Report on the 4th CaberNet Plenary Workshop

Introduction

The 4th CaberNet Plenary Workshop was held in the Area della Ricerca CNR di Pisa, Pisa, Italy, 9 – 12 October 2001. The Workshop was open to all member nodes of CaberNet and comprised presentations and reports back from the various CaberNet committees.

The technical presentations were aimed at describing recent research activity by CaberNet members, in the area of distributed and dependable systems. Presentations were selected by the Research Coordination and Training Committee, that reviewed the extended abstracts submitted by member nodes. Among the 35 submissions that were received, 29 were selected for contribution and inclusion in the workshop proceedings, according to their contribution to the state of the art and their being representative of ongoing work at CaberNet nodes.

The topics addressed were quite broad, including work on recent research areas such as peer-to-peer computing. Specifically, contributions were organized around the following research themes:

- Security
- Dependability evaluation
- Middleware support for dependability
- Distributed systems
- Peer-to-peer computing
- Mobile computing
- Real-time computing
- Network aspects

Research issues that were addressed during the workshop are summarized in the following sections, while further detail is provided in Appendix A, which gives the workshop programme and extended abstracts that were presented at the workshop (also available at http://www.newcastle.research.ec.org/cabernet/workshops/4th-plenary.htm).

Security

Contributions in the security area related to the verification of security protocols and the design of an authorization scheme for the Internet:

- Specifying, Verifying and Cracking Security Protocols, Logically by the University of Twente and CWI introduces a logic-based specification method that allows reasoning over cryptographic protocols and for implementing efficient and effective state-based verification. Practicality of the approach has further been demonstrated through the development of a supporting tool that allows the user to: (i) specify formally a cryptographic protocol in terms of simple Prolog rules, (ii) define the goals of a protocol and verify whether they are reachable, and (iii) define the goals of a potential intruder, and therefore check the protocol for flaws by verifying whether they are reachable.

- An Internet Authorization Scheme using Smart Card-Based Security Kernels by LAAS-CNRS presents authorization schemes that are being developed towards the Internet. The proposed schemes can grant fair rights to each participant involved in Internet-based transactions, while distributing to each one only the information strictly needed to execute its own task. These schemes are based on two levels of protection: (i) an authorization
server that is in charge of granting and denying rights for high-level operations involving several participants, and (ii) a security kernel on each participating host that is responsible for fine-grain authorization, which is partly implemented on a Java card.

**Dependability evaluation**

Contributions in the domain of dependability evaluation addressed formal methods towards supporting the analysis and validation of systems from the standpoint of dependability:

- **Formal Specification and Verification of Dependable Systems** that is a joint work among the University of Pisa, the University of Firenze, CNR Pisa, and CNUCE/CNR Pisa proposes a survey of the application of formal methods based on model checking towards verifying dependable systems, including its use in the context of system modeling using UML.

- **Bounding Regenerative Randomization** by the Universidad Politecnica Catalunya addresses the issue of quantifying dependability measures for repairable fault-tolerant systems. More precisely, this work describes an approach called “Bounding regenerative randomization” to speed up the processing of Continuous Timed Markov Chains featuring specific properties, nevertheless actually found in practical situations.

- **Performance Analysis of Fault-Tolerant Transactional Systems** by the University of Pisa addresses exact mathematical analysis of a transaction processing system subject to faults, where dependability is maintained by means of checkpointing and rollbacks. The work focuses more specifically on the evaluation of the optimal frequency of checkpoints.

- **Design Diversity and Failure Correlation: Recent Results and New Developments** by City University addresses the advantages and disadvantages of using diversity as a means for decreasing failure correlation between redundant components of a fault-tolerant system, out of work on reliability modeling that has been carried out at City University.

