1 Introduction

The 3rd Workshop on Recent Advances in Intrusion-Tolerant Systems, held in conjunction with DSN 2009, aims to provide the researchers and practitioners an intimate venue to discuss and collaborate on ground-breaking new ideas and fresh results.

Intrusion tolerance (IT) starts with the premise that bugs and misconfigurations are inevitable in software based systems. Moreover, the distributed and networked computer systems of today enable the discovery, exposition and exploitation of these flaws in increasingly new and easier ways. IT acknowledges that it is impossible to completely prevent intrusions and attacks, and it is often impossible to accurately detect the act of intrusion and stop it early enough. Intrusion-tolerant systems therefore must have the means to continue to operate correctly despite attacks and intrusions, and deny the attacker/intruder the success they seek as much as possible. For instance, an intrusion-tolerant system may suffer loss of service or resources due to the attack but it may continue to provide critical services in a degraded mode or trigger automatic mechanisms to regain and recover the compromised services and resources. Other descriptions used for similar themed or related research include Survivability, Trustworthy Systems, Byzantine Fault Tolerance, and Autonomic Self-Healing Systems.

The idea of tolerating intrusions gained prominence during the 1990s, especially after a number of thorough evaluations of intrusion detection systems revealed significant problems of false positives and false negatives. Around 2000 major research efforts were launched in the United States as well as in Europe. These and other affiliated and follow on projects led to the development of several intrusion-tolerant algorithms and architectures. It is now possible to start to grasp the fundamental principles of building practical intrusion-tolerant systems, the issues underlying the validation and acceptance/certification of intrusion-tolerant systems, and also the continued effective and intelligent management, maintenance and operation of such systems once they are put in operation.

Despite significant progress, the vision that most current systems will be built as intrusion-tolerant systems has not become a reality. There are a number of reasons for this ranging from a false sense of security, lack of understanding of the risk, absence of any major cyber-disaster that is publicly acknowledged, the perception that intrusion tolerance is expensive etc.

On the other hand, intrusion tolerance is a moving target that has not been completely achieved yet. Unlike fault tolerance, intrusion tolerance faces an intelligent adversary who can also adapt and evolve as the system adapts and recovers. New technologies make older solutions obsolete and introduce new vulnerabilities.

How to make intrusion tolerance an integral part of the psyche of the system developers and architects? How to continue to stay ahead of the increasingly sophisticated adversaries? How to enlighten and empower the practitioners to navigate the ever-changing technology landscape so that they can build systems that can be trusted, that can operate through attacks?

2 This Year’s Workshop

The goal of this year’s workshop is to understand, disseminate, cross-pollinate and collaborate on the challenges of building intrusion-tolerant systems and innovative ideas to address them. As a technical area, IT is at the intersection of Fault Tolerance and Security. As a practical discipline, it brings in additional topics ranging from software engineering, adaptive system development to reasoning, coordination and control of distributed resources and mechanisms, as well as validation and evaluation of security and survivability claims.

This year workshop includes a selection of 6 high quality
papers that provide a rich combination of perspectives about intrusion tolerance.

In the first paper, “What next in intrusion tolerance”, P. Pal, R. Schantz, J. Loyall, M. Atighetchi and F. Webber from BBN Technologies look into the near future and analyze the challenges that new technologies like SOA, cloud computing and the semantic web pose to intrusion tolerance. The paper opens interesting new directions for research in the area.

Q. Nguyen and A. Sood from the George Mason University in their article “Quantitative Approach to Tuning of a Time-Based Intrusion-Tolerant System Architecture” address the important issue of time-based intrusion tolerance by analyzing quantitatively how their Self Cleansing Intrusion Tolerance architecture (SCIT) can be tuned to attain a certain level of resilience.

In their paper “Network Intrusion Detection with Minimal Communication Overhead”, O. Kreidl and A. Willsky from the MIT provide a probabilistic model of network intrusion detection with limited communication between local detectors. This model allows making an accurate estimate of the threshold used at a node to determine if an attack is in progress.

D. Mónica, J. Leitão, L. Rodrigues and C. Ribeiro from INESC-ID/IST in their article “On the Use of Radio Resource Tests in Wireless ad hoc Networks” deal with a particularly pernicious form of intrusions in wireless environments, falsification of identities or “Sybil attacks”. The paper defines a framework to assess the power and performance of radio resource tests (RRTs) and uses the framework to compare a set of RRTs.

In “Enhancing Fault / Intrusion Tolerance through Design and Configuration Diversity”, a team of researchers from several institutions, A. Bessani, A. Daidone, I. Gashi, R. Obelheiro, P. Sousa and V. Stankovic, report results of project FOREVER about the use of diversity to obtain intrusion tolerance. The paper presents a set of mechanisms that allows creating diversity and evaluates the benefits obtained.

The last paper, “Practical Techniques for Regeneration and Immunization of COTS Applications”, by L. Li, R. Sekar, M. Cornwell, E. Hultman and J. Just from Global InfoTek and Stony Brook University presents RAMSES, a novel system for making software applications immune to a large number of current attacks. The idea is to instrument the software with lightweight code that checks if input reaches resources when that was not expected by the programmer.

We expect the discussion around these papers to identify the open problems and fundamental issues in IT that still need research and bring forward innovative ideas to address them, as well as to broaden our understanding of the issues that prevent IT technologies to become widely adopted in operational and deployed systems (including identification of the domains that stand to benefit most, evaluating IT systems for deployment, cost effective management and maintenance of operational IT system etc.)

3 Acknowledgments

We are very grateful to the members of the Program Committee for their work with reviewing the papers, helping us to assemble a very good program. It was a pleasure to collaborate with such a remarkable set of specialists. We are also thankful to all the authors who submitted papers for this edition of the workshop and to the DSN organization.

The program committee consisted of the following researchers: Aditya Bagchi (ISI, India), Manuel Costa (Microsoft Research, UK), Jay Lala (Raytheon, USA), Peng Liu (PSU, USA), O. Patrick Kreidl (MIT, USA), Dipanwita Roychowdhury (IIT Kharagpur, India), William H. Sanders (UIUC, USA), Paulo Verissimo (U. Lisbon, Portugal).