ARTES++ Travel Report to PRDC 2007

The 13th IEEE Pacific Rim International Symposium on
Dependable Computing (PRDC'07)
7-19 December, 2007, Melbourne, Australia.

Carl Bergenhem
January 7th, 2008

1 PRDC

PRDC 2007 is the thirteenth in this series of symposia started in 1989 that are devoted to dependable and fault tolerant computing. PRDC is now recognized as the main regular event of the Pacific area that is covering the many dimensions of dependability and fault tolerance, encompassing fundamental theoretical approaches, practical experimental projects, and commercial components and systems. As applications of computing systems have permeated in every aspects of daily life, the dependability of computing system has become increasingly critical. This symposium provides a forum for countries around the Pacific Rim and other areas of the world to exchange ideas for improving the dependability of computing systems. This years conference accepted around 30 full papers out of 100 submissions.

The symposium is returning to Melbourne in 2007 and will be held in one of the centrally located inner city hotels. Melbourne is a vibrant cosmopolitan city that has frequently been awarded one of the world's most "liveable" cities. Melbourne offers an excellent location for this Symposium with numerous local arts, cultural, architectural and sporting attractions. It also provides an excellent hub for many of the tourist attractions throughout Victoria and Australia.

Melbourne Central Business District,
close to the Yarra River

2 Thoughts

My presentation was alright and I received questions afterwards and valuable comments. As observed before, research into the membership problem differs depending on whether a synchronous or asynchronous system is targeted. The problems associated with each, target application and uses are largely different.

Several interesting keynote speeches were also held. Among others Paulo Verissimo held a keynote titled: “Computers meet the real world - Challenge of architecting dependable and secure CII (Critical Information Infrastructure)”. Critical infrastructure is for example gas fired furnace water works, electricity generation. All of these types of utilities are commonly geographically distributed and sites are interconnected via both internal corporate networks but also the Internet. Because of the distributed nature and not least that communication over the Internet is used, there are a number of threats.

There are several real examples of incidents.
*2003: Ohio, USA. Slammer worm causes shut-down of monitoring system of nuclear plant. The plant firewall prevented worm, but it penetrated the supplier network and then plant through backdoor network. Worm propagated to SCADA network, then overload control-network. Could have caused a serious incident.
*2002: Australia. An angry ex-employee at a sewage management plant remotely caused a control system disruption which lead to raw sewage being disposed into nearby river. This was possible despite hardwired logic - safety interlocks in the control system.

The road to CII security is taking a new approach. Securing individual component is not solution. It must be possible to build secure systems of out of insecure embedded components. No system can be completely free from intrusions, rather it must be made to be Intrusion tolerance – i.e. enough resources to meet the safety goal, despite attacks. Replicas of infrastructure components, e.g. distributed voting firewalls will be attacked but must also have recovery mechanism.
More information on this can be found in the EU FP6 project CRUTIAL.

The visit to the conference; to participate and contribute with a presentation of my paper was a success. It is inspiring to talk to other people and get new influences and ideas for new approaches to the research at hand. Many thanks to ARTES for giving the grant for the trip!