The application of Software Defined Networking on securing computer networks: A survey

Software Defined Networking (SDN) has emerged as a new networking paradigm for managing different kinds of networks ranging from enterprise to home network through software enabled control. The logically centralized control plane and programmability offers a great opportunity to improve network security, like implementing new mechanisms to detect and mitigate various threats, as well as enables deploying security as a service on the SDN controller. Due to the increasing and fast development of SDN, this paper provides an extensive survey on the application of SDN on enhancing the security of computer networks. In particular, we survey recent research studies that focus on applying SDN for network security including attack detection and mitigation, traffic monitoring and engineering, configuration and policy management, service chaining, and middlebox deployment, in addition to smart grid security. We further identify some challenges and promising future directions on SDN security, compatibility and scalability issues that should be addressed in this field.

General information
Publication status: Published
Organisations: Cyber Security, Department of Applied Mathematics and Computer Science
Corresponding author: Meng, W.
Contributors: Sahay, R., Meng, W., Jensen, C. D.
Pages: 89-108
Publication date: 1 Apr 2019
Peer-reviewed: Yes

Publication information
Journal: Journal of Network and Computer Applications
Volume: 131
Analyzing the communication security between smartphones and IoT based on CORAS

The exponential growth of Internet-of-Things (IoT) devices and applications may expose tremendous security vulnerabilities in practice, as there are different protocols in the application layer to exchange sensor data, e.g., MQTT, AMQP, CoAP. For the MQTT protocol, IoT devices would publish a plain message that could potentially cause loss of data integrity and data stealing. Motivated by this, we first present a risk assessment on the communication channel between smartphones and IoT using the method of CORAS, which is a model-based security risk analysis framework. Then the paper analyzes several known cryptographic methods and mechanisms to identify which cryptography solution best fits resource constrained IoT devices. Further, we discuss appropriate cryptographic algorithms that can help protect data integrity between smartphones and IoT.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Copenhagen Center for Health Technology, Technical University of Denmark
Contributors: Bhuyan, M. H., Azad, N. A., Meng, W., Jensen, C. D.
Pages: 251-265
Publication date: 2018

Host publication information
Title of host publication: Proceedings of 12th International Conference on Network and System Security
Volume: 11058
Publisher: Springer
ISBN (Print): 9783030027438
(Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 11058).
Keywords: CORAS, Data integrity, Internet-of-Things, Network security, Risk assessment, Smartphone security
DOI: 10.1007/978-3-030-02744-5_19
Source: FindIt
Source-ID: 2442900726

CodeTrust: Trusting Software Systems

The information society is building on data and the software required to collect and analyse these data, which means that the trustworthiness of these data and software systems is crucially important for the development of society as a whole. Efforts to establish the trustworthiness of software typically include parameters, such as security, reliability, maintainability, correctness and robustness.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Technical University of Denmark
Contributors: Jensen, C., Nielsen, M. B.
Pages: 58-74
Publication date: 2018

Host publication information
Title of host publication: Trust Management XII
Volume: 528
Publisher: Springer
CyberShip: An SDN-based Autonomic Attack Mitigation Framework for Ship Systems
The use of Information and Communication Technology (ICT) in the ship communication network brings new security vulnerabilities and make communication links a potential target for various kinds of cyber physical attacks, which results in the degradation of the performance. Moreover, crew members are burdened with the task of configuring the network devices with low-level device specific syntax for mitigating the attacks. Heavy reliance on the crew members and additional software and hardware devices makes the mitigation difficult and time consuming process. Recently, the emergence of Software-Defined Networking (SDN) offers a solution to reduce the complexity in the network management tasks.
To explore the advantages of using SDN, we propose a framework based on SDN and a use case to mitigate the attacks in an automated way for improved resilience in the ship communication network.

Feasibility study of context-awareness device Comfort calculation methods and their application to comfort-based access control
Mobile devices have become more powerful and are increasingly integrated in the everyday life of people; from playing games, taking pictures and interacting with social media to replacing credit cards in payment solutions. Some actions may only be appropriate in some situations, so the security of a mobile device is therefore increasingly linked to its context, such as its location, surroundings (e.g. objects in the immediate environment) and so on. However, situational awareness and context are not captured by traditional security models. In this paper, we examine the notion of Device Comfort, which captures a device's ability to secure and reason about its environment. Specifically, we study the feasibility of two device comfort calculation methods we proposed in previous work. We do trace driven simulations based on a large body of sensed data from mobile devices in the real world. This allows us to analyze the influence of the context on the comfort level of the device in different perceived contexts in the real world. Moreover, to demonstrate the utility of our device comfort calculation methods, we apply it to comfort-based access control for mobile devices. We present the policy enforcement framework and show how to enforce our two methods using an existing security policy specification language.

Feasibility study of context-awareness device Comfort calculation methods and their application to comfort-based access control
Mobile devices have become more powerful and are increasingly integrated in the everyday life of people; from playing games, taking pictures and interacting with social media to replacing credit cards in payment solutions. Some actions may only be appropriate in some situations, so the security of a mobile device is therefore increasingly linked to its context, such as its location, surroundings (e.g. objects in the immediate environment) and so on. However, situational awareness and context are not captured by traditional security models. In this paper, we examine the notion of Device Comfort, which captures a device's ability to secure and reason about its environment. Specifically, we study the feasibility of two device comfort calculation methods we proposed in previous work. We do trace driven simulations based on a large body of sensed data from mobile devices in the real world. This allows us to analyze the influence of the context on the comfort level of the device in different perceived contexts in the real world. Moreover, to demonstrate the utility of our device comfort calculation methods, we apply it to comfort-based access control for mobile devices. We present the policy enforcement framework and show how to enforce our two methods using an existing security policy specification language.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security
Contributors: Sahay, R., Sepúlveda Estay, D. A., Meng, W., Jensen, C. D., Barfod, M. B.
Pages: 191-198
Publication date: 2018

Host publication information
Title of host publication: International Conference on Science of Cyber Security
Publisher: Springer
ISBN (Print): 978-3-030-03025-4
(Lecture Notes in Computer Science, Vol. 11287).
DOI: 10.1007/978-3-030-03026-1_14
Source: PublicationPreSubmission
Source-ID: 151584213
Research output: Chapter in Book/Report/Conference proceeding – Annual report year: 2018
Research: peer-review
Identity management for e-government Libya as a case study

