ICIMP 2017

Forward

The Twelfth International Conference on Internet Monitoring and Protection (ICIMP 2017), held between June 25-29, 2017 in Venice, Italy, continued a series of special events targeting security, performance, vulnerabilities in Internet, as well as disaster prevention and recovery. Dedicated events focused on measurement, monitoring and lessons learnt in protecting the user.

The design, implementation and deployment of large distributed systems are subject to conflicting or missing requirements leading to visible and/or hidden vulnerabilities. Vulnerability specification patterns and vulnerability assessment tools are used for discovering, predicting and/or bypassing known vulnerabilities.

Vulnerability self-assessment software tools have been developed to capture and report critical vulnerabilities. Some of vulnerabilities are fixed via patches, other are simply reported, while others are self-fixed by the system itself. Despite the advances in the last years, protocol vulnerabilities, domain-specific vulnerabilities and detection of critical vulnerabilities rely on the art and experience of the operators; sometimes this is fruit of hazard discovery and difficult to be reproduced and repaired.

System diagnosis represent a series of pre-deployment or post-deployment activities to identify feature interactions, service interactions, behavior that is not captured by the specifications, or abnormal behavior with respect to system specification. As systems grow in complexity, the need for reliable testing and diagnosis grows accordingly. The design of complex systems has been facilitated by CAD/CAE tools. Unfortunately, test engineering tools have not kept pace with design tools, and test engineers are having difficulty developing reliable procedures to satisfy the test requirements of modern systems. Therefore, rather than maintaining a single candidate system diagnosis, or a small set of possible diagnoses, anticipative and proactive mechanisms have been developed and experimented. In dealing with system diagnosis data overload is a generic and tremendously difficult problem that has only grown. Cognitive system diagnosis methods have been proposed to cope with volume and complexity.

Attacks against private and public networks have had a significant spreading in the last years. With simple or sophisticated behavior, the attacks tend to damage user confidence, cause huge privacy violations and enormous economic losses.

The CYBER-FRAUD track focuses on specific aspects related to attacks and counterattacks, public information, privacy and safety on cyber-attacks information. It also targets secure mechanisms to record, retrieve, share, interpret, prevent and post-analyze of cyber-crime attacks.

Current practice for engineering carrier grade IP networks suggests n-redundancy schema. From the operational perspective, complications are involved with multiple n-box PoP. It is not guaranteed that this n-redundancy provides the desired 99.999% uptime. Two complementary solutions promote (i) high availability, which enables network-wide protection by providing fast recovery from faults that may occur in any part of the network, and (ii) non-stop routing. Theory on robustness stays behind the attempts for improving system reliability with regard to emergency services and containing the damage through disaster prevention, diagnosis and recovery.

Highly reliable emergency communications are required by public safety and disaster relief agencies to perform recovery operations or associated with disasters or serious network events. Future advanced network development and evolution should take into consideration these requirements through solutions: (a) Identification of suitable technologies, i.e., narrowband and broadband aspects, (b) Interoperability and interworking between emergency communications capabilities and public networks, (c) Preferential access to communications resources capabilities, applications, and facilities, (d) Preferential use of remaining operational resources.

The conference had the following tracks:

- Monitoring with Web technologies
- Internet traffic surveillance and interception

We take here the opportunity to warmly thank all the members of the ICIMP 2017 technical program committee, as well as all the reviewers. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors that dedicated much of their time and effort to contribute to ICIMP 2017. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

We also gratefully thank the members of the ICIMP 2017 organizing committee for their help in handling the logistics and for their work that made this professional meeting a success.

We hope that ICIMP 2017 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress in the field of Internet monitoring and protection. We also hope that Venice, Italy provided a pleasant environment during the conference and everyone saved some time to enjoy the unique charm of the city.

ICIMP 2017 Chairs

ICIMP Steering Committee
Sathiamoorthy Manoharan, University of Auckland, New Zealand
Terje Jensen, Telenor, Norway
Christian Callegari, University of Pisa, Italy

ICIMP Industry/Research Advisory Committee
Daisuke Mashima, Advanced Digital Sciences Center, Singapore
Bernhard Tellenbach, Zurich University of Applied Sciences, Switzerland
Miroslav Velev, Aries Design Automation, USA
Pethuru Raj, IBM Global Cloud Center of Excellence, India