Community Targeted Phishing: A Middle Ground Between Massive and Spear Phishing Through Natural Language Generation

Looking at today phishing panorama, we are able to identify two diametrically opposed approaches. On the one hand, massive phishing targets as many people as possible with generic and preformed texts. On the other hand, spear phishing targets high-value victims with hand-crafted emails. While nowadays these two worlds partially intersect, we envision a future where Natural Language Generation (NLG) techniques will enable attackers to target populous communities with machine-tailored emails. In this paper, we introduce what we call Community Targeted Phishing (CTP), alongside with some workflows that exhibit how NLG techniques can craft such emails. Furthermore, we show how Advanced NLG techniques could provide phishers new powerful tools to bring up to the surface new information from complex data-sets, and use such information to threaten victims' private data.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Örebro University
Corresponding author: Giaretta, A.
Contributors: Giaretta, A., Dragoni, N.
Pages: 86-93
Publication date: 1 Jan 2020

Host publication information
Title of host publication: Proceedings of 6th International Conference in Software Engineering for Defence Applications - SEDA 2018
Publisher: Springer
Editors: Ciancarini, P., Mazzara, M., Messina, A., Sillitti, A., Succi, G.
ISBN (Print): 9783030146863
(Advances in Intelligent Systems and Computing, Vol. 925).
Keywords: Natural Language Generation, NLG, Phishing, Security
DOIs: 10.1007/978-3-030-14687-0_8
Source: Scopus
Source ID: 85064148058
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2020 › Research › peer-review
Vulnerabilities and Security Breaches in Cryptocurrencies
Nowadays, 1375 different cryptocurrencies exist, and their market value totals up to $444.8 billion, at the time of writing. The interest revolving around cryptocurrencies is constantly growing, and this hype caused an increase of criminal attacks on various cryptocurrencies. In this paper, we cover the main aspects that concern cryptocurrencies vulnerabilities and related security breaches. Then, we propose possible solutions to prevent them, or to decrease the attackers’ profit margins by increasing the costs they have to face, in order to strike some of these attacks. Alongside, we briefly describe a few attacks that have occurred in the past.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Technical University of Denmark, Örebro University
Corresponding author: Giaretta, A.
Contributors: Sigurdsson, G., Giaretta, A., Dragoni, N.
Pages: 288-299
Publication date: 1 Jan 2020

Host publication information
Title of host publication: Proceedings of 6th International Conference in Software Engineering for Defence Applications - SEDA 2018
Publisher: Springer
Editors: Mazzara, M., Messina, A., Sillitti, A., Succi, G., Ciancarini, P.
ISBN (Print): 9783030146863
(Advances in Intelligent Systems and Computing, Vol. 925).
DOIs: 10.1007/978-3-030-14687-0_26
Source: Scopus
Source ID: 85064149824

When the Price Is Your Privacy: A Security Analysis of Two Cheap IoT Devices
The Internet of Things (IoT) is shaping a world where devices are increasingly interconnected, cheaper, and ubiquitous. The more we move toward this world, the more cybersecurity becomes paramount. Nevertheless, we argue that there exists a category of IoT devices which commonly overlooks security, despite dealing with sensitive information. In order to demonstrate this, in this work, we present the results of the security assessments we performed on two IoT devices that we consider emblematic of such category: the Rohs K88h smartwatch and the Sricam SP009 IP camera. The results demonstrate the existence of critical vulnerabilities that could be easily exploited, even by non-expert attackers, for extracting sensitive information and severely impacting on user’s privacy.

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Applied Mathematics and Computer Science, Technical University of Denmark
Corresponding author: Dragoni, N.
Contributors: Favaretto, M., Tran Anh, T., Kavaja, J., De Donno, M., Dragoni, N.
Pages: 55-75
Publication date: 1 Jan 2020

Host publication information
Title of host publication: Proceedings of 6th International Conference in Software Engineering for Defence Applications - SEDA 2018
Publisher: Springer
Editors: Mazzara, M., Messina, A., Sillitti, A., Succi, G., Ciancarini, P.
ISBN (Print): 9783030146863
(Advances in Intelligent Systems and Computing, Vol. 925).
DOIs: 10.1007/978-3-030-14687-0_6
Source: Scopus
Source ID: 85064156900
Cyber-storms come from clouds: Security of cloud computing in the IoT era
The Internet of Things (IoT) is rapidly changing our society to a world where every “thing” is connected to the Internet, making computing pervasive like never before. This tsunami of connectivity and data collection relies more and more on the Cloud, where data analytics and intelligence actually reside. Cloud computing has indeed revolutionized the way computational resources and services can be used and accessed, implementing the concept of utility computing whose advantages are undeniable for every business. However, despite the benefits in terms of flexibility, economic savings, and support of new services, its widespread adoption is hindered by the security issues arising with its usage. From a security perspective, the technological revolution introduced by IoT and Cloud computing can represent a disaster, as each object might become inherently remotely hackable and, as a consequence, controllable by malicious actors. While the literature mostly focuses on the security of IoT and Cloud computing as separate entities, in this article we provide an up-to-date and well-structured survey of the security issues of cloud computing in the IoT era. We give a clear picture of where security issues occur and what their potential impact is. As a result, we claim that it is not enough to secure IoT devices, as cyber-storms come from Clouds.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Örebro University, Fondazione Bruno Kessler, Innopolis University
Corresponding author: Bucchiarone, A.
Contributors: De Donno, M., Giaretta, A., Dragoni, N., Bucchiarone, A., Mazzara, M.
Publication date: 1 Jun 2019
Peer-reviewed: Yes

Publication information
Journal: Future Internet
Volume: 11
Issue number: 6
Article number: 127
ISSN (Print): 1999-5903
Ratings:
Web of Science (2019): Indexed yes
Original language: English
Keywords: Cloud computing, Internet of Things, Security
Electronic versions:
futureinternet_11_00127.pdf
DOIs:
10.3390/fi11060127
Source: Scopus
Source ID: 85067464961
Research output: Contribution to journal › Journal article – Annual report year: 2019 › Research › peer-review

BitFlow: Enabling real-time cash-flow evaluations through blockchain
Disbursement registration has always been a cumbersome, opaque, and inefficient process, up to the point that most businesses perform cash-flow evaluations only on a quarterly basis. We believe that automatic cash-flow evaluations can actively mitigate these issues. In this paper, we present BitFlow, a blockchain-based architecture that provides complete cash-flow transparency and diminishes the probability of undetected frauds through the BitKrone, a non-volatile cryptocurrency that maps to the Danish Krone (DKK). We show that confidentiality can be effectively achieved on a permissionless blockchain using Zero-Knowledge proofs, ensuring verifiable transfers and automatic evaluations. Furthermore, we discuss several experiments to evaluate our proposal, in particular, the impact that confidential transactions have on the whole system, in terms of responsiveness and from an economical expenditure perspective.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Technical University of Denmark, Örebro University
Corresponding author: Dragoni, N.
Contributors: Herskind, L., Giaretta, A., De Donno, M., Dragoni, N.
Number of pages: 14
Publication date: 1 Jan 2019
Peer-reviewed: Yes

Publication information
Journal: Concurrency Computation
Combining antibiotic with fog computing: Antibiotic 2.0

The Internet of Things (IoT) has been one of the key disruptive technologies over the last few years, with its promise of optimizing and automating current manual tasks and evolving existing services. From the security perspective, the increasing adoption of IoT devices in all aspects of our society has exposed businesses and consumers to a number of threats, such as Distributed Denial of Service (DDoS) attacks. Along the way, Fog computing was born: a novel paradigm that aims at bridging the gap between IoT and Cloud computing, providing a number of benefits, including security. As a result, in this paper, we present Antibiotic 2.0, an anti-malware that relies upon Fog computing to secure IoT devices and to overcome the main issues of its predecessor (AntibioTic 1.0). In particular, we discuss the design and implementation of the system, including possible models for deployment, security assumptions, interaction among system components, and possible modes of operation.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Technical University of Denmark
Contributors: De Donno, M., Dragoni, N.
Number of pages: 6
Publication date: 2019
Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog

In the last few years, Internet of Things, Cloud computing, Edge computing, and Fog computing have gained a lot of attention in both industry and academia. However, a clear and neat definition of these computing paradigms and their correlation is hard to find in the literature. This makes it difficult for researchers new to this area to get a concrete picture of these paradigms. This work tackles this deficiency, representing a helpful resource for those who will start next. First, we show the evolution of modern computing paradigms and related research interest. Then, we address each paradigm, neatly delineating its key points and its relation with the others. Thereafter, we extensively address Fog computing, remarking its outstanding role as the glue between IoT, Cloud, and Edge computing. In the end, we briefly present open challenges and future research directions for IoT, Cloud, Edge, and Fog computing.