Governments are strengthening their identity (ID) management strategies to deliver new and improved online services to their citizens. Such online services typically include applications for different types of permissions, requests for different types of official documents and management of different types of entitlements. The ID management scheme must therefore be able to correctly authenticate citizens and link online presence to real world identities.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security
Contributors: Elaswad, O., Jensen, C. D.
Pages: 106-113
Publication date: 2016

Introducing E-Government in Developing Countries: Analysis of Egyptian e-Government Services

Online Identification and Authentication is an essential requirement for providing e-services. Few studies have investigated the challenges facing e-Government and IDM in developing countries and, to the best of our knowledge, none of the existing research has studied the challenges facing online identification and remote authentication in developing countries, such as the North Africa Countries (NAC), where a relatively large proportion of citizens are illiterate. Therefore, the design of a national IDM system in a NAC must explicitly consider illiteracy to allow this group of citizens to benefit from online services. Egypt is one of the NAC, which has implemented online identification and authentication services that are widely recognized as the most advanced among the NAC. This paper analyses the Egyptian digital IDM in order to identify IDM requirements for online identification and authentication services that guarantee equal access to online services and an inclusive society. The study identifies strengths and weaknesses of the Egyptian e-Government and IDM services, which we believe are common to most NAC, since the NAC are quite similar in terms of social culture, citizen's education level and skills, citizen's behaviours, digital infrastructure and legislation, but also common to many other developing countries. Our analysis of the Egyptian e-Government services indicates that the security requirements and principle of equal access are not fully met, which illustrates the difficulty of introducing e-Government in developing countries.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security
Contributors: Elaswad, O., Jensen, C. D.
Pages: 1-13
Publication date: 2016
Attributes Enhanced Role-Based Access Control Model

Attribute-based access control (ABAC) and role-based access control (RBAC) are currently the two most popular access control models. Yet, they both have known limitations and offer features complementary to each other. Due to this fact, integration of RBAC and ABAC has recently emerged as an important area of research. In this paper, we propose an access control model that combines the two models in a novel way in order to unify their benefits. Our approach provides a fine-grained access control mechanism that not only takes contextual information into account while making the access control decisions but is also suitable for applications where access to resources is controlled by exploiting contents of the resources in the policy.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, University of Texas
Contributors: Mahmood Rajpoot, Q., Jensen, C. D., Krishnan, R.
Pages: 3-17
Publication date: 2015

Host publication information
Title of host publication: Proceedings of the 12th International Conference on Trust, Privacy and Security in Digital Business (TrustBus'15)
Publisher: Springer
Editors: Fischer-Huebner, S., Lambrinoudakis, C.
ISBN (Print): 978-3-319-22905-8
ISBN (Electronic): 978-3-319-22906-5
(Keywords: Context-aware access control, RBAC, Attributes, Content-based access control, Role-permission explosion, Role-explosion
Electronic versions:
AERBAC_TrustBus_20150618_.pdf
DOIs:
10.1007/978-3-319-22906-5_1
Source: PublicationPreSubmission
Source-ID: 110979339

Continuous Context-Aware Device Comfort Evaluation Method

Mobile devices have become more powerful and are increasingly integrated in the everyday life of people; from playing games, taking pictures and interacting with social media to replacing credit cards in payment solutions. The security of a mobile device is therefore increasingly linked to its context, such as its location, surroundings (e.g. objects and people in the immediate environment) and so on, because some actions may only be appropriate in some situations; this is not captured by traditional security models. In this paper, we examine the notion of Device Comfort and propose a way to calculate the sensitivity of a specific action to the context. We present two different methods for a mobile device to dynamically evaluate its security status when an action is requested, either by the user or by another device. The first method uses the predefined ideal context as a standard to assess the comfort level of a device in the current context. The second method is based on the familiarity of the device with doing the particular action in the current context. These two methods suit different situations of the device owner’s ability to deal with system security. The assessment result can activate responding action of the device to protect its resource.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Xidian University
Contributors: Guo, J., Jensen, C. D., Ma, J.
Pages: 203-211
Integrating Attributes into Role-Based Access Control

Role-based access control (RBAC) and attribute-based access control (ABAC) are currently the most prominent access control models. However, they both suffer from limitations and have features complimentary to each other. Due to this fact, integration of RBAC and ABAC has become a hot area of research recently. We propose an access control model that combines the two models in a novel way in order to unify their benefits. Our approach provides a fine-grained access control mechanism that takes into account the current contextual information while making the access control decisions.

Physical trust-based persistent authentication

Recently companies have applied two-factor user authentication. Persistent Authentication is one of the interesting authentication mechanisms to establish security and usability of two-factor authentication systems. However, there is room to improve its feasibility and usability. In this paper, we propose a new type of persistent authentication, called Persistent Authentication Based On physical Trust (PABOT). PABOT uses a context of "physical trust relationship" that is built by visual contact between users, and thus can offer a persistent authentication mechanism with better usability and higher feasibility.
Video Surveillance: Privacy Issues and Legal Compliance

Pervasive usage of video surveillance is rapidly increasing in developed countries. Continuous security threats to public safety demand use of such systems. Contemporary video surveillance systems offer advanced functionalities which threaten the privacy of those recorded in the video. There is a need to balance the usage of video surveillance against its negative impact on privacy. This chapter aims to highlight the privacy issues in video surveillance and provides a model to help identify the privacy requirements in a video surveillance system. The authors make a step in the direction of investigating the existing legal infrastructure for ensuring privacy in video surveillance and suggest guidelines in order to help those who want to deploy video surveillance while least compromising the privacy of people and complying with legal infrastructure.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Contributors: Mahmood Rajpoot, Q., Jensen, C. D.
Number of pages: 25
Publication date: 2015

Host publication information
Title of host publication: Promoting Social Change and Democracy through Information Technology
Publisher: IGI global
Editors: Kumar, V., Svensson, J.
ISBN (Print): 9781466685024
ISBN (Electronic): 9781466685031
Electronic versions:
Video_Surveillance_Privacy_issues_and_legal_compliance.pdf
Source: PublicationPreSubmission
Source-ID: 110605574
Research output: Chapter in Book/Report/Conference proceeding > Book chapter – Annual report year: 2015 > Research > peer-review

Editorial: Thematic series on best articles from IFIPTM and PST

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, University of Málaga
Contributors: Fernandez-Gago, C., Jensen, C. D.
Number of pages: 2
Publication date: 2014
Peer-reviewed: No

Publication information
Journal: Journal of Trust Management
Volume: 1
Issue number: 2
ISSN (Print): 2196-064X
Original language: English
Electronic versions:
Editorial.pdf
DOIs:
Improving Usability of Passphrase Authentication

The combination of user-names and passwords has become the predominant method of user authentication in computer systems. Most users have multiple accounts on different systems, which impose different constraints on the length and complexity of passwords that the user is allowed to select. This is done to ensure an appropriate degree of security, but instead, it makes it difficult for users to remember their password, which results in passwords that are either insecure, but easy to remember, or written down on paper. In this paper we address the problem of usability in user authentication. We promote the use of passphrases, which provide better security and are often easier to remember than passwords. Passphrases will be significantly longer than passwords, which makes them more difficult to enter correctly on a keyboard. We solve this problem by proposing a new passphrase validation algorithm, which accepts the most common typing mistakes. The proposed algorithm has been implemented in secure hardware and integrated into a standard Unix system. We present the design, implementation and preliminary evaluation of the developed passphrase authentication prototype.

