Preface

In this publication, we have assembled an entire year of contributions to the International Journal of Mobile Computing and Multimedia Communications. The papers published in the four issues of Vol. 3 of IJMCMC span a wide range of subjects, from authentication and intrusion detection to RFID middleware, visual speech recognition, and topology mismatch problems.

The papers in this volume can be divided into several broad categories: 1) security, with the subcategories of authentication, intrusion detection, and security policies; 2) commerce and logistics; 3) network performance in both fixed and ad hoc wireless networks; and 4) audiovisual recognition.

The topic of security is addressed from various perspectives:
- Dual-Level Attack Detection, Characterization and Response for Networks under DDoS Attacks by Anjali Sardana and Ramesh C. Joshi and Improving Effectiveness of Intrusion Detection by Correlation Feature Selection by Hai Than Nguyen, Katrin Franke, and Slobodan Petrović introduce new intrusion detection methods.
- Holger Schmidt discusses Threat and Risk-Driven Security Requirements Engineering, an approach that places great emphasis on gathering information, analyzing and modeling the environment in which a system is to be built.
- Individual user security is the topic of Establishing a Personalized Information Security Culture, in which Shuhaili Talib, Nathan L. Clarke, and Steven M. Furnell examine the transfer of security knowledge from workplace to home and propose a new approach to raising awareness about IT security issues.
- Another security aspect is authentication and data security. Anna Vapen and Nahid Shadmehri present 2-ClickAuth: Optical Challenge-Response Authentication Using Mobile Handsets, an interesting approach that uses two-dimensional barcodes in combination with cell phones in federated identity management system, thus reducing the risk of an attacker gaining access to all accounts of one user through one password. Another approach to protecting federated identity management against attacks is presented by Florian Kohlar, Jörg Schwenk, Meiko Jensen, and Sebastian Gajek in On Cryptographically Strong Bindings of SAML Assertions to Transport Layer Security. Yehia Elrakaiby, Frédéric Cuppens, and Nora Cuppens-Boulahia present An Integrated Approach for the Enforcement of Contextual Permissions and Pre-Obligations. Finally, Teddy Mantoro, Admir Milišić, and Media A. Ayu suggest a novel method for Online Authentication Using Smart Card Technology in Mobile Phone Infrastructure.
- In their paper, Anjali Sardana and Ramesh C. Joshi introduce a defense against DDoS attacks that operates on two levels: At the higher level, they use macroscopic level detectors to detect congestion-inducing attacks that cause an obvious reduction in network functionality, while at the lower, finer level, microscopic level detectors identify more sophisticated and stealthy attacks that reduce the performance in a less detectable way. The suspicious traffic flows are then rerouted to a honeypot for analysis, which
also helps reduce collateral damage in that misclassified legitimate flows can be detected and redirected to the actual server. This is a promising approach for dealing with the common problem of DDoS.

Hai Than Nguyen, Katrin Franke, and Slobodan Petrović present a method for improving the effectiveness of intrusion detection. Their automatic feature selection procedure is based on Correlation Feature Selection (CFS) - a filter method used in machine learning, which can consider correlations between different features and between features and classes. By looking at the CFS measure as an optimization problem that they transformed into a mixed 0-1 linear programming problem with constraints and variables and then solved with the branch-and-bound algorithm, they were able to find the globally optimal subset of relevant features. They evaluated their results by comparing them to two other feature selection methods. The authors were able to show that their method was equally or even more accurate than best-first-CFS and genetic algorithm CFS methods, while also removing considerably more redundant features than the others.

Holger Schmidt deals with the topic of security requirements engineering. His approach is a threat and risk-driven methodology with a heavy focus on gathering, modeling and analyzing the environment of the planned system. The environmental information is used to create threat and risk models, which are then used to select adequate security mechanisms and establish security requirements. The method is embedded into SEPP, a security engineering process based on patterns, and is illustrated with a case study. The author also relates the terminologies of security requirements engineering and of threat and risk analysis to each other to define security-relevant domain knowledge.

In their paper, Shuhaili Talib, Nathan L. Clarke, and Steven M. Furnell describe their work on information security at the individual level. The paper examines the relationship between information security practices at the workplace and at home. A survey showed that as most awareness-raising measures in this domain target organizations, the workplace with its clear regulations and security policies was where people learned most about the topic. However, they also frequently implemented this knowledge in their homes. The authors propose a new approach to security awareness with a user focus that helps individuals develop a comprehensive security culture that they will then employ in all environments in which they operate.

Anna Vapen and Nahid Shahmehri address user security from the perspective of password security. Many Internet users use the same password on many different Web sites, which can give an attacker who captures the password for one site access to all their accounts. The problem is similar with federated identity management systems, where authentication with only a single identity provider using a username and password gives users access to their accounts on various sites. To address this issue, the authors introduce 2-clickAuth, an optical challenge-response authentication solution that uses a Web camera or camera phone and two-dimensional barcodes. They also implement an identity provider that allows users to use 2-clickAuth on all sites that support the OpenID federated identity management system, such as Facebook, MySpace, and Sourceforge.

