Scientific report of the MiNEMA Summer School (7th MiNEMA workshop)

August 19th - 22nd, 2008
Lappeenranta, Finland

Jari Porras
Lappeenranta University of Technology
Jari.Porras@lut.fi

1 Summary

This document reports on the organization of the MiNEMA Summer School (with the 7th MiNEMA workshop), its scientific content and its outcome.

During the past four years, the MiNEMA workshop series has grown into an international forum for middleware research, supported by the European Science Foundation (ESF). The objective is to bring together a mixture of young and senior researchers working on middleware for network eccentric and mobile applications. The workshops help to foster further collaboration between existing MiNEMA members, with special emphasis on PhD students, to advertise and widen participation in the MiNEMA network and to establish links with the software industry. In addition to the workshops both winter and summer schools have been arranged under MiNEMA network.

The 7th MiNEMA workshop was organized by ComLab, the Communications software laboratory of the department of Information Technology, Lappeenranta University of Technology. The workshop took place in Lappeenranta, Finland on August 21, 2008 and was a part of 17th International Summer School on Telecommunications (named as MiNEMA Summer School). The MiNEMA Summer School on Telecommunications included two tutorial days on Tuesday and Wednesday, a scientific workshop (MiNEMA workshop) with selected scientific papers on Thursday and a Code Camp from Thursday afternoon until Friday.

The Summer School Tutorial Days were aimed at participants interested in security, privacy and trust issues in mobile and wireless communications. The workshop day included lectures and paper presentations concerning the research areas focused in MiNEMA. Presentations in summer school events proceeded from beginner's level (tutorial days) to an advanced level (workshop). MiNEMA workshop highlighted the latest research and developments in the middleware and architectures for mobile computing and communication environments. The summer school was ended by a code camp where students had the possibility to work together on the topics presented in summer school.

The tutorial days were arranged by professor Jari Porras (representative of Finland in MiNEMA network). The scientific program of the 7th MiNEMA workshop was organized by D.Sc. Pekka Jäppinen from the Lappeenranta University of Technology. Local arrangements were handled by the local university personnel. The summer school event attracted 54 participants from 9 different countries and 20 different institutions.

2 Meeting program

2.1 Summer school

2.1.1 Summer school program

The MiNEMA summer school was arranged in three events within four days Tuesday to Friday). Days 1 and 2 consisted of school days with invited experts in the theme of the event. On Tuesday speakers represented international research groups while on Wednesday Finnish experts from Nokia and VTT gave their insight to the security field. Steering committee meeting and welcome party was held on Tuesday evening and Social dinner on Wednesday.

Summer School - Security, privacy and trust in mobile and wireless communications

Day 1 - Tuesday, August 19, 2008

8:30 - 16:00 Registration

9:00 - 9:15 **Opening Speech**
Prof. Jari Porras, Lappeenranta University of Technology

9:15 - 10:30 **Security in wireless communications**
Mario Hoffmann, Fraunhofer SIT, Germany

10:30 - 11:00 Coffee Break

11:00 - 12:30 **Security in wireless communications**

12:30 - 13:30 Lunch

13:30 - 15:00 **Privacy issues in network environment**
Prof. Josef Noll, University Graduate Center, Norway

Josef Noll is professor at the University of Oslo in the area of Mobile Services. His group ConnectedLife concentrates on the working areas mobile-based trust and authentication, personalised and context-aware service provisioning, wireless broadband access, mobile-fixed integration and the evolution towards beyond 3G systems. He is also Senior Advisor in Movation, Norway's leading innovation company for mobile services.

15:00 - 15:30 Coffee Break

15:30 - 17:00 **Privacy issues in network environment**

17.00 - *18:00* MINEMA steering board meeting at the university, room 7630

18:00 - **Evening Program**

Wellcome reception at the beach sauna of Lappeenranta University of technologyu

Day 2 - Wednesday, August 20, 2008

8:30 - 16:00 Registration

9:00 - 10:30 **Trust4All**
M.Sc. Sami Lehtonen, Technical Research Center of Finland

M.Sc. Sami Lehtonen is working at the Technical Research Center of Finland in the Security team as a Research Scientist. He has participated in several European and industrial projects, including MAGNET, MAGNET Beyond, Trust4All, CRUISE, CoreGRID to name a few. He was also a member of the information security risk assesment group that operated under the Finnish National Information Security Advisory Board in the Finnish Ministry of Traffic and Communications and Committee on Information Security in Critical Infrastructure at Finnish Communications Regulatory Authority.