Remote Biometrics for Robust Persistent Authentication

This paper examines the problem of providing a robust non-invasive authentication service for mobile users in a smart environment. We base our work on the persistent authentication model (PAISE), which relies on available sensors to track principals from the location where they authenticate, e.g., through a smart card based access control system, to the location where the authentication is required by a location-based service. The PAISE model is extended with remote biometrics to prevent the decay of authentication confidence when authenticated users encounter and interact with other users in the environment. The result is a calm approach to authentication, where mobile users are transparently authenticated towards the system, which allows the provision of location-based services. The output of the remote biometrics are fused using error-rate-based fusion to solve a common problem that occurs in score level fusion, i.e., the scores of each biometric system are usually incompatible, as they have different score ranges as well as different probability distributions.

We have integrated remote biometrics with the PAISE prototype and the experimental results on a publicly available dataset, show that fusion of two remote biometric modalities, facial recognition and appearance analysis, gives a significant improvement over each of the individual experts. Furthermore, the experimental results show that using remote biometrics increases the performance of tracking in persistent authentication, by identifying principals who are difficult to track due to occlusions in crowded scenes.
Security and Privacy in Video Surveillance: Requirements and Challenges

Use of video surveillance has substantially increased in the last few decades. Modern video surveillance systems are equipped with techniques that allow traversal of data in an effective and efficient manner, giving massive powers to operators and potentially compromising the privacy of anyone observed by the system. Several techniques to protect the privacy of individuals have therefore been proposed, but very little research work has focused on the specific security requirements of video surveillance data (in transit or in storage) and on authorizing access to this data. In this paper, we present a general model of video surveillance systems that will help identify the major security and privacy requirements for a video surveillance system and we use this model to identify practical challenges in ensuring the security of video surveillance data in all stages (in transit and at rest). Our study shows a gap between the identified security requirements and the proposed security solutions where future research efforts may focus in this domain.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Contributors: Mahmood Rajpoot, Q., Jensen, C. D.
Pages: 169-184
Publication date: 2014

Host publication information
Publisher: Springer
Editors: Cuppens-Boulahia, N., Jajodia, S., El Kalam, A. A., Sans, T.
ISBN (Print): 978-3-642-55414-8
ISBN (Electronic): 978-3-642-55415-5
(IFIP AICT - Advances in Information and Communication technology, Vol. 428).
Keywords: Video Surveillance, Security, Privacy, Monitoring, Storage, Access Control, Encryption
DOIs: 10.1007/978-3-642-55415-5_14
Source: PublicationPreSubmission
Source-ID: 101151347
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2014 › Research › peer-review


General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, University of Luxembourg
Number of pages: 208
Publication date: 2014

Publication information
Publisher: Springer
ISBN (Print): 978-3-319-11850-5
ISBN (Electronic): 978-3-319-11851-2
Original language: English
(Lecture Notes in Computer Science, Vol. 8743).
DOIs: 10.1007/978-3-319-11851-2
Research output: Book/Report › Book – Annual report year: 2014 › Research › peer-review
The importance of trust in computer security

The computer security community has traditionally regarded security as a "hard" property that can be modelled and formally proven under certain simplifying assumptions. Traditional security technologies assume that computer users are either malicious, e.g. hackers or spies, or benevolent, competent and well informed about the security policies. Over the past two decades, however, computing has proliferated into all aspects of modern society and the spread of malicious software (malware) like worms, viruses and botnets have become an increasing threat. This development indicates a failure in some of the fundamental assumptions that underpin existing computer security technologies and that a new view of computer security is long overdue.

In this paper, we examine traditional models, policies and mechanisms of computer security in order to identify areas where the fundamental assumptions may fail. In particular, we identify areas where the "hard" security properties are based on trust in the different agents in the system and certain external agents who enforce the legislative and contractual frameworks.

Trust is generally considered a "soft" security property, so building a "hard" security mechanism on trust will at most give a spongy result, unless the underlying trust assumptions are made first class citizens of the security model. In most of the work in computer security, trust assumptions are implicit and they will surely fail when the environment of the systems change, e.g. when systems are used on a global scale on the Internet. We argue that making such assumptions about trust explicit is an essential requirement for the future of system security and argue why the formalisation of computational trust is necessary when we wish to reason about system security.

General information

Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Contributors: Jensen, C. D.
Pages: 1-12
Publication date: 2014

Host publication information

Title of host publication: Proceedings of the 8th IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2014)
Publisher: Springer
Editors: Zhou, J., Gal-Oz, N., Zhang, J., Gudes, E.
ISBN (Print): 978-3-662-43812-1
ISBN (Electronic): 978-3-662-43813-8
(IFIP AICT - Advances in Information and Communication technology, Vol. 430).
Keywords: Computer crime, Computer worms, Malware, Mobile security, Network security, Personal computing, Security systems, Computational trust, Computer security technology, Malicious software, Security community, Security mechanism, Security properties, Security technology, Simplifying assumptions, Security of data
DOIs: 10.1007/978-3-662-43813-8_1
Source: FindIt
Source-ID: 275304728
Research output: Chapter in Book/Report/Conference proceeding » Article in proceedings – Annual report year: 2015 » Research » peer-review

A collaborative approach to botnet protection

Botnets are collections of compromised computers which have come under the control of a malicious person or organisation via malicious software stored on the computers, and which can then be used to interfere with, misuse, or deny access to a wide range of Internet-based services. With the current trend towards increasing use of the Internet to support activities related to banking, commerce, healthcare and public administration, it is vital to be able to detect and neutralise botnets, so that these activities can continue unhindered. In this paper we present an overview of existing botnet detection techniques and argue why a new, composite detection approach is needed to provide efficient and effective neutralisation of botnets. This approach should combine existing detection efforts into a collaborative botnet protection framework that receives input from a range of different sources, such as packet sniffers, on-access anti-virus software and behavioural analysis of network traffic, computer sub-systems and application programs. Finally, we introduce ContraBot, a collaborative botnet detection framework which combines approaches that analyse network traffic to identify patterns of botnet activity with approaches that analyse software to detect items which are capable of behaving maliciously. © 2012 IFIP International Federation for Information Processing.

