Spring 2015 topics

Summary

- CU1: Security of Bluetooth Low Energy
- DY1: IPv6 over networks of resource-constrained nodes
- DV1: A comparative study of energy profiling methods for mobile devices
- JD1: Using Internet photos and videos for indoor mapping
- JD2: Indoor localization using fingerprinting techniques
- JD3: User trajectory recognition in an indoor environment
- JL1: Bitcoin and cryptography
- JN1: Improving the energy-efficiency of cellular base station
- JN2: Computer science challenges of 3D printing
- KH1: Cloud datastores
- KH2: Big data platforms
- KK1: Container cloud computing
- MB1: Delay-sensitive cloud computing and edge computing for road-safety systems
- MD1: Multimedia streaming over cognitive radios
- MD2: Bacteria nanonetworks
- MM1: Communication protocols and standards for the IoT
- MS1: Analysis of techniques and tools for automated mobile app testing
- MS2: Scalable vs non-scalable video coding for mobile video in practice
- NH1: Virtual machine consolidation with multi-resource usage prediction
- OH1: User authentication or identification through heartbeat sensing
- RB1: Proximity services using device-to-device communication
- SL1: Software market of network functions virtualization
- SS1: MOOCs and authentication
- SS2: Biometric authentication
- SS3: Password management
- SS4: ICT as enabler for energy behavioral change
- SS5: Security and privacy in smart energy communities
- ST1: Secure Instant messaging
- TN1: Survey of security-enhanced linux policy analysis techniques
- ZO1: How dense are cell towers? An experimental study of cell tower deployment
- ZO2: Simulation tools for wireless sensor network

CU1: Security of Bluetooth Low Energy

Tutor: Çaatay Ulusoy (Lukoton Oy)

Version 4 of the Bluetooth specifications includes a new short-range wireless communication technology known as Bluetooth Low Energy (BLE) or Bluetooth SMART. The diffusion of BLE has recently been very fast as smartphones (e.g., the iPhone) and smart objects (e.g., sport sensors) have started being equipped with BLE transceivers. The design goals of BLE include low cost and low energy consumption of devices. As a consequence, some security mechanisms of Bluetooth classic were redesigned in to reduce their complexity. The impact of these changes on the security of communications with BLE is still unclear. The student involved in this topic is expected to: learn the essential features of the BLE protocol stack; analyze the security features of the communication between BLE devices; analyze possible security issues in the protocol specification and propose solutions to overcome them.

References:

- Robin Heydon, "Bluetooth low energy: the developer's handbook", Prentice Hall, 2013
- Tomasz Rosa, "Bypassing Passkey Authentication in Bluetooth Low Energy", IACR Cryptology ePrint Archive, Report 2013/309, May 2013
- Mike Ryan, "How Smart Is Bluetooth Smart?", ShmooCon 2013

DY1: IPv6 over networks of resource-constrained nodes

Tutor: Deng Yang

IPv6 over Networks of Resource-constrained Nodes (6lo) is an IPv6-based network that connects constrained nodes with limited power, memory or processing resources. With the next mega-trend of the Internet of Things, 6lo is becoming more and more important as it provides an end-to-end solution and forms a solid base for interoperability. This student involved in this topic is expected to overview the transmission technologies supported by 6lo currently or in the near future. Some examples include ZigBee, Bluetooth Low Energy, Near Field Communication. The student also needs to understand how these technologies integrate into 6lo and then compare them in a comprehensive way to conclude what scenarios they are suitable for.

References:

- https://datatracker.ietf.org/wg/6lowpan/documents/
- https://datatracker.ietf.org/wg/6lo/documents/

DV1: A comparative study of energy profiling methods for mobile devices

Tutor: Vu Ba Tien Dung

A complete knowledge on how and where energy is consumed on a mobile device is of great interest not only to end users, but also software and system developers. Examining the energy consumption of a device is referred to as energy profiling and is typically classified as either hardware-based or software-based. Hardware-based techniques utilize hardware instruments to measure the power of the device directly, whereas software-based techniques employ a set of power models in order to estimate the device energy consumption. The work consists in surveying and comparing different energy profilers on mobile devices. First, profilers needs to be classified into categories, and then the advantages and disadvantages of the considered tools should be pointed out. Next, a few popular tools (e.g., Monsoon for hardware-based; PowerTutor and AppScope for software-based) are chosen and their accuracy is evaluated on a set of mobile phone usage scenarios. The final outcome of the work is to characterize in which scenarios and conditions one profiling method can be applied or not.

