Security and Survivability in Unbounded Networked Systems

Axel Krings[*]
Computer Science Dept.
University of Idaho, USA
krings@cs.uidaho.edu

Paul Oman
Computer Science Dept.
University of Idaho, USA
oman@cs.uidaho.edu

Azad Azadmanesh
Computer Science Dept.
Univ. of Nebraska - Omaha, USA
azad@unomaha.edu

Concerns about the security and survivability of computers and computer networks have been in the public eye more than ever. We have gotten used to the thought that many applications relying on computers and networks may be exposed to adverse conditions of different origin. Yet, there are no signs of slow-down in embracing networked computer systems to control many aspects of our daily lives.

For the average computer user security and survivability concerns are often equated with applying certain maintenance operations, e.g., frequent operating system updating, subscription to filtering software like virus checkers and spam filters, as well as a general adoption of a firewall mentality. However, despite our efforts to protect ourselves, counting on recovery mechanisms such as virus isolation or cleanup, we are seeing the limited success of adapting solutions that have local scope. We are bombarded with spam, emails attempting to tricking us to reveal information about security settings of bank or auction accounts, or luring us with fraudulent investments. It is the apparent inability to control such activities that lead us to the realization that local control alone cannot be the solution for problems originating elsewhere.

Security and survivability of unbounded systems address the aforementioned limitations. Such systems are characterized by the lack of a global administrative view of the systems. Nowadays most large systems are unbounded in nature. For example, the Internet is a highly unbounded system built on networks at different levels of management, with few global aspects other than addressability. Other unbounded systems include the control networks of our critical infrastructures such as electric, water and gas. At the extreme end of the spectrum one finds applications utilizing voluntary computing, e.g., the SETI@home, which constitute a collection of locally administered computers which volunteer their resources to the usually highly distributed application.

Unbounded systems and networks require methods and mechanisms that provide security and survivability despite the possibility that parts of the system might be untrustworthy, unreliable or perhaps malicious. This is a basic shift away from an egocentric view of a system, relying mainly on local mechanisms and policies. Whereas unbounded systems seem to be intimidating and threatening in one sense, they often include the notion of highly distributed and robust systems. This, of course, is under the assumption that unbounded systems do not only imply the lack of a global administrative view of the system, but a decentralized nature of the control itself. Recent natural disasters, e.g., hurricanes Katrina and Rita, actually exposed the positive aspects of unbounded systems where damage was relatively confined to the areas devastated without significant disturbances in non-affected regions.

This minitrack addresses issues of security and survivability in large, non-trivial, unbounded networked computer systems, with an emphasis on recovery and adaptation. It considers systems and networks, including dynamic paradigms. The session is organized as a research forum to further the dialogue between researchers from the areas of system survivability, software dependability, computer and network security, fault-tolerance and intrusion tolerance, and economic or statistical modeling of secure/survivable systems.

We are very pleased with the reviewers recommendations on the four papers included in this minitrack. Each paper tackles a different aspect of security and survivability of unbounded networks; together they provide a collective work exploring the issues of this difficult and important topic. The paper by H. Li and Singhai proposes an on-demand secure routing protocol using distributed authentication in ad hoc wireless networks. The research by Galla, Hummel and Peer describes how mobile agents can be used to inject software faults in distributed real-time systems as a mechanism to test the fault tolerance of those embedded systems.

The other two papers focus on modeling. The paper by W. Li and Vaughn shows how graphs are used to model exploitations (i.e., attacks) in computer networks. The paper by McQueen et al., walks through a method for estimating risk in a Supervisory Control and Data Acquisition (SCADA) system.

The security and survivability of unbounded networks is a vast and difficult issue. The papers included in this minitrack reflect the diversity and complexity, while providing positive guidance as to how it can be modeled and managed. We hope you enjoy reading the papers and attending the presentations.

[*] The author was supported in part by the French *Region Rhône-Alpes* Ragtime project.