Florian Kohlar, Jörg Schwenk, Meiko Jensen, and Sebastian Gajek present an approach to protect SAML-based federated identity management against man-in-the-middle attacks, especially for mobile devices that rely heavily on online security measures. Their novel approach allows the mobile browser to remain anonymous while still enabling the identity provider and the relying party, or service provider, to detect man-in-the-middle attacks. They achieve this by binding the SAML assertion to the transport layer security, creating a cryptographically strong dependency.
Contextual permissions and pre-obligations are at the center of the paper by Yehia Elrakaiby, Frédéric Cuppens, and Nora Cuppens-Boulahia. Pre-obligations, i.e., actions that are required before access is granted to a user – such as the payment for a song before access to the download – allow a more flexible enforcement of authorization policies. Therefore, neither traditional access control models nor newer contextual security models, which require a condition to be true at the moment of the access request, support pre-obligations. The authors present a formalized view of the interactions between the obligations and authorization policy states, providing declarative and operational semantics for pre-obligations. They present a framework that allows policy designers to easily evaluate pre-obligations both statically and dynamically, and demonstrate their approach on a practical example.

E-commerce also needs strong security and privacy protection. Teddy Mantoro, Admir Milišić, and Media A. Ayu present an innovative approach to secure online authentication. Their method uses the infrastructure of the mobile phone network and converts the phone’s SIM card into a tamper-resistant storage for security parameters, personal information and user credentials, similar to a smart card. This is combined with public key cryptography. The SIM card can then become a trusted entity that could be used for accessing sensitive applications, such as payments or online banking. The researchers developed two prototypes to demonstrate their approach, which has the added benefit of using a device users are familiar with, which could increase its acceptance.

Two papers exemplify how diverse the application of computing in commerce can be. While Muazzan Binsaleh and Shahizan Hassan propose a Systems Development Methodology for Mobile Commerce Applications, M. E. Ajana, H. Harroud, M. Boulmalf, and M. Elkoutbi look at the logistical side in FlexRFID Middleware in the Supply Chain: Strategic Values and Challenges.

Muazzan Binsaleh and Shahizan Hassan discuss system development methodologies and their suitability for the development of mobile commerce applications, which are used differently from regular e-commerce applications. In their paper, the authors present the first two phases of a study with the objective of proposing a system development methodology for mobile commerce applications. They investigate the currently used development methodologies and analyze their strengths and weaknesses. The paper provides a detailed overview of the methods and aims of the study and analyzes the special requirements arising from developing for mobile devices with small screens and other constraints.

M. E. Ajana, H. Harroud, M. Boulmalf, and M. Elkoutbi discuss the strategic values and challenges of RFID middleware in the supply chain. The paper provides an interesting overview of RFID technology, its components and its key concepts. It discusses how RFID technology can be used in the supply chain management to address typical problems, looking at both the benefits and the key issues. The authors also present FlexRFID, an RFID middleware solution that achieves the maximum benefits of RFID independently of the backend applications.

Two papers in this section address the optimization of wireless sensor networks: Surender Soni, Vivek Katiyar, and Narottam Chand improve energy efficiency and network lifetime in *An Energy-Efficient Multilevel Clustering Algorithm for Heterogeneous Wireless Sensor Networks*, while Sami J. Habib approaches the optimization problem of achieving maximum coverage at minimum cost in the deployment of the sensors in *Analysis of Sensors’ Coverage through Application-Specific WSN Provisioning Tool*.

Allam Mousa presents four queuing scenarios designed to improve system performance and quality of service by reducing the probability of call drop for both handoff and new calls in cellular phone networks. By simulating the different scenarios, where either new calls or handoff calls are queued, and either all or half of the available frequencies are used, the author was able to show that the proposed queuing technique reduced blocking probability for both handoff and new calls.

In their paper, J. Penhoat, K. Guillouard, S. Bonjour, and P. Seïté analyze 3GPP architectures and propose a method for improving their mobility management. They reviewed 3GPP architectures and identified five architectures that had well-designed inter-access mobility management capabilities, which they consider part of the solution for coping with the growing mobile data traffic. Their approach involves splitting mobility management into three phases and assessing their integration into the architectures in question using an evaluation grid designed for the purpose. They propose a method called “hierarchical and distributed handover” to address loopholes found in the design of inter-access mobility management.

Shashi Bhushan, M. Dave, and R. B. Patel present a method to reduce network overhead in peer-to-peer (P2P) systems, which is mainly due to a topology mismatch problem between the logical overlay network and the physical underlay that form a P2P system that generates large volumes of redundant traffic. Their Common Junction Methodology (CJM) identifies optimal physical links and routes traffic through these points instead of the previously identified paths between nodes, which become suboptimal due to the frequent connections and disconnections. Their method works for both structured and unstructured P2P networks without modifying the overlay topology and or reducing the search scope of the network. The paper also includes simulation results that show that CJM resolves the mismatch problem and reduces redundant traffic significantly, as well as the response time of the network.