References:

- Chanmin Yoon, Dongwon Kim, Wonwoo Jung, Chulkoo Kang, and Hojung Cha, "AppScope: application energy metering framework for android smartphones using kernel activity monitoring", the 2012 USENIX Annual Technical Conference (USENIX ATC'12), June 2012
- Sasu Tarkoma, Matti Siekkinen, Eemil Lagerspetz, and Yu Xiao, "Smartphone Energy Consumption – Modeling and Optimization", Cambridge University Press, First Edition, September 2014

JD1: Using Internet photos and videos for indoor mapping

Tutor: Jiang Dong

The indoor localization market is rapidly growing. However, up-to-date indoor maps are rarely available. Along with booming popularity of photo sharing services such as Instagram and Flickr, an ever-increasing number of photos and videos are shared and made publicly available on the Internet. This topic tries to explore the possibility of utilizing Internet photos and videos for building 3D models of indoor environment and providing indoor mapping using these models. There are several areas of interest: analyzing of different types of buildings from the perspective of indoor structure; using the APIs provided by different websites to download photos or videos for the selected typical buildings; using Structure-from-Motion techniques to build 3D models of the selected buildings; analyzing the usability of the models from the perspective of indoor mapping.

References:

- By Sameer Agarwal, Yasutaka Furukawa, Noah Snavely, Ian Simon, Brian Curless, Steven M. Seitz, Richard Szeliski, "Building rome in a day", C ommunications of the ACM, 54(10):105–112, October 2011
- Noah Snavely, Steven M. Seitz, and Richard Szeliski, "Photo tourism: exploring photo collections in 3D", ACM Transactions on Graphics, 25(3): 835–846, July 2006
- Visualsfm: A visual structure from motion system

JD2: Indoor localization using fingerprinting techniques

Tutor: Jiang Dong

While it is easy to utilize GPS to localize the user outdoors, indoor localization is still an open issue. Many indoor localization approaches have been proposed in the literature. This topic focuses on using fingerprinting approaches for indoor localization. Fingerprinting approaches decide locations based on geo-referenced fingerprints that have been collected for example through war-driving. Besides Wi-Fi fingerprints, others such as Bluetooth and the magnetic field have also been used for indoor localization. The student involved in this topic will survey fingerprinting-based indoor localization techniques first, then build a small Wi-Fi or magnetic field fingerprints map of the Aalto CS building. Based on the map, the student can implement their own indoor localization system by choosing state-of-art algorithms or designing their own solution.

References:

- Hui Liu, Houshang Darabi, Pat Banerjee, and Jing Liu, "Survey of Wireless Indoor Positioning Techniques and Systems", IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 37(6):1067-1080, November 2007
- Yanying Gu, Anthony Lo, and Ignas Niemegeers, "A survey of indoor positioning systems for wireless personal networks", IEEE Communications Surveys & Tutorials, 11(1):13-32, March 2009
- Jaewoo Chung, Matt Donahoe, Chris Schmandt, Ig-Jae Kim, Pedram Razavai, and Micaela Wiseman,"Indoor location sensing using geo-magnetism", the 9th international conference on Mobile systems, applications, and services (MobiSys '11) pp.141-154, June 2011

JD3: User trajectory recognition in an indoor environment

Tutor: Jiang Dong

Recording walking trajectories of users in an indoor environment is useful for analyzing their behavior. Furthermore, the fingerprints information along the trace can be collected efficiently if the walking trajectory is known. The work to be carried out in this topic explores using the built-in sensors of a smart-device together with map information to determine the walking trace of a user. Given a start position and the direction on the map, sensors including accelerometer and gyroscope can be used for dead reckoning. More information such as indoor maps can be used for calibrating the trace. A student involved in this topic would need to first survey the state-of-art in user trajectory recognition techniques. Based on the survey, a user trajectory recognition system could be implemented on a mobile platform. The work can further design the metrics to evaluate the accuracy of the collected traces.

References:

- Fan Li, Chunshui Zhao, Guanzhong Ding, Jian Gong, Chenxing Liu, and Feng Zhao, "A reliable and accurate indoor localization method using phone inertial sensors", the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12), pp.421-430, September 2012
- Anshul Rai, Krishna Kant Chintalapudi, Venkata N. Padmanabhan, and Rijurekha Sen, "Zee: zero-effort crowdsourcing for indoor localization", the 18th annual international conference on Mobile computing and networking (Mobicom '12), pp. 293-304, August 2012
- Pavel Davidson, Jussi Collin, and Jarmo Takala, "Application of particle filters for indoor positioning using floor plans", Ubiquitous Positioning Indoor Navigation and Location Based Service (UPINLBS), pp.1-4, October 2010

JL1: Bitcoin and cryptography

Tutor: Jian Liu

Bitcoin a widely adopted online payment system, which uses peer-to-peer technology to operate with no central authority or banks. As a result, users can enjoy many benefits by using Bitcoin, such as no third-party seizure, no (or low) transaction costs and no tracking. However, it has significant limitations regarding privacy. For example, payment transactions are recorded in a public decentralized ledger, which potentially leaks important information. This topic is about using cryptographic technologies to enhance the privacy of Bitcoin. Students who select this topic should survey the technologies that are currently used in Bitcoin, their limitations, and state-of-the-art cryptographic solutions.