10:30 - 11:00 Coffee Break

11:00 - 12:30 **Trust4All**

12:30 - 13:30 Lunch

13:30 - 15:00 **P2P on Handhelds**
Dr. Jukka K. Nurminen, Nokia Research Center

Jukka K. Nurminen received the M.Sc, Tech.Lic., and Ph.D. degrees from the Helsinki University. In 1986 he joined Nokia where he is currently working as a Principal Member of Research Stuff at Nokia Research Center in Helsinki, Finland. He is also Adjunct Professor at the Helsinki University of Technology. His current interests are mobile computing and peer-to-peer applications. With key contributions to several Nokia products, 25 submitted patent applications, and around 40 journal or conference publications he has wide practical and scientific experience on mobile applications and services.

15:00 - 15:30 Coffee Break

15:30 - 17:00 **P2P on Handhelds**

17:00 - **Evening Program**

Minema members: Cruise at lake Saimaa and some evening snack

2.1.2 Summer school evaluation

Tutorial 1: Security in wireless communications
Mario Hoffmann, Fraunhofer SIT, Germany

This presentation dealt with security in mobile and ambient environments. The background issues were covered well by introducing different methods and types of communication that happen in everyday scenarios: Devices communicate with different partners that might reside in our immediate vicinity as well as in a place on the other side of the planet. Thus the same device uses different communication technologies (Bluetooth, Wi-Fi, LAN) to make casual contacts with devices and services using numerous means (Bluetooth sockets, TCP/IP, RFID).

The variety of scenarios leads to the fact that security measures designed for static networks do not apply anymore. Devices leave the safe perimeters of firewalls and may return with malicious software at any time. Therefore the system administrators cannot ensure security by simply blocking connections from the outside. All networks must be protected, but with the existence of multiple networking technologies, one cannot rely on security mechanisms provided by particular networks. Some networks do not provide necessary security layers, and if they do, there are no guarantees that the implementation matches the specification, the network has been configured correctly by all counterparts and that there are no bugs in the system. The problem relies in design principles: The technology might provide secure links, but their utilization is not mandatory. One device might use secure channels by default, but fall back to non-secure operation due to its counterpart that does not utilize the same security methods.

The presentation introduced a model consisting of four different aspects of security: Context, Application, Device, and Transmission. Unfortunately only the transmission part was covered well, and the three more interesting parts were not introduced properly. A framework for tackling these issues, the Hydra, was introduced also. It aims at protecting user data protection and identity management in ambient environments.

Tutorial 2: Privacy issues in networked environment
Professor Josef Noll, University Graduate Center, Norway)

You have no privacy. Get over it! Privacy in general is protecting physical spaces or possessions, personal information and organizational secrets. When considering networks (Internet, social networks, computers and mobile devices), there exists vast amount of information concerning specific persons. Information concerning opinions, political views, images, relationships, medical information and credit card numbers. Parts of these pieces of information can be retrieved

because we have intended it to happen, but most of the data is there because we cannot do anything about it. Removing private information from the network might be impossible, and thus data meant just for safekeeping or published for a narrow audience should be protected well.

However, protection is never complete, and therefore individuals should consider their different identities or roles in the digital world. Every action we do increases our reputation and increases or decreases how others trust our different digital identities. Being a famous graffiti painter might improve our hobby identity, but it would definitely harm our identity in any serious context. Every time we input sensitive information anywhere, we should think about how this information would harm our different roles, if the information were to become public.

The presentation also showed how mobile transactions could be done in the near future. The mobile phone could be used for shopping, replacing traditional debit/credit cards. The mobile phone would contain our identity, which could be used to authenticate into different services enabling entertainment applications and usage of online banks. The future SIM card would work as a secure platform that would manage and deliver personal information in an appropriate way for each application.

Tutorial 3: Trust4All
M.Sc Sami Lehtonen, Technical Research Center of Finland

The immediate presumption regarding the presentation was that will this give methods on how to calculate trust. Although definitions of trust are important, the practical issue of whether it is possible to somehow numerically measure the actual trust is more interesting. There are numerous situations where users blindly trust that whatever they are doing is actually sane. For example, downloading an application from the web is something that gives the owner of the web page complete control over your machine. We trust it, because the name of the application seems to be right, but we have little control over the application being what it says it to be.