General information

Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering, Embedded Systems Engineering, Aalborg University
Collaborative trust evaluation for wiki security

Wiki systems form a subclass of the more general Open Collaborative Authoring Systems, where content is created and maintained by a user community. The ability of anyone to edit the content is, at the same time, their strength and their weakness. Anyone can write documents that improve the value of the wiki-system, but at the same time, anyone can also introduce errors into these documents, by accident or on purpose. A security model for wiki-style authoring systems has previously been proposed. This model is based on both static and dynamic document access controls that enforce a simple integrity based security policy. In this paper, we present a new policy for the existing wiki security model, which provides a higher degree of parameterization and adaptability. The new policy is analyzed and compared to the original policy. Our evaluation shows that this new policy provides stronger security when the number of malicious and colluding users is low, but it has a clearly defined level of tolerance in terms of the amount of work required by an attacker to achieve a given probability of violating the policy. Efforts beyond that level, can allow such users to take control of the system, but this is true for all soft security systems. We show that the system parameters can be tuned so that the amount of work required by malicious and colluding users to reach this level is well beyond most attackers' capabilities.

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering, Embedded Systems Engineering, Technical University of Denmark
Contributors: Lindberg, K., Jensen, C. D.
Pages: 176-184
Publication date: 2012

Host publication information
Title of host publication: 2012 Tenth Annual International Conference on Privacy, Security and Trust (PST)
Publisher: IEEE
DOIs: 10.1109/PST.2012.6297938
Source: dtu
Source-ID: n::oai:DTIC-ART:inspec/370240457::19686
Research output: Chapter in Book/Report/Conference proceeding – Article in proceedings – Annual report year: 2012 – Research – peer-review

Document and author promotion strategies in the secure wiki model
Wiki systems form a subclass of the more general Open Collaborative Authoring Systems, where content is created by a user community. The ability of anyone to edit the content is, at the same time, their strength and their weakness. Anyone can write documents that improve the value of the wiki-system, but this also means that anyone can introduce errors into documents, either by accident or on purpose. A security model for wiki-style authoring systems, called the Secure Wiki Model, has previously been proposed to address this problem. This model is designed to prevent corruption of good quality documents, by limiting updates, to such documents, to users who have demonstrated their ability to produce documents of similar or better quality. While this security model prevents all user from editing all documents, it does respect the wiki philosophy by allowing any author who has produced documents of a certain quality to edit all other documents of similar or poorer quality. Moreover, authors who consistently produce top quality documents will eventually
be allowed to edit all documents in the wiki. Collaborative filtering is used to evaluate the quality of documents that an author has contributed to the system, thus determining what other documents that the author can edit. This collaborative filtering mechanism, determines the promotion and demotion of documents and authors in the Secure Wiki Model. The original Secure Wiki Model only considers explicit promotion and demotion of documents, authors are implicitly promoted/demoted depending on the promotion/demotion of the documents that they contribute. In this paper, we revisit the question of promotion of documents and authors and propose a new security policy with explicit promotion of authors. This policy also incorporates a new collaborative filtering mechanism with a higher degree of parametrisation, so that the new policy can be adapted to the specific needs of a particular wiki. © 2012 IFIP International Federation for Information Processing.

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering, Embedded Systems Engineering, Technical University of Denmark
Contributors: Lindberg, K., Jensen, C. D.
Pages: 247-252
Publication date: 2012
Peer-reviewed: Yes

Publication information
Journal: IFIP AICT - Advances in Information and Communication technology
Volume: 374
ISSN (Print): 1868-4238
Ratings:
BFI (2012): BFI-level 1
Scopus rating (2012): CiteScore 0.15
ISI indexed (2012): ISI indexed no
Original language: English
Keywords: Information technology, Supervisory personnel
DOIs:
10.1007/978-3-642-29852-3_20
Source: dtu
Source-ID: n:oai:DTIC-ART:compendex/370668152::19905
Research output: Contribution to journal › Conference article – Annual report year: 2012 › Research › peer-review

First Workshop on Incentives and Trust in E-Commerce (WIT-EC’12)

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering, Embedded Systems Engineering, Communication Research Centre, Nanyang Technological University
Number of pages: 102
Publication date: 2012

Publication information
Original language: English
URLs:

Bibliographical note
Research output: Book/Report › Book – Annual report year: 2012 › Research

Post-Session Authentication
Entity authentication provides confidence in the claimed identity of a peer entity, but the manner in which this goal is achieved results in different types of authentication. An important factor in this regard is the order between authentication and the execution of the associated session. In this paper, we consider the case of post-session authentication, where parties authenticate each other at the end of their interactive session. This use of authentication is different from sessionless authentication (e.g., in RFID) and pre-session authentication (e.g., for access control.) Post-session authentication, although a new term, is not a new concept; it is the basis of at least a few practical schemes. We, for the first time, systematically study it and present the underlying authentication model. Further, we show that an important class of problems is solvable using post-session authentication as the only setup assumption. We hope post-session authentication can be used to devise new strategies for building trust among strangers.
The Role of Trust in Computer Security

Summary form only given. Traditional security technologies are based on numerous assumptions about the environment in which systems are used. This includes assumptions about the enforcement of legislative and contractual frameworks, limitations of particular technologies and the constraints on human behaviour imposed by social and religious norms. Most of these assumptions, however, are implicit and they will fail when the environment of the systems change, e.g., when systems are used on a global scale on the Internet. This talk identifies such implicit assumptions in current security technologies and show how many of them concern the placement of trust on human or system agents. We argue that making such assumptions about trust explicit is an essential requirement for the future of system security and argue why the formalisation of computational trust is necessary when we wish to reason about system security.