References:

- Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin", the 2013 IEEE Symposium on Security and Privacy (SP '13), pp. 397-411, May 2013
- Andrew Miller, Ari Juels, Elaine Shi, Bryan Parno, and Jonathan Katz, "Permacoin: Repurposing Bitcoin Work for Data Preservation", the 2014 IEEE Symposium on Security and Privacy (SP '14), pp. 475-490, May 2014

JN1: Improving the energy-efficiency of cellular base station

Tutor: Jukka K. Nurminen

In our lab, we have a long history of research on saving energy at the mobile phone. In this seminar, we are shifting our attention to the energy consumption of the base station and looking for ways how energy can be saved at the network endpoint. Some time ago, we had a thesis project that took a high-level look at the energy-efficiency of LTE networks. The main goal of this work is to go into a more technical direction by focusing on aspects that can be achieved with software-based solutions. Furthermore, a number of new options are available such as Cloud-RAN, cooperation of multiple base stations, or adaptation to variable availability of energy.

References:

- http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5722444&tag=1
- https://aaltodoc.aalto.fi/handle/123456789/11999
- http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5683654

JN2: Computer science challenges of 3D printing

Tutor: Jukka K. Nurminen

The target of this work is to investigate 3D printing and, in particular, look for the research challenges that it offers for computer science. The topic is rather open and the work can focus on some relevant aspect, such as the protocols for communicating with 3D printers, the role of mobile technology in 3D printing, or software platforms for sharing 3D printer artifacts.

References:

- http://3dprintingindustry.com/2014/06/27/ray-kurzweils-predictions-3d-printing-2014-google-io-conference/
- http://www.ijimai.org/journal/sites/default/files/IJIMAI20111_4_5.pdf
- http://sloanreview.mit.edu/article/innovation-lessons-from-3-d-printing/

KH1: Cloud datastores

Tutor: Keijo Heljanko

Cloud computing has risen as a new framework for doing highly scalable web based applications. One of the central building blocks are new database technologies developed to implement massively parallel database systems, called cloud datastores aka NoSQL databases. The main goal of this work is to survey this new class of datastores, discuss their design principles, categorize and compare them against each other and against traditional relational database systems.

Reference:

- Rick Cattell, "Scalable SQL and NoSQL data stores", SIGMOD Record, 39(4):12-27, December 2010

KH2: Big data platforms

Tutor: Keijo Heljanko

Big data is one of the currently highly discussed topics in cloud computing applications. In this topic you get to survey the most widely used big data platforms, such as Apache Hadoop, Apache Spark, and Facebook Presto. In this topic the main aim is to survey this new class of big data platforms, discuss their design principles, categorize and compare them against each other. Some of the issues in selecting the right tools and platforms for the big data application at hand need to be discussed.

References:

- Matei Zaharia et al., "Resilient distributed datasets: a fault-tolerant abstraction for in-memory cluster computing", the 9th USENIX conference on Networked Systems Design and Implementation (NSDI '12), April 2012
- Jeffrey Dean and Sanjay Ghemawat, "MapReduce: simplified data processing on large clusters", the 6th conference on Symposium on Opearting Systems Design & Implementation (OSDI '04), 6:10, December 2004
- Presto: Distributed SQL Query Engine for Big Data

KK1: Container cloud computing

Tutor: Kashif Khan

Containers are a new alternative to virtual machines for running tasks on the cloud. The goal of this work is to investigate container technologies and compare them especially from the performance perspective. The work could potentially perform experiments with scientific computing tasks through the physics computing infrastructure at CERN.

References:

- http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6184989&tag=1
- https://www.docker.com
- http://www.ubuntu.com/cloud/tools/lxd
- http://researcher.watson.ibm.com/researcher/view_group.php?id=5742

MB1: Delay-sensitive cloud computing and edge computing for road-safety systems

Tutor: Mehrdad Bagheri

The goal of this research is to investigate whether the response time of a cloud-computing system over conventional cellular Internet (e.g., LTE) is suitable for delay-sensitive safety applications, specifically, for road-safety systems in which the network nodes are mobile and might not be in small numbers either (e.g., all cars in a city connected). These safety applications require very quick response time (minimum network latency) as well as scalability. Another question is which cloud computing framework or model to use for development of such applications. For instance, the popular Apache Hadoop might not be suitable for delay-sensitive applications, as it was originally designed for large data and batch processing. Finally, if conventional cloud platforms fail to completely satisfy the requirements of these safety applications, does the more recent platform of Mobile Edge Computing (MEC) have the potential to address this requirement? If so, what is the gain in response time (delay) when MEC is used? Focus of this topic is on vehicular safety, however the results can be applied to any delay-sensitive system.