Protecting the Internet of Things with Security-by-Contract and Fog Computing

Nowadays, the Internet of Things (IoT) is a consolidated reality. Smart homes are equipped with a growing number of IoT devices that capture more and more information about human beings lives. However, manufacturers paid little or no attention to security, so that various challenges are still in place. In this paper, we propose a novel approach to secure IoT systems that combines the concept of Security-by-Contract (S×C) with the Fog computing distributed paradigm. We define the pillars of our approach, namely the notions of IoT device contract, Fog node policy and contract-policy matching, the respective life-cycles, and the resulting S×C workflow. To better understand all the concepts of the S×C framework, and highlight its practical feasibility, we use a running case study based on a context-aware system deployed in a real smart home.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Örebro University, University of Trento
Contributors: Giaretta, A., Dragoni, N., Massacci, F.
Pages: 1-6
Publication date: 2019
Towards a Systematic Survey of Industrial IoT Security Requirements: Research Method and Quantitative Analysis

Industry 4.0 and, in particular, Industrial Internet of Things (IIoT) represent two of the major automation and data exchange trends of the 21st century, driving a steady increase in the number of smart embedded devices used by industrial applications. However, IoT devices suffer from numerous security flaws, resulting in a number of large scale cyber-attacks. In this light, Fog computing, a relatively new paradigm born from the necessity of bridging the gap between Cloud computing and IoT, can be used as a security solution for the IIoT. To achieve this, the first step is to clearly identify the security requirements of the IIoT that can be subsequently used to design security solutions based on Fog computing. With this in mind, our paper represents a preliminary work towards a systematic literature review of IIoT security requirements. We focus on two key steps of the review: (1) the research method that will be used in the systematic work and (2) a quantitative analysis of the results produced by the study selection process. This lays the necessary foundations to enable the use of Fog computing as a security solution for the IIoT.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Technical University of Denmark
Corresponding author: Tange, K. P.
Contributors: Tange, K. P., De Donno, M., Fafoutis, X., Dragoni, N.
Number of pages: 8
Pages: 56-63
Publication date: 2019

Adding salt to pepper a structured security assessment over a humanoid robot: A Structured Security Assessment over a Humanoid Robot

The rise of connectivity, digitalization, robotics, and artificial intelligence (AI) is rapidly changing our society and shaping its future development. During this technological and societal revolution, security has been persistently neglected, yet a hacked robot can act as an insider threat in organizations, industries, public spaces, and private homes. In this paper, we perform a structured security assessment of Pepper, a commercial humanoid robot. Our analysis, composed by an automated and a manual part, points out a relevant number of security flaws that can be used to take over and command the robot. Furthermore, we suggest how these issues could be fixed, thus, avoided in the future. The very final aim of this work is to push the rise of the security level of IoT products before they are sold on the public market.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Örebro University
Contributors: Giaretta, A., De Donno, M., Dragoni, N.
Publication date: 2018
Analysis and Evaluation of SafeDroid v2.0, a Framework for Detecting Malicious Android Applications

Android smartphones have become a vital component of the daily routine of millions of people, running a plethora of applications available in the official and alternative marketplaces. Although there are many security mechanisms to scan and filter malicious applications, malware is still able to reach the devices of many end-users. In this paper, we introduce the SafeDroid v2.0 framework, that is a flexible, robust, and versatile open-source solution for statically analysing Android applications, based on machine learning techniques. The main goal of our work, besides the automated production of fully sufficient prediction and classification models in terms of maximum accuracy scores and minimum negative errors, is to offer an out-of-the-box framework that can be employed by the Android security researchers to efficiently experiment to find effective solutions: the SafeDroid v2.0 framework makes it possible to test many different combinations of machine learning classifiers, with a high degree of freedom and flexibility in the choice of features to consider, such as dataset balance and dataset selection. The framework also provides a server, for generating experiment reports, and an Android application, for the verification of the produced models in real-life scenarios. An extensive campaign of experiments is also presented to show how it is possible to efficiently find competitive solutions: the results of our experiments confirm that SafeDroid v2.0 can reach very good performances, even with highly unbalanced dataset inputs and always with a very limited overhead.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Sapienza - Università di Roma, Technical University of Denmark
Corresponding author: Spognardi, A.
Contributors: Argyriou, M., Dragoni, N., Spognardi, A.
Number of pages: 15
Publication date: 2018
Peer-reviewed: Yes

Publication information
Journal: Security and Communication Networks
Volume: 2018
Article number: 4672072
ISSN (Print): 1939-0114
Ratings:
Scopus rating (2018): CiteScore 1.81 SJR 0.311 SNIP 0.862
Web of Science (2018): Impact factor 1.376
Web of Science (2018): Indexed yes
Original language: English
Electronic versions:
4672072.pdf
DOIs:
10.1155/2018/4672072
Source: FindIt
Source ID: 2438890818
Research output: Contribution to journal > Journal article – Annual report year: 2018 > Research > peer-review

AntibIoTic: Protecting IoT Devices Against DDoS Attacks

The 2016 is remembered as the year that showed to the world how dangerous Distributed Denial of Service attacks can be. Gauge of the disruptiveness of DDoS attacks is the number of bots involved: the bigger the botnet, the more powerful the attack. This character, along with the increasing availability of connected and insecure IoT devices, makes DDoS and IoT the perfect pair for the malware industry. In this paper we present the main idea behind AntibIoTic, a palliative solution to prevent DDoS attacks perpetrated through IoT devices.
DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation

The Internet of Things (IoT) revolution has not only carried the astonishing promise to interconnect a whole generation of traditionally "dumb" devices, but also brought to the Internet the menace of billions of badly protected and easily hackable objects. Not surprisingly, this sudden flooding of fresh and insecure devices fueled older threats, such as Distributed Denial of Service (DDoS) attacks. In this paper, we first propose an updated and comprehensive taxonomy of DDoS attacks, together with a number of examples on how this classification maps to real-world attacks. Then, we outline the current situation of DDoS-enabled malwares in IoT networks, highlighting how recent data support our concerns about the growing in popularity of these malwares. Finally, we give a detailed analysis of the general framework and the operating principles of Mirai, the most disruptive DDoS-capable IoT malware seen so far.
From Monolithic to Microservices An Experience Report from the Banking Domain

Microservices have seen their popularity blossoming with an explosion of concrete applications in real-life software. Several companies are currently involved in a major refactoring of their back-end systems in order to improve scalability. This article presents an experience report of a real-world case study, from the banking domain, in order to demonstrate how scalability is positively affected by reimplementing a monolithic architecture into microservices. The case study is based on the FX Core system for converting from one currency to another. FX Core is a mission-critical system of Danske Bank, the largest bank in Denmark and one of the leading financial institutions in Northern Europe.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Vienna University of Technology, Danske Bank Group, IRST Fondazione Bruno Kessler, Innopolis University
Contributors: Bucchiarone, A., Dragoni, N., Dustdar, S., Larsen, S. T., Mazzara, M.
Pages: 50-55
Publication date: 2018
Peer-reviewed: Yes

Publication information
Journal: IEEE Software
Volume: 35
Issue number: 3
ISSN (Print): 0740-7459
Ratings:
BFI (2018): BFI-level 2
Scopus rating (2018): CiteScore 3.34 SJR 0.549 SNIP 2.272
Web of Science (2018): Impact factor 2.945
Web of Science (2018): Indexed yes
Original language: English
Electronic versions:
fulltext
DOIs:
10.1109/MS.2018.2141026
Source: FindIt
Source ID: 2434638122
Research output: Contribution to journal › Journal article – Annual report year: 2018 › Research › peer-review

Joining Jolie to Docker Orchestration of Microservices on a Containers-as-a-Service Layer

Cloud computing is steadily growing and, as IaaS vendors have started to offer pay-as-you-go billing policies, it is fundamental to achieve as much elasticity as possible, avoiding over-provisioning that would imply higher costs. In this paper, we briefly analyse the orchestration characteristics of PaaS/OA, a proposed architecture already implemented for Jolie microservices, and Kubernetes, one of the various orchestration plugins for Docker; then, we outline similarities and differences of the two approaches, with respect to their own domain of application. Furthermore, we investigate some ideas to achieve a federation of the two technologies, proposing an architectural composition of Jolie microservices on Docker Container-as-a-Service layer.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Innopolis University, Örebro University
Contributors: Giaretta, A., Dragoni, N., Mazzara, M.
Number of pages: 9
Pages: 167-175
Publication date: 2018

Host publication information
Title of host publication: Proceedings of 5th International Conference in Software Engineering for Defence Applications: SEDA 2016
Publisher: Springer
ISBN (Print): 978-3-319-70577-4
ISBN (Electronic): 978-3-319-70578-1
Electronic versions:
Microservices: How to make your application scale

The microservice architecture is a style inspired by service-oriented computing that has recently started gaining popularity and that promises to change the way in which software is perceived, conceived and designed. In this paper, we describe the main features of microservices and highlight how these features improve scalability.

