

# COMPUTING POSTGRADUATE (RESEARCH) MINI-CONFERENCE

## *Abstracts - Presentations on 8 Nov 2004*

---

### **9.00-9.15      *Authentication for Multicast Communication***

**Christophe TARTARY**

Supervisor: Dr Huaxiong WANG

Associate Supervisor: Prof Josef PIEPRZYK

#### Abstract

The purpose of this thesis is to study authentication processes for multicast communication. A large number of broadcast applications exist today and even more are emerging. They cover many domains: content distribution over the Internet, software distribution, sensor networks, online video games, financial markets and military applications for instance. This talk presents our approach to this problem. During its first part we describe the challenges that we have to face. The second one is dedicated to a description of some key schemes and the theories they rely on. In this part we enlight solutions provided by these techniques as well as the remaining problems.

### **9.15-9.30      *A Framework for Validating Requirements Engineering Process Improvements***

**Bhavani PALYAGAR**

Supervisor: Prof Ray OFFEN

#### Abstract

Requirements Engineering (RE) is a process for determining stakeholder needs during the development of a software system. Research finds that RE process quality critically influences the success of the Software Development Life Cycle (SDLC). This draws significant importance on RE process measurement. Unfortunately, however, RE process quality measurement is neglected, possibly because it is difficult to measure the quality of RE processes, and therefore, to determine what constitutes a good quality RE process across different types of organizations and software development projects. This makes it difficult to formalize RE processes from a quality perspective.

The objective of my PhD research is to arrive at a framework of activities and measurements to improve and validate Requirements Engineering (RE) processes. My research aims at measuring some low-level parameters and relating them to the effectiveness and efficiency of RE processes. The proposed improvement framework, when successful will measure the RE processes and improve them hence enhancing the RE Return On Investment (ROI).

### **9.30-9.45      *Cryptanalysis of Hash Functions***

**Krystian MATUSIEWICZ**

Supervisor: Prof Josef PIEPRZYK

Associate Supervisor: Dr Huaxiong WANG

#### Abstract

Cryptographic hash functions are one of the most important cryptographic primitives. They are used for information authentication, message integrity checking, digital signatures with appendix and password-based identification.

In my presentation, cryptographic hash functions are presented and their applications are briefly described. An outline of possible cryptographic attacks on hash functions is discussed. Then, selected aspects of my current research on cryptanalysis of the functions of SHA family are presented and the future work is outlined.

**9.45-10.00 Algebraic cryptanalysis on stream ciphers**  
**(Joe) Joo Yeon CHO**  
Supervisor: Prof Josef PIEPRZYK

Abstract

Stream ciphers are an important class of encryption algorithms, especially for mobile telephone communication or low latency telecommunication environment. Recently, algebraic attacks have appeared as a powerful tool for cryptanalysis and security evaluation of certain encryption schemes, in particular LFSR (Linear Feedback Shift Register)-based stream ciphers. In this talk, recent research works and directions on the algebraic cryptanalysis are briefly reviewed and my contribution on this area are reported. Several on-going research topics on the algebraic cryptanalysis will be shown. In addition, recent progress on design and analysis of stream ciphers is reported.

**10.00-10.15 A Secure PIM-SM Multicast Routing Protocol**  
**Jungi ZHANG**  
Supervisor: Prof Vijay VARADHARAJAN

Abstract

This paper presents a new secure scheme for Protocol Independent Multicast Sparse Mode (PIM-SM). PIM is the predominant multicast routing protocol in use on the Internet today, where members of the multicast group are distributed sparsely over a wide area. Security issues are particularly important in such multicast routing protocols. In this paper, we propose two distributed group key management schemes to build a secure PIM-SM multicast routing protocol. With these schemes, the network administrator can manage the secure PIM-SM multicast more efficiently, and the management of groups is made more flexible.

**10.15-10.30 Cryptographic Protocols in Electronic Payment Systems**  
**Vijaykrishnan PASUPATHINATHAN**  
Supervisor: Prof Josef PIEPRZYK  
Associate Supervisor: Dr Huaxiong WANG

Abstract

Electronic payments services are a convenient and efficient way to do financial transactions. At present most electronic payments mechanisms make use of credit cards and disclosure of personal information. Adequate security mechanisms are still not available that would protect the information that is stored (e.g. Credit card numbers). This report focuses on analysis of four existing electronic payment protocols and a design for an efficient and secure payment mechanism.