References:

- Seiya Kato, Matti Hiltunen, Kaustubh Joshi, and Richard Schlichting, "Enabling Vehicular Safety Applications over LTE Networks", the 2nd International Conference on Connected Vehicles & Expo (ICCVE '13), pp. 747–752, December 2013
- Dhruba Borthakur et al., "Apache Hadoop goes realtime at Facebook", the 2011 ACM SIGMOD International Conference on Management of Data, June 2011
- Pawe Jaworski, Tim Edwards, Jonathan Moore, and Keith Burnham, "Cloud Computing Concept for Intelligent Transportation Systems", the 14th International IEEE Conference on Intelligent Transportation Systems (ITSC '11'), pp. 391-936, October 2011
- David Bernstein, Nino Vidovic, and Sohrab Modi, "A Cloud PAAS for High Scale, Function, and Velocity Mobile Applications - With Reference Application as the Fully Connected Car", the Fifth International Conference on Systems and Networks Communications (ICSNC '10), pp. 117-123, August 2010

MD1: Multimedia streaming over cognitive radios

Tutor: Mario Di Francesco

Cognitive radio networks (CRNs) are able to sense a wide range of the spectrum and the agility to make use of the available resources dynamically. Accordingly, they can reclaim unused frequencies (i.e., whitespace) for wireless communications while avoiding interferences with between licensed and unlicensed users. One of the most promising applications of CRNs is represented by bandwidth-intensive multimedia services for mobile devices, such as video streaming, that are already facing a shortage of resources in the cellular networks. The student involved in this topic is expected to: learn the basics of CRNs; understand the different regulations in different countries; analyze the impact of the features peculiar to CRNs on streaming multimedia content.

References:

- William Lehr and the Spectrum Working Group, "Toward More Efficient Spectrum Management - New Models for Protected Shared Access", Tech. rep. of the Massachussets Institute of Technology, 2014
- Shiwen Mao, "Video over Cognitive Radio Networks: When Quality of Service Meets Spectrum", Springer, 2014

MD2: Bacteria nanonetworks

Tutor: Mario Di Francesco

Molecular communications have been recently proposed for building networks of nano-scale elements. A promising direction consists in exploiting bacteria as mobile carriers of messages that can be encoded as DNA fragments. Such messages can be then exchanged between bacteria when they are in close proximity through the process known as conjugation. Environmental factors such as the concentration of chemicals affect the motion of the bacteria and eventually the chance that a message can be successfully delivered from a source to a destination. The student involved in this topic is expected to: learn the basics of nano-scale bacterial communications; analyze the mobility pattern of bacteria and the conjugation process; develop mechanisms that affect the motion of bacteria so as to increase the chance of successful message delivery.

References:

- Maria Gregori and Ian F. Akyildiz, "A New NanoNetwork Architecture Using Flagellated Bacteria and Catalytic Nanomotors", IEEE Journal on Selected Areas in Communications, 28(4):612-619, May 2010
- Sasitharan Balasubramaniam and Pietro Liò, "Multi-Hop Conjugation Based Bacteria Nanonetworks", IEEE Transactions on NanoBioscience, 12 (1):47-59, March 2013

MM1: Communication protocols and standards for the IoT

Tutor: Manik Madhikermi

The Internet of Things (IoT) calls for easy ways to query and set up information flows between any kinds of products, devices, computers, users and information systems in general. However, sufficiently generic, powerful and standardized application-level interfaces are not currently available for exchanging the kind of information required by the IoT. One recent initiative is the Open Messaging Interface (O-MI) messaging standard by The Open Group. However, many other standardization organizations have also launched initiatives that claim to fulfill similar goals. The work consists in surveying of completed and ongoing "application-level" standardization activities for the IoT in organizations such as W3C, IETF, OASIS, ISO, and so on. The identified standards should be assessed against the requirements for a generic, application-level communication interface as presented in the references below. The assessment should be done also by taking into consideration their applicability to reference applications, as well as to other relevant IoT applications.

References:

- Kary Främling and Merina Maharjan, "Standardized communication between intelligent products for the IoT", the 11th IFAC Workshop on Intelligent Manufacturing Systems, vol. 11, pp. 157-162, May 2013
- Kary Främling, Sylvain Kubler, and Andrea Buda, "Universal Messaging Standards for the IoT From a Lifecycle Management Perspective", the IEEE Internet of Things Journal, 1(4):319-327, August 2014

MS1: Analysis of techniques and tools for automated mobile app testing

Tutor: Matti Siekkinen

There are many mobile app testing tools and services currently available for app developers. The objective of this work is to analyze the techniques used and features offered by these tools and to perform a comparative analysis highlighting their pros and cons. The outcome should describe the state of the art of automated mobile app testing and point out the limitations and open problems with current tools.