The presented context-aware trust system introduces components that handle the trust issues for us. Services require some certain trust level, and hierarchies of services and their trust levels are supported. However, the metrics of the Trust4All system and its approach of being completely autonomous do not seem to apply to anything else than the embedded world. Reliability and performance of the service may relate to embedded services, but not so much to day-to-day applications of regular people. Autonomous installation works when we know what we need and where to get it from, but not when we are searching for certain types of applications and where to get them. Better metrics for trust would be found from the reliability of the authors and the source of the download. In this case the architecture would need to add also some sort of rating system and define authorities who maintain basic concepts. Also the context would need to

take into account which machine we are using (home, public, work) and would the installation require administrators rights (e.g. are we taking a serious risk and compromising the integrity of the device).

Tutorial 4: P2P on Handhelds
D.Sc. Jukka K. Nurminen, Nokia Research Center, Finland

This research focuses on bringing P2P applications to handheld devices. As an example a file sharing application was shown to work on Symbian devices. Definitions of P2P seemed to cause some conversations, whether some applications belong under distributed or P2P world. In mobile devices, these low-power devices should work simultaneously as client and server, which might be a problem. Content search and delivery is a task that requires computation power which would require more energy from the battery. Different types of P2P types were shown from unstructured to structured networks. Some require central servers and some distribute the work of a central node to multiple servers. These approaches seem to be more suitable for the mobile world for two reasons: Content search does not require the mobile device to do the computation, and the content delivery does not cause as much traffic as the distributed servers can act as proxies, and maybe prioritize content delivery from machines that have fixed power supply.

An interesting point of view was given as an example mobile P2P application. The handheld could be used as a miniature web server, allowing distribution of data in a new way. The personal data could be combined with the context, which would we for example the location of the device. So taking a picture with your mobile phone could be delivered to your peers with the added information of location, so that the information about your personal actions would be more complete. Also this context data could be used to find people near you, or in specific places, and allow new types of uses like delivering real-time data from a certain location. Apart from entertainment and personal value, this kind of data could be used to gather information for commercial and scientific purposes. For example, weather data could be gathered more accurately than it is done today, when billions of mobile phones could deliver the information, instead of a handful of weather stations.

2.2 7th MiNEMA Workshop

2.2.1 Workhop arrangements

Thursday was reserved for scientific presentations i.e. the 7th MiNEMA Workshop. The research scope of the workshop followed the Summer school theme “security, privacy and trust in wireless and mobile communications” though traditional MiNEMA topics were included into the scope:

MiNEMA focus:

- Communication paradigms
  - Peer-to-peer
  - Pub/sub
  - Group communications
- Networking
  - Ad hoc
  - Sensor networks
  - BAN/PAN/LAN/...
- Architecture issues
- Performance issues
- Routing
- Context awareness
- Applications/Application areas

Summer school focus:

- Authentication
- Privacy threats and protection
- Trust
- Automation and Simplicity
- Lightweight cryptography
- Availability
- Threat analysis
- User-Centric security
- Feasible security solution(s)
- Security Management
- Touch zone security
- Payment systems

The type of contributions was in line with previous MiNEMA workshops. The scientific program consisted of either research papers or work in progress papers:

- **Research papers**. New research results on the selected workshop area or summaries of completed research projects. These submissions could not exceed 10 pages.
- **Work-in-progress papers**. Work that is still in progress and could benefit of open discussion in the workshop. These submissions could not exceed 3 pages.

Each paper, in order to be accepted, was reviewed by three members of the workshop program committee. The program committee consisted of MiNEMA steering group members and the work was lead by D.Sc. Pekka Jäppinen from the Lappeenranta University of Technology:

The selected research as well as work-in-progress papers created a dynamic program which encouraged fruitful discussions during the workshop. For each accepted submission, one author was invited to give a presentation at the workshop. Research papers were presented in 40 minute slots and work in progress papers in 20 minute slots. The authors of accepted submissions were requested to revise their contribution by considering the feedback of reviewers. The papers were published by the Lappeenranta University of Technology in university's scientific publication series. The proceedings will be later on available through the workshop web pages (www.it.lut.fi/ssotc).