**11.00-11.15 Challenges to Data Transport in Supporting Heterogeneous Web Services Protocol Stacks**  
**Alex NG**  
Supervisor: Prof Ray OFFEN  
Associate Supervisor: Mr Rajan SHANKARAN  
Adjunct Supervisor: Paul GREENFIELD

Abstract

Alex will present his findings in the investigation of the performance of SOAP Web Services in the transport layer, summarise the key issues affecting the performance of SOAP Web Services, and propose his idea: the Table Driven XML (TDXML) message packaging technique which is Alex's solution to address the fundamental issue of XML parsing and object serialisation overheads.

**11.15-11.30 Authorisation for XML Web Services**  
**Sarath INDRAKANTI**  
Supervisor: Prof Vijay VARADHARAJAN

Abstract

Security for Web Services is a broad and complex area covering a range of technologies. At present, there are several efforts being made on the provision of security services such as authentication between participating entities, confidentiality and integrity of communications. However, currently most Web Service applications have schemes that carry out their own authorisation decisions using application specific access control functions in conjunction with local files, which are inflexible and inadequate.

In this talk, I will talk about the survey of the distributed systems authorization architectures I have carried out this year. Then I will introduce the Web Service authorization architecture design principles and requirements that we have laid out. Then I will briefly discuss the Web Services authorization architecture that we are currently designing. I will conclude with our thoughts on future work.

**11.30-11.45 Counteracting DDoS Attacks**  
**Udaya Kiran TUPAKULA**  
Supervisor: Prof Vijay VARADHARAJAN

Abstract

We propose a technique to counteract TCP SYN flood attacks nearest to the attacking source. Once invoked, our technique is able to identify the approximate source of attack with a single packet using our new packet marking technique and agent design. We will also consider a simple attack scenario and discuss the practical implementation of our technique using our prototype model. It should be noted that we are not solving the TCP SYN problem, but we are enabling the victim to differentiate between the traffic originating from good and bad network domains, trace the router that is nearest to attacking source with a single packet even if the source address is spoofed and prevent the traffic at the identified router. Since our model is invoked only during attack times, it has very less overhead and the main advantage of this technique is the victim can provide better service for traffic originating from good network domain and completely eliminate or provide limited service for the traffic originating from bad network domain.

**11.45-12.00 Securing Mobile Ad hoc Networks**  
**Venkatesan BALAKRISHNAN**  
Supervisor: Prof Vijay VARADHARAJAN  
Adjunct Supervisor: A/Prof D HOANG; Dr Yi MU

Abstracts

In recent years the widespread availability of wireless communications, mobile computing and handheld devices has led to the development of ad hoc networks, which is an emerging networking paradigm for mobile nodes. Security issues are paramount in such networks even more so than in wired networks. This project proposal is aimed at understanding the security requirements in mobile ad hoc networks and developing security models and techniques to counteract security threats in this new context. We consider the various principles involved in the design of security services to counteract threats in the context of mobile ad hoc networks.

Though there have been many works in the recent years on secure routing protocols, in particular using cryptographic based techniques, the aspect we propose on "fellowship" amongst the nodes has not been adequately addressed. We analyze a class of protocols such as SAODV, ARAN, Ariadne and SRP that employ crypto based techniques to secure routing, void of detection-response methods and show that they are vulnerable to other attacks that depend on fellowship. We also investigate protocols such as CONFIDANT that cater for detection-response through trust models but fail due to not having security based prevention mechanisms ultimately falling prey to fellowship denial attacks.

Even if fellowship instates a functional MANET, security cannot be achieved until the circular dependency between the prevention mechanisms (based on secure cryptographic methods) and detection-reaction mechanism (based on trust methods) is broken. This leads us to consider a more complete "Secure Architecture for MANET" (SAM) that incorporates both prevention mechanisms and detection-reaction mechanisms, together with an enforcement mechanism (based on fellowship concept) to achieve an operative and secure MANET.