References:

- Domenico Amalfitano, Anna Rita Fasolino, Porfirio Tramontana, Salvatore De Carmine, and Atif M. Memon, "Using GUI ripping for automated testing of Android applications", the 27th IEEE/ACM International Conference on Automated Software Engineering (ASE 2012), pp. 258-261, September 2012
- Saswat Anand, Mayur Naik, Mary Jean Harrold, and Hongseok Yang, "Automated concolic testing of smartphone apps", the ACM SIGSOFT 20th I nternational Symposium on the Foundations of Software Engineering (FSE '12), article no. 59, November 2012

MS2: Scalable vs non-scalable video coding for mobile video in practice

Tutor: Matti Siekkinen

Scalable Video Coding (SVC) is a decade old video coding solution for flexible quality selection over bandwidth varying communication paths. The basic idea is that SVC produces a layered video that allows choosing the video stream playback quality by downloading a specific number of layers: base layer provides lowest quality and downloading additional layers improves the video quality proportionally. Although SVC has been around for a long time, it appears to be less used than non-scalable coding in which a single video is transcoded into multiple versions (beforehand or in real time). However, there is now a renewed interest for SVC as quality adaptive streaming (DASH) is taking over mobile video streaming. The objective of this work is to study the pros and cons of the two approaches (e.g. computational complexity, coding and storage and bandwidth overheads) with a special focus on mobile video streaming. Also exploration of the usage of the two approaches in real mobile video services is part of the work.

References:

- Heiko Schwarz, Detlev Marpe, and Thomas Wiegand, "Overview of the Scalable Video Coding Extension of the H.264/AVC Standard", IEEE Transactions on Circuits and Systems for Video Technology, 17(9):1103–1120, September 2007
- Travis Andelin, Vasu Chetty, Devon Harbaugh, Sean Warnick, and Daniel Zappala, "Quality Selection for Dynamic Adaptive Streaming over HTTP with Scalable Video Coding", the 3rd Multimedia Systems Conference (MMSys '12), pp. 149–154, February 2012

NH1: Virtual machine consolidation with multi-resource usage prediction

Tutor: Nguyen Trung Hieu

Consolidation of virtual machines (VM) on the minimum number of physical servers is an efficient solution to reduce the power consumption. However, most of the existing solution rely on eager migration of VMs, thus resulting in unnecessarily migrations. These solutions increases the energy that includes the VM migration cost on the source and destination hosts and extra traffic volume that generated from VM migration. The focus of this topic is predicting short-time future utilization including multiple types of resources based on the past history of resource usage in each host. The current and predicted utilization metrics are then used as the main criterion to: decide when a physical server is considered to be overloaded, so that some already placed VMs should be migrated to improve the quality of provided services; decide when a physical server is considered to be underloaded, so that all the already placed VMs should be migrated for energy efficiency. The student involved in this topic is expected to: learn the basics of VM consolidation; survey the forecasting paradigms to predict the short-time future utilization; review the relevant metrics proposed in the literature to determine overload and underload of physical resources; eventually, characterize the performance of proposed solution in term of energy consumption and number of VM migrations by simulation using CloudSim toolkit.

References:

- Zhen Xiao, Weijia Song, and Qi Chen, "Dynamic Resource Allocation Using Virtual Machines for Cloud Computing Environment", IEEE Transactions on Parallel and Distributed Systems, 24(6):1107-1117, June 2013
- Anton Beloglazov, and Rajkumar Buyya, "Optimal Online Deterministic Algorithms and Adaptive Heuristics for Energy and Performance Efficient Dynamic Consolidation of Virtual Machines in Cloud Data Centers", Concurrency and Computation: Practice and Experience (CCPE), 24(13): 1397-1420, John Wiley & Sons, Ltd, New York, USA, 2012

OH1: User authentication or identification through heartbeat sensing

Tutor: Otto Huhta

Despite years of research into various alternative authentication methods, passwords still remain the most common method when authenticating ourselves to devices and services. However, as wearable devices become cheaper and more interconnected, efforts are being made to leverage their capabilities for seamless authentication. Various wearable heart rate monitors have been available for a long time, but with more sophisticated models, interest for using one's heartbeat for authentication has been renewed for both industry and academia (e.g., Bionym Nymi, Apple, Intel). The student involved in this seminar topic is supposed to look at the security and usability aspects of using heartbeat information for user authentication or identification. More specifically, the goal of the work is to look into how such information can be effectively used to identify an individual, how reliable heartbeat monitoring is as an authentication method, and what are the potential vulnerabilities.