Analysis of DDoS-capable IoT malwares

The Internet of Things (IoT) revolution promises to make our lives easier by providing cheap and always connected smart embedded devices, which can interact on the Internet and create added values for human needs. But all that glitters is not gold. Indeed, the other side of the coin is that, from a security perspective, this IoT revolution represents a potential disaster. This plethora of IoT devices that flooded the market were very badly protected, thus an easy prey for several families of malwares that can enslave and incorporate them in very large botnets. This, eventually, brought back to the top Distributed Denial of Service (DDoS) attacks, making them more powerful and easier to achieve than ever. This paper aims at provide an up-to-date picture of DDoS attacks in the specific subject of the IoT, studying how these attacks work and considering the most common families in the IoT context, in terms of their nature and evolution through the years. It also explores the additional offensive capabilities that this arsenal of IoT malwares has available, to mine the security of Internet users and systems. We think that this up-to-date picture will be a valuable reference to the scientific community in order to take a first crucial step to tackle this urgent security issue.
A taxonomy of distributed denial of service attacks
The Internet of Things revolution promises to make our lives much easier by providing us cheap and convenient smart devices, but all that glitters is not gold. This plethora of devices that flooded the market, generally poorly designed with respect to security aspects, brought back to the top Distributed Denial of Service (DDoS) attacks which are now even more powerful and easier to achieve than the past. Understanding how these attacks work, in all their different forms, represents a first crucial step to tackle this urgent issue. To this end, in this paper we propose a new up-to-date taxonomy and a comprehensive classification of current DDoS attacks.

Microservices: Yesterday, Today, and Tomorrow
Microservices is an architectural style inspired by service-oriented computing that has recently started gaining popularity. Before presenting the current state of the art in the field, this chapter reviews the history of software architecture, the reasons that led to the diffusion of objects and services first, and microservices later. Finally, open problems and future challenges are introduced. This survey primarily addresses newcomers to the discipline, while offering an academic viewpoint on the topic. In addition, we investigate some practical issues and point out a few potential solutions.
Security And Privacy Issues in Healthcare Monitoring Systems: A Case Study

Security and privacy issues are rarely taken into account in automated systems for monitoring elderly people in their home, exposing inhabitants to a number of threats they are usually not aware of. As a case study to expose the major vulnerabilities these systems are exposed to, this paper reviews a generic example of automated healthcare monitoring system. The security and privacy issues identified in this case study can be easily generalised and regarded as alarm bells for all the pervasive healthcare professionals.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Copenhagen Center for Health Technology, Embedded Systems Engineering, Technical University of Denmark
Contributors: Handler, D. T., Hauge, L., Spognardi, A., Dragoni, N.
Pages: 383-388
Publication date: 2017

Host publication information
Title of host publication: Proceedings of the 10th International Joint Conference on Biomedical Engineering Systems and Technologies
Volume: 5
Publisher: SCITEPRESS Digital Library
ISBN (Print): 9789897582134
Electronic versions: HEALTHINF_2017_84.pdf
DOIs: 10.5220/0006224603830388
Source: FindIt
Source ID: 2392771503

Security flows in OAuth 2.0 framework: A case study

The burst in smartphone use, handy design in laptops and tablets as well as other smart products, like cars with the ability to drive you around, manifests the exponential growth of network usage and the demand of accessing remote data on a large variety of services. However, users notoriously struggle to maintain distinct accounts for every single service that they use. The solution to this problem is the use of a Single Sign On (SSO) framework, with a unified single account to authenticate userâ€™s identity throughout the different services. In April 2007, AOL introduced OpenAuth framework. After several revisions and despite its wide adoption, OpenAuth 2.0 has still several flaws that need to be fixed in several implementations. In this paper, we present a thorough review about both benefits of this single token authentication mechanism and its open flaws.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Technical University of Denmark
Contributors: Argyriou, M., Dragoni, N., Spognardi, A.
Pages: 396-406
Publication date: 2017

Host publication information
Publisher: Springer
Keywords: Theoretical Computer Science, Computer Science (all), Computer Science, Logics and Meanings of Programs, Programming Languages, Compilers, Interpreters, Software Engineering, Systems and Data Security, Computer Applications, Computer Systems Organization and Communication Networks
DOIs: 10.1007/978-3-319-66284-8_33
Source: FindIt
Source ID: 2390613130
The Internet of Hackable Things
The Internet of Things makes possible to connect each everyday object to the Internet, making computing pervasive like never before. From a security and privacy perspective, this tsunami of connectivity represents a disaster, which makes each object remotely hackable. We claim that, in order to tackle this issue, we need to address a new challenge in security: education.

A Survey of Man in the Middle Attacks
The Man-In-The-Middle (MITM) attack is one of the most well known attacks in computer security, representing one of the biggest concerns for security professionals. MITM targets the actual data that flows between endpoints, and the confidentiality and integrity of the data itself. In this paper, we extensively review the literature on MITM to analyse and categorize the scope of MITM attacks, considering both a reference model, such as the open systems interconnection (OSI) model, as well as two specific widely used network technologies, i.e., GSM and UMTS. In particular, we classify MITM attacks based on several parameters, like location of an attacker in the network, nature of a communication channel, and impersonation techniques. Based on an impersonation techniques classification, we then provide execution steps for each MITM class. We survey existing countermeasures and discuss the comparison among them. Finally, based on our analysis, we propose a categorisation of MITM prevention mechanisms, and we identify some possible directions for future research.
Evaluation of Professional Cloud Password Management Tools

Strong passwords have been preached since decades. However, a lot of the regular users of IT systems resort to simple and repetitive passwords, especially nowadays in the "service era". To help alleviate this problem, a new class of software grew popular: password managers. Since their introduction, password managers have slowly been migrating into the cloud. In this paper we review and analyze current professional password managers in the cloud. We discuss several functional and nonfunctional requirements to evaluate existing solutions and we sum up their strengths and weaknesses. The main conclusion is that a silver bullet solution is not available yet and that this type of tools still deserve a significant research effort from the privacy and security community.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Technical University of Denmark
Contributors: Schougaard, D., Dragoni, N., Spognardi, A.
Pages: 16-28
Publication date: 2016

Host publication information
Title of host publication: Current Trends in Web Engineering : Revised Selected Papers of the ICWE 2016 International Workshops DUI, TELERISE, SoWeMine, and Liquid Web
Publisher: Springer
ISBN (Print): 978-3-319-46962-1
ISBN (Electronic): 978-3-319-46963-8
(Lecture Notes in Computer Science, Vol. 9881).
Electronic versions:
TELERISE.pdf. Embargo ended: 06/10/2017
DOIs:
10.1007/978-3-319-46963-8_2
Source: PublicationPreSubmission
Source ID: 127114545
Research output: Chapter in Book/Report/Conference proceeding – Article in proceedings – Annual report year: 2016
Research › peer-review

Mind the tracker you wear: a security analysis of wearable health trackers

Wearable tracking devices have gained widespread usage and popularity because of the valuable services they offer, monitoring human's health parameters and, in general, assisting persons to take a better care of themselves. Nevertheless, the security risks associated with such devices can represent a concern among consumers, because of the sensitive information these devices deal with, like sleeping patterns, eating habits, heart rate and so on. In this paper, we analyse the key security and privacy features of two entry level health trackers from leading vendors (Jawbone and Fitbit), exploring possible attack vectors and vulnerabilities at several system levels. The results of the analysis show how these devices are vulnerable to several attacks (perpetrated with consumer-level devices equipped with just bluetooth and Wi-Fi) that can compromise users' data privacy and security, and eventually call the tracker vendors to raise the stakes against such attacks.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Technical University of Denmark
Contributors: Goyal, R., Dragoni, N., Spognardi, A.
Number of pages: 6
Pages: 131-136
Publication date: 2016

Host publication information
Title of host publication: Proceedings of the 31st ACM Symposium on Applied Computing (SAC’16)
Publisher: ACM
ISBN (Print): 978-1-4503-3739-7
Keywords: Privacy, Security, Wearable health trackers
DOIs:
SafeDroid: A Distributed Malware Detection Service for Android

Android platform has become a primary target for malware. In this paper we present SafeDroid, an open source distributed service to detect malicious apps on Android by combining static analysis and machine learning techniques. It is composed by three micro-services, working together, combining static analysis and machine learning techniques. SafeDroid has been designed as a user friendly service, providing detailed feedback in case of malware detection. The detection service is optimized to be lightweight and easily updated. The feature set on which the micro-service of detection relies on has been selected and optimized in order to focus only on the most distinguishing characteristics of the Android apps. We present a prototype to show the effectiveness of the detection mechanism service and the feasibility of the approach.

Security And Privacy Issues in Health Monitoring Systems: eCare@Home Case Study

Automated systems for monitoring elderly people in their home are becoming more and more common. Indeed, an increasing number of home sensor networks for healthcare can be found in the recent literature, indicating a clear research direction in smart homes for health-care. Although the huge amount of sensitive data these systems deal with and expose to the external world, security and privacy issues are surprisingly not taken into consideration. The aim of this paper is to raise some key security and privacy issues that home health monitor systems should face with. The analysis is based on a real world monitoring sensor network for healthcare built in the context of the eCare@Home project.
Why Hackers Love eHealth Applications

The tsunami of Internet-of-Things and mobile applications for healthcare is giving hackers an easy way to burrow deeper into our lives as never before. In this paper we argue that this security disaster is mainly due to a lack of consideration by the healthcare IT industry in security and privacy issues. By means of a representative healthcare mobile app, we analyse the main vulnerabilities that eHealth applications should deal with in order to protect user data and related privacy.