Towards Symbolic Encryption Schemes

Symbolic encryption, in the style of Dolev-Yao models, is ubiquitous in formal security models. In its common use, encryption on a whole message is specified as a single monolithic block. From a cryptographic perspective, however, this may require a resource-intensive cryptographic algorithm, namely an authenticated encryption scheme that is secure under chosen ciphertext attack. Therefore, many reasonable encryption schemes, such as AES in the CBC or CFB mode, are not among the implementation options. In this paper, we report new attacks on CBC and CFB based implementations of the well-known Needham-Schroeder and Denning-Sacco protocols. To avoid such problems, we advocate the use of refined notions of symbolic encryption that have natural correspondence to standard cryptographic encryption schemes.
Adaptable Authentication Model: Exploring Security with Weaker Attacker Models

Most methods for protocol analysis classify protocols as "broken" if they are vulnerable to attacks from a strong attacker, e.g., assuming the Dolev-Yao attacker model. In many cases, however, exploitation of existing vulnerabilities may not be practical and, moreover, not all applications may suffer because of the identified vulnerabilities. Therefore, we may need to analyze a protocol for weaker notions of security. In this paper, we present a security model that supports such weaker notions. In this model, the overall goals of an authentication protocol are broken into a finer granularity; for each fine level authentication goal, we determine the "least strongest-attacker" for which the authentication goal can be satisfied. We demonstrate that this model can be used to reason about the security of supposedly insecure protocols. Such adaptability is particularly useful in those applications where one may need to trade-off security relaxations against resource requirements.

Building a Reputation System for Wikipedia

Wikipedia is a web-based encyclopedia, written and edited collaboratively by Internet users. Wikipedia has an extremely open editorial policy that allows anybody to create or modify articles. This has promoted a broad and detailed coverage of subjects, but also introduced problems relating to the quality of articles. The Wikipedia Recommender System (WRS) was developed to help users determine the credibility of articles based on feedback from other Wikipedia users. The WRS provides a rating which emphasizes feedback from recommenders that the user has agreed with in the past. This paper presents some of the work that has gone into the development of the Wikipedia Recommender System. We first
developed a generic architecture for integrating a reputation system into existing legacy systems and based our design of the WRS on this architecture. Both the generic architecture and our design of the WRS are outlined in this paper. Finally, we present ongoing work to improve the reputation rating of the WRS by determining the areas of expertise for the different feedback providers in the WRS. This will allow more accurate recommendations because the system can assign a higher weight to feedback from recommenders that have previously demonstrated competence in the area of the article. In order to determine the areas of expertise of recommenders, however, we first need to identify a way to classify content in Wikipedia. We outline current efforts to evaluate different classification schemes and illustrate how knowing the expertise of recommenders may help us when we calculate the rating for a Wikipedia article.

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Contributors: Jensen, C. D.
Pages: 89-112
Publication date: 2011

Host publication information
Title of host publication: New Forms of Collaborative Innovation and Production on the Internet: An Interdisciplinary Perspective
Publisher: Universitätsverlag Göttingen
Editors: Wittke, V., Hanekop, H.
ISBN (Print): 978-3-86395-020-0
Electronic versions: 395250.pdf
URLs: http://oapen.org/search?identifier=395250

Bibliographical note
This work is licensed under the Creative Commons License 3.0 “by-nd”, allowing you to download, distribute and print the document in a few copies for private or educational use, given that the document stays unchanged and the creator is mentioned. You are not allowed to sell printed copies of the free version.

Source: orbit
Source-ID: 316280
Research output: Chapter in Book/Report/Conference proceeding > Book chapter – Annual report year: 2011 > Research > peer-review

Classification of Recommender Expertise in the Wikipedia Recommender System
The Wikipedia is a web-based encyclopedia, written and edited collaboratively by Internet users. The Wikipedia has an extremely open editorial policy that allows anybody, to create or modify articles. This has promoted a broad and detailed coverage of subjects, but also introduced problems relating to the quality of articles. The Wikipedia Recommender System (WRS) was developed to help users determine the credibility of articles based on feedback from other Wikipedia users. The WRS implements a collaborative filtering system with trust metrics, i.e., it provides a rating of articles *which emphasizes feedback from recommenders that the user has agreed with in the past. This exposes the problem that most recommenders are not equally competent in all subject areas. The first WRS prototype did not include an evaluation of the areas of expertise of recommenders, so the trust metric used in the article ratings reflected the average competence of recommenders across all subject areas. We have now developed a new version of the WRS, which evaluates the expertise of recommenders within different subject areas. In order to do this, we need to identify a way to classify the subject area of all the articles in the Wikipedia. In this paper, we examine different ways to classify the subject area of Wikipedia article according to well established knowledge classification schemes. We identify a number of requirements that a classification scheme must meet in order to be useful in the context of the WRS and present an evaluation of four existing knowledge classification schemes with respect to these requirements. This evaluation helped us identify a classification scheme, which we have implemented in the current version of the Wikipedia Recommender System.

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling, Technical University of Denmark
Contributors: Jensen, C. D., Pilkauskas, P., Lefevre, T.
Pages: 884-902
Publication date: 2011
Peer-reviewed: Yes

Publication information
Journal: Information and Media Technologies
Volume: 6
Classification of Recommender Expertise in the Wikipedia Recommender System

The Wikipedia is a web-based encyclopedia, written and edited collaboratively by Internet users. The Wikipedia has an extremely open editorial policy that allows anybody to create or modify articles. This has promoted a broad and detailed coverage of subjects, but also introduced problems relating to the quality of articles. The Wikipedia Recommender System (WRS) was developed to help users determine the credibility of articles based on feedback from other Wikipedia users. The WRS implements a collaborative filtering system with trust metrics, i.e., it provides a rating of articles which emphasizes feedback from recommenders that the user has agreed with in the past. This exposes the problem that most recommenders are not equally competent in all subject areas. The first WRS prototype did not include an evaluation of the areas of expertise of recommenders, so the trust metric used in the article ratings reflected the average competence of recommenders across all subject areas. We have now developed a new version of the WRS, which evaluates the expertise of recommenders within different subject areas. In order to do this, we need to identify a way to classify the subject area of all the articles in the Wikipedia. In this paper, we examine different ways to classify the subject area of Wikipedia articles according to well established knowledge classification schemes. We identify a number of requirements that a classification scheme must meet in order to be useful in the context of the WRS and present an evaluation of four existing knowledge classification schemes with respect to these requirements. This evaluation helped us identify a classification scheme, which we have implemented in the current version of the Wikipedia Recommender System.