2.2.2 Workshop program

7th MiNEMA Workshop

Thursday, August 21, 2008

8:00 - 16:00	Registration
9:00 - 10:00	**Opening Speech and tutorial** **XX** [presentation] Pekka Jäppinen, Lappeenranta University of Technology
10:00 - 10:30	Coffee Break
10:30 - 11:30	**Session I** **Session chairman:**
10:30 - 11:10	**"A Framework for Data Dissemination In Mobile Ad Hoc Networks"** [publication], [presentation] Hugo Miranda, Simone Leggio, Luís Rodrigues and Kimmo Raatikainen University of Lisbon, University of Helsinki and INESC-ID/IST
11:10 - 11:30	**"Controlling Epidemics in Wireless Networks"** [publication], [presentation] Ranjan Pal, Ayan Nandy, Satya Ardhy Wardana, Neeli Rashmi Prasad and Ramjee Prasad University of Southern California, Indian Institute of Technology and Aalborg University
11:30 - 12:30	Lunch
12:30 - 13:30	**Session II** **Session chairman:**
12:30 - 13:10	**"A Distributed Middleware for Container Transport: Lessons Learned"** [publication], [presentation] Klaas Thoelen, Sam Michiels and Wouter Joosen IBBT, DistriNet and Department of Computer Science, K.U.Leuwen
13:10 - 13:30	**"FREEMOTE: A Wireless Sensor Networks Emulation System"** [publication], [presentation] Timothée Maret, Raphaël Kummer, Peter Kropf, and Jean-Frédéric Wagen TIC Institute, University of Applied Science of Fribourg and Computer Science Department, University of Neuchâtel
13:30 - 14:00	Coffee Break
14:00 - 15:00	**Session II** **Session chairman:**

14:00 -14.40	**"Security and Privacy in Ubiquitous Information Screen"** [publication], [presentation] Were Oyomno and Pekka Jäppinen Lappeenranta University of Technology
14.40-15.00	**"Anonymity in Mobile Ad Hoc Networks"** [publication], [presentation] Roy Friedman and Neer Roggel Technion, Israel Institute of Technology, Computer Science Department MiNEMA Book
15:00 - 15:15	**End of the workshop** Pekka Jäppinen, Lappeenranta University of Technology

2.2.3 Workshop evaluation

Altogether 6 paper presentations were given in the workshop.

A Framework for Data Dissemination in Mobile Ad Hoc Networks

Mobile Ad Hoc networks require new types of approaches for data delivery and retrieval. Everything starts from the idea that we do not know who are around us, and when will they disappear. The research proposes PAMPA, a Power Aware Message Propagation system, which uses timed broadcasts for delivering data to nearby devices. So instead of constantly broadcasting incoming messages, the nodes wait for a short period. This prevents flooding of the network with messages, as we can deduce if we need to broadcast messages at all. If we hear the same messages again for a certain amount, we know that there is no need to retransmit as the message has probably been captured by all the devices in out vicinity. Furthermore, the number of hops required is less, as the message can travel from a device which is on one side of the transmission range to the other without being retransmitted by the nodes in the middle. These broadcast messages have also a Time to Live value, so one message cannot travel to the other side of the world accidentally.

The delivery algorithm also makes data retrieval more robust, as there multiple copies of the message divided geographically. When retrieving data, a device makes a query with a small TTL value. When there are multiple copies and the TTL value is small enough, the query is answered by a device that is close to us. This ensures that the message will be retrieved by a very small number of hops. Furthermore the system scales well, as the amount of nodes per square meter increases the number of copied data, but does not result in increased network traffic.

Controlling Epidemics in Wireless Networks

In wireless sensor networks or social networks, there are a large number of nodes communicating between each other. In this type of a scenario, viruses and other malicious beasts, can invade a huge number of nodes in a small period of time. This would be called an epidemic. Unfortunately the presentation was missed due to other activities, and the slides and the article do not present anything concrete. The connectivity matrix is formed, but the actual algorithms and procedures on what to do next is missing. Also the practical ways on how to discover infected nodes lacks both information and references. The same applies on conversation on how to make the connectivity matrix on dynamic networks instead of static ones.

