Because Facebook is available on hundreds of millions of desktop and mobile computing platforms around the world and because it is available on many different kinds of platforms (from desktops and laptops running Windows, Unix, or OS X to hand held devices running iOS, Android, or Windows Phone), it would seem to be the perfect place to conduct steganography. On Facebook, information hidden in image files will be further obscured within the millions of pictures and other images posted and transmitted daily. Facebook is known to alter and compress uploaded images so they use minimum space and bandwidth when displayed on Facebook pages. The compression process generally disrupts attempts to use Facebook for image steganography. This paper explores a method to minimize the disruption so JPEG images can be used as steganography carriers on Facebook.

Workshop MFSec II – Forensic analysis of audiovisual data

Session Chair: Edgar Weippl (SBA Research, Austria)
Location: Lecutre Hall C
Time: 14:00-15:30

1. Image Watermaking With Biometric Data For Copyright Protection

Morgan Barbier, Jean-Marie Le Bars, Christophe Rosenberger (ENSICAEN-UNICAEN-CNRS, GREYC, France)

Abstract: In this paper, we deal with the proof of ownership or legitimate usage of a digital content, such as an image, in order to tackle the illegitimate copy. The proposed scheme based on the combination of the watermarking and cancellable biometrics does not require a trusted third party, all the exchanges are between the provider and the customer. The use of cancellable biometrics allows us to provide a privacy compliant proof of identity. We illustrate the robustness of this method against intentional and unintentional attacks of the watermarked content.

3. Video spatio-temporal filtering based on cameras and target objects trajectories – Videosurveillance forensic framework

Dana Codreanu, Andre Peninou, Florence Sedes (Universite de Toulouse, France)

Abstract: This paper presents our work about assisting video surveillance agents in the search for particular video scenes of interest in transit network. This work has been developed based on requirements defined within different projects with the French National Police in a forensic goal. The video-surveillance agent inputs a query in the form of a hybrid trajectory (date, time, locations expressed with regards to different reference systems) and potentially some visual descriptions of the scene. The query processing starts with the interpretation of the hybrid trajectory and continues with a selection of a set of cameras likely to have filmed the spatial trajectory. The main contributions of this paper are: (1) a definition of the hybrid trajectory query concept, trajectory that is constituted of geometrical and symbolic segments represented with regards to different reference systems (e.g., geodesic system, road network), (2) a spatiotemporal filtering framework based on a spatio-temporal modelling of the transit network and associated cameras.

4. Concept Detection on Multimedia Web Resources about Home Made Explosives

George Kalpakis, Theodora Tsikrika, Foteini Markatopoulou, Nikiforos Pittaras, Stefanos Vrochidis, Vasileios Mezaris (Information Technologies Institute, CERTH, Greece), Ioannis Patras(Queen Mary University of London, UK), Ioannis Kompatsiaris (Information Technologies Institute, CERTH, Greece)

Abstract: This work investigates the effectiveness of a stateof-the-art concept detection framework for the automatic classification of multimedia content, namely images and videos, embedded in publicly available Web resources containing recipes for the synthesis of Home Made Explosives (HMEs), to a set of predefined semantic concepts relevant to the HME domain. The concept detection framework employs advanced methods for video (shot) segmentation, visual feature extraction (using SIFT, SURF, and their variations), and classification based on machine learning techniques (logistic regression). The evaluation experiments are performed using an annotated collection of multimedia HME content discovered on the Web, and a set of concepts, which emerged both from an empirical study, and were also provided by domain experts and interested stakeholders, including Law Enforcement Agencies personnel. The experiments demonstrate the satisfactory performance of our framework, which in turn indicates the significant potential of the adopted approaches on the HME domain.

15:30 – 16:00 Coffee Break

16:00 – 17:30 Parallel Sessions

ARES Full V – Mobile Security & Cyber Physical Systems

Session Chair: Peter Kieseberg (SBA Research, Austria)
Location: Lecture Hall A
Time: 16:00 – 17:30

1. A Lightweight Framework for Cold Boot Based Forensics on Mobile Devices

Benjamin Taubmann, Manuel Huber, Sascha Wessel (Fraunhofer Research Institute AISEC, Germany), Lukas Heim (Technische Universität München, Germany), Hans Peter Reiser (University of Passau, Germany), Georg Sigl (Technische Universität München, Germany)

Abstract: Mobile devices, like tablets and smartphones, are common place in everyday life. Thus, the degree of security these devices can provide against digital forensics is of particular interest. A common method to access arbitrary data in main memory is the cold boot attack. The cold boot attack exploits the remanence effect that causes data in DRAM modules not to

lose the content immediately in case of a power cut-off. This makes it possible to restart a device and extract the data in main memory. In this paper, we present a novel framework for cold boot based data acquisition with a minimal bare metal application on a mobile device. In contrast to other cold boot approaches, our forensics tool overwrites only a minimal amount of data in main memory. This tool requires no more than five kilobytes of constant data in the kernel code section. We hence sustain all of the data relevant for the analysis of the previously running system. This makes it possible to analyse the memory with data acquisition tools. For this purpose, we extend the memory forensics tool Volatility in order to request parts of the main memory dynamically from our bare metal application. We show the feasibility of our approach by comparing it to a traditional memory dump based analysis using the Samsung Galaxy S4 mobile device.

2. Dynamic Self-Protection and Tamperproofing for Android Apps using Native Code

Mykola Protsenko, Sebastien Kreuter, Tilo Müller (Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany)

Abstract: With over one billion sold devices, representing 80% market share, Android remains the most popular platform for mobile devices. Application piracy on this platform is a major concern and a cause of significant losses: about 97% of the top 100 paid apps were found to be hacked in terms of repackaging or the distribution of clones. Therefore new and stronger methods aiming to increase the burden on reverse engineering and modification of proprietary mobile software are required. In this paper, we propose an application of the Android native code component to implement strong software self-protection for apps. Within this scope, we present three dynamic obfuscation techniques, namely dynamic code loading, dynamic re-encryption, and tamperproofing. We provide a practical evaluation of this approach, assessing both the cost and efficiency of its achieved protection level. Our results indicate that with the proposed methods one can reach significant complication of the reverse-engineering process, while being affordable in terms of execution time and application size.

3. Don't brick your car: Firmware confidentiality and rollback for vehicles

Hafizah Mansor, Konstantinos Markantonakis, Raja Naeem Akram, Keith Mayes (Royal Holloway, University of London, UK)

Abstract: In modern cars, there are a number of controllers that play a major role in the overall operations of the vehicles. The secure and updated firmware of these controllers is crucial to the overall security and reliability of the vehicle and its electronic system(s). Therefore, the life cycle of these controllers should be carefully managed. In this paper, we examine the vehicular firmware updates process and their associated security issues. We have analysed the security of the firmware update protocol proposed in the EVITA project, referred as EVITA protocol, which is considered as a main industrial effort in this field and found some potential shortcomings. Based on the analysis, in this paper we have suggested a number of improvements to the EVITA protocol, related with safety and security measures. The proposed improved protocol, also referred as EVITA+ protocol includes a rollback mechanism while preserving the confidentiality of the firmware. The integrity and authenticity of the flash driver are also considered in the EVITA+ protocol. The EVITA+ protocol is formally analysed using CasperFDR and Scyther to ensure the security of the firmware update process. Finally, we provide an insight analysis and our experience in relation to the efficiency, suitability and performance of the aforementioned tools in the field of automotive security.

Workshop IWCC IV – Information Hiding II

Session Chair: Krzysztof Szczypiorski (Warsaw University of Technology, Poland)
Location: Lecture Hall B
Time: 16:00 – 17:30

1. Color Images Steganalysis Using Correlation Between RGB Channels

Hasan Abdulrahman, Marc Chaumont (Montpellier University, France), Philippe Montesinos and Baptiste Magnier (Ecole des Mines d´Al, France)

Abstract: Digital images, especially color images, are very widely used, as well as traded via Internet, e-mail and posting on websites. Images have a large size which allows embedding secret mes- sages of large size, so they are a good medium for digital steganography. The main goal of steganalysis is to detect the presence of hidden messages in digital media. In this paper, we propose a steganalysis method based on color feature correlation and machine learning classification. Fusing features with features obtained from color-rich models allows to in- crease the detectability of hidden messages in the color im- ages. Our novel proposition uses the correlation between different channels of color images. Features are extracted from the channel correlation and co-occurrence correlation. In this work, all stego images are created with a range of different payload sizes using two steganography S-UNIWARD and WOW algorithms. To validate the proposed method, his efficiency is demonstrated by comparison with color rich model steganalysis.

2. Steganalysis of Low bit-rate Speech Based on Statistic Characteristics of Pulse Positions

Hui Tian, Yanpeng Wu (National Huaqiao University, China), Yongfeng Huang (Tsinghua University China), Yonghong Chen, Tian Wang and Yiqiao Cai (National Huaqiao University, China)

Abstract: Steganography in low bit-rare speech streams is an important branch of Voice-over-IP steganography. From the point of preventing cybercrimes, it is significant to design effective steganalysis methods. In this paper, we present a support-vector-machine based steganalysis of low bit-rate speech exploiting statistic characteristics of pulse positions. Specifically, we utilize the probability distribution of pulse positions as a long-time distribution feature, extract Markov transition probabilities of pulse positions according to the short-time invariance characteristic of speech signals, and employ joint probability matrices to characterize the pulseto-pulse correlation. We evaluate the performance of the proposed method with a large number of G.729a encoded samples, and compare it with the state-of-the-art methods. The experimental results demonstrate that our method significantly outperforms the previous ones on detection accuracy at any given embedding rates or with any sample lengths. Particularly, this method can successfully detect steganography employing only one or a few of the potential cover bits, which is hard to be effectively detected by the existing methods.

3. A JPEG-Compression Resistant Adaptive Steganography Based on Relative Relationship between DCT Coefficients

Yi Zhang, Xiangyang Luo, Chunfang Yang and Fenlin Liu (Zhengzhou Science and Technology Institute, China)

Abstract: Current typical adaptive Steganography algorithms cannot extract the embedded secret messages correctly after compression. In order to solve this problem, a JPEG compression resistant adaptive steganography algorithm is proposed. Utilizing the relationship between DCT coeffi- cients, the domain of messages embedding is determined. The modifying magnitude of different DCT coefficients can be determined according to the quality factors of JPEG compression. To ensure the completely correct extraction of embedded messages after JPEG compression, the RS codes is used to encode the messages to be embedded. Besides, based on the current energy function in the PQe steganography and the distortion function in J-UNIWARD Steganography, the corresponding distortion value of DCT coefficients is calculated. With the help of that, STCs is used to embed the encoded messages into the DCT coefficients, which have a smaller distortion value. The experimental results under different quality factors of JPEG compression and different payloads demonstrate that the proposed algorithm not only has a high correct rate of extracted messages after JPEG compression, which increases from about 60% to nearly 100% comparing with J-UNIWARD steganography under quality factor 75 of JPEG compression, but also has a strong detection resistant performance.

Workshop WCSF – International Workshop on Cloud Security and Forensics

Session Chair: Mark Scanlon (University College Dublin, Ireland)
Location: Lecture Hall C
Time: 16:00 – 17:30

1. Evaluation of a Sector-hash Based Rapid File Detection Method for Monitoring Infrastructure-as-a-Service Cloud Platforms

Manabu Hirano, Hayate Takase, Koki Yoshida (Toyota College, Japan)

Abstract: Current computer forensics tools have some limitations on anti-forensics attacks, cloud computing, and a large increase in the size of forensics targets. To solve these problems, this paper proposes a system that preserves storage data on virtual machines by acquiring all data sectors with time stamps. The proposed system can restore a previous state of a block device at any date and time that is specified by an investigator. The proposed system aims to monitor users' behaviour in Infrastructure-as-a-Service (IaaS) cloud platforms. This paper also presents a rapid file detection system that finds a target file from a large collection of the acquired data sectors by using sector-hashes and parallel distributed processing. This system enables investigators to track and to find a target file that is related to incidents or crimes in the cloud. First, this paper reports the preliminary experiments of a sector-hash based file detection method on three major operating systems for evaluating its effectiveness. We present a design and an implementation of the proposed monitoring and target file detection system by

using Xen hypervisor and MapReduce. We report results of its performance evaluation. Finally, we discuss possible methods to improve the performance and the limitations of the current proposed mechanism.

2. Enabling Constraints and Dynamic Preventive Access Control Policy Enforcement in the Cloud

Somchart Fugkeaw, Hiroyuki Sato (The University of Tokyo, Japan)

Abstract: Existing access control solutions applying Ciphertext Policy Attribute based Encryption (CP-ABE) scheme usually rely on the static access enforcement based on the access control policy. In real-world scenario, the static pattern of access control policy may not be sufficient to effectively respond the security problems or advanced access control requirements. In this paper, we enhance our collaborative access control model: C-CP-ARBE, to be capable to support a more rigorous access control with security constraints and preventive access policy (PAP) enforcement feature. To this end, we design constraints specification model and PAP enforcement scheme in multi- authority cloud storage systems. We employ Multi-Agent System (MAS) to automate the authentication and authorization function as well as to increase the performance of overall cryptographic processes. As of MAS concept, the scalability and separation of security functions of our access control system are enhanced. Finally, we present the experiments to demonstrate the improved efficiency and practicality of our proposed scheme.

3. Advanced Attribute-based Key Management for Mobile Devices in Hybrid Clouds

Jaemin Park, Eunchan Kim, Sungjin Park, Cheoloh Kang (The Attached Institute of ETRI, Republic of Korea)

Abstract: Mobile cloud computing requires the efficient approach to access the outsourced data in public clouds due to resource scarceness of mobile devices. To this end, the outsourced data should be protected efficiently from being accessed in plaintext by unauthorized users and public clouds. User revocation should be appropriately managed to guarantee backward secrecy, collusion resistance, and key freshness. In this paper, we present AKMD (Advanced Attribute-based Key Management for Mobile Devices in Hybrid Clouds), an improved key management in hybrid clouds using ciphertext-policy attribute-based encryption to allow only authorized users to access the outsourced data stored in public clouds while guaranteeing the efficiency by delegating the key management tasks to private clouds. We introduce new two procedures to handle user revocations, rekey of data encryption keys and policy renewal to support the backward secrecy and key freshness. Our implementation and analysis show that AKMD improves efficiency in security computations and key storage space for mobile devices and guarantees the improved security.