Demarcation of Security in Authentication Protocols

Security analysis of communication protocols is a slippery business; many "secure" protocols later turn out to be insecure. Among many, two complaints are more frequent: inadequate definition of security and unstated assumptions in the security model. In our experience, one principal cause for such state of affairs is an apparent overlap of security and correctness, which may lead to many sloppy security definitions and security models. Although there is no inherent need to separate security and correctness requirements, practically, such separation is significant. It makes security analysis easier, and enables us to define security goals with a fine granularity. We present one such separation, by introducing the notion of binding sequence as a security primitive. A binding sequence, roughly speaking, is the only required security property of an authentication protocol. All other authentication goals, the correctness requirements, can be derived from the binding sequence.
Security of Dependable Systems

Security and dependability are crucial for designing trustworthy systems. The approach “security as an add-on” is not satisfactory, yet the integration of security in the development process is still an open problem. Especially, a common framework for specifying dependability and security is very much needed. There are many pressing challenges however; here, we address some of them. Firstly, security for dependable systems is a broad concept and traditional view of security, e.g., in terms of confidentiality, integrity and availability, does not suffice. Secondly, a clear definition of security in the dependability context is not agreed upon. Thirdly, security attacks cannot be modeled as a stochastic process, because the adversary’s strategy is often carefully planned. In this chapter, we explore these challenges and provide some directions toward their solutions.

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Contributors: Ahmed, N., Jensen, C. D.
Pages: 230-264
Publication date: 2011

Host publication information
Title of host publication: Dependability and Computer Engineering : Concepts for Software Intensive Systems
Publisher: IGI global
Editor: Petre, L.
Edition: 1
ISBN (Print): 1609607473
Source: orbit
Source-ID: 268872
Research output: Chapter in Book/Report/Conference proceeding › Book chapter – Annual report year: 2011 › Education › peer-review
Towards Secure Intelligent Buildings

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Contributors: Ingwar, M. I., Jensen, C. D.
Publication date: 2011

Host publication information
Title of host publication: Proceedings of the 5th Nordic Workshop on Dependability and Security (NODES’11)
URLs:
Source: orbit
Source-ID: 316295
Research output: Chapter in Book/Report/Conference proceeding

Trust Management V: 5th IFIP WG 11.11 International Conference, IFIPTM 2011, Copenhagen, Denmark, June 29 - July 1, 2011, Proceedings

This book constitutes the refereed proceedings of the 5th IFIP WG 11.11 International Conference, IFIPTM 2011, held in Copenhagen, Denmark, in June/July 2011. The 14 revised full papers and 8 short papers presented together with the abstracts of 4 keynote talks were carefully reviewed and selected from 42 submissions. The papers feature both theoretical research and real-world case studies from academia, business and government focusing on areas such as: trust models, social and behavioral aspects of trust, trust in networks, mobile systems and cloud computation, privacy, reputation systems, and identity management.

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Number of pages: 335
Publication date: 2011

Host publication information
Title of host publication: Trust Management V
Publisher: Springer
ISBN (Print): 978-3-642-22199-6
URLs:
Source: orbit
Source-ID: 316397
Research output: Chapter in Book/Report/Conference proceeding

Workshop Proceedings of the Fifth IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2011)

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Publication date: 2011

Host publication information
Title of host publication: Workshop Proceedings of the Fifth IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2011)
Source: orbit
Source-ID: 316400
Research output: Chapter in Book/Report/Conference proceeding

Adaptable Authentication Model - for Exploring the Weaker Notions of Security

There are at least a few hundred published protocols that fall in the category of authentication and key establishment. Under a naive definition of authentication and key establishment, the existence of so many protocols is quite fascinating and somewhat stunning for a newcomer to the field of communication security. One potent argument often presented is we keep designing new protocols due the demand of new type of applications and due to the discovery of flaws in existing
protocols. While designing new protocols for new type of applications, such as RFID, is definitely an important driving factor nevertheless the most among the published protocols are in fact the result of discovery of flaws in their predecessors. As our understanding of cryptography and protocol analysis is getting mature, the ability to discover new flaws in the protocols also increases. We now have a better understanding of actual operational environment. In past, this often caused increasing the power of attacker model, for instance, now a days we also consider privacy concerns and side channel leakage beside the classic Dolev-Yao attacker. A protocol is labeled as insecure protocol once an effective attack or flaw is found in it. In fact, the most of the published protocols are considered insecure from this point of view. In practice, however, this approach has a side effect, namely, we rarely bother to explore how much insecure is the protocol. This question asks us to explore the area between security and insecurity; after all neither a flawed protocol is always completely insecure neither all applications require the security against an all powerful attacker. The current approach towards security analysis, which we call strict security, considers a protocol along with a powerful attacker, such as Dolev-Yao attacker and sometimes with additional capabilities such as dynamic corruption of communicating nodes. Then, one tries to show that the protocol achieves its objective under this specific attacker. Naturally there are three possibilities: one may succeed in constructing a security proof; one may fail in proving security, which often makes the protocol suspicious; or one may discover a concrete attack, which definitely makes the protocol insecure under such strict definition of the attacker. There is however an alternate — adaptable security, which we propose as a more general approach to the security problem. The approach considers correct protocols, i.e., protocols that achieve their objectives when there exist no effective attacker. All correct protocols are assumed to be secure and the challenge we pose for a security analyst is to derive the least strongest attacker (LSA) model for which the, so-called, a priori assumption about security holds. In this way, the security definition of a protocol can be adapted to suitable choice of LSA. Another aspect of the proposed approach is the flexible treatment of security goals; we decompose high level security goals in many fine level goals and a protocol may achieve only a subset of all fine level goals. We believe that these flexible choices of attackers and security goals are more practical in many real world scenarios. An applications may require the protection against a weaker attacker and may require to achieve fewer security goals.
the emerging energy distribution infrastructure. In particular, we examine the security problems that arise in the area of wind power communication infrastructures based on the IEC 61400-25 and IEC 62351 standards. These standards define ways of representing elements of the wind power infrastructure in a software domain in a manufacturer independent manner as well as establishing secure communication and authenticating the other parties in electrical power infrastructures, but they do not address the problem of access control. We therefore propose a generic model for access control in wind power systems, which is based on the widely used role-based access control model. The proposed model is tested using a prototype designed in conformance with the standards that are in use in modern wind power infrastructure and the results are presented to determine the overhead in communication caused while adhering to the proposed access model.