**Middleware support for dependability**

Contributions in the area of middleware support for dependability covered support for fault-tolerance regarding both base protocols and replication management:

- **Fault-Tolerant Real-Time Videocommunication via Best-Effort Networks** by the University of Hamburg discusses fault-tolerance strategies for video transmission over networks with impaired QoS. Different fault-tolerance techniques for compressed video streams are presented. In the first technique, the receiver asks the sender for a complete picture frame if video quality gets too low using the received delta frames. In the second class of techniques, receivers mask data losses.

- **Chasing the FLP Impossibility Result in a LAN or How Robust Can a Fault Tolerant Server Be?** by EPFL describes an experiment aimed at assessing the robustness of an atomic broadcast protocol for asynchronous systems, in the face of the FLP impossibility result.

- **Is Reliable Multicast too Expensive? Let's be Optimistic** by the Technical University of Madrid and ETH Zurich makes the case for the use of optimistic delivery to improve the performance of replicated data management systems.

- **Intrusion Tolerant Transactional Support** by the University of Newcastle presents a CORBA-like transaction service that copes with intrusion. As a result, the service implements active replication and its composing managers are replicated.

- **Enhancing Availability of Cooperative Applications through Interoperable Middleware** by the University of La Sapienza di Roma describes some FT-Corba based middleware for building fault-tolerance systems of information systems for the Italian public administration.
Fault Tolerant Platform for Parallel Applications using MPI by Critical Software SA describes planned work to extend the MPI (Message Passing Interface) standard with fault-tolerance mechanisms. Fault tolerance will be realized by a process-state checkpointing system. Process states will be distributed to the process environment to be available if a recovery of a process, node, or cluster should become necessary.

**Distributed systems**

Contributions in the area of distributed system related to system support towards supporting various classes of applications, and in particular Internet-based systems. Note further that most of the contributions to the workshop were actually related to the distributed system domain, addressing specific sub-topics as outlined in this report.

- **Representing and Enforcing Electronic Commerce Contracts over a Wide Range of Platforms using Occurrence Stores** by the University of Cambridge describes an approach called "occurrence stores" for constructing ontologies of electronic commerce policies, including concepts such as obligations and prohibitions.
- **Assessing the Performance Advantage of Mobile Agents in Distributed Searching** by the University of Kaiserslautern discusses one application for assessing the benefit of using mobile agents. The application is based on search in Usenet and the benefit of mobile agents in this specific context is assessed in terms of performance evaluation from the standpoint of execution time and workload.
- **A High Performance Wireless Fieldbus in Industrial Multimedia-Related Environment** by the Polytechnic Institute of Porto describes the RFieldbus project. The goals of this project are to extend fieldbusses so that they support multimedia traffic and wireless mobile communication. Some of the essential challenges for achieving these goals are discussed.
- **BabalonLite: Improvements to Java-Based Distributed Object Systems** by the University of Cambridge presents work about the Babylon system that supports the development of distributed Java applications. It focuses more specifically on the latest version of Babylon, called BabalonLite, which improves previous versions from the standpoint of performance.
- **Improving WRC for GC+mobility: Another small step towards managing references in distributed systems** by the University of Glasgow discusses ongoing work at the University of Glasgow in the area of distributed systems, which relates to addressing the following issues: scalability, heterogeneity, dependability.
- **Policy Based Management of Large Distributed Systems** by BTexact Technologies deals with the management of distributed systems at the Internet scale, raising the issue of supporting decentralized control and enabling information exchange among systems. The proposed solution consists in the definition of policies based on ECA rules, where common information representation relies on XML schemas.

**Peer-to-peer computing**

Contribution in the area of P2P systems addressed the development of various types of applications over P2P infrastructures, as they should not be considered as being restricted to supporting file sharing. In addition, work on supporting the evaluation of P2P architectures through simulation was introduced:

- **Peer-to-peer Computing: More than Sharing Files?** by Microsoft Research discusses how a peer-to-peer middleware can be used for a number of very different applications.
- **Anthill: A Framework for Designing Peer-to-Peer Systems** by the University of Bologna and the Norwegian University of Science and Technology presents a framework for the development of P2P applications, based on Multi-Agent Systems (MAS). The objective of
the work is to ease experimentation/evaluation of new techniques for the P2P application domains.