A Distributed Middleware for Container Transport: Lessons Learned

A distributed middleware is proposed to incorporate different types of Wireless Sensor Networks that gather information from product residing in all kinds of warehouses. In short, the middleware would offer a web service that would aggregate information from different sources into coherent knowledge database. Although not mentioned, the same approach could be also used to include support for legacy systems without any wireless, real-time monitoring of cargo. The middleware needs to ensure end-to-end interoperability by providing data exchange interfaces for heterogeneous data and fault tolerance accounting for losing connections to a part of the wireless nodes. Some common services are also required, like authentication and encryption. In addition, the lessons learned includes that most operators will continue to use their existing systems, and there is still need to develop methodologies to locate where containers are. There can never be a system that has direct access to individual companies databases, and therefore address resolving systems are needed. Each object will need unique identifiers, that can be used to track cargo and these identifiers must be included in the Wireless Sensor Network.

FREEMOTE: A Wireless Sensor Networks Emulation System

The current state of Wireless Sensor Networks consists of hard-to-use interfaces and application specific virtual machines that execute applications. FREEMOTE introduces a Java based approach where the same Java application can be executed in a physical wireless sensor, and at the same time can emulate huge numbers of nodes by using the same Java code. The system allows different kinds of configurations and provides different routing algorithms and communication layers for the simulated sensors. In addition, the system provides visual feedback of the organization of the different sensors (emulated and physical ones) and shows how they communicate between each other. The simulation allows also the measurement of important metrics. Energy consumption and CPU usage can be measured in some way. Furthermore, while the network is alive and nodes are moving inside the network, their connectivity can be changed, I.e. simulate the effects of broken wireless links.

Security and Privacy in Ubiquitous Information Screen

This research envisions the usage of public information screens that can deliver personalized information for nearby individuals, and discusses the security and privacy concerns in this kind of a system. For any personalized information, the premise requires that information about the user is delivered to the system. In this case the information is transmitted using wireless links, which opens a world of possible attack scenarios. The normal scenario is eavesdropping, where persons near to you can steal the personal information sent over the air, and track your movements in the ubiquitous environment. In the case of public information screens, rogue access points can change your personal data, and cause harm to your person as your preferences are not what you really are. Nobody wants other people to know about your interests in dwarves, if all you want is the latest hockey news. Encryption is shown as an answer to these problems, and the impact of introducing encryption is discussed. One aspect of the information screen is the time in which it can react. Complete graphs of the run-time of different parts of the encryption were shown well. A limit of 15 seconds was introduced by the authors, and it seems that their implementation always completes the task under this time. Although the time limit can be criticized, as a moving person can pass the through the area of Bluetooth range in this time. As the implementation in most cases keeps clearly below this limit with suitable hardware, the time limit should be decreased. This would prevent the deployment of this kind of a system of becoming too complex by not having to monitor movements beyond the range of a single Bluetooth device.

Anonymity in Mobile Ad Hoc Networks

Anonymity schemes in fixed networks are quite simple. Traffic can be routed through an anonymizer proxy, and the end point does not know the originator of the query. In this study, a multi-hop system is proposed to allow two endpoints in a Mobile Ad Hoc Network to start an anonymous transfer. Its idea differs from the fixed network solutions in such a way, that the anonymity is an increasing value along the multiple hops in the Ad Hoc network. Assuming that the attacker cannot listen the entire Ad Hoc network, but resides somewhere along the path, it cannot know the location or identity of the original sender, and also cannot decipher the message that returns back from the endpoint. A question is raised by the fact that the authors state that in the case of a man-in-the-middle -scenario, where the attacker is one of the hops along the path, the attacker can form a key with both sides of the communication and thus can access the data transmitted between them. At the same time, they assume the attacker is part of the communication chain. These statements defy logic. Also, they have devised a system for fragile Mobile Ad Hoc Networks that creates a static communication path between two endpoints. Assuming the network is small, the probability of having the attacker in the communication path increases. On the other hand as the system grows larger, the probability of being able to maintain the static

communication link grows. As suggested, the system contains no real practical value.