References:

- Sufi, Fahim, Ibrahim Khalil, and Jiankun Hu. "ECG-based authentication", Handbook of Information and Communication Security. Springer Berlin Heidelberg, 2010. 309-331.
- Guha Balakrishnan, Fredo Durand, and John Guttag, "Detecting pulse from head motions in video", the 26th IEEE Conference on Computer Vision and Pattern Recognition (CVPR '13), June 2013
- Bionym Nymi

RB1: Proximity services using device-to-device communication

Tutor: Ravishankar Borgaonkar

As LTE Advanced is evolving, it is opening new frontiers for Device-to-Device (D2D) communication and proximity services (Prose). LTE D2D allows devices to communicate and provide services within a proximity radius of 500 m, unlike in existing Bluetooth, NFC, and WiFi technologies. Qualcomm has recently introduced LTE Direct to enable mobile subscribers to employ proximity services using D2D communication. The new features of this technologies are privacy sensitive and allow battery-efficient discovery of thousands of devices and services. The platform also enables new services for mobile network operators such as national security and public safely. The student involved in this topic is expected to: provide a detailed overview of proximity services using D2D communication; compare them with existing D2D communication technologies from the privacy perspective; analyze potential privacy issues from the point of view of the end users.

References:

- Qualcomm Technologies, "LTE Direct Always-on Device-to-Device Proximal Discovery", August 2014
- Gabor Fodor, Stefan Parkvall, Stefano Sorrentino, Pontus Wallentin, Qianxi Lu, and Nadia Brahmi, "Device-to-Device Communications for National Security and Public Safety", IEEE Access, 2:1510–1520, December 2014
- Xingqin Lin, Jeffrey G. Andrews, Amitabha Ghosh, and Rapeepat Ratasuk, "An Overview of 3GPP Device-to-Device Proximity Services", IEEE Communications Magazine, 52(4):40–48, April 2014

SL1: Software market of network functions virtualization

Tutor: Sakari Luukkainen

Cloud computing has become an important architecture in today's ICT sector. The telecommunications industry considers introducing the cloud approach to mobile networks, because the usage of dedicated network hardware is a significant cost source. In that approach, the network functions would be implemented in software and provided on top of cheap computing and networking hardware. The introduction of open cloud technologies to the mobile networks would enable a new market for virtualized network functions solutions. The goal of this study is to analyze business models of future software companies in this emerging market.

References:

- http://www.etsi.org/technologies-clusters/technologies/nfv
- https://www.sdncentral.com/education/sdn-nfv-dramatically-increasing-importance-networking-ecosystem/2014/11/
- https://www.sdncentral.com/education/open-networking-ecosystem-for-the-sdn-nfv-era/2014/12/

SS1: MOOCs and authentication

Tutor: Sanna Suoranta

Many top level universities are offering Massive Open Online courses (MOOCs). For example, MIT (Massachusetts Institute of Technology) and University of Harvard offer their courses using EdX and University of Stanford and École Polytechnique Fédérale de Lausanne offer their courses in Coursera. Also Aalto University offers MOOC courses. These courses pave the way to learn about university-level courses even for people that are not enrolled in the related programs. There are two types of courses: courses with a timetable given by a teacher and courses that can be taken any time. Participation often requires that students complete some assignments that are usually automatically graded in a learning environment. After the successful participation in a course, students may get a certificate. But who was the student? This is an essential issue if the student can get a right to complete a degree based on previous studies in an open university, as it is possible in some Finnish universities. Thus, the identity of the student must be verified from a trustworthy source. Maybe also during the course assignments the student should be authenticated. What kind of authentication systems do the currently used MOOCs have? What needs to be done next?

References:

- Jorge Miguel, Santi Caballé, and Josep Prieto, "Providing Information Security to MOOC: Towards Effective Student Authentication", the 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS '13), pp. 289-292, September 2013
- Markus Krause, "A behavioral biometrics based authentication method for MOOC's that is robust against imitation attempts", the first ACM conference on Learning @ scale (L@S '14), pp. 201-202, March 2014

SS2: Biometric authentication

Tutor: Sanna Suoranta

Biometric authentication is considered by many as the definitive solution for authentication, since it saves users from the password fatigue. For instance, fingerprints and eyes' retina are considered to be unique enough to be used for authentication purposes. To this end, fingerprints are scanned at the border control in several countries, including the USA. Biometric information for identification, such as a picture of the face and fingerprints, are added to the smart card embedded in passports. In recent years, several manufacturers (including IBM, Motorola and Apple) have added fingerprint readers to laptop computers and mobile phones. However, there are severe problems with biometric authentication: fingerprints cannot be changed but they are left on all surfaces and objects touched. Crackers have claimed that they can easily break the biometric authentication of mobile phones. What does the research community think about biometric authentication today?