4. Overview of the Forensic Investigation of Cloud Services

Jason Farina, Mark Scanlon, NhienAn LeKhac, Tahar Kechadi (University College Dublin, Ireland)

Abstract: Cloud Computing is a commonly used, yet ambiguous term, which can be used to refer to a multitude of differing dynamically allocated services. From a law enforcement and forensic investigation perspective, cloud computing can be thought of as a double edged sword. While on one hand, the gathering of digital evidence from cloud sources can bring with it complicated technical and cross-jurisdictional legal challenges. On the other, the employment of cloud storage and processing capabilities can expedite the forensics process and focus the investigation onto pertinent data earlier in an investigation. This paper examines the state-of-the-art in cloud-focused, digital forensic practises for the collection and analysis of evidence and an overview of the potential use of cloud technologies to provide Digital Forensics as a Service.

18:30 – 20:00 Sightseeing Tour – Toulouse’s Hidden Treasures

Toulouse’s Hidden Treasures

A guided visit out of the beaten path. Discover the unusual and secret side of the City: a Moorish-style ceiling, a truncated tower, a pair of hidden feet… Toulouse as you’ve never suspected it to be.

Meeting point: Place du Capitol, 18.20
Tour start: 18.30
Tour end: 20.00 at Place du Capitol (City Centre)

How to get from the conference venue to the Sightseeing Tour meeting point

Take the metro line “B” direction “Borderouge TOULOUSE” and change to metro line “A” at “Jean Jaurès” direction “Basso Cambo TOULOUSE”. Get out at the stop “Capitole”. The City Hall of Toulouse is about 150 metres away from the underground stop.

Wednesday, August 26th 2015

08:00 – 15:00 Registration desk open

09:00 – 10:00 Plenary Session

Keynote

Location: Lecture Hall A
Time: 09:00 – 10:00

Data Security and Privacy in the Cloud

Pierangela Samarati (Università degli Studi di Milano, Italy)

Abstract: The rapid advancements in Information and Communication Technologies (ICTs) have enabled the emerging of the "cloud" as a successful paradigm for conveniently storing, accessing, processing, and sharing information. With its significant benefits of scalability and elasticity, the cloud paradigm has appealed companies and users, which are more and more resorting to the multitude of available providers for storing and processing data. Unfortunately, such a convenience comes at a price of loss of control over these data and consequent new security threats that can limit the potential widespread adoption and acceptance of the cloud computing paradigm. In this talk I will illustrate some security and privacy issues arising in the cloud scenario, focusing in particular on the problem of guaranteeing confidentiality and integrity of data stored or processed by external cloud Providers.

10:00 – 10:15 Coffee Break

10:15 – 11:45 Parallel Sessions

ARES Full VI – Security Management

Session Chair: Stefan Katzenbeisser (TU Darmstadt, Germany)
Location: Lecture Hall A
Time: 10:15 – 11:45

1. Modeling Fraud Prevention of Online Services using Incident Response Trees and Value at Risk

Dan Gorton (KTH Royal Institute of Technology, Sweden)

Abstract: Authorities like the Federal Financial Institutions Examination Council in the US and the European Central Bank in Europe have stepped up their expected minimum security requirements for financial institutions, including the requirements for risk analysis. In a previous article, we introduced a visual tool and a systematic way to estimate the probability of a successful incident response process, which we called an incident response tree (IRT). In this article, we present several scenarios using the IRT which could be used in a risk analysis of online financial services concerning fraud prevention. By minimizing the problem of underreporting, we are able to calculate the conditional probabilities of prevention, detection, and response in the incident response process of a financial institution. We also introduce a quantitative model for estimating expected loss from fraud, and conditional fraud value at risk, which enables a direct comparison of risk among online banking channels in a multi-channel environment.

2. The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001

Bahareh Shojaie, Hannes Federrath (University of Hamburg, Germany), Iman Saberi (Technical University of Hamburg, Germany)

Abstract: The ISO 27001 is the most adopted international information security management standard, by several countries and industries. This paper looks closely to the impacts of cultural characteristics on different phases of developing ISO 27001, based on three levels (country, organisational, and personal), which is especially helpful for Small and Medium Enterprises

(SMEs). Cultural dimensions can significantly affect organisational administration and achievements such as decision-making, innovation and new practices, work motivation, negotiation, human resource practices, and leadership. The results are mainly based on a literature review, such as Hofstede and their relationship with the ISO 27001 Annex A. The outcomes of this paper illustrate that national (country level) cultural dimensions have high impact on the success and effectiveness of the ISO 27001 development phases.

ARES Short I – Network and Probing

Session Chair: Edgar Weippl (SBA Research, Austria)
Location: Lecture Hall B
Time: 10:15 – 11:45

1. On the Isofunctionality of Network Access Control Lists

Malek Belhaouane, Joaquin Garcia-Alfaro, Hervé Debar (Institut Mines-Telecom, Téléecom SudParis, France)

Abstract: In a networking context, Access Control Lists (ACLs) refer to security rules associated to network equipment, such as routers, switches and firewalls. Methods and tools to automate the management of ACLs distributed among several equipment shall verify if the corresponding ACLs are functionally equivalent. In this paper, we address such a verification process. We present a formal method to verify when two ACLs are isofunctional and illustrate our proposal over a practical example.

2. Trust me, I'm a Root CA! Analyzing SSL Root CAs in modern Browsers and Operating Systems

Tariq Fadai, Sebastian Schrittwieser (FH St. Pölten, Austria) Peter Kieseberg, Martin Mulazzani (SBA Research, Austria)

Abstract: The security and privacy of our online communications heavily relies on the entity authentication mechanisms provided by SSL. Those mechanisms in turn heavily depend on the trustworthiness of a large number of companies and governmental institutions for attestation of the identity of SSL services providers. In order to offer a wide and unobstructed availability of SSL-enabled services and to remove the need to make a large amount of trust decisions from their users, operating systems and browser manufactures include lists of certification authorities which are trusted for SSL entity authentication by their products. This has the problematic effect that users of such browsers and operating systems implicitly trust those certification authorities with the privacy of their communications while they might not even realize it. The problem is further complicated by the fact that different software vendors trust different companies and governmental institutions, from a variety of countries, which leads to an obscure distribution of trust. To give insight into the trust model used by SSL this thesis explains the various entities and technical processes involved in establishing trust when using SSL communications. It furthermore analyses the number and origin of companies and governmental institutions trusted by various operating systems and browser vendors and correlates the gathered information to a variety of indexes to illustrate that some of these trusted entities are far from trustworthy. Furthermore it points out the fact that the number of entities we trust with the security of our SSL communications keeps growing over time and displays the negative effects this might have as well as shows that the trust model of SSL is fundamentally broken.

3. On Reconnaissance with IPv6: A Pattern-Based Scanning Approach

Johanna Ullrich, Peter Kieseberg, Katharina Krombholz, Edgar Weippl (SBA Research, Austria)

Abstract: Today's capability of fast Internet-wide scanning allows insights into the Internet ecosystem; but the on-going transition to the new Internet Protocol version 6 (IPv6) makes the approach of probing all possible addresses infeasible, even at current speeds of more than a million probes per second. As a consequence, the exploitation of frequent patterns has been proposed to reduce the search space. Current patterns are manually crafted and based on educated guesses of administrators. At the time of writing, their adequacy has not yet been evaluated. In this paper, we assess the idea of pattern-based scanning for the first time, and use an experimental set-up in combination with three real-world data sets. In addition, we developed a pattern-based algorithm that automatically discovers patterns in a sample and generates addresses for scanning based on its findings. Our experimental results confirm that pattern-based scanning is a promising approach for IPv6 reconnaissance, but also that currently known patterns are of limited benefit and are outperformed by our new algorithm. Our algorithm not only discovers more addresses, but also finds implicit patterns. Furthermore, it is more adaptable to future changes in IPv6 addressing and harder to mitigate than approaches with manually crafted patterns.

4. A Time Series Approach for Inferring Orchestrated Probing Campaigns by Analyzing Darknet Traffic

Elias Bou-Harb, Mourad Debbabi, Chadi Assi (NCFTA Canada & Concordia University, Canada)

Abstract: This paper aims at inferring probing campaigns by investigating darknet traffic. The latter probing events refer to a new phenomenon of reconnaissance activities that are distinguished by their orchestration patterns. The objective is to provide a systematic methodology to infer, in a prompt manner, whether or not the perceived probing packets belong to an orchestrated campaign. Additionally, the methodology could be easily leveraged to generate network traffic signatures to facilitate capturing incoming packets as belonging to the same inferred campaign. Indeed, this would be utilized for early cyber-attack warning and notification as well as for simplified analysis and tracking of such events. To realize such goals, the proposed approach models such challenging task as a problem of interpolating and predicting time series with missing values. By initially employing trigonometric interpolation and subsequently executing state space modelling in conjunction with a time varying window algorithm, the proposed approach is able to pinpoint orchestrated probing campaigns by only monitoring few orchestrated flows. We empirically evaluate the effectiveness of the proposed model using 330 GB of real darknet data. By comparing the outcome with a previously validated work, the results indeed demonstrate the promptness and accuracy of the proposed approach.

Workshop ASSD I – Experiences in agile development of secure software

Session Chair: Juha Röning (University of Oulu, Finland)
Location: Lecture Hall C
Time: 10:15 – 11:45

1. Keynote: Agile Secure Software Development in a Large Software Development Organisation: Security Testing

Achim Brucker (SAP SE, Germany)

Abstract: Security testing is an important part of any (agile) secure software development lifecycle. Still, security testing is often understood as an activity done by security testers in the time between „end of development „and „offering the product to customers“. Learning from traditional testing that the fixing of bugs is the more costly the later it is done in development, we believe that security testing should be integrated into the daily development activities. To achieve this, we developed a security testing strategy, as part of SAP’s security development lifecycle which supports the specific needs of the various software development models at SAP. In this presentation, we will briefly presents SAP’s approach to an agile secure software development process in general and, in particular, present SAP’s Security Testing Strategy that enables developers to find security vulnerabilities early by applying a variety of different security testing methods and Tools.

2. Independent Security Testing on Agile Software Development: a Case Study in a Software Company

Jesus Choliz, Julian Vilas, and Jose Moreira (Scytl Secure Electronic Voting, S.A., Spain)

Abstract: Agile methodologies are becoming increasingly common on Software Engineering Teams. Unfortunately, their relation with the security activities is complex to approach, even more complex when the Security Team has strong requirements of independence. This paper shows a case study of a software security testing process, based on the Microsoft Software Development Lifecycle for Agile, on a company moving their Software Engineering Teams from waterfall to agile. The results of this case study show a successful synchronization between the tasks of agile Software Engineering Teams and the independent Security Team.

3. Incremental Development of RBAC-controlled E-marking System Using the B Method

Nasser Al-Hadhrami, Benjamin Aziz (University of Portsmouth, UK), Shantanu Sardesai (Technical University of Darmstadt, Germany), and Lotfi ben Othmane (Fraunhofer SIT Germany)

Abstract: Role Based Access Control (RBAC) models are access policies that associate access rights to roles of subjects on objects. The incremental development of software by adding new features and the insertion of new access rules potentially render the model inconsistent and create security flaws. This paper proposes modelling RBAC models using the B language such that it is possible to re-evaluate the consistency of the models following model changes. It shows the mechanism of formalizing RBAC policies of an Electronic Marking System (EMS) using B specifications and illustrates the verification of the consistency of the RBAC specification, using model checking and proof obligations.

4. Security testing as a Part of Agile Process: Fuzzing (presentation only)

Juha Röning, Pekka Pietikäinen, Aki Helin, Atte Kettunen (University of Oulu, Finland)

Workshop WSDF I – 8th International Workshop on Digital Forensics

Session Chair: Richard Overill (King's College London, UK)
Location: Lecture Hall D
Time: 10:15 – 11:45

1. Watch what you wear: preliminary forensic analysis of smart watches

Ibrahim Baggili, Kyle Anthony, Jeff Oduru, Frank Breitinger, Glenn McGee (University of New Haven, USA)

Abstract: This work presents preliminary forensic analysis of two popular smart watches, the Samsung Gear 2 Neo and LG G. These wearable computing devices have the form factor of watches and sync with smart phones to display notifications, track footsteps and record voice messages. We posit that as smart watches are adopted by more users, the potential for them becoming a haven for digital evidence will increase thus providing utility for this preliminary work. In our work, we examined the forensic artefacts that are left on a Samsung Galaxy S4 Active phone that was used to sync with the Samsung Gear 2 Neo watch and the LG G watch. We further outline a methodology for physically acquiring data from the watches after gaining root access to them. Our results show that we can recover a swath of digital evidence directly from the watches when compared to the data on the phone that is synced with the watches. Furthermore, to root the LG G watch, the watch has to be reset to its factory settings which is alarming because the process may delete data of forensic relevance. Although this method is forensically intrusive, it may be used for acquiring data from already rooted LG watches. It is our observation that the data at the core of the functionality of at least the two tested smart watches, messages, health and fitness data, e-mails, contacts, events and notifications are accessible directly from the acquired images of the watches, which affirms our claim that the forensic value of evidence from smart watches is worthy of further study and should be investigated both at a high level and with greater specificity and granularity.

2. Cold Boot Attacks on DDR2 and DDR3 SDRAM

Simon Lindenlauf, Hans Höfken, Marko Schuba (Aachen University of Applied Sciences, Germany)

Abstract: Cold boot attacks provide a means to obtain a dump of a computer’s volatile memory even if the machine is locked. Such a dump can be used to reconstruct hard disk encryption keys and get access to the content of Bitlocker or Truecrypt encrypted drives. This is even possible, if the obtained dump contains errors. Cold boot attacks have been demonstrated successfully on DDR1 and DDR2 SDRAM. They have also been tried on DDR3 SDRAM using various types of equipment but all attempts have failed so far. In this paper we describe a different hardware setup which turns out to work for DDR3 SDRAM as well. Using this setup it will be possible for digital forensic investigators to recover keys from newer machines that use DDR3 SDRAM.

3. Behavioural Evidence Analysis Applied to Digital Forensics: An Empirical Analysis of Child Pornography Cases using P2P Networks

Noora Al Mutawa, Joanne Bryce (University of Central Lancashire, UK), Virginia Franqueira (University of Derby, UK), Andrew Marrington (Zayed University, UAE)

Abstract: The utility of Behavioural Evidence Analysis (BEA) has gained attention in the field of Digital Forensics in recent years. It has been recognized that, along with technical examination of digital evidence, it is important to learn as much as possible about the individuals behind an offence, the victim(s) and the dynamics of a crime. This can assist the investigator in producing a more accurate and complete reconstruction of the crime, in interpreting associated digital evidence, and with the description of investigative findings. Despite these potential benefits, the literature shows limited use of BEA for the investigation of cases of the possession and dissemination of Sexually Exploitative Imagery of Children (SEIC). This paper represents a step towards filling this gap. It reports on the forensic analysis of 15 SEIC cases involving P2P file sharing networks, obtained from the Dubai Police. Results confirmed the predicted benefits and indicate that BEA can assist digital forensic practitioners and prosecutors.