**12.00-12.15 *Enhancing Mobile Agent Security with Trust Management***  
**Ching LIN**

Supervisor: Prof Vijay VARADHARAJAN  
Associate Supervisor: Dr Yi MU

Abstract

We present the design of a trust management system (MobileTrust) for mobile agent security. The proposed design is a trust based security architecture which provides a new direction for mobile security solutions. This new approach goes beyond traditional security models by incorporating a trust model into the security architecture design. This approach enables explicit management of important security related trust relationships in mobile agent systems, which is not possible with traditional security models. Furthermore, with the ability to integrate trust into security decision making, the proposed architecture provides several desirable emerging properties such as increased level of security for mobile code and host; improved flexibility and scalability of security system design and operation. A Java based prototype of MobileTrust has been implemented and integrated with IBM's Aglet mobile agent platform successfully. The experimental investigations are ongoing and preliminary results are confirming the emerging properties.

**12.15-12.30 *Trust-based Access Control Framework for P2P Systems***  
**Huu TRAN**

Supervisor: Prof Vijay VARADHARAJAN  
Associate Supervisor: Dr Michael HITCHENS  
Adjunct Supervisor: Dr Paul WATTERS

Abstract

Peer-to-peer (P2P) file sharing systems have become popular as a new paradigm for information exchange. However, the decentralized and anonymous characteristics of P2P environments make the task of controlling access to sharing information more difficult, which cannot be done by traditional access control methods. In this paper, we identify access control requirements in such environments and propose a trust based access control framework for P2P file-sharing systems. The framework integrates aspects of trust and recommendation models, fairness based participation schemes and access control schemes, and applies them to P2P file-sharing systems. We believe that the proposed scheme is realistic and argue that our approach preserves P2P decentralized structure and peers' autonomy property whilst enabling collaboration between peers.

**14.00-14.15 *A Theory of Error Recognition and Repair***  
**Stephen CHOULARTON**

Supervisor: Prof Robert DALE

Abstract

Errors made by automatic speech recognisers are ubiquitous; often over one in ten hypotheses are wrong. This confounds the management of dialogues introducing wrong facts or instructions, increasing the chance of subsequent errors and creating repetitive re-prompting. Recognition is a classification task and errors are likely to continue. We must, therefore, develop a theory that will allow a system to realize when it is mishearing and to take action to repair the mishearing.

Until this problem is solved the semantic and syntactic analysis of utterances will often fail and users will continue to face frustration and task failure in an unacceptable number of cases.

**14.15-14.30 *Capture and re-use of troubleshooting knowledge at the call centre - an MCRDR approach***

**Megan VAZEY**

Supervisor: Dr Deborah RICHARDS

Abstract

This thesis considers some of the knowledge management issues facing the support / call centre of a large multinational high-tech organisation dealing with the complexities of the burgeoning Information Technology (IT) field. While vendor solutions focus on tracking incoming problem cases, and separately tracking and archiving solutions in a corporate knowledge-base, there is a huge stone left unturned in the form of problem diagnosis, where-to-search, and what-to-search-for knowledge. Our solution embraces the multiple classification ripple down rules (MCRDR) knowledge acquisition technique, which has addressed many of the shortcomings of first generation expert systems. The key MCRDR implementation issues are reviewed and a number of novel extensions are offered to fit the complexity and volatility of the IT support centre.

**14.30-14.45 *Investigating the Efficiency of a Code-compression Method***

**Kate KRASTEV**

Supervisor: Dr Anthony SLOANE

Abstract

Code-size reduction has become an important research area in recent years due to the widespread use of small devices with limited and fixed memory. While there have been dozens of practical approaches suggested already, the theoretical side of the topic has not been much investigated.

This talk looks at the theory of space optimisation through code compression. Two issues are treated in detail -- what is the optimal compression for a particular source program and what are the critical factors when investigating the efficiency of a code-compression method.

**15.30-15.45 *Cluster-based Visualization in Knowledge Discovery in Database***

**Kebing ZHANG**

Supervisor: A/Prof Mehmet ORGUN

Adjunct Supervisor: Dr Kang ZHANG

Abstract

Knowledge Discovery in Database (KDD, also called Data Mining) is the process to extract unknown and potential useful knowledge from massive data. Visualization offers an efficient approach to assist data miners doing data analysing and choosing appropriate algorithms, and gives users an intuitive result of a data mining process in visual form. Clustering algorithms can be both used in the phases of data mining process, and commonly used in information visualization. My PhD research attempts to explore a novel cluster-based visualization approach which gives users more intuitive and easy followed insights in data mining.