References:

- James Wayman, Anil Jain, Davide Maltoni, and Dario Maio, "An Introduction to Biometric Authentication Systems", Chapter 1 in Biometric Systems, pp. 1-20, 2005
- Nathan Clarke and Steven Furnell, "Authentication of users on mobile telephones – A survey of attitudes and practices", Computers & Security, 24 (7):519–527, October 2005
- David Meyer, "The Risks of the IPhone Fingerprint Lock", Bloomberg Businessweek Technology, 23 September 2013
- http://www.bbc.com/news/technology-30623611

SS3: Password management

Tutor: Sanna Suoranta

According to Florêncio, every days users log in to eight services that use password as authentication method. Such services require unique and long passwords which are difficult to remember. Web browsers offer to remember the passwords on behalf of the user. There are also password management applications available both on mobile devices and computer environments, both commercial and open-source. However, many security expert avoid using such services and prefer coding their own solution. In this work, the student should survey password managers and evaluate their security.

References:

- Dinei Florêncio and Cormac Herley, "A large-scale study of web password habits", the 16th international conference on World Wide Web (WWW '07), pp. 657-666, May 2007
- Ambarish Karole, Nitesh Saxena, and Nicolas Christin, "A Comparative Usability Evaluation of Traditional Password Managers", the 13th International Conference on Information Security and Cryptology (ICISC 2010), pp. 233-251, December 2011
- Dinei Florêncio, Cormac Herley, and Paul C. van Oorschot, "Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts", the 23rd USENIX Security Symposium, August 2014

SS4: ICT as enabler for energy behavioral change

Tutor: Sanja Šepanovi

Recent research and practical efforts have increased on how ICT tools can best influence behavioral change when it comes to energy spending habits. The focus of such research has so far been mostly on improving energy efficiency (and conservation) by influencing individuals or communities. More limited are research efforts on changing the consumption patterns (time of use of energy), which becomes one of the most important challenges in new smart energy systems due to the introduction of more renewable sources. Besides solutions involving both software and hardware, in particular in the context of Internet of Things and Smart Home communication trends, studies involving user feedback are less frequent, while very important. Gamification is expected to be important as well in this context. Furthermore, some business solutions are already in place, such as Opower, and are capable of delivering promising results in practice. The student is expected to prepare a well structured review of the current research and industry solutions. The work prepared for this seminar topic is relevant as part of EU Civis project.

References:

- Antimo Barbato, Luca Borsani, Antonio Capone, and Stefano Melzi, "Home energy saving through a user profiling system based on wireless sensors", the First ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings (BuildSys '09), pp. 49-54, 2009
- Dario Bonino, Fulvio Corno, and Luigi De Russis, "Home energy consumption feedback: A user survey", Energy and Buildings, 47:383-393, April 2012
- Friedemann Mattern, Thorsten Staake, and Markus Weiss, "ICT for green: how computers can help us to conserve energy", the 1st International Conference on Energy-Efficient Computing and Networking (e-Energy '10), pp. 1-10 2010
- Sami Karjalainen, "Consumer preferences for feedback on household electricity consumption", Energy and Buildings, 43(2–3):458-467, February–March 2011

SS5: Security and privacy in smart energy communities

Tutor: Sanja Šepanovi

The energy system is expectedly approaching the largest transformation since its beginning. The EU commission aims to achieve 80% smart grid coverage by 2020, and many countries are rolling out smart meters implementation at a large scale (in Finland currently close to 100% of the households are supplied with smart meters). The data from smart meters and smart sensors are intended for use in decisions in automation system in the context of Smart Homes.

While building and implementing such solutions, it is vital to consider privacy and security concerns. The questions range from the data security (that can impact individual user privacy and energy distribution), to intelligent operations in the grid (that can directly or indirectly harm the users or cause inconvenience). Finally, malicious users taking part in the smart grid ICT solutions and pretending to be cooperative may cause most unconventional and perhaps unpredictable types of issues.

In this seminar paper, the student is expected to prepare a comparative study of current research and practical studies on security and privacy in the context of smart grid ICT solutions with particular focus on the hackers pretending to be a part of the energy community. A question to address is to which extent reputation-type of trust that functions well in other domains (such as expertise, e.g. Stack Overflow or marketplaces services, e.g. eBay) shows to be resilient to such malicious users in the energy system context. The work prepared for this seminar topic is relevant as part of EU Civis project.

References:

- http://www.smartgrids.ch/sgeranetplus/docs/event2/20130514%20Jan%20Segerstam.pdf
- Tassos Dimitriou and Ghassan Karame. 2014. Privacy-Friendly Planning of Energy Distribution in Smart Grids. In Proceedings of the 2nd Workshop on Smart Energy Grid Security (SEGS '14). ACM, New York, NY, USA, 1-6. http://doi.acm.org/10.1145/2667190.2667191
- Henrique Dantas, Zekeriya Erkin, Christian Doerr, Raymond Hallie, and Gerrit van der Bij. 2014. eFuzz: A Fuzzer for DLMS/COSEM Electricity Meters. In Proceedings of the 2nd Workshop on Smart Energy Grid Security (SEGS '14). ACM, New York, NY, USA, 31-38. http://doi.acm.org/10.1145/2667190.2667194
- http://www.mtu.edu/news/stories/2015/january/hackers-could-make-smart-homes-stupid-or-worse.html

ST1: Secure Instant messaging

Tutor: Sandeep Tamrakar

Instant messaging (IM) is the most widely used communication over the Internet generally used for sending short messages. Popular IMs communicates over TLS to protect against eavesdropping yet the TLS does not guarantee against eavesdropping at the server end. There are number of IM services that provides end-to-end secure messaging such as TextSecure. Similarly BitTorrent recently released decentralized private chat application known as Bleep. Off-the-record messaging protocol developed by Goldberg et. al. [1] describe secure messaging protocol with deniability, which ensures the authenticity of the message during communication yet it allows anyone to forge messages after the conversation that look like they were real communication between the participants.