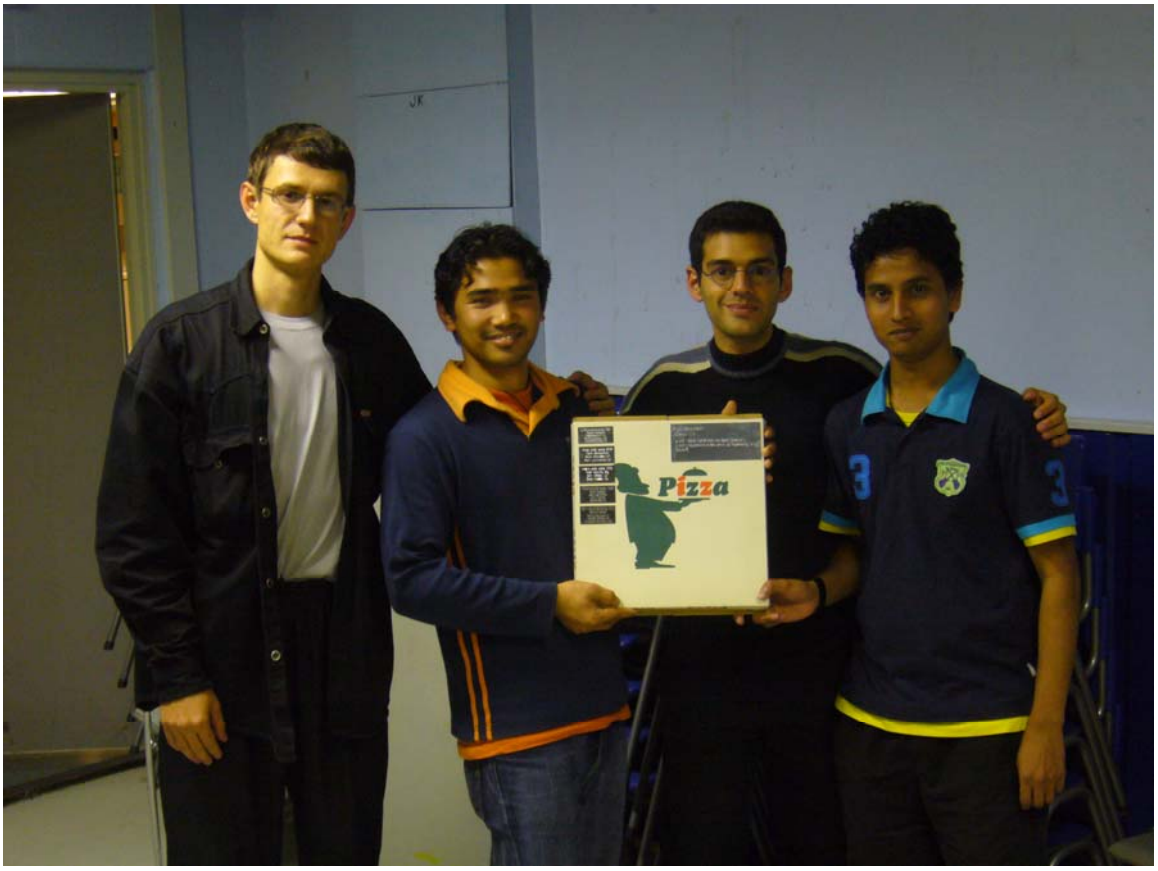
2.3 Code camp

The MiNEMA summer school was ended with the practical part, code camp, where students/participants implemented security, privacy or trust aware applications for Maemo environment on Nokia 810 devices. Altogether 30 students were working on their applications for 22 hours.

Code Camp - Thursday, August 21 - Friday, August 22, 2008

Thu 16:30 - 17:00	Registration
17:00 - 17:30	**Opening Speech (Student Union Auditorium)** Arto Hämäläinen, Lappeenranta University of Technology
Thu 17:30 - Fri 15:00	**Coding (Student Union Basement)** Food and refreshments available for the students
Fri 15:00 -16:00	**The Best Code Award Ceremony** Grading committee:

All works were graded by a grading committee and finally the work **File Encryption/Decryption** was selected as the best application of the code camp.



This part concluded the summer school and student's work for the credits. Students were required to participate in the summer school actively and to return half a page report on each presentation and to complete the implementation project for 2 ECTS credits.

3 Assessment of the summer school

The summer school clearly reached the research field and succeeded in attracting a diverse public from academic institutions as well as industry. The summer school event attracted 54 participants from 9 different countries and 20 different institutions. Financially the organizers used less money than reserved for the event. We can happily state that the summer school event achieved its goals.