**15.45-16.00 *Learning Dynamic Bayesian Networks from Gene Expression Microarray Data***  
**Akther SHERMIN**  
Supervisor: A/Prof Mehmet ORGUN

Abstract

Genes encode for proteins. Some of these proteins in turn regulate other genes. In this fashion, the molecular components of a cell such as, genes, proteins form an interaction network to collectively carry out any cellular functions. Constructing such a network from available microarray data is a major challenge in post-genomic research. Dynamic Bayesian networks (DBN) are considered as a promising model to address this challenge. In my talk, I will discuss the suitability and effectiveness of DBN in modelling gene networks and point out the existing challenges that yet to be solved.

**16.00-16.15 *Aspects of Ontology based interoperability in multi-agent smart-spaces***  
**Bhavna ORGUN**  
Supervisor: Dr Mark DRAS  
Associate Supervisor: Dr Stephen CASSIDY  
Adjunct Supervisor: Dr Cecile PARIS

Abstract

Smart Spaces are work environments with multiple agents, both machine and human. The knowledge associated with the agent's domain is captured in a structured specification of concepts called ontology. An important problem in smart spaces is automating ontological interoperability when communicating between heterogeneous multi agent systems (MAS). There are many aspects of data and domain heterogeneity increasing the possibilities of conflicts and mismatches when combining MAS ontologies. These include syntactic differences due to the proliferation of ontology languages and semantic differences like the use of synonyms and homonyms for equivalent ontology components, as well as intentional conflicts that are part of the domain heterogeneity. This is exacerbated by the underlying differences in the communication protocols and modes of interaction among MAS. In my talk I will discuss current approaches of interoperation among ontologies, focusing on the degree of automation covered by them and identify as a relatively unexplored area the development of fully automated approaches in the context of MAS. I will then outline my chosen approach of "dialogue based automation of semantic interoperability in MAS", to attack this class of problem.

**16.15-16.30 *Beyond Identity***  
**Brett Keith WATSON**  
Supervisor: Dr Len HAMEY  
Associate Supervisor: Mr Rajan SHANKARAN

Abstract

Email sender identification technologies have been a hot topic recently. In this presentation, I consider the advantages that sender identification offers to the fight against spam, and also consider the problem from an economic perspective, on the grounds that an anti-spam solution must be economically viable. I then evaluate those anti-spam technologies which seem most promising in the light of sender identification and intrinsic costs, drawing conclusions as to the direction anti-spam technology must be developed.

**16.30-16.45 Analysis, Specification and Generation of Mobile Computer Data Synchronisation**

**Qingsong YE**

Supervisor: Dr Anthony SLOANE

Associate Supervisor: A/Prof Dominic VERITY

Abstract

In this talk, I will describe my efforts to analyse current Palm OS data synchronisation problems and apply embedded domain-specific language (DSEL) techniques in this domain to improve the current situation. In current technologies, Palm OS conduits are developed by hand-written or partial hand-written code. Consequently, they are error-prone and time-consuming. Our DSEL allows equivalent code to be generated automatically from higher-level expressions, enabling domain developers to express their ideas quickly and concisely, to work more productively and to avoid certain kinds of coding error. The benefits gained by using this formal method such as user specification and automatic code generation, are the main emphasis of our presentation.

**16.45-17.00 Pattern Enforcing Compiler for Java**

**Howard LOVATT**

Supervisor: Dr Anthony SLOANE

Associate Supervisor: A/Prof Dominic VERITY

Abstract

A pattern enforcing compiler(tm) (PEC(tm)) allows classes to be marked as having a given design pattern, e.g. Singleton. The PEC(tm) then checks that the marked class conforms to the pattern and issues an error message if it does not, thus the pattern checking is much like type checking. The PECs(tm) downloadable from the web site require no new syntax and therefore they can be used with existing: editors, IDEs, pretty printers, etc. The downloadable PECs(tm) their own patterns and have the PEC(tm) enforce these.

The talk covers:

1. Background to the PhD
2. Establishing PhD web site (<https://pec.dev.java.net/>)
3. Describes the Load API (Application Program Interface)
4. Describes the Compile API and Compiler
5. Immediate work plan
6. Publication of Paper

~~~~~End of presentations on 8 Nov 2004~~~~~