Abstract

A system that can continue critical operations, perhaps in a degraded mode, in the face of a partially successful cyber attack can be termed “intrusion tolerant.” The workshop will provide a forum for the presentation and discussion of current efforts to develop subsystems and systems that display some degree of intrusion tolerance. The workshop will also provide the opportunity for demonstrations of some experimental prototype intrusion tolerant systems. The goal of the workshop is to have a critical and productive discussion of the state of current research and development efforts in the area of intrusion tolerant systems and to identify promising directions for future research in the area.

Workshop Organization

The Workshop co-chairs selected a program committee and solicited contributions for the workshop. Submitted papers were reviewed by the Co-Chairs and the Program Committee, and authors were given the opportunity to publish their contributions in the Supplementary Proceedings volume. After considering the range of contributions and the nascent state of the field of intrusion tolerant systems, the Co-Chairs, in consultation with the Program Committee, decided to try a novel approach for the workshop. The structure calls for a set of technology presenters, a red team panel, and an evaluation/R&D panel. The day will be divided into three sessions, one focusing on each panel.

Session 1: ITS Technology Presentations

The developers of at least three, and no more than six, intrusion tolerant systems or technologies will present:

- Technology description: scope, components, interconnections, operational characteristics
- Assumptions: what parts of the problem is the project depending on others to solve?
- Planned reactions to attacks: How are the tolerance mechanisms expected to behave in normal operation and in the face of attacks?
- What level of degradation is expected in response to particular attacks?
- Results, if any, of experiments, prototypes

Each presenter will be provided an equal period of uninterrupted presentation time, followed by a short period during which the red team panelists will be allowed to ask specific questions about the technology. During the break following this session, the Red Team panel may convene to coordinate its session.

Session 2: Red Team Session

This session is expected to mirror the morning session: each architecture will be reviewed by the red team in turn. The red team, which will be drawn from the program committee and other experts will briefly address:

- Realism of the assumptions,
- Weaknesses in the structures presented,
- Attacks that could defeat the system’s goals, and
- other topics as appropriate.

Following each presentation by the red team, the technology presenter will have an opportunity to respond, and there will be a brief period for discussion by the workshop participants.

Session 3: Evaluation/R&D Planning Session

During the preceding sessions, the members of the evaluation panel will have been noting both the technology descriptions and the red team’s comments. In this session, the evaluation panel will comment on the earlier discussions and propose potentially fruitful
avenues of research. Again, contributions from all workshop participants will be welcome.

**Demonstrations**

Facilities will be provided to permit workshop participants to demonstrate prototype intrusion tolerant system technologies. However, because of the intensive nature of the program, the time available for demonstrations will be limited to the period preceding the workshop start, during the lunch and inter-session breaks, and following the workshop.

**Systems to be presented**

As of the deadline for this proceedings, three presenters have agreed to participate by presenting their technologies:

- Paul Ezhilchelvan of the University of Newcastle-Upon-Tyne will present his middleware architecture for intrusion tolerant and fault tolerant service replication,
- Peng Liu of University of Maryland Baltimore County will present his architecture for an adaptive intrusion tolerant database system, and
- James Just of Teknowledge will present the technology under development in the HACQIT (Hierarchical Adaptive Control for QoS Intrusion Tolerance) project.

Other technologies may be added prior to the opening of the workshop.

**Program Committee**

The workshop Program Committee includes:

Lee Badger, NAI Labs
Sekar Chandersekaran, Institute for Defense Analyses
Marc Dacier, IBM-Zurich
Walt Heimerdinger, Honeywell Technology Center
Gary McGraw, Cigital
Michael Reiter, Carnegie Mellon University
Fred Schneider, Cornell University
Wietse Venema, IBM-Watson