Workshop IWSMA I – Android Security

Session Chair: Peter Kieseberg (SBA Research, Austria)

Location: Lecture Hall E

Time: 10:15 – 11:45

1. Composition-malware: building Android malware at run time

Gerardo Canfora, Francesco Mercaldo, Corrado Aaron Visaggio, Giovanni Moriano (University of Sannio, Italy)

Abstract: We present a novel model of malware for Android, named composition-malware, which consists of composing fragments of code hosted on different and scattered locations at run time. A key feature of the model is that the malicious behaviour could dynamically change and the payload could be activated under logic or temporal conditions. These characteristics allow a malware written according to this model to evade current malware detection technologies for Android platform, as the evaluation has demonstrated. The aim of the paper is to propose new approaches to malware detection that should be adopted in anti-malware tools for blocking a composition-malware.

2. Network Security Challenges in Android Applications

Damjan Buhov (SBA Research, Austria), Markus Huber (FH St. Pölten, Austria) Georg Merzdovnik, Edgar Weippl (SBA Research, Austria), Vesna Dimitrova (Ss. Cyril and Methodius University, R. Macedonia)

Abstract: The digital world is in constant battle for improvement - especially in the security field. Taking into consideration the revelations from Edward Snowden about the mass surveillance programs conducted by governmental authorities, the number of users that raised awareness towards security is constantly increasing. More and more users agree that additional steps must be taken to ensure the fact that communication will remain private as intended in the first place. Taking in consideration the ongoing transition in the digital world, there are already more mobile phones than people on this planet. According to [19] there are around 7 billion active cell phones by 2014 out of which nearly 2 billion are smartphones. The use of smartphones by itself could open a great security hole. The most common problem when it comes to Android applications is the common misuse of the HTTPS protocol. Having this in mind, this paper addresses the current issues when it comes to misuse of the HTTPS protocol and proposes possible solutions to overcome this common problem. In this paper we evaluate the SSL implementation in a recent set of Android applications and present some of the most common missuses. The goal of this paper is to raise awareness to current and new developers to actually consider security as one of their main goals during the development life cycle of applications.

3. Effectiveness of Opcode ngrams for Detection of Multi Family Android Malware

Francesco Mercaldo (University of Sannio, Italy), Corrado Aaron Visaggio, Eric Medvet (University of Trieste, Italy), Andrea De Lorenzo, Gerardo Canfora (University of Sannio, Italy)

Abstract: With the wide diffusion of smartphones and their usage in a plethora of processes and activities, these devices have been handling an increasing variety of sensitive resources. Attackers are hence producing a large number of malware applications for Android (the most spread mobile platform), often by slightly modifying existing applications, which results in malware being organized in families. Some works in the literature showed that opcodes are informative for detecting malware, not only in the Android platform. In this paper, we investigate if frequencies of ngrams of opcodes are effective in detecting Android malware and if there is some significant malware family for which they are more or less effective. To this end, we designed a method based on state-of-the-art classifiers applied to frequencies of opcodes ngrams. Then, we experimentally evaluated it on a recent dataset composed of 11120 applications, 5560 of which are malware belonging to several different families. Results show that an accuracy of 97% can be obtained on the average, whereas perfect detection rate is achieved for more than one malware family.

11:45 – 12:00 Coffee Break

12:00 – 13:00 Plenary Session

Keynote

Location: Lecture Hall A

Time: 12:00 – 13:00

In blocks we trust: the case of crypto-currencies

Rainer Böhme (University of Innsbruck, Austria)

Abstract: Cryptographic currencies, such as Bitcoin, have received considerable attention from researchers and practitioners in various fields. In this talk, I analyse the potential of block chain technologies — a term referring to Bitcoin's underlying authenticated data structure — for general purpose distributed arbiters. I share observations on the success factors driving initial adoption and long-term sustainability of the Bitcoin system as we know it. I try to motivate research questions that address fundamental obstacles to the theoretical analysis and practical implementation of block chain technologies, and I sketch a vision of how they might be overcome.

13:00 – 14:15 Lunch

14:15 – 15:45 Parallel Sessions

ARES Short II – Hardware and Physical Layer Security

Session Chair: Stefan Katzenbeisser (TU Darmstadt, Germany)

Location: Lecture Hall A

Time: 14:15 – 15:45

1. Hardware Security Evaluation Using Assurance Case Models

Henrique Kawakami, Roberto Gallo, Ricardo Dahab, Erick Nascimento (University of Campinas, Brazil)

Abstract: The security of computing systems relies heavily on their hardware architecture. Currently, hardware is evaluated using mostly manual processes that are prone to errors, and generate a large, complex workload. In this paper, we are the first to report the use of the Assurance Case methodology to guide a hardware architecture security analysis. We were able to analyse real-world systems, and to detect known and some possibly unknown vulnerabilities. We also show that, by employing Assurance Cases, other benefits are gained, such as better security analysis coverage and better documentation of the security-relevant aspects of the system.

2. Error/Intrusion target identification on the physical layer over a BICM scheme

Sihem Chaabouni, Amel Makhlouf (ENET'COM, Tunisia)

Abstract: We propose in this work an error detection process for wireless networks, applied to a previously published transmitter/Receiver system model. This model is based on a bit interleaved coded modulation (BICM) scheme over a frequency selective channel. The detection process is able to discern the attacked block: encoder, modulator or channel. We prove using simulations that the deployed intrusion detection system (IDS) is competitive by comparing it to existing intrusion detection systems.

3. Physically Secure Code and Data Storage in Autonomously Booting Systems

Johannes Götzfried, Johannes Hampel, Tilo Müller (Friedrich-Alexander University of Erlangen-Nuremberg, Germany)

Abstract: Today, full disk encryption is a common practice to protect data on desktop computers and notebooks from unauthorized physical access. For embedded systems, however, the situation is different and they often lack physical protection. Usually no user or remotely connected system is involved during the boot phase which requires autonomously booting systems. For this paper an entire software stack for secure code and data storage in embedded systems has been designed, implemented and evaluated regarding security aspects and performance. For the security evaluation, physical attacks on the flash chip and RAM access have been taken into account. The system is a combined hardware and software solution and provides a considerable amount of security without a second party involved that could participate in a trust bootstrapping protocol. A symmetric key hierarchy enables the use of applications from different vendors which are not able to decrypt each other's software. For code, a signature chain ensures the authenticity of the code being run. For data, integrity is ensured on a per sector basis such that targeted manipulations are not only mitigated but can be detected as well. This is a novel technique that is currently not known from any publicly available full disk encryption system. We show that the confidentiality, integrity and authenticity of code and data protected with our system can be ensured provided that small parts of the hardware are considered trusted.

4. Towards Abuse Detection and Prevention in IaaS Cloud Computing

Jens Lindemann (University of Hamburg, Germany)

Abstract: Cloud computing is frequently being used to host online services. Abuse of cloud resources poses an important problem for cloud service providers. If third parties are affected by abuse, bad publicity or legal liabilities may ensue for the provider. There is an unsatisfactory level of protection against abuse of cloud offerings at the moment. In this paper, we analyse the current state of abuse detection and prevention in IaaS cloud computing. To establish what constitutes abuse in an IaaS environment, a survey of acceptable use policies of cloud service providers was conducted. We have found that existing intrusion detection and prevention techniques are only of limited use in this environment due to the high level of control that users can exercise over their resources. However, cloud computing opens up different opportunities for intrusion detection. We present possible approaches for abuse detection, which we plan to investigate further in future work.

ARES Short III – Social Networks, Voting and Usable Security

Session Chair: Edgar Weippl (SBA Research, Austria)
Location: Lecture Hall B
Time: 14:15 – 15:45

1. A Model Implementing Certified Reputation and its Application to TripAdvisor

Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo, Antonino Nocera (Università Mediterranea of Reggio Calabria, Italy)

Abstract: Many real-life reputation models suffer from classical drawbacks making the systems where they are used vulnerable to users' misbehaviour. TripAdvisor is a good example of this problem. Indeed, despite its popularity, the weakness of its reputation model is resulting in loss of credibility and growth of legal disputes. In this paper, we propose a reputation model abstractly considering service providers, users and feedbacks, and implementing the theoretical notion of certified reputation to concretely define a strategy to normalize feedback scores towards reliable values. We apply the model to the case of TripAdvisor, by proposing a solution to improve its dependability not increasing invasiveness nor reducing usability of the system. Moreover, it fully guarantees backward compatibility. In the context of project activities, we are in progress to fully implement the system and validate it on real-life data.

2. QR Code Security – How Secure and Usable Apps Can Protect Users Against Malicious QR Codes

Katharina Krombholz, Peter Frühwirt (SBA Research, Austria), Thomas Rieder (TU Wien, Austria), Ioannis Kaspsalis (Aalto University, Finland), Johanna Ullrich, Edgar Weippl (SBA Research, Austria)

Abstract: QR codes have emerged as a popular medium to make content instantly accessible. With their high information density and robust error correction, they have found their way to the mobile ecosystem. However, QR codes have also proven to be an efficient attack vector, e.g. to perform phishing attacks. Attackers distribute malicious codes under false pretenses in busy places or paste malicious QR codes over already existing ones on billboards. Ultimately, people depend on reader software to ascertain if a given QR code is benign or malicious. In this paper, we present a comprehensive analysis of QR code security. We determine why users are still susceptible to QR code based attacks and why currently deployed smartphone apps are unable to mitigate these attacks. Based on our findings, we present a set of design recommendations to build usable and secure mobile applications. To evaluate our guidelines, we implemented a prototype and found that secure and usable apps can effectively protect users from malicious QR codes.

3. Efficiency Evaluation of Cryptographic Protocols for Boardroom Voting

Oksana Kulyk, Stephan Neumann, Jurlind Budurushi, Melanie Volkamer (TU Darmstadt/CASED, Darmstadt, Germany)

Abstract: Efficiency is the bottleneck of many cryptographic protocols towards their practical application in different contexts. This holds true also in the context of electronic voting, where cryptographic protocols are used to ensure a diversity of security requirements, e.g. secrecy and integrity of cast votes. A new and promising application area of electronic voting is boardroom voting, which in practice takes place very frequently and often on simple issues such as approving or refusing a budget. Hence, it is not a surprise that a number of cryptographic protocols for boardroom voting have been already proposed. In this work, we introduce a security model adequate for the boardroom voting context. Further, we evaluate the efficiency of four boardroom voting protocols, which to best of our knowledge are the only boardroom voting protocols that satisfy our security model. Finally, we compare the performance of these protocols in different election settings.

4. Event Prediction with Community Leaders

Jun Pang, Yang Zhang (University of Luxembourg, Luxembourg)

Abstract: With the emerging of online social network services, quantitative studies on social influence become achievable. Leadership is one of the most intuitive and common forms for social influence; understanding it could result in appealing applications such as targeted advertising and viral marketing. In this work, we focus on investigating leaders' influence for event prediction in social networks. We propose an algorithm based on events that users conduct to discover leaders in social communities. Analysis on the leaders that we found on a real-life social network dataset leads us to several interesting observations, such as that leaders do not have significantly higher number of friends but are more active than other community members. We demonstrate the effectiveness of leaders' influence on users' behaviours by learning tasks: given a leader has conducted one event, whether and when a user will perform the event. Experimental results show that with only a few leaders in a community the event predictions are always very effective.

Workshop ASSD II – Assessment of research on agile development of secure software

Session Chair: Lotfi ben Othame (Fraunhofer SIT, Germany)
Location: Lecture Hall C
Time: 14:15 – 15:45

1. Literature Review of the Challenges of Developing Secure Software Using the Agile Approach

Hela Oueslati, Mohammad Masudur Rahman (TU Darmstadt, Germany), Lotfi ben Othmane (Fraunhofer SIT, Germany)

Abstract: A set of challenges of developing secure software using the agile development approach and methods are reported in the literature. This paper reports about a systematic literature review to identify these challenges and evaluates the causes of each of these challenges, with respect to the agile values, the agile principles, and the security assurance practices. We identified in this study 20 challenges, which are reported in 10 publications. We found that 14 of these challenges are valid and 6 are neither caused by the agile values and principles, nor by the security assurance practices. We also found that 2 of the valid challenges are related to the software development life-cycle, 4 are related to incremental development, 4 are related to security assurance, 2 are related to awareness and collaboration, and 2 are related to security management. These results justify the need for research to make developing secure software smooth.

2. Method Selection and Tailoring for Agile Threat Assessment and Mediation

Stephan Renatus, Clemens Teichmann, Jörn Eichler (Fraunhofer Institute for Applied and Integrated Security AISEC, Germany)

Abstract: Security engineering and agile development are often perceived as a clash of cultures. To address this clash, several approaches have been proposed that allow for agile security engineering. Unfortunately, agile development organization differ in their actual procedures and environmental properties resulting in varying requirements. We propose an approach to compare and select methods for agile security engineering. Furthermore, our approach addresses adaptation or construction of a tailored method taking the existing development culture into account. We demonstrate the feasibility of our proposal and report early experiences from its application within a small development organization for digital solutions in the automotive domain.

3. The human factor: philosophy and engineering (presentation only)

Albert Zenkoff (Software AG, Germany)

Workshop WSDF II – 8th International Workshop on Digital Forensics

Session Chair: Martin Mulazzani (SBA Research, Austria)
Location: Lecture Hall D
Time: 14:15 – 15:45

1. Keynote: Remote Evidence Acquisition

Marc Scanlon (UCD School of Computer Science and Informatics, Ireland)

Abstract: In an increasing trend, more and more consumer and enterprise data is being accessed on-the-fly and synchronised from remote machines or cloud services. Providing the ability to transfer, store and analyse digital evidence from these remote sources could prove invaluable to a variety of investigations. In a typical investigation, a number of impeding factors might result in traditional local evidence acquisition becoming extremely time consuming, if not entirely impossible, for example device encryption, data corruption, device destruction, etc. This talk provides an overview of the techniques available for the acquisition and handling of digital forensic evidence from a variety of remote sources including physical media, peer-to-peer networks and file synchronisation services, and discusses the methods available for the verification of the evidence collected.

1. Challenges of Data Provenance for Cloud Forensic Investigations

Victoria Katilu, Virginia Franqueira, Olga Angelopoulou (University of Derby, UK)

Abstract: Cloud computing has gained popularity due to its efficiency, robustness and cost effectiveness. Carrying out digital forensic investigations in the cloud is currently a relevant and open issue. The root of this issue is the fact that servers cannot be physically accessed, coupled with the dynamic and distributed nature of cloud computing with regards to data processing and storage. This renders traditional methods of evidence collection impractical. The use of provenance data in cloud forensics is critical as it provides forensic investigators with data history in terms of people, entities and activities involved in producing related data objects. Therefore, cloud forensics requires effective provenance collection mechanisms. This paper provides an overview of current provenance challenges in cloud computing and identifies limitations of current provenance collection mechanisms. Recommendations for additional research in digital provenance for cloud forensics are also presented.