General information

Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Technical University of Denmark
Contributors: Goyal, R., Dragoni, N.
Number of pages: 6
Publication date: 2016

Host publication information

Title of host publication: Proceedings of the 3rd EAI International Conference on IoT Technologies for HealthCare (HealthyIoT), 2016, LNICST
Publisher: Springer
Editors: Uddin Ahmed, M., Begum, S., Raad, W.
ISBN (Print): 978-3-319-51233-4
ISBN (Electronic): 978-3-319-51234-1
(Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Adaptive Multipath Key Reinforcement for Energy Harvesting Wireless Sensor Networks

Energy Harvesting - Wireless Sensor Networks (EH-WSNs) constitute systems of networked sensing nodes that are capable of extracting energy from the environment and that use the harvested energy to operate in a sustainable state. Sustainability, seen as design goal, has a significant impact on the design of the security protocols for such networks, as the nodes have to adapt and optimize their behaviour according to the available energy. Traditional key management schemes do not take energy into account, making them not suitable for EH-WSNs. In this paper we propose a new multipath key reinforcement scheme specifically designed for EH-WSNs. The proposed scheme allows each node to take into consideration and adapt to the amount of energy available in the system. In particular, we present two approaches, one static and one fully dynamic, and we discuss some experimental results.

General information

Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Contributors: Di Mauro, A., Dragoni, N.
Pages: 48–55
Publication date: 2015
Peer-reviewed: Yes

Publication information

Journal: Procedia Computer Science
Volume: 63
ISSN (Print): 1877-0509
Ratings:
BFI (2015): BFI-level 1
Scopus rating (2015): CiteScore 0.85 SJR 0.266 SNIP 0.774
Web of Science (2015): Indexed yes
Original language: English
Electronic versions:
Adaptive_Multipath_Key.pdf
DOIs:
10.1016/j.procs.2015.08.311
Research output: Contribution to journal > Conference article – Annual report year: 2015 > Research > peer-review

Energy Harvesting Wireless Sensor Networks (EH-WSNs) represent an interesting new paradigm where individual nodes forming a network are powered by energy sources scavenged from the surrounding environment. This technique provides numerous advantages, but also new design challenges. Securing the communications under energy constraints represents one of these key challenges. The amount of energy available is theoretically infinite in the long run but highly variable over short periods of time, and managing it is a crucial aspect. In this paper we present an adaptive approach for security in multihop EH-WSNs which allows different nodes to dynamically choose the most appropriate energy-affecting parameters such as encryption algorithm and key size, providing in this way energy savings. In order to provide evidence of the approach's feasibility in a real-world network, we have designed and implemented it as extension of on-demand medium access control (ODMAC), a receiver-initiated (RI) MAC protocol specifically designed and developed to address the foundational energy-related needs of Energy Harvesting Wireless Sensor Networks.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Department of Informatics and Mathematical Modeling, Embedded Systems Engineering, University of Bristol, Örebro University
Contributors: Di Mauro, A., Fafoutis, X., Dragoni, N.
Number of pages: 11
Publication date: 2015
Peer-reviewed: Yes

Publication information
Journal: International Journal of Distributed Sensor Networks
Volume: 2015
Article number: 760302
ISSN (Print): 1550-1329
Ratings:
Scopus rating (2015): CiteScore 1.1 SJR 0.256 SNIP 0.891
Web of Science (2015): Impact factor 0.906
Web of Science (2015): Indexed yes
Original language: English
Keywords: COMPUTER, TELECOMMUNICATIONS, BLOCK CIPHER, PROTOCOLS
Electronic versions:
760302.pdf
DOIs:
10.1155/2015/760302
Source: FindIt
Source ID: 275106193
Research output: Contribution to journal › Journal article – Annual report year: 2015 › Research › peer-review

A Framework and Classification for Fault Detection Approaches in Wireless Sensor Networks with an Energy Efficiency Perspective

Wireless Sensor Networks (WSNs) are more and more considered a key enabling technology for the realisation of the Internet of Things (IoT) vision. With the long term goal of designing fault-tolerant IoT systems, this paper proposes a fault detection framework for WSNs with the perspective of energy efficiency to facilitate the design of fault detection methods and the evaluation of their energy efficiency. Following the same design principle of the fault detection framework, the paper proposes a classification for fault detection approaches. The classification is applied to a number of fault detection approaches for the comparison of several characteristics, namely, energy efficiency, correlation model, evaluation method, and detection accuracy. The design guidelines given in this paper aim at providing an insight into better design of energy-efficient detection approaches in resource-constraint WSNs.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, East China Normal University
Contributors: Zhang, Y., Dragoni, N., Wang, J.
Number of pages: 11
Publication date: 2015
Peer-reviewed: Yes

Publication information
Journal: International Journal of Distributed Sensor Networks
Volume: 2015
Article number: 678029
ISSN (Print): 1550-1329

Fault-tolerant event detection is fundamental to wireless sensor network applications. Existing approaches usually adopt neighborhood collaboration for better detection accuracy, while need more energy consumption due to communication. Focusing on energy efficiency, this paper makes an improvement to a hybrid algorithm for dynamic event region detection, such as real-time tracking of chemical leakage regions. Considering the characteristics of the moving away dynamic events, we propose a return back condition for the hybrid algorithm from distributed neighborhood collaboration, in which a node makes its detection decision based on decisions received from its spatial and temporal neighbors, to local non-communicative decision making. The simulation results demonstrate that the improved algorithm does not degrade the detection accuracy of the original algorithm, while it has better energy efficiency with the number of messages exchanged in the network decreased.

Fault Detection in WSNs - An Energy Efficiency Perspective Towards Human-Centric WSNs

Energy efficiency is a key factor to prolong the lifetime of wireless sensor networks (WSNs). This is particularly true in the design of human-centric wireless sensor networks (HCWSN) where sensors are more and more embedded and they have to work in resource-constraint settings. Resource limitation has a significant impact on the design of a WSN and the adopted fault detection method. This paper investigates a number of fault detection approaches and proposes a fault detection framework based on an energy efficiency perspective. The analysis and design guidelines given in this paper aims at representing a first step towards the design of energy-efficient detection approaches in resource-constraint WSN, like HCWSNs.
Receiver-initiated medium access control protocols for wireless sensor networks

One of the fundamental building blocks of a Wireless Sensor Network (WSN) is the Medium Access Control (MAC) protocol, that part of the system governing when and how two independent neighboring nodes activate their respective transceivers to directly interact. Historically, data exchange has always been initiated by the node willing to relay data, i.e. the sender. However, the Receiver-Initiated paradigm introduced by Lin et al. in 2004 with RICER and made popular by Sun et al. in 2008 with RI-MAC, has spawned a whole new stream of research, yielding tens of new MAC protocols. Within such paradigm, the receiver is the one in charge of starting a direct communication with an eligible sender. This allows for new useful properties to be satisfied, novel schemes to be introduced and new challenges to be tackled. In this paper, we present a survey comprising of all the MAC protocols released since the year 2004 that fall under the receiver-initiated category. In particular, keeping in mind the key challenges that receiver-initiated MAC protocols are meant to deal with, we analyze and discuss the different protocols according to common features and design goals. The aim of this paper is to provide a comprehensive and self-contained introduction to the fundamentals of the receiver-initiated paradigm, providing newcomers with a quick-start guide on the state of the art of this field and a palette of options, essential for implementing applications or designing new protocols.


In receiver-initiated medium access control (MAC) protocols for wireless sensor networks, communication is initiated by the receiver node which transmits beacons indicating its availability to receive data. In the case of multiple senders having traffic for a given receiver, such beacons form points where collisions are likely to happen. In this paper, we present altruistic backoff (AB), a novel collision avoidance mechanism that aims to avoid collisions before the transmission of a beacon. As a result of an early backoff, senders spend less time in idle listening waiting for a beacon, thus saving significant amounts of energy. We present an implementation of AB for Texas Instruments' eZ430-rf2500 sensor nodes and we evaluate its performance with simulations and experiments.
Detecting and Preventing Beacon Replay Attacks in Receiver-Initiated MAC Protocols for Energy Efficient WSNs

In receiver-initiated MAC protocols for Wireless Sensor Networks (WSNs), communication is initiated by the receiver of the data through beacons containing the receiver's identity. In this paper, we consider the case of a network intruder that captures and replays such beacons towards legitimate nodes, pretending to have a fake identity within the network. To prevent this attack we propose RAP, a challenge-response authentication protocol that is able to detect and prevent the beacon replay attack. The effectiveness of the protocol is formally verified using OFMC and ProVerif. Furthermore, we provide an analysis that highlights the trade-offs between the energy consumption and the level of security, defined as the resilience of the protocol to space exhaustion.
Dynamic allocation and admission policies for QoS-aware provisioning systems

We present an architecture of a hosting system consisting of a set of hosted web services subject to QoS constraints, and a certain number of servers used to run user's demand. The traffic is session–based, while provider and users agree on SLAs specifying the expected level of service performance such that the service provider is liable to compensate his/her customers if the level of performance is not satisfactory. The system is driven by a utility function which tries to optimise the average earned revenue per unit time. The middleware collects demand and performance statistics, and estimates traffic parameters in order to make dynamic decisions concerning server allocation and admission control. We empirically evaluate the effects of admission policies, resource allocation and service differentiation schemes on the achieved revenues, and we find that our system is robust enough to successfully deal with session–based traffic under different conditions.