- **Adaptable Network Architectures** by the University of Cambridge introduces a general simulator for evaluating different P2P architectures.

**Mobile computing**

Contribution in the area of mobile computing covered a number of related issues, such as content adaptation to devices, and supporting wireless network and middleware:

- **Context-Based Specifications for Data Mediation to Support Mobile Systems** by Imperial College proposes a specification technique enabling to adapt data access to the device.
- **Towards a Network File System for Roaming Users** by INRIA motivates the need for building a file system for roaming users. The work concentrates more specifically on the exploitation of ad hoc WLANs so as to not rely on any infrastructure for accessing shared files.
- **New Mechanisms for Routing in Ad Hoc Networks through World Models** by the University of Stuttgart addresses routing in constantly changing MANET, exploiting in particular environment models.
- **A Framework for Dynamic Adaptation in Wireless Environments** by INRIA describes a framework for developing software for wireless environments. The mechanisms embedded in the framework support the detection of events in the environment, notification of interested components, and reaction to events.

**Real-time computing**

Contribution in the area of real-time computing was more specifically focused on the development of hard real-time systems, and in particular associated development and analysis support:

- **Java for Real-Time Systems** by the Technical University of Wien discusses the use of Java for the development of RT Systems (in the sense of hard RT). It is based on a profile (adaptation) of the RTSJ standard for meeting requirements associated with hard RT systems. The work further addresses support for WCET analysis that is done in two phases, the first being hardware independent and the second used the result of the first to generate hardware-specific results.
- **Re-targetable Framework for Worst-Case Execution Time Analysis** by the University of York describes a framework for WCET analysis that is not platform-specific, but can be used for different platforms. The hardware architecture and characteristics are described in a special-purpose platform-description language.

**Network aspects**

Contributions in the networking domain related to support for the analysis of the network behavior:

- **Observing Web Browser Behaviour using the Nprobe Passive Monitoring Architecture** by the University of Cambridge discusses a mechanism to analyse traffic by using information from different network layers. Application of the mechanism is also addressed in the context of observing Web browser behaviour.
- **Generating Interactive Protocol Simulations and Visualizations for Learning Environments** by the University of Stuttgart addresses automatic building of a simulation and visualization environment for a protocol, based on a formal specification.
Appendix A – Workshop proceedings

A1. Workshop Programme

Day 1: Tuesday, 9 October 2001
10.00 - 12.30 Information Services Committee
13.00 -14.00 Lunch
14.00 -19.00 Executive Board Meeting
19.30 Registration and welcome reception for workshop participants

Day 2: Wednesday, 10 October 2001
08.30 Registration (continued)
09.00 - 09.30 Welcome/Introduction (Dick Snow)
09.30 -10.30 Security
(Chair: Ian Pratt)
• Specifying, Verifying and Cracking Security Protocols, Logically (G. Delzanno - U. Genova, S. Etalle - U. Twente and CWI)
• An Internet Authorization Scheme using Smart Card-Based Security Kernels (N. Abghour, Y. Deswartes, V. Nicommete, D. Powell - LAAS-CNRS)
10.30-11.00 Break
11.00-12:30 Middleware Support for Dependability (I)
(Chair: Paulo Verissimo)
• Fault-Tolerant Real-Time Videocommunication via Best-Effort Networks (K. Heidtmann - U. Hamburg)
• Chasing the FLP Impossibility Result in a LAN or How Robust Can a Fault Tolerant Server Be? (P. Urban, X. Defago, A. Schiper - EPFL)
• Intrusion Tolerant Transactional Support (I. Welch, R. Stroud, B. Randell, J. Armstrong - U. Newcastle)
12.30-14.00 Lunch
14.00-15.30 P2P Computing
(Chair: Valerie Issarny)
• Peer-to-peer Computing: More than Sharing Files? (A. Rowstron - Microsoft Research)
• Adaptable Network Architectures (M. Palomino - U. Cambridge)
15.30-16.00 Break
16:00-18:00 Dependability Validation
(Chair: David Powell)
• Bounding Regenerative Randomization (J. Carrasco - U. Politecnica Catalunya)
• Performance Analysis of Fault-Tolerant Transactional System (M. Misra, L. Kumar, I. Mitrani - U. Pisa)
• Design Diversity and Failure Correlation: Recent Results and New Developments (Strigini - City U.)
Day 3: Thursday, 11 October 2001