Workshop IWSMA II – Networks Security

Session Chair: Peter Kieseberg (SBA Research, Austria)
Location: Lecture Hall E
Time: 14:15 – 15:45

1. Risk Assessment of Public Safety and Security Mobile Service

Matti Peltola, Pekka Kekolahti (Aalto University, Finland)

Abstract: A deeper understanding of the availability of Public Safety and Security (PSS) mobile networks and their service under different conditions offers decision makers guidelines on the level of investments required and the directions to take in order to decrease the risks identified. In the study, a risk assessment model for the existing PSS mobile service is implemented for both a dedicated TETRA PSS mobile network as well as for a commercial 2G/3G mobile network operating under the current risk conditions. The probabilistic risk assessment is carried out by constructing a Bayesian Network. According to the analysis, the availability of the dedicated Finnish PSS mobile service is 99.1%. Based on the risk assessment and sensitivity analysis conducted, the most effective elements for decreasing availability risks would be duplication of the transmission links, backup of the power supply and real-time mobile traffic monitoring. With the adjustment of these key control variables, the service availability can be improved up to the level of 99.9%. The investments needed to improve the availability of the PSS mobile service from 99.1 % to 99.9% are profitable only in highly populated areas. The calculated availability of the PSS mobile service based on a purely commercial network is 98.8%.The adoption of a Bayesian Network as a risk assessment method is demonstrated to be a useful way of documenting different expert knowledge as a common belief about the risks, their magnitudes and their effects upon a Finnish PSS mobile service.

2. Trust Negotiation Based Approach to Enforce MANET Routing Security

Aida Ben chehida Douss (University of Carthage, Tunisia), Samiha Ayed (Telecom Bretagne, France), Ryma Abassi (University of Carthage, Tunisia), Nora Cuppens, Samiha Ayed (Telecom Bretagne, France), Sihem Guemara EL Fatmi (University of Carthage, Tunisia)

Abstract: MANETs (Mobile Ad hoc Networks) are described as sets of mobile nodes connected with wireless links. To be efficient, routing protocols in MANETs should, in fact, manage mobility, handle nodes energy dissipation and ensure security. We argue in this paper that trust negotiation is appropriate in such context to enhance the network performances. Trust concept is of concern to communication and network protocol designers. Thus, building trust relationships among participating nodes is critical to enabling collaborative optimization of system metrics. The main contribution of this paper is an extension of our previous proposition DTMCA (Delegation Trust Mobility-based Clustering Approach) which defines a new clustering approach, a trust management process and a delegation process. This environment allows the localization and the isolation of malicious nodes in MANETs. The extension proposed in this paper extends the trust management process by adding a trust negotiation module used in order to minimize the risk that malicious nodes join the MANETs.

3. A Model for Specification and Validation of a Trust Management based Security Scheme in a MANET Environment

Aida Ben Chehida Douss, Ryma Abassi, Sihem Guemara El Fatmi (University of Carthage, Tunisia)

Abstract: Recently, we proposed a reputation based trust management scheme built upon a Mobility-based Clustering Approach (MCA) organizing Mobile Ad hoc NETwork MANET and detecting and isolating malicious behaviours. The whole scheme was called TMCA (Trust based MCA) and was extended in a second time with a delegation process resulting a proposition baptized DTMCA (Delegation TMCA based process). However, deploying such scheme is error prone and it appears necessary to validate it before its real implementation. In fact, scheme specification and validation constitute two fundamental challenges in the development of secure communication systems ensuring that the scheme is correctly enforced and complete. Hence, the main contribution of this paper concerns a validation framework for DTMCA scheme. The first step towards validation process is its formal specification. This is our first concern in this paper: a formal specification language called SCMSL (Secured Clustered MANET Specification Language) defined through a syntax based on authorization and obligation rules and a clear semantics. The second part of this paper proves the two major characteristics that must be guaranteed in such case: consistency and completeness. Consistency is proved by showing that there is no conflict in our scheme whereas completeness is proved by assessing that all potential situations are handled. The proof of consistency and completeness is made using automated systems through the definition of adequate algorithms.

16:00 – 23:30 Sightseeing tour Carcassonne
Conference Dinner Château de Pennautier

The Conference Dinner will take place at the Château de Pennautier, which is located in the area of Carcassonne, about one hour from Toulouse. The Château de Pennautier, known as „Petit Versailles“, was built in 1620. In 1670 Le Vau, the architect of Versailles, completed the construction. Before enjoying a delicious Conference Dinner in the wonderful Château de Pennautier, we have organized a tour through the cité de Carcassonne. The town has about 2,500 years of history and was added 1997 to UNESCO’s list of World Heritage Sites.

Meeting point: Université Paul Sabatier, busses leave at 16.00 (shortly after the last session)

Back in Toulouse: 23.30

Thursday, August 27th 2015

08:30 – 11:00 Registration desk open

09:15 – 10:45 Parallel Sessions

Workshop FARES I – Monitoring and Identification

Session Chair: Edgar Weippl (SBA Research, Austria)

Location: Lecture Hall B

Time: 09:15 – 10:45

1. Towards the Forensic Identification and Investigation of Cloud Hosted Servers through Non-Invasive Wiretaps

Hessel Shut (Korps Landelijke Politiediensten, Netherlands), Mark Scanlon, Jason Farina, NhienAn LeKhac (University College Dublin, Ireland)

Abstract: When conducting modern cybercrime investigations, evidence has often to be gathered from computer systems located at cloud-based data centres of hosting providers. In cases where the investigation cannot rely on the cooperation of the hosting provider, or where documentation is not available, investigators can often find the identification of which distinct server among many is of interest difficult and extremely time consuming. To address the problem of identifying these servers, in this paper a new approach to rapidly and reliably identify these cloud hosting computer systems is presented. In the outlined approach, a handheld device composed of an embedded computer combined with a method of undetectable interception of Ethernet based communications is presented. This device is tested and evaluated, and a discussion is provided on its usefulness in identifying of server of interest to an investigation.

2. Privacy and Trust in Smart camera sensor networks

Michael Loughlin, Asma Adnane (University of Derby, UK)

Abstract: The emerging technologies of Smart Camera Sensor Networks (SCSN) are being driven by the social need for security assurance and analytical information. SCSN are deployed for protection and for surveillance tracking of potential criminals. A smart camera sensor does not just capture visual and audio information but covers the whole electromagnetic spectrum. It constitutes of intelligent on-board processor, autonomous communication interfaces, memory and has the ability to execute algorithms. The rapid deployment of smart camera sensors with ubiquitous imaging access causes security and privacy issues for the captured data and its metadata, as well as the need for trust and cooperation between the smart camera sensors. The intelligence growth in this technology requires adequate information security with capable privacy and trust protocols to prevent malicious content attacks. This paper presents, first, a clear definition of SCSN. It addresses current methodologies with perspectives in privacy and trust protection, and proposes a multi-layer security approach. The proposed approach highlights the need for a public key infrastructure layer in association with a Reputation-Based Cooperation mechanism.

3. Security Monitoring of HTTP Traffic Using Extended Flows

Martin Husák, Petr Velan, Jan Vykopal (Masaryk University, Czech Republic)

Abstract: In this paper, we present an analysis of HTTP traffic in a large-scale environment which uses network flow monitoring extended by parsing HTTP requests. In contrast to previously published analyses, we were the first to classify patterns of HTTP traffic which are relevant to network security. We described three classes of HTTP traffic which contain brute force password attacks, connections to proxies, HTTP scanners, and web crawlers. Using the classification, we were able to detect up to 16 previously undetectable brute-force password attacks and 19 HTTP scans per day in our campus network. The activity of proxy servers and web crawlers was also observed. Symptoms of these attacks may be detected by other methods based on traditional flow monitoring, but detection using the analysis of HTTP requests is more straightforward. We, thus, confirm the added value of extended flow monitoring in comparison to the traditional method.

Workshop SAW I – Security Design and Validation

Session Chair: Simon Tjoa (FH St. Pölten, Austria)
Location: Lecture Hall C
Time: 09:15 – 10:45

1. How Much Cloud Can You Handle?

Martin Jaatun, Inger Anne Tøndel (SINTEF ICT, Norway)

Abstract: Outsourcing computing and storage to the cloud does not eliminate the need for handling of information security incidents. However, the long provider chains and unclear responsibilities in the cloud make incident response difficult. In this paper we present results from interviews in critical infrastructure organisations that highlight incident handling needs that would apply to cloud customers, and suggest mechanisms that facilitate inter-provider collaboration in handling of incidents in the cloud, improving the accountability of the cloud service providers.

2. Generation of local and expected behaviours of a smart card application to detect software anomaly

Germain JOLLY, Baptiste HEMERY, Christophe ROSENBERGER (Normandie Universite, France)

Abstract: The electronic payment transaction involves the use of a smart card. A card application is a software, corresponding to standards and non-proprietary and proprietary specifications, and is stored in the smart card. Despite increased security with Europay Mastercard Visa (EMV) specifications, attacks still exist due to anomalies in the card application. The validation of the card application enables the detection of any anomaly, improving the overall security of electronic payment transactions. Among the different ways of validating a card application, we can use the verification of required behaviours. These behaviour can be materialized as properties of commands sent by the terminal and responses from the smart card, using the Application Protocol Data Unit (APDU) from the ISO/IEC 7816 standard [1]. However, the creation of these behaviours is complicated. We propose in this article a way to automatically create such behaviours by using a genetic algorithm technique.

3. Securing web applications with better „patches“: an architectural approach for systematic input validation with security patterns

Jung-Woo Sohn, Jungwoo Ryoo (The Pennsylvania State University-Altoona, USA)

Abstract: Some of the most rampant problems in software security originate from improper input validation. This is partly due to ad hoc approaches taken by software developers when dealing with user inputs. Therefore, it is a crucial research question in software security to ask how to effectively apply well-known input validation and sanitization techniques against security attacks exploiting the user input-related weaknesses found in software. This paper examines the current ways of how input validation is conducted in major open-source projects and attempts to confirm the main source of the problem as these ad hoc responses to the input validation-related attacks such as SQL injection and cross-site scripting (XSS) attacks through a case study. In addition, we propose a more systematic software security approach by promoting the adoption of proactive, architectural design-based solutions to move away from the current practice of chronic vulnerability-centric and reactive approaches.

4. Towards a CERT-Communication Model as Basis to Software Assurance

Gerald Quirchmayr, Otto Hellwig (University of Vienna, Austria)

Abstract: This paper describes an approach towards modelling the communication in and between CERTs, of CERTs with their constituents, and of CERTs with other stakeholders and partners. As achieving their sometimes diverging goals is essential for CERTs, an extended goalscenario model is suggested.

10:45 – 11:15 Coffee Break

11:15 – 12:45 Parallel Sessions

Workshop FARES II – Cryptography and Resilience

Session Chair: Edgar Weippl (SBA Research, Austria)

Location: Lecture Hall B

Time: 11:15 – 12:45

1. Towards a process centered resilience framework

Thomas Koslowski, Christian Brenig, Richard M. Zahoransky (University of Freiburg, Germany)

Abstract: The turbulent organizational environment and the intensive use of interconnected, complex IT-systems incur operational risks with increasingly severe and uncertain disruptive effects. The increasing reliance on Information Systems (IS) such as Business Process Management (BPM) systems brought up an urgent need to ensure continuous business operations despite unexpected challenging conditions. In contrast to well-established risk-aware BPM which mainly addresses risk mitigation at design-time and only for known risks, we propose resilient BPM as a complementary approach focusing either at run-time or off-time. Such approaches seek the adjustment and maintenance of operations under disruption. We report on our ongoing work towards the development of a decision support framework to realize resilience in the BPM context. For this approach, measuring resilience on a process level is crucial, since it provides information that allow for better decision-making, learning, and improvement. Nevertheless, there are no suitable holistic measurement systems for resilient BPM available by now. Specifically, this paper motivates the need for operational resilience measurement at the level of processes. It presents the components and operation of our measurement framework, which helps to detect resilience properties of processes based on measures by analysing process-logs. This information is then exploited to drive a resilience-oriented decision support to increase process resilience.

2. Complexity Estimates of a SHA-1 Near-Collision Attack for GPU and FPGA

Stefan Gradinger, Bernhard Greslehner-Nimmervoll (FH OÖ Research and Development Hagenberg, Austria), Jürgen Fuß, Robert Kolmhofer (University of Applied Sciences Upper Austria Hagenberg, Austria)

Abstract: The complexity estimate of a hash collision algorithm is given by the unit hash compressions. This paper shows that this figure can lead to false runtime estimates when accelerating the algorithm by the use of graphics processing units (GPU) and field-programmable gate arrays (FPGA). For demonstration, parts of the CPU reference implementation of Marc Stevens' SHA-1 NearCollision Attack are implemented on these two accelerators by taking advantage of their specific architectures. The implementation, runtime behaviour and performance of these ported algorithms are discussed, and in conclusion, it is shown that the acceleration results in different complexity estimates for each type of coprocessor.

3. Impacts of Tourist Accommodations as Temporal Shelter on Evacuee Overflow for the Reassignment of Shelters Jurisdiction

Yu Ichifuji (Research Organization of Information and Systems Japan), Noriaki Koide (Osaka University, Japan) Noboru Sonehara (National Institute of Informatics, Japan)

Abstract: Effective measures against natural disasters are needed worldwide, and the jurisdiction assignment of evacuation shelters during natural disasters is one such measure. In this paper, we discuss two evacuation cases involving tourist accommodations as temporary shelters. One involves evacuation to the closest shelter, and the other involves using our previously proposed optimization method for assigning jurisdiction for shelters. The impact of tourist accommodations on evacuee overflow for each case was investigated. We also explain that tourist accommodations as temporary shelter reduce the evacuee overflow at shelters by using a numerical example. We argue that its impact is limited by giving an example of a city in Japan where the evacuation and residential areas are widely spaced.

