1 Introduction

Design and operational vulnerabilities are accepted as inevitable in today’s complex computer systems. The distributed and networked nature of the systems that are currently in use and being developed facilitate discovery and exploitation of these flaws in increasingly new and easier ways. Intrusion Tolerance acknowledges that it is impossible to completely prevent attacks and intrusions, and that it is often impossible to accurately detect the act of intrusion and stop it early enough. Intrusion Tolerance research therefore aims to develop technologies that enable computer systems to continue to operate correctly despite attacks, and deny the attacker/intruder the success they seek. For instance, an intrusion-tolerant system may suffer partial loss of service or resources due to the attack, but it will continue to provide critical services in a degraded mode or trigger automatic mechanisms to regain and recover the compromised services and resources. Similar goals are being pursued in Survivability, Byzantine Fault Tolerance, Self-regenerative and Autonomic Systems.

The idea of tolerating intrusions gained prominence during the late 1990s and early 2000s. Major research efforts led to the development of several intrusion-tolerant algorithms and architectures. It is now possible 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 and operation of such systems once they are in operation.

Despite significant progress, most modern systems are still not built as intrusion-tolerant systems. There are a number of reasons for this ranging from a false sense of security, such as lack of understanding of the risk, absence of any major cyber-disaster that is publicly acknowledged, the continued and fast paced innovation in information and software construction technologies, and the perception that Intrusion Tolerance is expensive.

Combined with changing technology landscape, Intrusion Tolerance is a moving target that also needs to accommodate and adapt to changes. Unlike fault tolerance, Intrusion Tolerance faces an intelligent adversary who can 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 software engineering of modern information systems? What can be done to make system developers and architects more comfortable and confident about Intrusion Tolerance technologies? 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, and can operate through attacks?

The 4th Workshop on Recent Advances in Intrusion-Tolerant Systems, held in conjunction with DSN 2010, aims to provide the researchers and practitioners an intimate venue to discuss and collaborate on ground-breaking new ideas and fresh results on such issues.

2 This Year’s Workshop

The goal of the WRAITS 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, Intrusion Tolerance 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.

One common theme underlying the papers accepted in this year’s workshop is gaining confidence in Intrusion Tolerance technologies and solutions. We start with a keynote speech by Robert L. Constable, from Cornell University. Bob’s talk, entitled “Using Formal Methods to Build Systems that Survive Attacks”, is about recent work on systems that survive attacks and intrusions by dynamically substituting protocols by others that are more resilient. The alternative protocols are picked from libraries of protocol variants.
that are formally synthesized and correct-by-construction. The correct by construction approach to Intrusion Tolerant system development has the potential to raise the confidence level of system owners and architects.

The keynote is followed by 9 papers, divided in 3 sessions, that represent a rich collection of ideas in the Intrusion Tolerance research space.

The first session is about “Detection and Analysis” of vulnerabilities and intrusions. In the first paper, “Analysis of the Effect of Java Software Faults on Security Vulnerabilities and Their Detection by Commercial Web Vulnerability Scanner Tool”, Tania Basso, Plinio Fernandes, Mario Jino and Regina Moraes from UNICAMP, Brazil, report experiments with software faults injection in Java web applications, to assess the ability of web vulnerability scanners do detect the vulnerabilities introduced. They discovered that these scanners fail to find many vulnerabilities.

O. Patrick Kreidl from the MIT, USA, in “Analysis of a Markov Decision Process Model for Intrusion Tolerance”, uses Markov decision processes to model systems that execute defensive responses during an attack that involves several steps. The analysis shows that employing defensive responses while under attack is sub-optimal, i.e., can have a higher overhead than the risk involved.

In a position paper entitled “On Rootkit and Malware Detection in Smartphones”, Bryan Dixon and Shivank Mishra from the University of Colorado, USA, discuss recent research on detection and mitigation of the propagation of malicious code in smartphones. They also present a strategy and a preliminary prototype to detect the presence of rootkits and other malware in these devices.

The second session is dedicated to “Systems and Architecture”. The first paper, “SCIT and IDS Architectures for Reduced Data Ex-filtration” by Ajay Nagarajan and Arun Sood from George Mason University, USA, combines the Self-Cleansing Intrusion Tolerance (SCIT) approach with intrusion detections systems. These architectures are evaluated using decision trees and simulations.

“RAVE: Replicated AntiVirus Engine” by Carlos Silva, Paulo Sousa and Paulo Verissimo from the University of Lisboa, Portugal, presents the design and implementation of a replicated antivirus system for email servers. The system uses several antivirus applications running in parallel to increase the overall detection capability, while tolerating intrusions in a subset of the replicas.

In the third paper of this session, “Realizing S-Reliability for Services via Recovery-driven Intrusion Tolerance Mechanism”, Quyen Nguyen and Arun Sood from George Mason University, USA, propose the notion of Intrusion Tolerance QoS (IT-QoS) and a new quality metric that measures reliability in the presence of attacks, S-Reliability. The paper is specially concerned with Web Services and the Service-Oriented Architecture (SOA).

The third and last session is about “Evaluation, Assessment and Governance”. In the first paper, “Assessing the Attack Resilience Capabilities of a Fortified Primary Backup System”, Dylan Clarke and Paul Ezhilchelvan from the Newcastle University, UK, present an approach for making primary-backup replication intrusion-tolerant. The paper presents a comparison of the resulting solution with the state machine approach using simulations.

The session’s second paper is “A Security Evaluation of a Novel Resilient Web Serving Architecture: Lessons Learned through Industry/Academia Collaboration”, by Yih Huang, Anup Ghosh, Tom Bracewell and Brian Mastropietro, from George Mason University and Raytheon Company, USA. The paper starts by reporting penetration tests done against an intrusion-tolerant web-serving system. Then, it presents enhancements to the original architecture that address the vulnerabilities that were found.

The session and the workshop finish with an interesting position paper entitled “Survivability and Information Assurance in the Cloud”, by Melvin Greer, Lockheed Martin, USA. The paper presents the security risks that are faced by cloud computing and does recommendations that should guide organizations that aim to use this technology.

We expect the discussion around these papers to identify open problems and fundamental issues in Intrusion Tolerance that still need research and bring forward innovative ideas to address them. We expect to broaden our understanding of the issues that prevent Intrusion Tolerance technologies to become widely adopted in operational and deployed systems including identification of the domains that stand to benefit most, assessment and formal approaches to develop intrusion tolerant building block components and protocols, and government initiatives.

3 Acknowledgments

We are very grateful to the members of the Program Committee for their work with reviewing and selecting the papers, helping us to assemble a very good program. It was once more 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 workshop was partially supported by the FCT through the Multi-annual Programme.

The program committee was the following: Saurabh Bagchi (Purdue U., USA), Byung-Gon Chun (Intel Labs Berkeley, USA), Manuel Costa (Microsoft Research, UK), Flavio Junqueira (Yahoo! Research, Spain), Rama Kotla (Microsoft Research, USA), Patrick Kreidl (MIT, USA), Peng Liu (Penn State U., USA), Jean-Phillipe Martin (Microsoft Research, UK), Nuno Neves (U. Lisboa, Portugal), Rodrigo Rodrigues (MPI-SWS, Germany), William H. Sanders (U. Illinois UC, USA), Arun Sood (George Mason U., USA) and Paulo Verissimo (U. Lisboa, Portugal).