Shailendra Mishra and D. S. Chauha discuss technologies for enabling high-speed packet data access, specifically MIMO. They developed a new scheduling and selection algorithm for MIMO systems to calculate the optimum number of transmit antennas needed to satisfy a user’s demands at a given moment. The authors present the results of a simulation carried out to examine the performance of this resource allocation and scheduling method is investigated for two types of traffic nodes: voice or Web browsing on the one hand and data transfer and streaming on the other, modeled as Pareto and Weibull distributions, respectively.

Yaser Khamayseh, Muneer Bani Yassein, Iman I. Badran, and Wail Mardini address the common problem of collision in MANETs. While a number of backoff algorithms have been proposed in the past to avoid the issue, the paper shows that no algorithm is superior in all cases. The authors therefore propose an adaptive algorithm, which chooses the best backoff mechanism for each situation from a set of mechanisms based on network density and mobility parameters. They address the time issue by implementing their algorithm in two phases, an offline phase where the algorithm can perform some computations before being deployed, and the online phase. Several simulations were carried out that showed that the proposed Square Root Backoff (SRB) was superior to the Binary Exponential Backoff (BEB) and the Linear Backoff (LB) in terms of throughput and end-to-end delay performance as well as in overall performance.
The paper by Naveen Chauhan, Lalit K. Awasthi, Narottam Chand, R. C. Joshi, and Manoj Misra deals with another issue of MANETs, frequent disconnections and, as a result, lower data availability than in traditional networks. The authors discuss the special characteristics of mobile ad hoc networks that result from limited resources, insufficient bandwidth and high user mobility, where caching is often the decisive factor for allowing rescue, military or other highly mobile operations to use MANETs successfully. They present their own caching method, where the network topology is partitioned into clusters based on physical proximity in the network. This global cluster cooperation (GCC) method allows them to utilize the pull mechanism fully for cache sharing. Their paper also presents the results of simulations that showed that the GCC mechanism performed better than other caching strategies in terms of message overheads and data accessibility.

Prashant Kumar, Naveen Chauhan, Lalit K. Awasthi, and Narottam Chand present another cooperative caching algorithm that also improves the availability of data and the overall performance of the network. This algorithm, ProCoCa, has a proactive approach. Each node is associated with a zone, and the data of nodes that are leaving a zone is cached by neighboring nodes to ensure that the data is available in the zone even after the node leaves. The results of a simulation showed that ProCoCa outperformed previously used algorithms.

Surender Soni, Vivek Katiyar, and Narottam Chand use multilevel clustering to improve not only the connectivity but also the energy efficiency and lifetime of wireless sensor networks. While there are numerous approaches to multilevel clustering, most only consider homogeneous wireless sensor networks. The authors discuss the strengths of heterogeneous networks and propose HMCA, an energy-efficient multilevel clustering scheme for heterogeneous wireless sensor networks. It is based on an existing multilevel clustering protocol EEMC for homogeneous networks, but outperforms it in a simulation in a number of categories, including energy efficiency, lifetime and data delivery ratio.

Wireless sensor networks are also the topic of Sami J. Habib’s contribution, which presents an automated, application-specific provisioning tool for the deployment of sensors in wireless sensor networks that aims to achieve maximum coverage at minimum deployment cost. The coverage problem was modeled as two separate sub-problems, floor plan and placement, which were then combined into one optimization problem. By partitioning the area into M by N cells and assigning sensors into the cells, the author reduced the continuous design space into a discrete one. He then examined the relationship between varying numbers of cells with correspondingly varying sizes used to cover the area and the total number of sensors. He describes the coverage problem and solution process and provides first experimental results.

The final category is dedicated to a fundamental part of audiovisual recognition, with the chapter Primary Research on Arabic Visemes, Analysis in Space, and Frequency Domain.

The paper by Fatma Zohra Chelali, and Amar Djeradi focuses on the analysis of visemes in Arabic. Visemes are the visible mouth shapes needed to produce phonemes, the smallest phonetic units of any given language. Mapping visemes to phonemes – for linguistic research but also for applications such as lip reading or audiovisual recognition – is not simple, since not only do many phonemes look alike visually, i.e., are in the same visemic category, but also, one phoneme may have different visual forms depending on the neighboring phonemes, which can also influence lip shape. As each language has a different set of phonemes, viseme systems must be defined separately for each. The authors recorded a corpus of Arabic phonemes spoken by male and female Algerian test subjects as the basis for an Arabic viseme system. Using statistical analysis and geometrical parameters such as the height and weight of
the lips, and mapping the visemes to the corresponding phonemes, the authors were able to create an
Arabic viseme system that allows the recognition of the phonemes included in the corpus.

With the papers in this volume, we have sought to provide insights into the wide range of topics in
this field. We hope the research, ideas, findings, and methodologies presented in the contributions are a
useful source for students, developers, engineers, researchers, and managers to read about new develop-
ments and the state of the art in various application domains, to gain deeper knowledge, and to see the
possibilities this field provides.

Ismail Khalil
Johannes Kepler University Linz, Austria

Edgar Weippl
Secure Business Austria - Security Research, Austria