Medium Access Control for Thermal Energy Harvesting in Advanced Metering Infrastructures

In this paper we investigate the feasibility of powering wireless metering devices, namely heat cost allocators, by thermal energy harvested from radiators. The goal is to take a first step toward the realization of Energy-Harvesting Advanced Metering Infrastructures (EH-AMIs). While traditional battery-powered devices have a limited amount of energy, energy harvesting can potentially provide an infinite amount of energy for continuous operating lifetimes, thus reducing the cost involved in installation and maintenance. The contribution of this work is twofold. First, we experimentally identify the potential energy that can be harvested from Low Surface Temperature (LST) radiators. The experiments are based on a developed Energy-Harvesting Heat Cost Allocator (EH-HCA) prototype. On the basis of this measured power budget, we model and analytically compare the currently used Medium Access Control (MAC) scheme of an industrial case study (IMR+) to a MAC scheme specifically designed for energy harvesting systems (ODMAC). Our analytical comparison shows the efficiency of the latter, as well as its ability to adapt to harvested ambient energy.
MITHYS: Mind The Hand You Shake - Protecting Mobile Devices from SSL Usage Vulnerabilities

Recent studies have shown that a significant number of mobile applications, often handling sensitive data such as bank accounts and login credentials, suffer from SSL vulnerabilities. Most of the time, these vulnerabilities are due to improper use of the SSL protocol (in particular, in its handshake phase), resulting in applications exposed to man-in-the-middle attacks. In this paper, we present MITHYS, a system able to: (i) detect applications vulnerable to man-in-the-middle attacks, and (ii) protect them against these attacks. We demonstrate the feasibility of our proposal by means of a prototype implementation in Android, named MITHYSApp. A thorough set of experiments assesses the validity of our solution in detecting and protecting mobile applications from man-in-the-middle attacks, without introducing significant overheads. Finally, MITHYSApp does not require any special permissions nor OS modifications, as it operates at the application level. These features make MITHYSApp immediately deployable on a large user base.

Social Networks and Collective Intelligence: A Return to the Agora

Nowadays, acquisition of trustable information is increasingly important in both professional and private contexts. However, establishing what information is trustable and what is not, is a very challenging task. For example, how can information quality be reliably assessed? How can sources' credibility be fairly assessed? How can gatekeeping processes be found trustworthy when filtering out news and deciding ranking and priorities of traditional media? An Internet-based solution to a human-based ancient issue is being studied, and it is called Polidoxa, from Greek "poly", meaning "many" or "several" and "doxa", meaning "common belief" or "popular opinion". This old problem will be solved by means of ancient philosophies and processes with truly modern tools and technologies. This is why this work required a collaborative and interdisciplinary joint effort from researchers with very different backgrounds and institutes with significantly different agendas. Polidoxa aims at offering: 1) a trust-based search engine algorithm, which exploits stigmergic behaviours of users' network, 2) a trust-based social network, where the notion of trust derives from network activity and 3) a holonic system for bottom-up self-protection and social privacy. By presenting the Polidoxa solution, this work also describes the current state of traditional media as well as newer ones, providing an accurate analysis of major search engines such as Google and social network (e.g., Facebook). The advantages that Polidoxa offers, compared to these, are also clearly detailed and motivated. Finally, a Twitter application (Polidoxa@twitter) which enables experimentation of basic Polidoxa principles is presented.
Sustainable medium access control: Implementation and evaluation of ODMAC

Harvesting small-scale ambient energy constitutes a promising source of power for wireless embedded devices. Due to the unpredictable nature of the harvested energy, adaptive radio duty cycling can lead to a long-term sustainable operation. In energy constrained conditions, very low duty cycles are vital to guarantee the sustainability of the system; whereas, in the opposite case, the system should use the energy surplus to increase the application performance. In this paper, we implement and evaluate On-Demand MAC (ODMAC), the first receiver-initiated MAC protocol specifically designed for energy harvesting applications. In particular, we provide a basic yet fully operational implementation of ODMAC for the Texas Instruments' MSP430 microprocessor family. Furthermore, we verify the theoretical results of our previous work by achieving sustainable operation of an energy harvesting node in various cases of energy input using a real test-bed.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Contributors: Fafoutis, X., Di Mauro, A., Dragoni, N.
Pages: 407 - 412
Publication date: 2013

Host publication information
Publisher: IEEE
ISBN (Print): 9781467357531
Keywords: Communication, Networking and Broadcast Technologies
DOIs: 10.1109/ICCW.2013.6649268
Source: dtu
Source ID: n:oai:DTIC-ART:arxiv/425273435::36185

Sustainable Performance in Energy Harvesting - Wireless Sensor Networks

In this practical demo we illustrate the concept of "sustainable performance" in Energy-Harvesting Wireless Sensor Networks (EH-WSNs). In particular, for different classes of applications and under several energy harvesting scenarios, we show how it is possible to have sustainable performance when nodes in the network are powered by ambient energy.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Contributors: Fafoutis, X., Di Mauro, A., Dragoni, N.
Pages: 267-268
Publication date: 2013

Host publication information
Title of host publication: Proceedings of the fourth international conference on Future energy systems : e-Energy '13
Publisher: Association for Computing Machinery
ISBN (Print): 978-1-4503-2052-8
Keywords: Wireless sensor networks, MAC Protocols
Electronic versions: eenergy-demo.pdf
DOIs: 10.1145/2487166.2487200

Bibliographical note
Conference demonstration.
Source: dtu
Adaptive Media Access Control for Energy Harvesting - Wireless Sensor Networks

ODMAC (On-Demand Media Access Control) is a recently proposed MAC protocol designed to support individual duty cycles for Energy Harvesting — Wireless Sensor Networks (EH-WSNs). Individual duty cycles are vital for EH-WSNs, because they allow nodes to adapt their energy consumption to the ever-changing environmental energy sources. In this paper, we present an improved and extended version of ODMAC and we analyze it by means of an analytical model that can approximate several performance metrics in an arbitrary network topology. The simulations and the analytical experiments show ODMAC's ability to satisfy three key properties of EH-WSNs: adaptability of energy consumption, distributed energy-aware load balancing and support for different application-specific requirements.

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Embedded Systems Engineering
Contributors: Fafoutis, X., Dragoni, N.
Number of pages: 4
Publication date: 2012

Host publication information
Title of host publication: 2012 Ninth International Conference on Networked Sensing Systems (INSS)
Publisher: IEEE
ISBN (Print): 978-1-4673-1784-9
ISBN (Electronic): 978-1-4673-1785-6
DOI: 10.1109/INSS.2012.6240557
Source: dtu

Analytical Comparison of MAC Schemes for Energy Harvesting - Wireless Sensor Networks

MAC protocols for multi-hop WSNs have to address the challenge of coordinating duty-cycling transmitters with duty-cycling receivers. All the suggested protocols can be classified into three basic paradigms: the synchronization, the preamble and the beaconing paradigm. In this paper, we discuss the suitability of the three paradigms in the context of Energy Harvesting — Wireless Sensor Networks (EH-WSNs) in which nodes are powered by energy that they harvest from their surrounding environment. The two suitable paradigms are modeled and compared to each other. The analysis indicates the specific conditions under which a scheme is more suitable than the other.

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Embedded Systems Engineering
Contributors: Fafoutis, X., Dragoni, N.
Number of pages: 6
Publication date: 2012

Host publication information
Title of host publication: 2012 Ninth International Conference on Networked Sensing Systems (INSS)
Publisher: IEEE
ISBN (Print): 978-1-4673-1784-9
ISBN (Electronic): 978-1-4673-1785-6
Keywords: Wireless sensor networks
DOI: 10.1109/INSS.2012.6240580
Source: dtu

Declarative Specification of Fault Tolerant Auction Protocols: The English Auction Case Study

Auction mechanisms are nowadays widely used in electronic commerce Web sites for buying and selling items among different users. The increasing importance of auction protocols in the negotiation phase is not limited to online marketplaces. In fact, the wide applicability of auctions as resource-allocation and negotiation mechanisms have also led to a great deal of interest in auctions within the agent community. A challenging issue for agents operating in open
Multiagent Systems (such as the emerging semantic Web infrastructure) concerns the specification of declarative communication rules which could be published and shared allowing agents to dynamically engage well-known and trusted negotiation protocols. To cope with real-world applications, these rules should also specify fault tolerant patterns of interaction, enabling negotiating agents to interact with each other tolerating failures, for instance terminating an auction process even if some bidding agents dynamically crash. In this paper, we propose an approach to specify fault tolerant auction protocols in open and dynamic environments by means of communication rules dealing with crash failures of agents. We illustrate these concepts considering a case study about the specification of an English Auction protocol which tolerate crashes of bidding agents and we discuss its properties.

