Welcome to the third issue of JRPIT for 2007. This year is an especially interesting one in Australia. For years a major political issue has been the privatisation of Australia's largest telecommunications company, Telstra. The particularly sensitive issue was whether a privatised Telstra would service the large rural and remote areas of this continent despite the most profitable regions being the largest five cities. With a national election just a few months away, a major issue is the provision of fast broadband – and once again the question is, how can the regional and remote areas of the continent be serviced. The debate now centres on two technical issues: How fast should fast broadband be? Can wireless be the medium of fast broadband now and in the medium term future? This leaves aside any question about how secure wireless technology can be. At one point in time, WEP (Wired Equivalent Privacy) was considered to offer some level of security but today we know just how vulnerable WEP is.

Now let us turn to this issue. The first paper is "A Research of Consumers' Initial Trust in Online Stores in China" by Lu Yaobin and Zhou Tao. The authors say "With the development of e-commerce in China, some obstacles, such as poor Internet infrastructure and logistics problems, have been gradually removed. Consumers' distrust of online stores becomes the main problem impeding the acceptance of online shopping. Initial trust is the focus of this study because most Internet users in China have no experience of online shopping." "The findings of this study can shed light on e-commerce practices in China. For those companies that have built online stores on the Internet, the first challenge is to attract new visitors and establish their initial trust in their online stores. The results of this research demonstrate that, at present, consumers are more concerned with usefulness of websites, website security and vendor reputation."

The second paper, "Obfuscated Malicious Executable Scanner" by Jianyun Xu, Andrew H. Sung, Srinivas Mukkamala and Qingzhong Liu, begins "The proliferation of malware (viruses, Trojans, and other malicious code) in recent years has presented a serious threat to individual users, enterprises, and organizations alike. Current static scanning techniques for malware detection have serious limitations; on the other hand, sandbox testing fails to provide a complete satisfactory solution either due to time constraints (e.g., time bombs cannot be detected before its preset time expires). What is making the situation worse is the ease of producing polymorphic (or variants of) computer viruses that are even more complex and difficult than their original versions to detect." In this paper, the authors "propose a new approach for detecting polymorphic malware in the Windows platform." The authors state that "a methodology for composing signatures of Win32 PE malicious codes is presented that aims at supporting polymorphic malicious code detection. The key assumption is that to preserve its functionality, a polymorphic malware should contain a sufficiently similar API calling sequence."

The third paper in this issue is "Flash Memory Shadow Paging Scheme for Portable Computers: Design and Performance Evaluation" by Siwoo Byun, Seongyun Cho and Moonhaeng Huh. The authors state in their conclusion: "Currently, flash memory is the most popular storage media for information management in portable computing systems. We proposed Flash Memory Shadow Paging (FMSP) which is a new page management scheme for the flash memory database storage. FMSP removes additional storage overhead for keeping shadow pages by reusing invalidated data pages. We also devised a deferred cleaning procedure and its operation interface in flash memory file systems. Unlike previous shadow paging schemes, FMSP could contribute to overcome additional space overhead and slow access speed. We also proposed a simulation model based on closed queuing system to show the performance of FMSP. Our simulation results show that FMSP outperforms the traditional shadow paging scheme in terms of response time and transaction throughput, especially in a high data contention environment."

The final paper is "Adaptive Partitioned Indexes for Efficient XML Keyword Search" by Sung Jin Kim, Hyungdong Lee and Hyoung-Joo Kim. In their abstract the authors say "A query result of an XML keyword search is usually defined as a set of the most specific elements containing all query keywords. Search systems find the query result by considering the combinations of all elements in the inverted indexes of the query keywords. However, we conclude that it is not necessary to consider the combinations of all the elements, when an 'effective result depth' (which represents how deeply nested elements are eligible for the query result) is given. This paper describes a way to construct partitioned indexes on the effective result depth, guaranteeing that the combinations of elements in different partitions never produce result elements. Therefore, search systems can find query results by considering only combinations of elements in the same partitions. Partitioned indexes are adaptable; when an effective result depth is changed, partitioned indexes constructed on the original depth can be used efficiently without being reconstructed physically on the changed depth. The experimental results show that our approach worked quite well in most cases."

Professor Sidney A. Morris
Editor-in-Chief
University of Ballarat
http://uob-community.ballarat.edu.au/~smorris/