Workshop SAW II – Software Testing and Assurance

Session Chair: Jungwoo Ryoo (Pennsylvania State University, USA)
Location: Lecture Hall C
Time: 11:15 – 12:45

1. Towards Black Box Testing of Android Apps

Yury Zhauniarovich, Anton Philippov (University of Trento, Italy), Olga Gadyatskaya (University of Luxembourg, Luxembourg), Bruno Crispo, Fabio Massacci (University of Trento, Italy)

Abstract: Many state-of-art mobile application testing frameworks (e.g., Dynodroid [1], EvoDroid [2]) enjoy Emma [3] or other code coverage libraries to measure the coverage achieved. The underlying assumption for these frameworks is availability of the app source code. Yet, application markets and security researchers face the need to test third-party mobile applications in the absence of the source code. There exists a number of frameworks both for manual and automated test generation that address this challenge. However, these frameworks often do not provide any statistics on the code coverage achieved, or provide coarse-grained ones like a number of activities or methods covered. At the same time, given two test reports generated by different frameworks, there is no way to understand which one achieved better coverage if the reported metrics were different (or no coverage results were provided). To address these issues we designed a framework called BBOXTESTER that is able to generate code coverage reports and produce uniform coverage metrics in testing without the source code. Security researchers can automatically execute applications exploiting current stateof-art tools, and use the results of our framework to assess if the security-critical code was covered by the tests. In this paper we report on design and implementation of BBOXTESTER and assess its efficiency and effectiveness.

2. Personal Agent for Services in ITS

Shinsaku Kiyomoto, Toru Nakamura, Haruo Takasaki, Tatsuhiko Hirabayashi (KDDI Research Institute Inc., Japan)

Abstract: In this paper, we introduce the concept of a privacy enhancing personal agent that manages a user's privacy policy settings and provides access control functions to ITS services. The personal agent acts as a proxy between a vehicle and service providers, and it automatically decides whether personal data can be sent to a service provider based on the privacy policy settings. The functions of the personal agent are also described. The personal agent provides a common web-based interface, and the quality of data can be controlled through anonymization levels. Our research provides a conceptual model of the personal agent and considers the design of the personal agent based on privacy requirements. Drivers can delegate their user consent role to the personal agent by configuring privacy policy settings on the personal agent. The personal agent is a key component for achieving a secure and reliable data transfer platform between vehicles and service providers.

3. A Performance Evaluation of Hash Functions for IP Reputation Lookup using Bloom Filters.

Hugo Gonzalez, Natalia Stakhanova (University of New Brunswick, Canada)

Abstract: IP reputation lookup is one of the traditional methods for recognition of blacklisted IPs, i.e., IP addresses known to be sources of spam and malware-related threats. Its use however has been rapidly increasing beyond its traditional domain reaching various IP filtering tasks. One of the solutions able to provide a necessary scalability is a Bloom filter. Efficient in memory consumption, Bloom filters provide a fast membership check, allowing to confirm a presence of set elements in a data structure with a constant false positive probability. With the increased usage of IP reputation check and an increasing adoption of IPv6 protocol, Bloom filters quickly gained popularity. In spite of their wide application, the question of what hash functions to use in practice remains open. In this work, we investigate a 10 cryptographic and noncryptographic functions for on their suitability for Bloom filter analysis for IP reputation lookup. Experiments are performed with controlled, randomly generated IP addresses as well as a real dataset containing blacklisted IP addresses. Based on our results we recommend two hash functions for their performance and acceptably low false positive rate.

4. An Open Source Code Analyzer and Reviewer (OSCAR) Framework

Simon Tjoa, Patrick Kochberger, Christoph Malin, Andreas Schmoll (FH St. Pölten, Austria)

Abstract: Due to the intense usage of IT and the growing number of fields of application, we rely more than ever on functional software components. In conjunction with this development it could be observed that in the last years the popularity of open source software was on the rise for various reasons. However, in the recent past, serious vulnerabilities have been discovered. In order to support open source developers testing their source code for security bugs, in this paper, we present the idea of a

framework which combines existing open source security checkers. After presenting the architecture of the framework we demonstrate the functionality of the framework using the vulnerable application WebGoat.

12:45 – 14:00 Lunch

15:15 – 19:00 Tour I – Let's visit Airbus

We have organized a tour through the Toulouse Airbus sites.

Meeting Point: 15.15, Airbus site (directions will be provided)
Tour end: 19.00

The tour starts with the Panoramic Tour: A bus tour with commentary through the Toulouse Airbus sites: The company headquarters, the design offices and development centres, the assembly lines (A320, A330, and A350), cabin equipping, the delivery centre a must see covering 700 hectares. Afterwards we will visit the A 380 site: The J.L. Lagardère site is entirely dedicated to final assembly and flight preparations of the A380. It occupies an area of 50 hectares, including a 10-hectare assembly hall. The Airbus A380 tour will reveal all the secrets of the world's only true double-decker, from the design stage through to the commercial Service.

The tour is free of charge for all registered participants of ARES 2015 and will also take place on Friday, 28th August 2015, however the tour can only be joined once. **Registration beforehand was necessary**. Please only participate in the tour you signed up for (either Thursday or Friday).

How to get from the conference venue to Let´s visit Airbus

Address of Let´s visit Airbus:
Allée André Turcat
31700 Blagnac, France

Take the metro line "B" direction "Borderouge TOULOUSE" and change to tram line "1" at "Palais de Justice" direction "Aéroconstellation BEAUZELLE". Get out at the stop "Beauzelle" from there it is about 900 meters to Let´s visit Airbus. In total it takes about 1 hour to get there.

Friday, August 28th 2015

15:15 – 19:00 Tour II – Let's visit Airbus

We have organized a tour through the Toulouse Airbus sites.

Meeting Point: Airbus site (directions will be provided) 15.15
Tour end: 19.00

The tour starts with the Panoramic Tour: A bus tour with commentary through the Toulouse Airbus sites: The company headquarters, the design offices and development centres, the assembly lines (A320, A330, and A350), cabin equipping, the delivery centre…a must see covering 700 hectares. Afterwards we will visit the A 380 site: The J.L. Lagardère site is entirely dedicated to final assembly and flight preparations of the A380. It occupies an area of 50 hectares, including a 10-hectare assembly hall. The Airbus A380 tour will reveal all the secrets of the world's only true double-decker, from the design stage through to the commercial Service.

The tour is free of charge for all registered participants of ARES 2015 and will also take place on Thursday, 27th August 2015, however the tour can only be joined once. **Registration beforehand was necessary**. Please only participate in the tour you signed up for (either Thursday or Friday).

How to get from the city centre to Let´s visit Airbus

Address of Let´s visit Airbus:
Allée André Turcat
31700 Blagnac, France

Get in the metro at "Capitole". Take the metro line "A" direction "Basso Cambo" and change to tram line "1" at "Arènes" direction "Aéroconstellation BEAUZELLE". Get out at the stop "Beauzelle" from there it is about 900 meters to Let´s visit Airbus. In total it takes about 1 hour to get there.

Keynotes

Peter Eckersley

EFF Technology Projects Director, USA

Keynote: Let's Encrypt: Deploying free, secure, and automated HTTPS certificates for the entire Web

Tuesday, August 25th 2015, 09:45 – 10:45, Lecture Hall A

Abstract: *EFF Technology Projects Director Peter Eckersley will discuss the obstacles that have prevented us from transitioning to a secure, encrypted Web that uses HTTPS by default. He will provide an overview of the Let's Encrypt CA which EFF is building with Mozilla, Cisco, Akamai and IdentTrust, to offer free and automated deployment of certificates for HTTPS/TLS/SSL, and of other standards initiatives that will be necessary to make Web communications safe by default against surveillance, censorship, and tampering on the network.*

Peter Eckersley is Chief Computer Scientist for the Electronic Frontier Foundation. He leads a team of technologists who watch for technologies that, by accident or design, pose a risk to computer users' freedoms—and then look for ways to fix them. They write code to make the Internet more secure, more open, and safer against surveillance and censorship. They explain gadgets to lawyers and policymakers, and law and policy to gadgets.

Peter's work at EFF has included privacy and security projects such as the Let's Encrypt CA, Panopticlick, HTTPS Everywhere, and the SSL Observatory; helping to launch a movement for open wireless networks; fighting to keep modern computing platforms open; helping to start the campaign against the SOPA/PIPA Internet blacklist legislation; and running the first controlled tests to confirm that Comcast was using forged reset packets to interfere with P2P protocols.

Rainer Böhme

University of Innsbruck, Austria

Keynote: In blocks we trust: the case of crypto-currencies

Wednesday, August 26th 2015, 12:00 – 13:00, Lecture Hall A

Abstract: *Cryptographic currencies, such as Bitcoin, have received considerable attention from researchers and practitioners in various fields. In this talk, I analyse the potential of block chain technologies — a term referring to Bitcoin's underlying authenticated data structure — for general purpose distributed arbiters. I share observations on the success factors driving initial adoption and long-term sustainability of the Bitcoin system as we know it. I try to motivate research questions that address fundamental obstacles to the theoretical analysis and practical implementation of block chain technologies, and I sketch a vision of how they might be overcome.*

Rainer Böhme is Professor of Security and Privacy at the Institute of Computer Science, Universität Innsbruck, Austria. A common thread in his scientific work is the interdisciplinary approach to solving exigent problems in information security and privacy, specifically concerning cyber risk, digital forensics, cybercrime, and crypto finance. Prior affiliations in his academic career include TU Dresden and Westfälische Wilhelms-Universität Münster (both in Germany) as well as the International Computer Science Institute in Berkeley, California.

Pierangela Samarati
Università degli Studi di Milano, Italy

Keynote: Data Security and Privacy in the Cloud
Wednesday, August 26th 2015, 09:00- 10:00, Lecture Hall A

Abstract: *The rapid advancements in Information and Communication Technologies (ICTs) have enabled the emerging of the "cloud" as a successful paradigm for conveniently storing, accessing, processing, and sharing information. With its significant benefits of scalability and elasticity, the cloud paradigm has appealed companies and users, which are more and more resorting to the multitude of available providers for storing and processing data. Unfortunately, such a convenience comes at a price of loss of control over these data and consequent new security threats that can limit the potential widespread adoption and acceptance of the cloud computing paradigm. In this talk I will illustrate some security and privacy issues arising in the cloud scenario, focusing in particular on the problem of guaranteeing confidentiality and integrity of data stored or processed by external cloud Providers.*

Pierangela Samarati is a Professor at the Department of Computer Science of the Universita 'degli Studi di Milano. Her main Research interests are access control policies, models and systems, data security and privacy, information system security, and Information protection in general. She has participated in several projects involving different aspects of information protection. On these topics she has published more than 240 peer-reviewed articles in international journals, conference proceedings, and book chapters. She is the Coordinator of the ESCUDO-CLOUD European project (H2020). She has been Computer Scientist in the Computer Science Laboratory at SRI, CA (USA). She has been a visiting researcher at the Computer Science Department of Stanford University, CA (USA), and at the Centre for Secure Information Systems of George Mason University, VA (USA).

She is the chair of the IEEE Systems Council Technical Committee on Security and Privacy in Complex Information Systems (TCSPCIS), of the Steering Committees of the European Symposium on Research in Computer Security (ESORICS), and of the ACM Workshop on Privacy in the Electronic Society (WPES). She is member of several steering committees. She is ACM Distinguished Scientist (named 2009) and IEEE Fellow (named 2012). She has been awarded the IFIP TC11 Kristian Beckman award (2008) and the IFIP WG 11.3 Outstanding Research Contributions Award (2012).

Afonso Ferreira
Trust & Security Unit, European Commission

Keynote: The European Strategic Agenda for Research and Innovation in Cybersecurity
Tuesday, August 25th 2015, 09:00- 09:45, Lecture Hall A

Abstract: *This talk will present the European Strategic Research and Innovation Agenda (SRA) for cybersecurity as it is being released by the Working Group on Secure ICT Research and Innovation (aka WG3) of the Network and Information Security Platform, which is a public-private partnership put in place by the European Commission in 2013. Members of WG3 are close to two hundred. They address issues related to cybersecurity research and innovation in the context of the EU Strategy for Cyber Security and of the Network and Information Security Platform. WG3 identified the key challenges and corresponding desired outcomes in terms of innovation-focused, applied but also basic research in cybersecurity, privacy, and trust. The European SRA for cybersecurity*

designed by WG3 serves as main input for the drafting of Horizon 2020 Work Programmes by the European Commission and is source of inspiration for the coordination of, and collaboration between, research agendas across Europe, including industry research roadmaps and national research and innovation programmes of the Member States.

Afonso Ferreira is currently in charge, amongst others, of the general secretariat of the Working Group on "Secure ICT Research and Innovation" of the European Network and Information Security Platform, which provides the input for Horizon 2020 Work-Programmes in Digital Security, and is leading the planning and financing of cybersecurity activities through the Connecting Europe Facility programme. He has been seconded as a French expert to the European Commission since 2011, working now as policy officer at the Trust and Security unit of the DG CONNECT. Other assignments included the Future and Emerging Technologies unit and the Digital Futures task force.

Social Events

This year we have planned a truly diverse social program for ARES 2015. We hope to see you all there!

Monday, 24th of August 2015 – Mayor's Reception

The City of Toulouse invites us for a Mayor's Reception, taking place shortly after the last session in the City Hall of Toulouse. We will meet directly in the City Hall of Toulouse.

18.30 – 22.00

Address:
Place du Capitole
31000 Toulouse

How to get from the conference venue to the Mayor´s Reception

Take the metro line "B" direction "Borderouge TOULOUSE" and change to metro line "A" at "Jean Jaurès" direction "Basso Cambo TOULOUSE". Get out at the stop "Capitole". The City Hall of Toulouse is about 150 metres away from the underground stop.

Tuesday, 25th August 2015 – Sightseeing Tour Toulouse

Toulouse's Hidden Treasures
A guided visit out of the beaten path. Discover the unusual and secret side of the City: a Moorish-style ceiling, a truncated tower, a pair of hidden feet… Toulouse as you've never suspected it to be.

Registration beforehand was necessary. Please only participate in the tour if you are signed up for it. If you are not signed up but would like to join the tour – please come to the registration desk.

Meeting Point: Place du Capitol, 18.20
Tour start: 18.30
Tour end: 20.00 at Place du Capitol (City Centre)

How to get from the conference venue to the Sightseeing Tour meeting point

Take the metro line "B" direction "Borderouge TOULOUSE" and change to metro line "A" at "Jean Jaurès" direction "Basso Cambo TOULOUSE". Get out at the stop "Capitole". The City Hall of Toulouse is about 150 metres away from the underground stop.

Wednesday, 26th of August 2015 – Conference Dinner

The Conference Dinner will take place at the Château de Pennautier, which is located in the area of Carcassonne, about one hour from Toulouse. The Château de Pennautier, known as „Petit Versailles“, was built in 1620. In 1670 Le Vau, the architect of Versailles, completed the construction. Before enjoying a delicious Conference Dinner in the wonderful Château de Pennautier, we have organized a tour through the cité de Carcassonne, a medieval citadel located in the city of Carcassonne. The town has about 2,500 years of history and was added 1997 to UNESCO's list of World Heritage Sites.