The goal of this work is to look at different secure IM services and protocols, and make a survey based on the security features that these IM offers.

References:

- Borisov, Nikita, Ian Goldberg, and Eric Brewer. "Off-the-record communication, or, why not to use PGP." Proceedings of the 2004 ACM workshop on Privacy in the electronic society. ACM, 2004.
- Bleep: private chat
- TextSecure

TN1: Survey of security-enhanced linux policy analysis techniques

Tutor: Thomas Nyman

Security Enhanced Linux (SELinux) is an implementation of Mandatory Access Control (MAC) for Linux. SELinux allows system administrators to define policies for how processes and users are allowed to access system resources, such as files, devices and Inter Process Communication (IPC) primitives. The centralized SELinux policy is more amenable to analysis compared to highly distributed policies, such as traditional Unix file system permissions. However, the increased expressibility and large size of SELinux policies make such analysis often a daunting task. Widely used tools for SELinux policy analysis include the open source SETools suite developed by Tresys technologies. The topic has also received some attention in the academic community, and several more sophisticated analysis techniques have been proposed. The goal of this seminar topic is a survey of different approaches to SELinux policy analysis. Ambitious students should aim to identify potential gaps in the current state of the art and open research problems in the area. Prior skills required: Basic knowledge of the SELinux policy language is highly recommended.

References:

- SETools v3 – Policy Analysis Tools for SELinux
- Peter Amthor, Winfried E. Kühnhauser, Anja Pölck, "Model-based safety analysis of SELinux security policies", the 5th International Conference on Network and System Security (NSS '11), pp. 208–215, September 2011
- Said Marouf and Mohamed Shehab, "SEGrapher: Visualization-based SELinux policy analysis", the 4th Symposium on Configuration Analytics and Automation (SAFECONFIG '11), pp.1–8, October 2011
- Patrice Clemente, Bangaly Kaba, Jonathan Rouzaud-Cornabas, Marc Alexandre, and Guillaume Aujay, "SPTrack: Visual Analysis of Information Flows within SELinux Policies and Attack Logs", 8th International Conference on Active Media Technology (AMT '12), pp 596–605, December 2012

ZO1: How dense are cell towers? An experimental study of cell tower deployment

Tutor: Zhonghong Ou

More and more cell towers are deployed to provide better throughput and quality for mobile users. It is interesting to analyze how dense cell towers are deployed, how big coverage a single tower can provide, and whether different mobile phones will connect to different cell towers from the same location. In this task, the student is required to conduct experiments on different locations of the large-Helsinki area (including city center, and other suburban areas). The signal collecting software is available, but may need to be revised slightly; the student is mostly expected to collect the data and analyze them to get different kinds of statistics.

References: not available.

ZO2: Simulation tools for wireless sensor network

Tutor: Zhonghong Ou

Nowadays Wireless Sensor Networks (WSNs) play a pivotal role in the Internet of Things. However, building a WSN testbed is often costly, and running real experiments is always time-consuming. Therefore, simulation tools are very important for WSN development. With its help, protocols, algorithms, or even new applications can be validated or evaluated in a large scale, which is more economic and efficient than running them in a testbed. Several simulation tools are currently available for WSNs. The task of the student is to choose one of them as an example to make a deeper understanding of what are its internal mechanisms and how it works in practice. As part of the task, the student is also expected to run some experiments and investigate the resource utilization, including CPU and memory, simulation time, or any other indicators for performance evaluation purposes.

References:

- Harsh Sundani, Haoyue Li, Vijay K. Devabhaktuni, Mansoor Alam, and Prabir Bhattacharya, "Wireless sensor network simulators a survey and comparisons", International Journal of Computer Networks 2(5):249–265, 2010
- E. Egea-Lopez, J. Vales-Alonso, A. S. Martinez-Sala, P. Pavon-Marino, and J. Garcia-Haro, "Simulation Tools for Wireless Sensor Networks", Summer Simulation Multiconference SPECTS, 2005, pp. 2–9, 2005
- Jevti, Miloš, Nikola Zogovi, and Goran Dimi, "Evaluation of wireless sensor network simulators", the 17th Telecommunications Forum (TELFOR '09), 2009