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Embedded Systems Engineering, University of Bologna
Contributors: Dragoni, N., Gaspari, M.
Pages: 617-641
Publication date: 2012
Peer-reviewed: Yes

Publication information
Journal: Computational Intelligence
Volume: 28
Issue number: 4
ISSN (Print): 0824-7935
Ratings:
BFI (2012): BFI-level 1
Scopus rating (2012): CiteScore 1.75 SJR 0.463 SNIP 1.473
Web of Science (2012): Impact factor 1
ISI indexed (2012): ISI indexed yes
Web of Science (2012): Indexed yes
Original language: English
Keywords: Declarative specification of market mechanisms, Rule based specification, Open dynamic multiagent systems, English Auction protocol, Fault tolerant agent communication
DOIs: 10.1111/j.1467-8640.2012.00448.x
Source: dtu
Source ID: n::oai:DTIC-ART:blackwell/373112926::20718
Research output: Contribution to journal › Journal article – Annual report year: 2012 › Research › peer-review

Energy-Harvesting Wireless Sensor Networks
Energy Harvesting comprises a promising solution to one of the key problems faced by battery-powered Wireless Sensor Networks, namely the limited nature of the energy supply (finite battery capacity). By harvesting energy from the surrounding environment, the sensors can have a continuous lifetime without any needs for battery recharge or replacement. However, energy harvesting introduces a change to the fundamental principles based on which WSNs are designed and realized. In this poster we sketch some of the key research challenges as well as our ongoing work in designing and realizing Wireless Sensor Networks with energy harvesting capability.

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Embedded Systems Engineering, Computer Science and Engineering
Contributors: Fafoutis, X., Vuckovic, D., Di Mauro, A., Dragoni, N., Madsen, J.
Pages: 84-85
Publication date: 2012

Host publication information
Title of host publication: 9th European Conference on Wireless Sensor Networks, EWSN 2012 : Poster and Demo Proceedings
Electronic versions:
EWSN12_abstract.pdf
URLs:
Source: dtu
Source ID: u::5680
Research output: Chapter in Book/Report/Conference proceeding › Conference abstract in proceedings – Annual report year: 2012 › Research › peer-review
Implementing Workflow Reconfiguration in WS-BPEL
This paper investigates the problem of dynamic reconfiguration by means of a workflow-based case study used for discussion. We state the requirements on a system implementing the workflow and its reconfiguration, and we describe the system's design in BPMN. WS-BPEL, a language that would not naturally support dynamic change, is used as a target for implementation. The WS-BPEL recovery framework is here exploited to implement the reconfiguration using principles derived from previous research in process algebra and two mappings from BPMN to WS-BPEL are presented, one automatic and only mostly manual. Differences between the two are finally detailed.

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Embedded Systems Engineering, Newcastle University, Technical University of Denmark
Contributors: Mazzara, M., Dragoni, N., Zhou, M.
Pages: 73-92
Publication date: 2012
Peer-reviewed: Yes

Publication information
Journal: Journal of Internet Services and Information Security
Volume: 2
Issue number: 1/2
ISSN (Print): 2182-2069
Original language: English
Keywords: Workflow Reconfiguration, BPMN, WS-BPEL
URLs: http://isyou.info/jisis/vol2/no12/5.htm
Source: dtu
Source ID: u::5677
Research output: Contribution to journal – Journal article – Annual report year: 2012 – Research – peer-review

Modelling and Analysis of Dynamic Reconfiguration in BP-Calculus
The BP-calculus is a formalism based on the π-calculus and encoded in WS-BPEL. The BP-calculus is intended to specifically model and verify Service Oriented Applications. One important feature of SOA is the ability to compose services that may dynamically evolve along runtime. Dynamic reconfiguration of services increases their availability, but puts accordingly, heavy demands for validation, verification, and evaluation. In this paper we formally model and analyze dynamic reconfigurations and their requirements in BP-calculus and show how reconfigurable components can be modeled using handlers that are essential parts of WS-BPEL language.

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Embedded Systems Engineering, Polytechnique Montreal, University of Montreal, Newcastle University
Contributors: Abouzaid, F., Mullins, J., Mazzara, M., Dragoni, N.
Pages: 534-543
Publication date: 2012

Host publication information
Publisher: Springer
ISBN (Print): 978-3-642-30946-5
ISBN (Electronic): 978-3-642-30947-2
(Lecture Notes in Computer Science, Vol. 7327).
DOIs: 10.1007/978-3-642-30947-2_58
Source: dtu
Source ID: n:oai:DTIC-ART:compendex/370713268::21786
Research output: Chapter in Book/Report/Conference proceeding – Article in proceedings – Annual report year: 2012 – Research – peer-review

SC²: Secure Communication over Smart Cards: How to Secure Off-Card Matching in Security-by-Contract for Open Multi-application Smart Cards
The Security-by-Contract (S×C) framework has recently been proposed to support software evolution in open multi-application smart cards. The key idea lies in the notion of contract, a specification of the security behavior of an application
that must be compliant with the security policy of the card hosting the application. In this paper we address a key issue to
realize the S×C idea, namely the outsourcing of the contractpolicy matching service to a Trusted Third Party (TTP). In
particular, we present the design and implementation of (SC)2 (Secure Communication over Smart Cards), a system
securing the communication between a smart card and the TTP which provides the S×C matching service.

**General information**
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling, University of Zaragoza
Contributors: Dragoni, N., Lostal, E., Papini, D., Fabra, J.
Pages: 32-48
Publication date: 2012

**Host publication information**
Publisher: Springer
ISBN (Print): 978-3-642-27900-3
ISBN (Electronic): 978-3-642-27901-0
(Lecture Notes in Computer Science; No. 6888).
DOIs: 10.1007/978-3-642-27901-0_4
Source: orbit
Source ID: 318502
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2012 › Research › peer-review

Security challenges for energy-harvesting wireless sensor networks
With the recent introduction of Energy-Harvesting nodes, security is gaining more and more importance in sensor
networks. By exploiting the ability of scavenging energy from the surrounding environment, the lifespan of a node has
dramatically increased. This is one of the reason why security needs a new take in this topic. Traditional solutions may not
work in this new field. Brand new challenges and threats may arise and new solutions have to be designed. In this paper
we present a taxonomy of attacks, focusing on how they change in the energy harvesting scenario compared to regular
sensor networks. Finally, we present and discuss existing security solutions for EH-WSNs.

**General information**
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Embedded Systems Engineering
Contributors: Di Mauro, A., Papini, D., Dragoni, N.
Pages: 422-425
Publication date: 2012

**Host publication information**
Title of host publication: PECCS 2012 - Proceedings of the 2nd International Conference on Pervasive Embedded Computing and Communication Systems
Publisher: SciTePress
ISBN (Print): 978-989-8565-00-6
Keywords: Communication systems, Embedded software, Energy harvesting, Wireless sensor networks, Sensor nodes
Source: dtu
Source ID: n:doi:DTIC-ART:compendex/370756376::19988
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2012 › Research › peer-review

Social Networks and Collective Intelligence - A Return to the Agora (with the Polidoxa Shift)

**General information**
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Embedded Systems Engineering, Newcastle University, Polidoxa.com
Contributors: Biselli, L., Dragoni, N., Goldoni, E., Greco, P. P., Marraa, A., Mazzara, M., Papageorgiou, G.
Pages: 347-348
Publication date: 2012

**Host publication information**
Toward a Threat Model for Energy-Harvesting Wireless Sensor Networks

Security is a crucial matter for Wireless Sensor Networks. With the recent introduction of Energy-Harvesting nodes, it has gained even more importance. By exploiting the ability of scavenging energy from the surrounding environment, the lifespan of a node has drastically increased. This is one of the reasons why security needs a new take in this topic. Traditional solutions may not work in this new domain. Brand new challenges and threats may arise and new solutions have to be designed. In this paper we present a first taxonomy of attacks, focusing on how they change in the energy-harvesting context compared to regular sensor networks. We also discuss existing security solutions specific for the energy harvesting world and comment on the trend that this topic may follow in the future. Finally, we draw a comparison between the cyber-physical attacker we define in our model and adversary models belonging to security protocols verification literature.

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Language-Based Technology, Embedded Systems Engineering
Contributors: Di Mauro, A., Papini, D., Vigo, R., Dragoni, N.
Pages: 289-301
Publication date: 2012

Host publication information
Title of host publication: Networked Digital Technologies : 4th International Conference, NDT 2012 Dubai, UAE, April 24-26, 2012 Proceedings, Part II
Publisher: Springer
ISBN (Print): 978-3-642-30566-5
ISBN (Electronic): 978-3-642-30567-2
(Communications in Computer and Information Science, Vol. 294).
DOIs: 10.1007/978-3-642-30567-2_24
Source: dtu
Source ID: u::5212
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2012 › Research › peer-review

Toward a Unified Framework for Web Service Trustworthiness

The intrinsic openness of the Service-Oriented Computing vision makes crucial to locate useful services and recognize them as trustworthy. What does it mean that a Web service is trustworthy? How can a software agent evaluate the trustworthiness of a Web service? In this paper we present an ongoing research aiming at providing an answer to these key issues to realize this vision. In particular, starting from an analysis of the weaknesses of current approaches, we discuss the possibility of a unified framework for Web service trustworthiness. The founding principle of our novel framework is that “hard trust” and “soft trust” provisioning techniques should be embodied in a unified hybrid model.