Meeting point: Université Paul Sabatier, busses leave at 16.00 (shortly after the last session) **Back** in Toulouse: 23.30

Thursday, 27th of August 2015 / 28th of August – Let's visit Airbus

On Thursday, 27th of August 2015, and Friday, 28th of August we have organized a tour through the Toulouse Airbus sites. **Registration beforehand was necessary. Please only participate in the tour you signed up for (either Thursday or Friday).**

Meeting Point (on both days): Airbus site 15.15
Tour end: 19.00

The tour starts with the Panoramic Tour: A bus tour with commentary through the Toulouse Airbus sites: The company headquarters, the design offices and development centres, the assembly lines (A320, A330, and A350), cabin equipping, the delivery centre…a must see covering 700 hectares. Afterwards we will visit the A 380 site: The J.L. Lagardère site is entirely dedicated to final assembly and flight preparations of the A380. It occupies an area of 50 hectares, including a 10-hectare assembly hall.

Address of Let´s visit Airbus:
Allée André Turcat
31700 Blagnac, France

How to get from the conference venue to Let´s visit Airbus

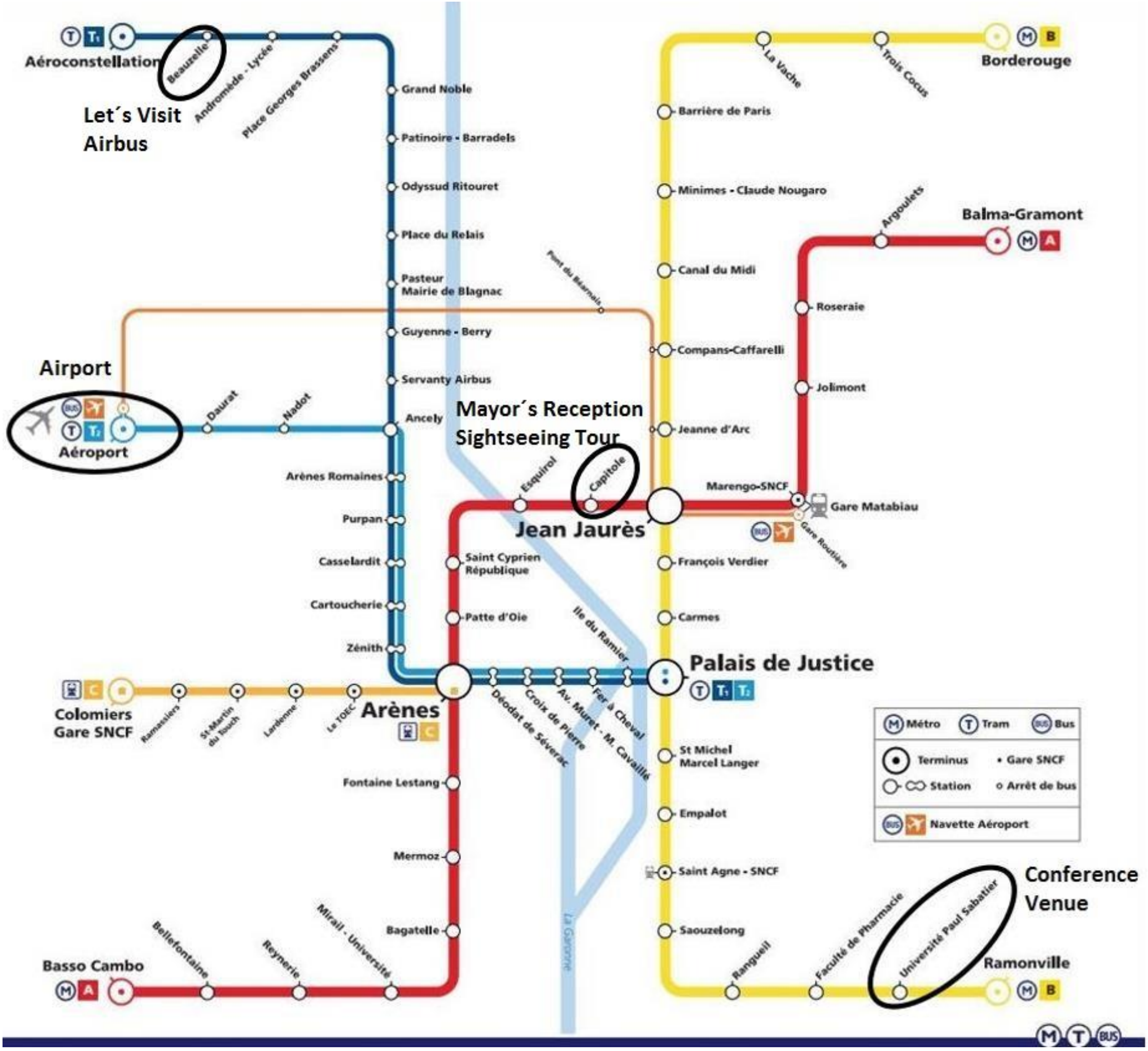
Take the metro line "B" direction "Borderouge TOULOUSE" and change to tram line "1" at "Palais de Justice" direction "Aéroconstellation BEAUZELLE". Get out at the stop "Beauzelle" from there it is about 900 meters to Let´s visit Airbus. In total it takes about 1 hour to get there.

How to get from the city centre to Let´s visit Airbus

Get in the metro at "Capitole". Take the metro line "A" direction "Basso Cambo" and change to tram line "1" at "Arènes" direction "Aéroconstellation BEAUZELLE". Get out at the stop "Beauzelle" from there it is about 900 meters to Let´s visit Airbus. In total it takes about 1 hour to get there.

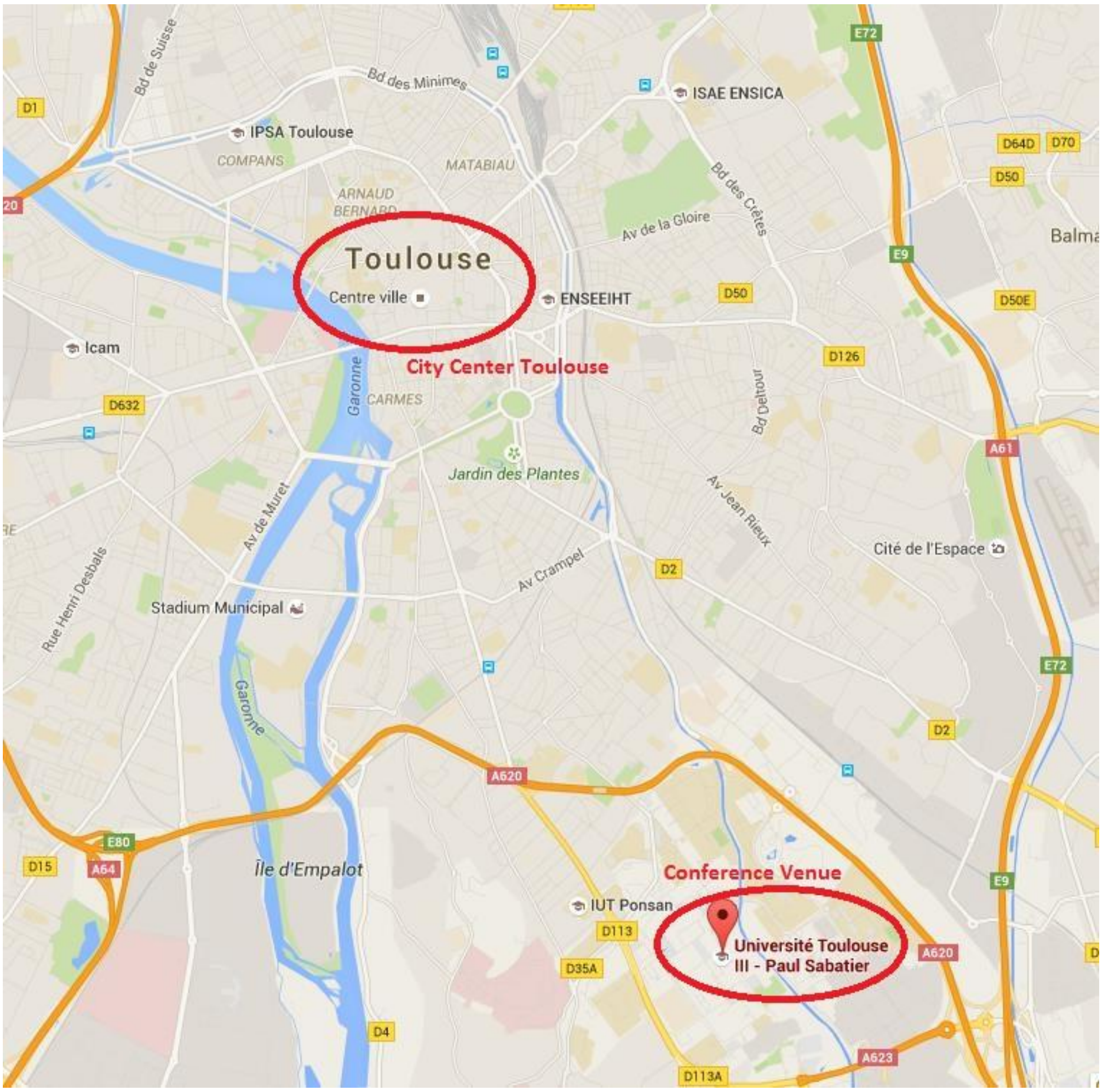
Public Transportation Social Events Overview

Below you can find the public transportation map of Toulouse with all the social event locations of ARES 2015. Detailed directions, e.g. how to get to the social events, will be provided at the Conference.



Map 1: Map Social Events ARES 2015

Venue Overview

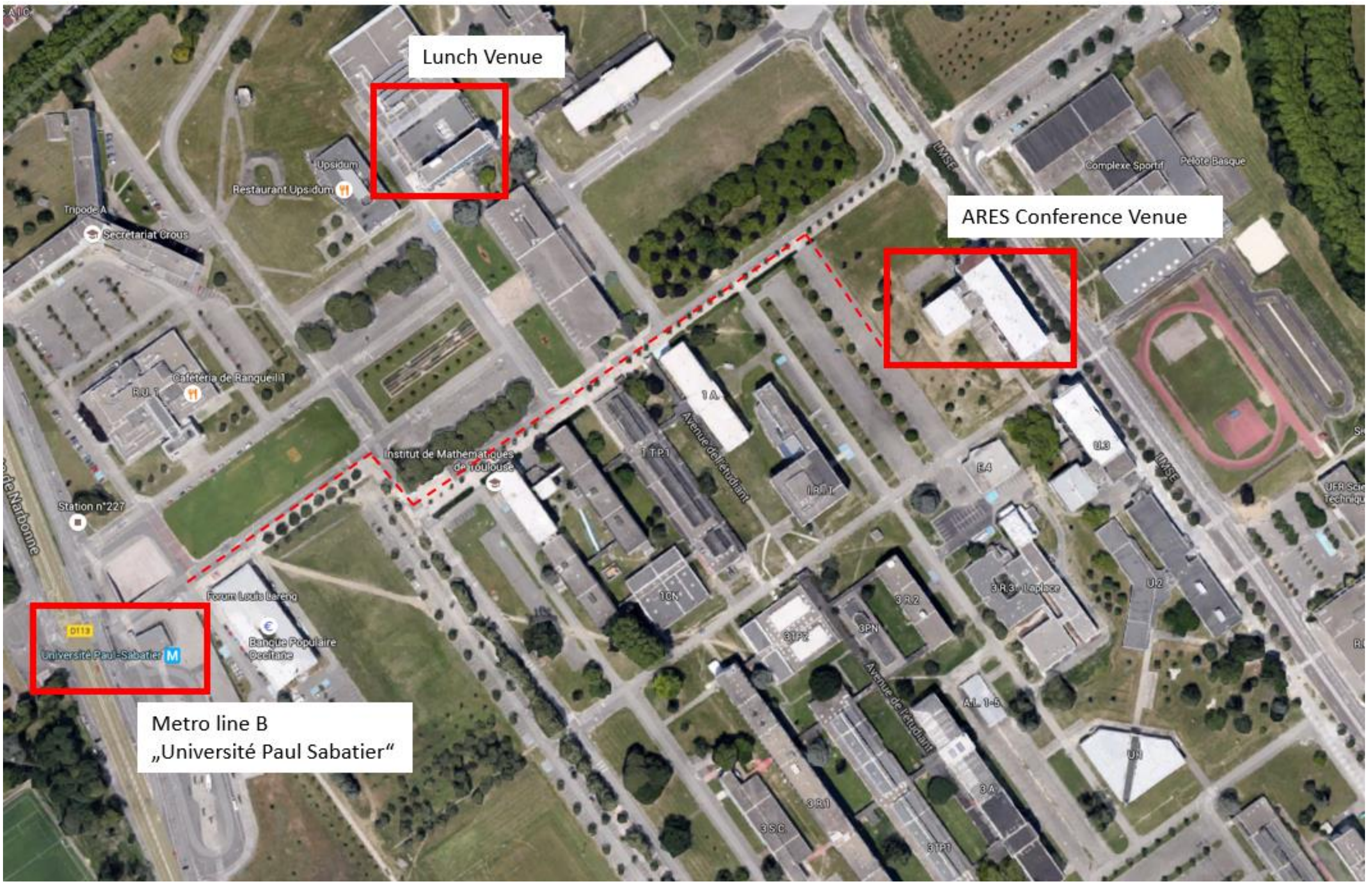


Map 2: Venue Overview

Conference Venue

Address of the Conference Venue:
Université Paul Sabatier
118 Route de Narbonne
31062 Toulouse, France