09.00-09.30  CaberNet news
09:30-10:30  **Network monitoring**  
(Chair: Juergen Nehmer)

- Observing Web Browser Behaviour using the Nprobe Passive Monitoring Architecture  
  (J. Hall, I. Pratt, I. Leslie - U. Cambridge)
- Generating Interactive Protocol Simulations and Visualizations for Learning Environments  
  (S. Papakosta, C. Burger - U. Stuttgart)

10:30-11:00  Break
11:00-12:30  **Middleware Support for Dependability (II)**  
(Chair: Pieter Hartel)

- Is Reliable Multicast too Expensive? Let's be Optimistic  
  (R. Jimenez-Peris, M. Patino-Martinez - TU. Madrid, G. Alonso - ETH Zurich)
- Fault Tolerant Platform for Parallel Applications using MPI  
  (H. Pedroso - Critical Software SA)
- Enhancing Availability of Cooperative Applications through Interoperable Middleware  
  (R. Baldoni, C. Marchetti - U. La Sapienza di Roma)

12:30-14:00  Lunch
14:00-16:00  **Mobile Systems**  
(Chair: Luca Simoncini)

- Context-Based Specifications for Data Mediation to Support Mobile Systems  
  (D. Chalmers, N. Dulay, M. Sloman – Imperial College)
- Towards a Network File System for Roaming Users  
  (D. Mentre, M. Boulkenafed, V. Issarny - INRIA)
- New Mechanisms for Routing in Ad Hoc Networks through World Models  
  (C. Becker, G. Schiele - U. Stuttgart)
- A Framework for Dynamic Adaptation in Wireless Environments  
  (M-T. Segarra, F. Andre - INRIA/IRISA)

16:00-16:30  Break
16:30-18:00  **Distributed Systems (I)**  
(Chair: Peter Puschner)

- Representing and Enforcing Electronic Commerce Contracts over a Wide Range of Platforms using Occurrence Stores  
  (A. Abrahams, J. Bacon - U. Cambridge)
- Assessing the Performance Advantage of Mobile Agents in Distributed Searching  
  (H. Peine - U. Kaiserslautern)
- A High Performance Wireless Fieldbus in Industrial Multimedia-Related Environment  
  (Tovar, Pacheco, Alves, Ferreira, Pereira, Machado, Brandao - Polytechnic Institute Porto)

20.00  Workshop dinner

Day 4: Friday, 12 October 2001

9:00-9:30  CaberNet news
9:30-10:30  **Real-Time Systems**  
(Chair: Dick Snow)

- Java for Real-Time Systems  
  (P. Puschner - TU Wien)
- Re-targetable Framework for Worst-Case Execution Time Analysis  
  (I. Bate - U. York)

10:30-11:00  Break
11:00-12:30 **Distributed Systems (II)**  
(Chair: Paolo Ciancarini)

- BabylonLite: Improvements to Java-Based Distributed Object Systems (S. Gilmore - U. Edinburgh, M. Palomino - U. Cambridge)
- Improving WRC for GC+mobility: Another small step towards managing references in distributed systems (P. Dickman - U. Glasgow)
- Policy Based Management of Large Distributed Systems (M. Fisher, P. McKee - BTexact Technologies)

12:30-12:45 Close workshop
12:45-14:00 Lunch
A2. Extended Abstracts