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Embedded Systems Engineering, Technical University of Denmark
Contributors: Miotto, N., Dragoni, N.
Pages: 555-558
Publication date: 2012

Host publication information
Title of host publication: Proceedings of IADIS e-Society
Publisher: International Association for Development, IADIS
ISBN (Print): 978-972-8939-67-0
Keywords: Web Service, Service-Oriented Computing, Trustworthiness
Source: dtu
A Load Time Policy Checker for Open Multi-Application Smart Cards

Applications on multi-application smart cards contain sensitive data and can exchange information. Thus a major concern is that these applications should not exchange data unless permitted by their respective policy. As modern smart cards allow post-issuance installation and removal of applications, traditional approaches for information flow analysis are not suitable. We suggest the Security-by-Contract approach for loading time application certification on the card, that will enable the stakeholders with the means to ensure the compliance of every update of the card with their security policy. We describe an extension of the card security architecture to deal with verification for different types of updates and present a Java Card prototype implementation of the Policy Checker with performance measurements.

Analysis of Trust-Based Approaches for Web Service Selection

The basic tenet of Service-Oriented Computing (SOC) is the possibility of building distributed applications on the Web by using Web services as fundamental building blocks. The proliferation of such services is considered the second wave of evolution in the Internet age, moving the Web from a collection of pages to a collections of services. Consensus is growing that this Web service revolution wont eventuate until we resolve trust-related issues. Indeed, the intrinsic openness of the SOC vision makes crucial to locate useful services and recognize them as trustworthy. In this paper we review the field of trust-based Web service selection, providing a structured classification of current approaches and highlighting the main limitations of each class and of the overall field.

Dependable Workflow Reconfiguration in WS-BPEL

This paper describes a workflow reconguration and how to implement it in WS-BPEL, a language that would not naturally support reconguration. We state the requirements on a system implementing the work ow and its reconguration, and we
describe the system's design in BPMN. The WS-BPEL recovery framework is then exploited to implement the reconfiguration.

**General information**
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling, Newcastle University, Technical University of Denmark
Contributors: Mazzara, M., Dragoni, N., Zhou, M.
Publication date: 2011

**Host publication information**
Title of host publication: Proceedings of the 5th Nordic Workshop on Dependability and Security (NODES’11)
Electronic versions:
NODES_2011.pdf
URLs:
Source: orbit
Source ID: 312625
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2011 › Research › peer-review

**Design, Modelling and Analysis of a Workflow Reconfiguration**
This paper describes a case study involving the reconfiguration of an office workflow. We state the requirements on a system implementing the workflow and its reconfiguration, and describe the system's design in BPMN. We then use an asynchronous pi-calculus and Web.1 to model the design and to verify whether or not it will meet the requirements. In the process, we evaluate the formalisms for their suitability for the modelling and analysis of dynamic reconfiguration of dependable systems.

**General information**
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Embedded Systems Engineering, Newcastle University, Polytechnique Montreal
Contributors: Mazzara, M., Abouzaid, F., Dragoni, N., Bhattacharyya, A.
Pages: 10-24
Publication date: 2011

**Host publication information**
Title of host publication: Proceedings of the International Workshop on Petri Nets and Software Engineering (PNSE’11)
URLs:
http://ceur-ws.org/Vol-723/
http://conferences.ncl.ac.uk/pn-acsd-11/
Source: orbit
Source ID: 312567
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2011 › Research › peer-review

**Guest Editorial: Special Issue on Frontiers in Trust Management**

**General information**
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling, Tokai University, The Open University
Contributors: Jensen, C. D., Dragoni, N., Basu, A., Mancini, C.
Pages: 1-4
Publication date: 2011
Peer-reviewed: Yes

**Publication information**
Journal: Journal of Internet Services and Information Security
Volume: 1
Issue number: 4
ISSN (Print): 2182-2069
Original language: English
Electronic versions:

Energy Harvesting (EH) provides a promising solution to one of the biggest problems faced by Wireless Sensor Networks (WSN), namely the energy supply. By harvesting energy from the surrounding environment, the sensors can have an infinite lifetime without any needs for battery recharge or replacement. Battery-powered WSNs are typically designed to maximize the energy conservation in order to postpone as much as possible the inevitable battery depletion. Instead, EH-WSNs are being designed on a different principle. The focus is on maximizing the network performance while operating at a state that is energetically sustainable. In this paper, we present ODMAC, an on demand MAC protocol for EH-WSNs which is able to support individual duty cycles for nodes with different energy profiles. Hence, each node is able to increase its energy consumption, thus its performance, to the level that the energy consumed is at the same level to the energy harvested. The protocol is implemented and evaluated using the OPNET simulator [7].


The Security-by-Contract (SC) framework has recently been proposed to support software evolution in open multi-application smart cards. The key idea lies in the notion of contract, a specification of the security behavior of an application that must be compliant with the security policy of the smart card hosting the application. In this demonstration we show (SC)² (Secure Communication over Smart Cards), a system developed to address a key issue of the SC framework, namely the secure outsourcing of the SC contract-policy matching service to a Trusted Third Party (TTP). (SC)² secures the communication between a smart card and the TTP that provides the SC matching service.
Supporting Software Evolution for Open Smart Cards by Security-by-Contract

Open multi-application smart cards that allow post-issuance evolution (i.e. loading of new applets) are potentially very attractive for both smart card developers and card users. Yet we find only few of them on the market as no satisfactory solution exists for the assurance that these coming-and-going applications will not exchange data unless permitted by their respective policies. If all applications could be loaded at the start this would boil down to information flow analysis for which many solutions exist, but this is precisely what we want to overcome. When applications are not known in advance and can be updated asynchronously and possibly without connection to trusted third parties, we must preserve the security policies of the various owners of the applets during such autonomous evolution. This chapter illustrates the extension of the Security-by-Contract approach from mobile phones to smart cards: Security-by-Contract is based on the loading time application certification on the card that will enable the card to make autonomous decisions on application and policy updates while ensuring the compliance of every change of the platform with the security policy of each application’s owner.

Toward Design, Modelling and Analysis of Dynamic Workflow Reconfigurations - A Process Algebra Perspective

This paper describes a case study involving the dynamic re-conguration of an oce work ow. We state the requirements on a sys- tem implementing the work ow and its reconguration, and describe the system's design in BPMN. We then use an asynchronous -calculus and Web1 to model the design and to verify whether or not it will meet the requirements. In the process, we evaluate the formalisms for their suitability for the modelling and analysis of dynamic recongu- ration of dependable systems. The ultimate aim of this research is to identify strengths and weaknesses of formalisms for modelling dynamic reconfiguration and verifying requirements.
A Survey on Trust-Based Web Service Provision Approaches

The basic tenet of Service-Oriented Computing (SOC) is the possibility of building distributed applications on the Web by using Web Services as fundamental building blocks. The proliferation of such services is considered the second wave of evolution in the Internet age, moving the Web from a collection of pages to a collections of services. Consensus is growing that this Web Service "revolution" won't eventuate until we resolve trust-related issues. Indeed, the intrinsic openness of the SOC vision makes crucial to locate useful services and recognize them as trustworthy. In this paper we review the field of trust-based Web Service selection, providing a structured classification of current approaches and highlighting the main limitations of each class and of the overall field. As a result, we claim that a soft notion of trust lies behind such weaknesses and we advocate the need of a new approach based on a stronger (semantics-based) notion of trust.