**General information**
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling, Technical University of Denmark
Contributors: Nagarajan, A., Jensen, C. D.
Pages: 35-49
Publication date: 2010
Peer-reviewed: Yes

**Publication information**
Journal: Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications
Volume: 1
Issue number: 4
ISSN (Print): 2093-5374
Original language: English
Source: orbit
Source-ID: 270643

**Building a reputation system for the Wikipedia**

**General information**
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Embedded Systems Engineering
Contributors: Jensen, C. D.
Publication date: 2010

**Event information**
Event: New Forms of Collaborative Production and Innovation : Economic, Social, Legal and Technical Characteristics and Conditions
Location: Lichtenberg Kolleg, Georg-August-Universität, Göttingen
Source: orbit
Source-ID: 270638
Research output: Non-textual form – Sound/Visual production (digital) – Annual report year: 2010 – Research

**Classifying Areas of Expertise in the wikipedia Recommender System**

**General information**
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling, Technical University of Denmark
Contributors: Jensen, C. D., Lefévre, T.
Publication date: 2010

**Host publication information**
Title of host publication: Short Paper Proceedings of the Fourth IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2010)
Source: orbit
Source-ID: 270637

**Definition of Entity Authentication**
Authentication is considered a pre-requisite for communication security, but the definition of authentication is generally not agreed upon. Many attacks on authentication protocols are the result of misunderstanding of the goals of authentication.
This state of affairs indicate limitations in theoretical understanding of the meanings of authentication. We provide a new insight in this direction and formalize it in CFPS (Common Framework for authentication Protocols’ Specifications). CFPS provides a precise scope of definition for authentication protocols, which could make the design and analysis process more systematic.

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Contributors: Ahmed, N., Jensen, C. D.
Number of pages: 7
Publication date: 2010

Host publication information
Title of host publication: Proceedings of 2nd International Workshop on Security and Communication Networks (IWSCN), 2010
Publisher: IEEE Xplore
Keywords:
DOIs:
10.1109/IWSCN.2010.5498000
URLs:
http://ieeexplore.ieee.org/Xplore/guesthome.jsp
Source: orbit
Source-ID: 260071
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2010 › Research › peer-review

Entity Authentication: Analysis using Structured Intuition
In this paper, we propose a new method for the analysis that uses intuition of the analyst in a structured way. First we define entity authentication in terms of fine level authentication goals (FLAGs). Then we use some relevant structures in protocol narrations and use them to justify FLAGs for the protocol. All along this process, we discover vulnerabilities and unstated assumptions of the protocol. As the method is intuition based, the quality of results depends on the expertise of the security analyst, however, the structured intuition has two major advantages: Firstly we get a precise specification of security in terms of FLAGs; and secondly the outcome can be used to transform basic protocol narrations into more detailed specifications, which makes a subsequent formal analysis much more meaningful.

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Contributors: Ahmed, N., Jensen, C. D.
Publication date: 2010

Host publication information
Title of host publication: Technical Report on NODES10 Proceedings
URLs:
http://nodes.imm.dtu.dk/nodes2010.html
Source: orbit
Source-ID: 262568
Research output: Chapter in Book/Report/Conference proceeding › Conference abstract in proceedings – Annual report year: 2010 › Research › peer-review

Et visionært teknologidesign
General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, Embedded Systems Engineering
Contributors: Jensen, C. D.
Publication date: 2010

Event Information
Event: PrivatTek 2010
Location: Landstingssalen, Christiansborg
Electronic versions:
PrivatTek2010-CDJ.pdf
Supporting Multi-Agent Reputation Calculation in the Wikipedia Recommender System

The Wikipedia is a web-based encyclopedia, written and edited collaboratively by Internet users. Over the past decade, the Wikipedia has experienced a dramatic growth in popularity and is considered by many the primary source of information on the Internet. The Wikipedia has an extremely open editorial policy that allows anybody, to create or modify articles. This has resulted in a broad and detailed coverage of subjects, but it has also caused problems relating to the quality of articles. The Wikipedia Recommender System (WRS) was developed to help human users determine the credibility of an article based on feedback from other Wikipedia users. The WRS calculates a personalised rating for any Wikipedia article based on feedback (recommendations) provided by other Wikipedia users. As part of this process, WRS users are expected to provide their own feedback about the quality of Wikipedia articles that they have read. This makes the WRS a rating-based collaborative filtering system, which implements trust metrics to determine the weight of feedback from different recommenders. In this paper the authors describe the WRS outlining some of the requirements and constraints that shaped the design of the system. The authors also provide a brief overview of the implementation of the WRS prototype. The WRS addresses the general problem of establishing trust in a collaboratively generated resource in a distributed multi-agent system, so the authors believe that the general architecture that underlies the WRS applies to many other applications in such systems.

General information
Publication status: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Contributors: Jensen, C. D.
Pages: 273-282
Publication date: 2010
Peer-reviewed: Yes

Publication information
The Role of Trust in Persistent Authentication

A Mechanism for Identity Delegation at Authentication Level

Authentication and access control are normally considered separate security concepts that have separate goals and are supported by separate security mechanisms. In most operating systems, however, access control is exclusively based on the identity of the requesting principal, e.g., an access control mechanism based on Access Control Lists simply verifies that the authenticated identity of the requesting principal is on the list of authorized users. In this paper we propose a delegation mechanism for nomadic users, which exploits the amalgamation of authentication and access control in most operating systems, by delegating privileges at the identity level. The complexity of classic delegation models, especially if it strictly follows the principle of least privileges, often leads to poor usability which motivates a user to circumvent the default delegation mechanism. On the other hand, the identity delegation makes good use of trust relationships between users of a particular environment and offers the possibility of improved usability. Although it might violate the principle of least privileges, but practically it could increase the overall security of a nomadic environment where users need to frequently delegate their duties. The proposed mechanism is independent of the choice of access control mechanism, as there is no distinction between a delegator and a delegatee for the rest of the system and the delegation event is only logged at the authentication level. Due to its improved usability, the motivation of sharing authentication tokens is reduced.
An Authentication Framework for Nomadic Users

Security and usability are often horn locked and system administrators tend to configure systems so that they favor security over usability. In many cases, however, the increased security results in usability that is so poor that users feel the need to circumvent the security mechanisms. This is probably best explained by considering password based authentication, where a user is actively involved in the process. If the time required to log in to an account is considered too high, users tend to leave their terminals logged in throughout the day and share their account with other users. This is particularly true for nomadic users who move around in ubiquitous computing environments and avail from different IT services from many different locations. In many ubiquitous computing environments, where information processing is not considered the main priority, management often accepts this practise in order to increase productivity, e.g., in a hectic hospital environment, medical staff has to login and logout of various machines several times in an hour, but the repeated interactions consume a considerable amount of time, causing organizational inefficiency, job frustration and a tendency towards defeating the obstacle by leaving terminals logged in or choosing short and easy to type passwords. Therefore, a password based authentication mechanism, which is quite simple and secure in personal computing, has become too cumbersome for nomadic users, which means that other means of authentication must be developed for nomadic users. In this paper, we focus on usability of authentication for nomadic users in a ubiquitous computing environment. We identify requirements for authentication of nomadic users and propose an authentication framework for this class of users. A prototype of the proposed authentication framework has been developed, which supports persistent and multi-factor authentication without the active intervention of a user. We evaluate the usability of the developed mechanism by considering the time required to authenticate when logging in to a workstation and compare this to classic password based authentication. The evaluation shows that the proposed mechanism saves a significant amount of time for the nomadic users, which reduces the incentive to circumvent the authentication mechanism. Thus, the mechanism will both provide users with better job satisfaction and increased organizational efficiency, while at the same time increase the effective level of security of the system.