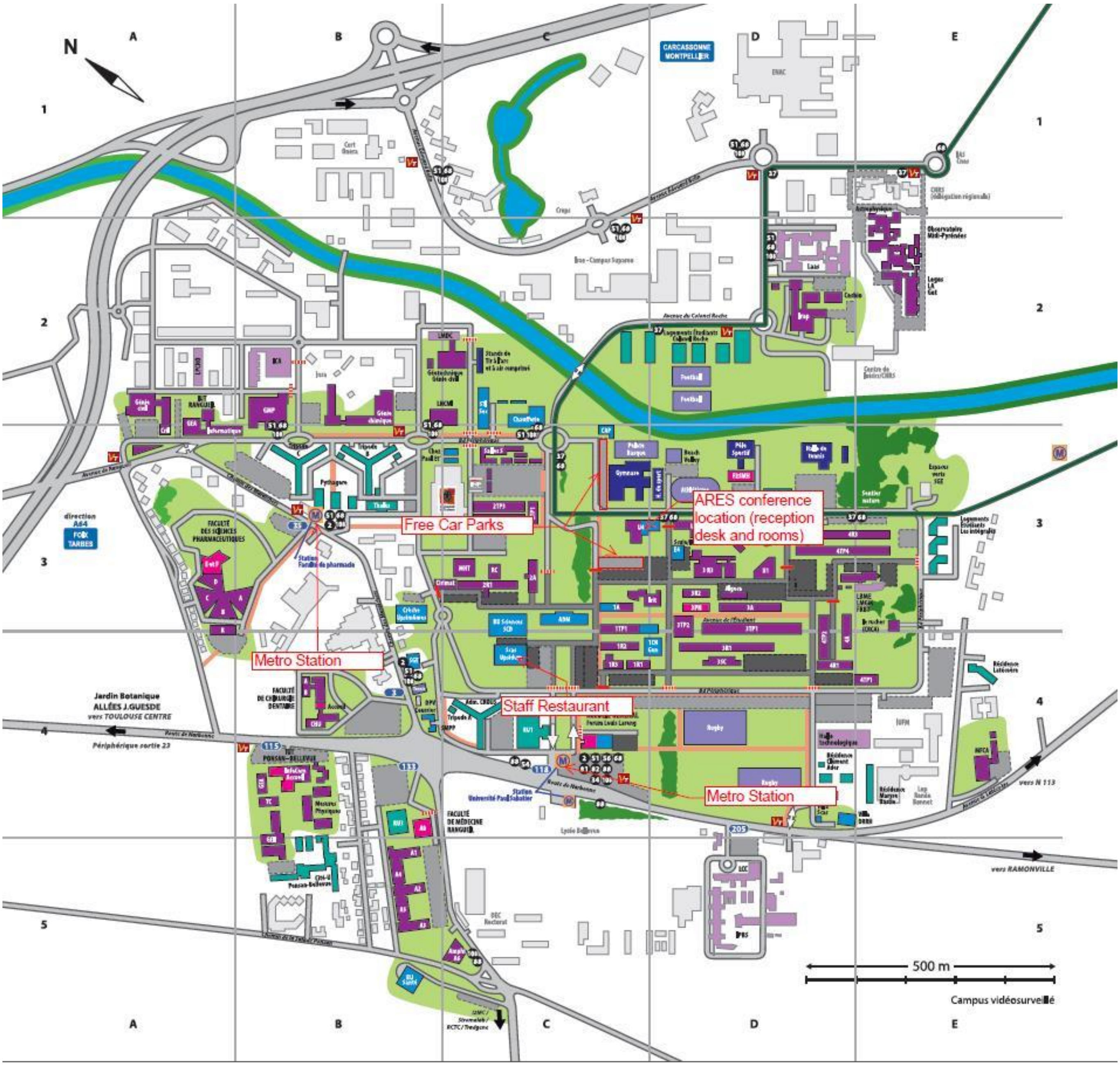
The Conference Venue (Université Paul Sabatier) is located along the underground line “Métro ligne B”, stop "Université Paul Sabatier", direction “Ramonville-Saint-Agne”. There are also free car parking spaces available.



Map 3: Conference Venue/ Underground Stop

Map 4: ARES Conference Venue (Université Paul Sabatier)

Here you can find an overview map of the Université Paul Sabatier:


N
A
B
C
D
E
1
2
3
4
5
CARCASSONNE MONTPELLIER
ARES conference location (reception desk and rooms)
Free Car Parks
Metro Station
Staff Restaurant
Metro Station
direction A64 FOIX TARBES
FACULTÉ DES SCIENCES PHARMACEUTIQUES
Jardin Botanique ALLÉES J.GUESDE vers TOULOUSE CENTRE
Périphérique sortie 23
FACULTÉ DE CHIRURGIE DENTAIRE
FACULTÉ DE MÉDECINE RANGUEIL
Station Université Paul Sabatier
Station Faculté de pharmacie
vers RAMONVILLE
vers N 113
Observatoire Midi-Pyrénées
Rugby
Gymnase
500 m
Campus vidéosurveillé

Map 5: Overview Université Paul Sabatier

Directions

How to get from the airport to the city centre

Take the tram line “T2” to “Palais de Justice TOULOUSE”. Connect at “Arènes”. Then take the metro line “A” direction “Balma-Gramont BALMA” and get out at the stop “Capitole” which is directly in the city center of Toulouse.

Alternately you can also take the bus “AREO” direction “Gare routière TOULOUSE” and get out at the stop “Jeanne d´Arc”. This stop is about 550m away from the Place du Capitole in the city center.

You can also take a taxi for your convenience, a fare to the city center costs about 30€ to 40€.

There is also an airport shuttle called “Navette Aeroport” available. It departs every 20 minutes. A single trip costs 8€.

How to get from the airport directly to the Conference Venue

Address of the Conference Venue:
Université Paul Sabatier
118 Route de Narbonne
31062 Toulouse, France

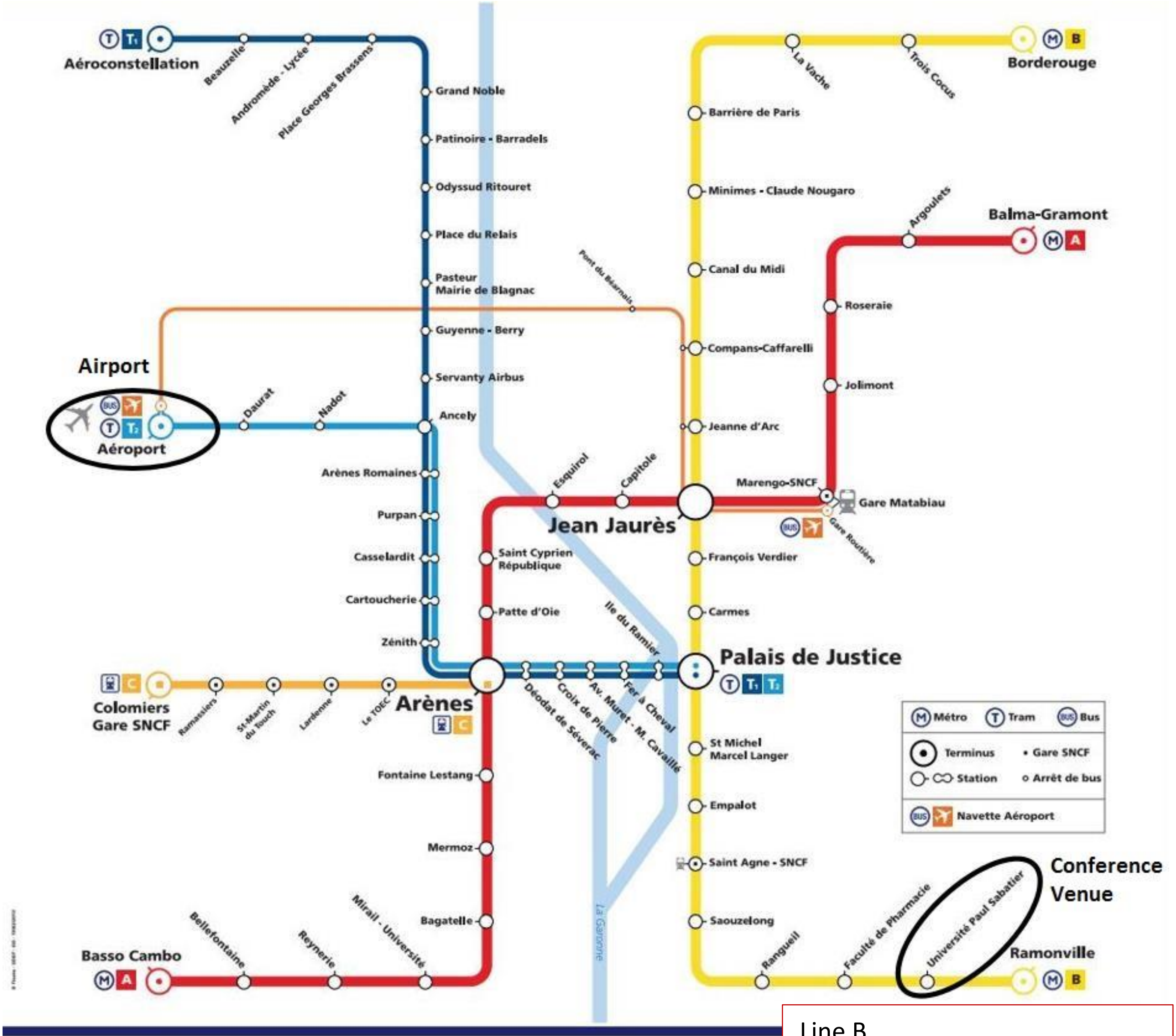
Take the bus line “AREO” direction “Gare routière TOULOUSE”, get out at the stop “Compans-Caffarelli” and change to metro line “B” direction “Ramonville-Saint-Agne” and get out at the stop Université Paul Sabatier”. It takes about 35 minutes to get from the airport to the conference venue.

How to get from the city centre to the Conference Venue

Take the metro line “A” at the station “Capitole” direction “Balma-Gramont BALMA”. Change to metro line “B” at “Jean Jaurès” direction “Ramonville Saint Agne”. Get out at the stop “Université Paul Sabatier”.

Public Transport

Below you can see the general public transportation map of Toulouse. For all directions (e.g. from your hotel to the Conference Venue) you can also visit the website http://www.tisseo.fr/en/home



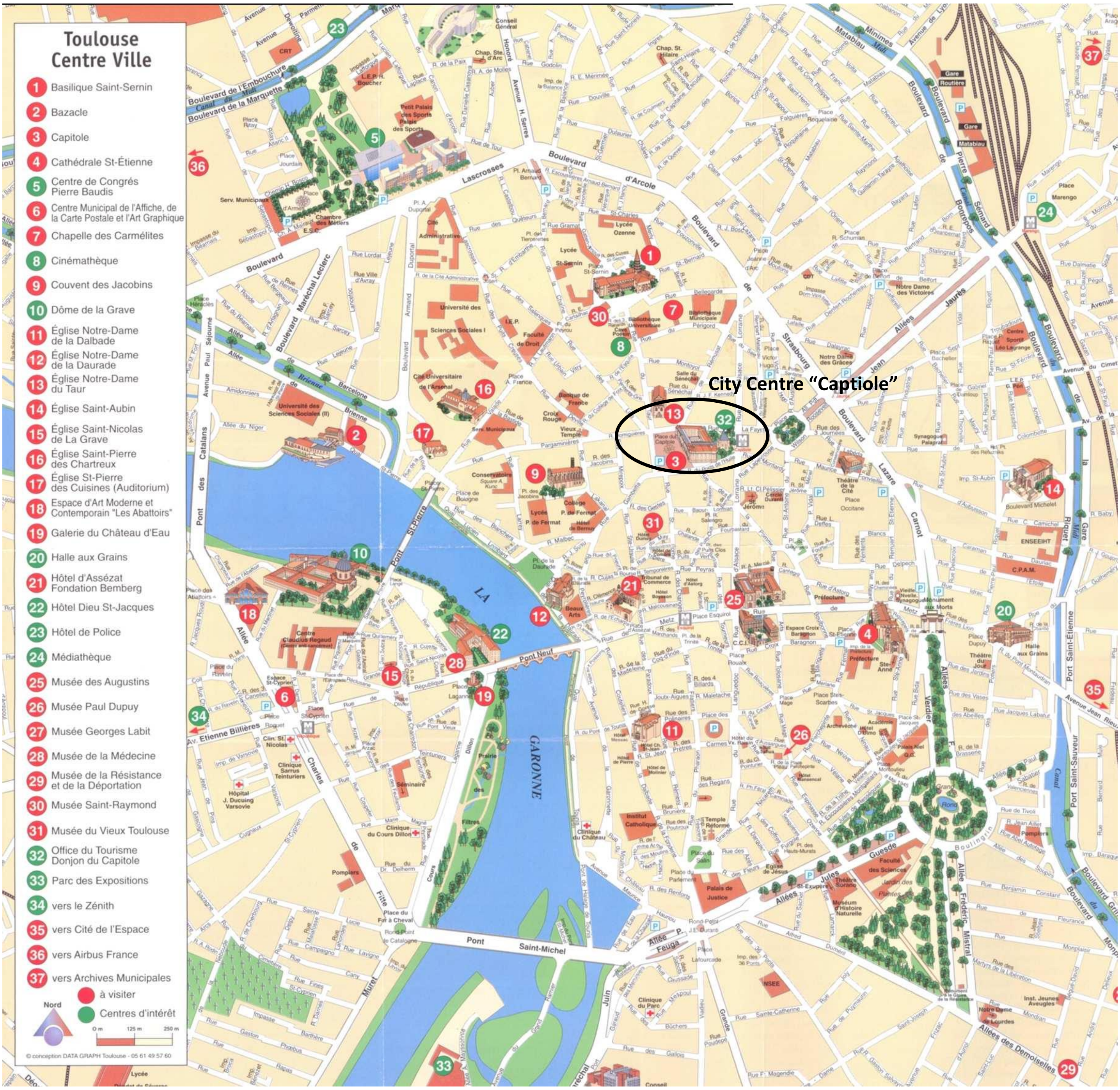
Line B

Direction: "Ramonville"

Stop: "Université Paul Sabatier"

Map 6: Public Transport Toulouse

City Map Toulouse


Toulouse Centre Ville
1 Basilique Saint-Sernin
2 Bazacle
3 Capitole
4 Cathédrale St-Étienne
5 Centre de Congrès Pierre Baudis
6 Centre Municipal de l'Affiche, de la Carte Postale et l'Art Graphique
7 Chapelle des Carmélites
8 Cinémathèque
9 Couvent des Jacobins
10 Dôme de la Grave
11 Église Notre-Dame de la Dalbade
12 Église Notre-Dame de la Daurade
13 Église Notre-Dame du Taur
14 Église Saint-Aubin
15 Église Saint-Nicolas de La Grave
16 Église Saint-Pierre des Chartreux
17 Église St-Pierre des Cuisines (Auditorium)
18 Espace d'Art Moderne et Contemporain "Les Abattoirs"
19 Galerie du Château d'Eau
20 Halle aux Grains
21 Hôtel d'Assézat Fondation Bemberg
22 Hôtel Dieu St-Jacques
23 Hôtel de Police
24 Médiathèque
25 Musée des Augustins
26 Musée Paul Dupuy
27 Musée Georges Labit
28 Musée de la Médecine
29 Musée de la Résistance et de la Déportation
30 Musée Saint-Raymond
31 Musée du Vieux Toulouse
32 Office du Tourisme Donjon du Capitole
33 Parc des Expositions
34 vers le Zénith
35 vers Cité de l'Espace
36 vers Airbus France
37 vers Archives Municipales
● à visiter
● Centres d'intérêt
Nord
0 m 125 m 250 m
© conception DATA GRAPH Toulouse - 05 61 49 57 60
City Centre “Captiole”
LA GARONNE
Pont Neuf
Pont Saint-Michel

Map 7: City Map Toulouse

Welcome to Toulouse!