Design of QoS-aware Provisioning Systems

Security-by-Contract (S×C) is a paradigm providing security assurances for mobile applications. In this work, we present the an extension of S×C, called Security-by-Contract-with-Trust (S×C×T). Indeed, we enrich the S×C architecture by integrating a trust model and adding new modules and configurations for managing contracts. Indeed, at deploy-time, our system decides the run-time configuration depending on the credentials of the contract provider. The run-time environment can both enforce a security policy and monitor the declared contract. According to the actual behaviour of the running program our architecture updates the trust level associated with the contract provider. We also present a possible application of our framework in the scenario of a mobile application marketplace, e.g., Apple AppStore, Cydia, Android Market, that, nowadays, are considered as one of the most attractive e-commerce activity for both mobile application developers and industries of mobile devices. Since the number of applications increases, Mobile Applications Marketplace (MAMp) sets up recommendation systems that rank and highlight mobile applications by category, social activity, etc. The S×C×T framework we propose is applied in this scenario for providing security on customers' mobile devices as well as help Mobile Applications Marketplaces to enhance their recommendation systems with security feedback. The main advantage of this method is an automatic management of the level of trust of software and contract releasers and a unified way for dealing with both security and trust.
Extending Security-by-Contract with Quantitative Trust on Mobile Devices

Securing Off-Card Contract-Policy Matching in Security-By-Contract for Multi-Application Smart Cards

Security-by-Contract for Applications Evolution in Multi-Application Smart Cards
Supporting Applications’ Evolution in Multi-Application Smart Cards by Security-by-Contract

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling, University of Trento
Contributors: Dragoni, N., Gadyatskaya, O., Massacci, F.
Publication date: 2010

Host publication information
Title of host publication: Proceedings of the 4th Workshop in Information Security Theory and Practices
Source: orbit
Source ID: 256610
Research output: Chapter in Book/Report/Conference proceeding – Annual report year: 2010
Research > peer-review

A Formal Semantics for the WS-BPEL Recovery Framework - The Pi-Calculus Way

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling, Newcastle University
Contributors: Dragoni, N., Mazzara, M.
Publication date: 2009

Host publication information
Title of host publication: 6th International Workshop on Web Services and Formal Methods (WS-FM'09)
Publisher: Springer (LNCS).
Source: orbit
Source ID: 256527
Research output: Chapter in Book/Report/Conference proceeding – Annual report year: 2009
Research > peer-review

A self-protecting and self-healing framework for negotiating services and trust in autonomic communication systems

In a federation of heterogeneous nodes that organize themselves, the lack of a trusted third party does not allow establishing a priori trust relationships among strangers. Automated trust negotiation (TN) is a promising approach to establish sufficient trust among parties, allowing them to access sensitive data and services in open environments. Although the literature on TN is growing, two key issues have still to be addressed. The first one concerns a typical feature of real-life negotiations: we are usually willing to trade the disclosure of personal attributes in exchange for additional services and only in a particular order (according to our preferences). The second one concerns dependability. By their nature TN systems are used in unreliable contexts where it is important not only to protect negotiations against malicious attack (self-protection), but also against accidental failures (self-healing). In this paper we address these issues proposing a novel dependable negotiation framework where services, needed credentials, and behavioral constraints on the disclosure of privileges are bundled together. (C) 2008 Elsevier B.V. All rights reserved.

General information
Publication status: Published
Organisations: University of Trento
Contributors: Dragoni, N., Massacci, F., Saidane, A.
Pages: 1628-1648
Publication date: 2009
Peer-reviewed: Yes

Publication information
Journal: Computer Networks
Volume: 53
Issue number: 10
ISSN (Print): 1389-1286
Matching in security-by-contract for mobile code
We propose the notion of security-by-contract, a mobile contract that an application carries with itself. The key idea of the framework is that a digital signature should not just certify the origin of the code but rather bind together the code with a contract. We provide a description of the workflow for the deployment and execution of mobile code in the setting of security-by-contract, describe a structure for a contractual language and propose a number of algorithms for one of the key steps in the process, the contract-policy matching issue. We also describe the prototype for matching policies with security claims of mobile applications that we have currently implemented. We argue that security-by-contract would provide a semantics for digital signatures on mobile code thus being a step in the transition from trusted code to trustworthy code. (C) 2009 Published by Elsevier Inc.

General information
Publication status: Published
Organisations: University of Trento
Contributors: Bielova, N., Dragoni, N., Massacci, F., Naliuka, K., Siahaan, I.
Pages: 340-358
Publication date: 2009
Peer-reviewed: Yes

Publication information
Journal: Journal of Logic and Algebraic Programming
Volume: 78
Issue number: 5
ISSN (Print): 1567-8326
Ratings:
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 0.668 SNIP 1.748
Web of Science (2009): Indexed yes
Original language: English
DOIs:
10.1016/j.jlap.2009.02.013
Source: orbit
Source ID: 263898
Research output: Contribution to journal › Journal article – Annual report year: 2009 › Research › peer-review

Security-By-Contract (SxC) for Mobile Systems

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling, University of Trento
Contributors: Dragoni, N., Massacci, F.
Pages: 107-116
Publication date: 2009
Peer-reviewed: Yes

Publication information
Journal: Telektronikk Journal
Volume: 1
Original language: English
Source: orbit
Source ID: 256523
Research output: Contribution to journal › Journal article – Annual report year: 2009 › Research › peer-review
Where are All the Agents? On the Gap Between Theory and Practice of Agent-Based Referral Networks: An Inter-Agent Communication Perspective

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Contributors: Dragoni, N.
Publication date: 2009

Host publication information
Title of host publication: Principles of Practice in Multi-Agent Systems
Place of publication: Berlin
Publisher: Springer
(Lecture Notes in Artificial Intelligence, Vol. 5925).
Source: orbit
Source ID: 256526
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2009 › Research › peer-review

Projects:

Reusch, N., PhD Student, Department of Mathematics
Pop, P., Main Supervisor
Dragoni, N., Supervisor
01/10/2019 → 30/09/2022
Project: PhD

Bottom-up blockchain valuechains in the food sector
Jensen, H. H., PI, National Food Institute
Boelskifte, M., PI, National Food Institute
Riis, M. B., PI, Department of Applied Mathematics and Computer Science
Dragoni, N., PI, Department of Applied Mathematics and Computer Science
Bager, F., PI, National Food Institute
Deleuran, R. G., PI, Office for Innovation & Sector Services
01/05/2019 → 30/06/2020
Keywords: blockchain, food, autenticitet, fraud, Food Safety Data Management
Project: Research

Fog Computing Security
Tange, K. P., PhD Student, Department of Mathematics
Dragoni, N., Main Supervisor
Fafoutis, X., Supervisor
01/10/2018 → 30/09/2021
Project: PhD

Software Architecture and Platform for Multi-study and Multi-source Digital Phenotyping Research
Kumar, D., PhD Student, Department of Applied Mathematics and Computer Science, Department of Health Technology
Bardram, J. E., Main Supervisor, Department of Applied Mathematics and Computer Science
Dragoni, N., Supervisor, Department of Applied Mathematics and Computer Science
Fonde
01/02/2018 → 31/01/2021
Award relations: Software Architecture and Platform for Multi-study and Multi-source Digital Phenotyping Research
Project: PhD

Security in Fog Computing
De Donno, M., PhD Student, Department of Mathematics
Dragoni, N., Main Supervisor
Probst, C. W., Supervisor, Department of Applied Mathematics and Computer Science
Fafoutis, X., Supervisor
Technical University of Denmark
01/09/2017 → 31/08/2020
Award relations: Security in Fog Computing
Project: PhD

Certifiable Java for Embedded Systems
Rios Rivas, J. R., PhD Student, Department of Mathematics
Schoeberl, M., Main Supervisor
Pop, P., Supervisor
Dragoni, N., Examiner
Puschner, P., Examiner
Uhrig, S., Examiner
Forskningsrådskonsortiet
15/03/2011 → 25/09/2014
Award relations: Certifiable Java for Embedded Systems
Project: PhD

Optimized Networking for Energy Harvesting Wireless Sensor Networks
Fafoutsis, X., PhD Student, Department of Mathematics
Dragoni, N., Main Supervisor
Madsen, J., Supervisor
Nannarelli, A., Examiner
Plosila, J. P., Examiner
Vain, J., Examiner
Technical University of Denmark
01/12/2010 → 26/05/2014
Award relations: Optimized Networking for Energy Harvesting Wireless Sensor Networks
Project: PhD

Round-trip Engineering of Service-Oriented Architectures
Carvalho Quaresma, J. N., PhD Student, Department of Informatics and Mathematical Modeling
Probst, C. W., Main Supervisor
Nielsen, F., Supervisor
Dragoni, N., Examiner
Gollmann, D., Examiner
Kammuller, F., Examiner
Technical University of Denmark
01/09/2010 → 22/11/2013
Award relations: Round-trip Engineering of Service-Oriented Architectures
Project: PhD

Formal methods for design and simulation of embedded systems
Jakobsen, M. K., PhD Student, Department of Informatics and Mathematical Modeling
Madsen, J., Main Supervisor
Hansen, M. R., Supervisor
Dragoni, N., Examiner
Plosila, J. P., Examiner
Vain, J., Examiner
1/3 FUU, 1/3 inst 1/3 Andet
01/06/2009 → 30/08/2013
Award relations: Formal methods for design and simulation of embedded systems
Project: PhD

Optimized Networking for Energy Harvesting Wireless Sensor Network
Vuckovic, D., PhD Student, Department of Mathematics
Madsen, J., Main Supervisor
Sørensen, T., Supervisor
Dragoni, N., Examiner
Ellevee, P., Examiner
Nielsen, P. Ø., Examiner
Ansatt eksternt
01/03/2011 → 30/09/2014
Award relations: Optimized Networking for Energy Harvesting Wireless Sensor Network
Di Mauro, A., PhD Student, Department of Mathematics
Dragoni, N., Main Supervisor
Probst, C. W., Supervisor
Schoeberl, M., Examiner
Gaspari, M., Examiner
Mazzara, M., Examiner
Technical University of Denmark
15/08/2011 → 19/12/2014
Award relations: Adaptive Security in Energy Harvesting Wireless Sensor Networks
Project: PhD