Useful Information

Tourist Information

Toulouse Tourist Office
Donjon du Capitole - BP 38001
31080 Toulouse Cedex 6 - France

Opening Hours:
Monday to Saturday from 9 am to 7 pm.
Sundays and bank holidays from 10.30 am to 5.15 pm.

Emergency Numbers	
Fire service	18
Police	17
Ambulance/ rescue	15
European emergency	112

Drinking Water

It is perfectly safe to drink the tap water in France. However only drink water from public water dispensers if it is mentioned there that the water is drinkable.

Opening hours shops in Toulouse

Shops are usually open Monday to Saturday from 9.00 am – midday and 2.00 pm - 6.30 pm. Shopping is available on Sundays and holidays at the large railway stations, at the airport and in the museum shops.

Public Transport Information

Ticket Prices:

Ticket Type	Price	Additional Information
Single Ticket	1.6 €	
2 Trips by person	3.1 €	
10 Trips	13.4 €	
Evening pass	3.10 €	Unlimited trips from 7pm to closing time
Day Pass	5.5 €	Unlimited trips during 1 day
2 Days Pass	8.5 €	Unlimited trips during 2 consecutive days
3 Days Pass	10.5 €	Unlimited trips during 3 consecutive days

Métro

Line A - Basso Cambo / Balma Gramont. Serving 18 stations, journey time 22 minutes.
Line B - Borderouge / Ramonville. Serving 20 stations, journey time 26 minutes.
Connections between the two lines can be made in the town centre at Jean Jaurès station. Lines A and B run every day from 5.15 am until midnight from Sunday to Thursday and until 3am on Friday and Saturday.

Tram & Bus

Line T1 - Palais de Justice / Aéroconstellation. 24 stations from Toulouse to Beauzelle via Blagnac. Journey time 45 minutes. There are also 81 scheduled bus services.

Transport on Demand (TAD)

Complementary to the bus, tram and metro, there are 10 on demand lines, serving the areas on the periphery of Toulouse, requiring a simple telephone reservation at least 2 hours before departure. You can reserve using the Itinerary calculator or by phoning 0800 929 929 between the hours of 6.30 am and 10.30 pm.

Night service

From 9.30 pm to 3 am on Friday and Saturday and from 9.30 pm to midnight from Sunday to Thursday the following lines run in at night:

- Metro lines A and B.

From 9.30 pm to 1 am on Friday and Saturday and from 9.30 pm to midnight from Sunday to Thursday the following lines run in at night:

- Tram line T1,
- Bus lines L16 2S 10S 12S 22S 38S 78S 79S 81S and 88S,
- TAD 106 119 and 120.

The City Centre Shuttle

The town centre shuttle is electric, free and will take you to the heart of the historic city, « les quais de la Garonne », « les Carmes », « le quartier Saint-Etienne », « la place Wilson », « le boulevard de Strasbourg », « la place Jeanne d'Arc », « la place du Capitole ». The shuttle operates between 9 am and 7 pm, Monday to Saturday. A simple wave and the driver will stop for you.

The Airport Shuttle

The shuttle provides a link between the airport at Toulouse-Blagnac and the station at Matabiau (train, metro, local bus, coach) departing every 20 minutes, every day. The shuttle also serves the Pierre Baudis Convention Centre (Compans-Caffarelli stop), the centre of Toulouse and the Jean Jaurès metro station (lines A and B). This shuttle has its own specific fares, 8€ for one trip and 15€ for two trips.

Where to buy your ticket

- Automatic Ticket Dispenser found in every metro and tram station
- On board from the bus driver
- from a Tisséo Sales Points
- From certain approved retailers (Newsagents, tobacconists and bakeries) in the metropolitan area

Connections

The tickets allow you to travel on any metro, tram or bus (with the exception of the airport shuttle). In any journey you may change 3 times on 3 different lines within one hour from the first time your ticket is validated. **Attention**: making a return journey on the same line, or recommencing your journey on the same line, will be considered as 2 separate journeys.

Eating out in France: how much does it cost?

In 2015, average rates for a "Menu du jour" seem to be about 15 €. Average prices depend on local factors, including the competitive environment, and the neighbourhood. Many restaurants now offer an alternative and cheaper two-course option, "Entrée + plat" or "Plat + dessert" (starter and main course, or main course and dessert). In many restaurants, the Menu du jour is only available for lunch: in the evening, it is necessary to choose a more expensive menu or choose à la carte. Most respectable restaurants offer a menu of some sort in the region of 20 €. In gourmet restaurants, menus can be quite a bit more expensive.

Tipping:

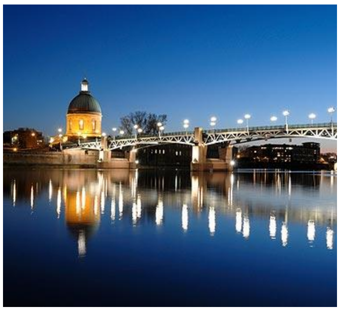
Tipping in restaurants in France is the norm - but there is no fixed rate. A normal tip in France will amount up to 10% of the bill, left discreetly on the table in coins or small notes. That is in addition to the "service compris" which nowadays is basically a service charge, not to a tip.

About Toulouse

Toulouse, a city with an exceptional heritage, has some wonderful surprises in store for you. Private mansions from the golden age of woad (a plant grown in the 16th century for its blue pigment), religious buildings with brick and stone decorations, rich collections in museums based in remarkable monuments and converted industrial sites: so many amazing places to see!

Let the pink city reveal all its history and charm as you travel among its streets and monuments. In the evening, the façades, the River Garonne and the city's monuments take on a new look with clever lighting**.**

Enjoying the gentle way of life in the Toulouse area of Southern France means taking the time to live. Wander the bustling streets for a spot of shopping, stroll around the markets, or take a break on a café terrace. The atmosphere here reveals the personality of people in the South: authentic and friendly. While Toulouse knows how to live, it also knows how to entertain guests, often around a table laden with local products to savour: foie gras, duck breast, cassoulet, Toulouse sausage, wine (Fronton, Gaillac, and Armagnac), cheese (Roquefort, Tomme des Pyrénées), violet treats and more.



Toulouse is an active, bustling city whose pronounced taste for celebration makes it similar to nearby Spain. Its enthusiastic personality finds expression at the rugby matches of the Stade Toulousain, and football games with the TFC “violets". Its cultural life gives free rein to creativity and emerging new trends at festivals such as Río Loco, Toulouse en piste and La Novela, as well as events such as the Violet Festival, carnival, the Toulouse Metropole Marathon, Toulouse plages beach festival and more. The cinemas, theatres, restaurants, casinos, bars and discos are also great places to continue your evening.

Since the end of the 19th century, Toulouse has witnessed many daring innovations: Clément Ader and his curious “aeroplane" machine, then the Aéropostale connections with his heroes such as Antoine de Saint-Exupéry. Today, the A380 sets the standard for research and innovation. Enthusiasts can visit the Airbus production lines. A visit to Toulouse is also an opportunity to learn about the sciences of the Universe through the new activities and exhibition spaces on offer at the Cité de l’espace theme park: the ArianeV rocket, Mir space station, IMAX, planetarium and more.

Toulouse is resolutely modern and cosmopolitan, yet also retains a human aspect and offers a pleasant combination of green and blue. It's easy to tour the city on foot, by bicycle or on a boat along the water. The canal du Midi, a UNESCO World Heritage Site, and the many parks and gardens offer plenty of natural areas that are ideal for relaxing, walking or playing sports. The River Garonne is the soul of the city: its waters run through the middle of the city and its banks are focal points for life in Toulouse.

Feeling adventurous? Want to get away from the urban environment for a while? As the gateway to the Midi-Pyrénées region, next to Languedoc-Roussillon, Toulouse's geographical location makes it the ideal starting point for discovering an area that's full of exceptional sites, listed among the “Most Beautiful Villages of France" or identified as “Great Sites of Midi-Pyrénées". Albi, Lourdes, Moissac, Rocamadour, Carcassonne… Let Toulouse show you the way to admire local treasures of architecture and nature, gems of Romanesque and medieval art, and great bastions of spirituality.

Tourism Information Toulouse:

Here are some websites that provide further information and suggestions for your stay in Toulouse:
http://www.toulouse-visit.com/
http://www.lonelyplanet.fr/destinations/europe/france/toulouse
http://about-france.com/
http://www.tripadvisor.com/Tourism-g187175-Toulouse_Haute_Garonne_Midi_Pyrenees-Vacations.html

Survive in France… ☺

1. S’il vous plaît (see-voo-play) - please
2. Je suis (zheu swee) – I am
3. Je cherche (zheu share-sh) – I’m looking for
4. Je veux (zheu veu) – I want
5. Un hôtel (ern otell) – A hotel
6. Une chambre (une shombre) - A room
7. Manger (mon-zhay) - To eat
8. Boire (bwar) – to drink
9. Payer (pay-yeh) – to pay
10. Acheter (ash-tay) – to buy
11. Petit-déjeuner (peuti – dayzheurnay) - Breakfast
12. Diner (dee-nay) - Dinner
13. Un demi (ern deu-mee) – A half pint of draught beer
14. Un verre (ern vair) - a glass
15. De l’eau (deu-lo) - some water
16. Un thé (au lait) (ern tay olay) - a tea (with milk)
17. La toilette (lar twa-lette) - the washroom, toilet.
18. Prix (pree) - price
19. Carte de crédit (kart deu cray-dee) - Credit card
20. Une banque (une bonk) – A bank
21. Des magasins (day magga-zan) - Shops
22. Un supermarché (ern supair-mar-shay) – A supermarket
23. La gare (lar gar) – The train station
24. L’aeroport (l’aero-por) – the airport

Where to eat in your free time

Here you can find some restaurant suggestions for Toulouse. These restaurants are in the top ranking of TripAdvisor for restaurants in Toulouse. See also: http://www.tripadvisor.com/Restaurants-g187175-Toulouse_Haute_Garonne_Midi_Pyrenees.html

- L´Ouverture Restaurant Musical
  - Italian
  - Price: 20€ - 25€
  - Website: http://www.l-ouverture.fr/
- Le Grenier de Pépé
  - European, Fondue
  - Price: 8€ - 20€
  - Website: http://www.legrenierdepepe.com/
- Miam Thai
  - Thai
  - Price: 7€ - 11€
  - Website: http://www.miamthai.com/
- Roulez Papilles
  - French
  - Price: 12€ - 30€
  - Website: http://www.roulezpapilles.fr/
- Le P’tit Louis
  - Asian, Korean
  - Website: www.leptitlouis.fr/
- Les Mecs au Camion
  - American
  - Website: http://lesmecsaucamion.com/
- Rajasthan Villa
  - Indina
  - Price: 12€ - 18€
  - Website: http://www.lerajasthanvilla.com/
- Le Point d’Ogre
  - French
  - Website: http://www.lepointdogre.com/
- Le Foxy
  - Spanish
  - Website: http://www.restaurant-foxy.fr/

Conference Office / Contact

If you need any support, please do not hesitate to contact us.

Yvonne Poul
ypoul@sba-research.org
Tel: +43 699 100 41 066

Bettina Bauer
bbauer@sba-research.org
Tel: +43 664 254 03 14

Notes

Notes

Preliminary Schedule ARES 2015
24 - 28 August 2015, Université Paul Sabatier, Toulouse, France

MONDAY, 24.08.

	LH A	LH B	LH C	LH D
08:00 - 17:00	Registration			
09:15 - 10:45	*ARES EU Symposium*			
		FCCT I	STAM I	AU2EU I
10:45 - 11:15	Break			
11:15 - 12:45	*ARES EU Symposium*			
		FCCT II	STAM II	AU2EU II
12:45 - 14:00	Lunch			
14:00 - 14:20	Opening			
14:20 - 15:50	ARES I - BEST PAPER SESSION *LH A*			
15:50 - 16:20	Break			
16:20 -17:50	ARES Full II	IWCC I	ARES EU Symposium - Poster Session & Get2Gether *Coffee Break Area*	
18:30 - 22:00	Mayor's Reception City Hall Toulouse *Meeting point: Place du Capitol*			

TUESDAY, 25.08.

	LH A	LH B	LH C
08:00 - 17:00	Registration		
09:00 - 09:45	*Invited Talk LH A* Afonso Ferreira, European Commission		
09:45 - 10:45	*Keynote LH A* Peter Eckersley, EFF		
10:45 - 11:15	Break		
11:15 - 12:45	ARES Full III	IWCC II	MFSec I
12:45 - 14:00	Lunch		
14:00 - 15:30	ARES Full IV	IWCC III	MFSec II
15:30 - 16:00	Break		
16:00 - 17:30	ARES Full V	IWCC IV	WCSF
18:30 - 20:00	Sightseeing Tour Toulouse *Meeting point: Place du Capitol*		

WEDNESDAY, 26.08.

	LH A	LH B	LH C	LH D	LH E
08:00 - 15:00	Registration				
09:00 - 10:00	*Keynote LH A* Pierangela Samarati, Università degli Studi di Milano				
10:00 - 10:15	Break				
10:15 - 11:45	ARES FULL VI	ARES Short I	ASSD I	WSDF I	IWSMA I
11:45 - 12:00	Break				
12:00 - 13:00	*Keynote LH A* Rainer Böhme, University of Innsbruck				
13:00 - 14:15	Lunch				
14:15 - 15:45	ARES Short II	ARES Short III	ASSD II	WSDF II	IWSMA II
16:00 - 23:30	Sigthseeing Tour Carcassonne Conference Dinner Château de Pennautier *Meeting point: University*				

THURSDAY, 27.08.

	LH B	LH C
08:30 - 11:00	Registration	
09:15 - 10:45	FARES I	SAW I
10:45 - 11:15	Break	
11:15 - 12:45	FARES II	SAW II
12:45 - 14:00	Lunch	
15:15 - 19:00	Airbus-Tour "Let's Visit Airbus" *Meeting point: Airbus site*	

FRIDAY, 28.08.

15:15 - 19:00	Airbus-Tour "Let's Visit Airbus" *Meeting point: Airbus site*

Plenary Sessions
ARES EU Symposium
ARES Sessions
Workshop Sessions
Social Event