Context-Aware Identity Delegation

In emerging ubiquitous computing, related nomadic users often perform similar tasks and share the same computing infrastructure. This means that security of the shared resources is of prime importance. Frequent delegation of tasks among users must be anticipated as most nomadic environments are hectic and very dynamic. A delegation mechanism with a slightly complicated user interface will not only reduce the productivity but also provide nomadic users with a strong motivation to circumvent the mechanism itself. Delegation in access control domain is not practical for the most of nomadic users due to its complicated and complex structure. Identity delegation at authentication level provides improved usability, which reduces the risk of circumventing the delegation mechanism; at the same time, however, identity delegation violates the principle of least privileges. We use contextual information of a delegatee to mitigate this violation, which helps to achieve a higher level of practical security in nomadic environments.
Security in Wiki-Style Authoring Systems

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Jensen, C. D.
Number of pages: 322
Pages: 81-98
Publication date: 2009

Host publication information
Title of host publication: Trust Management III : Third IFIP WG 11.11 International Conference
Publisher: Springer
ISBN (Print): 978-3-642-02055-1
(IFIP Advances in Information and Communication Technology; No. 300).
Source: orbit
Source-ID: 245899
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2009 › Research › peer-review

Why Security is Bad for Trust

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

Event information
Event: 3rd IFIP International Conference on Trust Management
Location: Purdue University, West Lafayette, United States

Bibliographical note
Slides from Panel on "Social Trust and Computational Norms"
Source: orbit
Source-ID: 249764
Research output: Non-textual form › Sound/Visual production (digital) – Annual report year: 2009 › Research

WRS Demonstration Posters

General information
Publication status: Published
Organisations: System Security, Department of Informatics and Mathematical Modeling
Contributors: Jensen, C. D.
Publication date: 2009
Peer-reviewed: Yes
Event: Poster session presented at 3rd IFIP International Conference on Trust Management, West Lafayette, United States.

Bibliographical note
The two posters in the deposited files were used as a back drop for the demonstration. Posters were not reviewed, but the proposal for demonstration was.
Source: orbit
Source-ID: 246036
Research output: Contribution to conference › Poster – Annual report year: 2009 › Research › peer-review

WRS: The Wikipedia Recommender System

General information
Publication status: Published
Organisations: System Security, Department of Informatics and Mathematical Modeling
Contributors: Lefêvre, T., Jensen, C. D., Thomas Rune, K.
Dynamics of Trust Evolution: Auto-configuration of dispositional trust dynamics

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling, System Security
Contributors: Jensen, C. D., Korsgaard, T. R.
Number of pages: 558
Pages: 509-518
Publication date: 2008

Host publication information
Title of host publication: Proceedings of International Conference on Security and Cryptography
Place of publication: Portugal
Publisher: Institute for Systems and Technologies of Information, Control and Communication
Keywords: security, trust management, auto-configuration
Source: orbit
Source-ID: 223465
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2008 › Research › peer-review

On the Need for Relaxed Security Models

General information
Publication status: Published
Organisations: System Security, Department of Informatics and Mathematical Modeling
Contributors: Jensen, C. D.
Publication date: 2008

Event information
Event: International Conference on E-business and Telecommunication networks
Location: Porto, Portugal
Source: orbit
Source-ID: 222589
Research output: Non-textual form › Sound/Visual production (digital) – Annual report year: 2008 › Research

Persistent Authentication in Smart Environments

General information
Publication status: Published
Organisations: System Security, Department of Informatics and Mathematical Modeling
Contributors: Hansen, M. S., Kirschmeyer, M., Jensen, C. D.
Pages: 31-44
Publication date: 2008

Host publication information
Title of host publication: Proceedings of the 2nd International Workshop on Combining Context with Trust, Security and Privacy (CAT 08)
Practical Privacy Assessment
This chapter proposes a privacy assessment model called the Operational Privacy Assessment Model that includes organizational, operational and technical factors for the protection of personal data stored in an IT system. The factors can be evaluated in a simple scale so that not only the resulting graphical depiction can be easily created for an IT system, but graphical comparisons across multiple IT systems are also possible. Examples of factors presented in a Kiviat graph are also presented. This assessment tool may be used to standardize privacy assessment criteria, making it less painful for the management to assess privacy risks on their systems.

General information
Publication status: Published
Organisations: System Security, Department of Informatics and Mathematical Modeling
Contributors: Peen, S., Jansen, T. W., Jensen, C. D.
Number of pages: 462
Publication date: 2008

Host publication information
Title of host publication: Online Consumer Protection: : Theories of Human Relativism
Publisher: Idea Group Publishing
Editors: Chen, K., Fadlalla, A.
ISBN (Print): 978-1-60566-012-7
Source: orbit
Source-ID: 224087
Research output: Chapter in Book/Report/Conference proceeding › Book chapter – Annual report year: 2008 › Research › peer-review

Reengineering the Wikipedia for Reputation
The Wikipedia is a free online encyclopedia collaboratively edited by Internet users with a minimum of administration. Anybody can write an article for the Wikipedia and there is no verification of the author’s expertise on the particular subject. This may lead to problems relating to the quality of articles, especially completeness and correctness of information, and inaccuracies in the Wikipedia have been rumoured to cause students to fail courses; innocent people have been associated with the killing of John F. Kennedy, etc. Providing a means to assess the correctness, completeness and impartiality of information in the Wikipedia is therefore vitally important for the users to build trust in the Wikipedia and ensure the continued success and growth of the system. Integrating a reputation system into the Wikipedia would help users assess the quality of articles and provide a powerful incentive for authors to improve the quality of their articles. There are currently more than 7.5 million articles in the Wikipedia, and more than a thousand new articles are added daily, so the investment in the existing system is significant. The introduction of a recommendation system should therefore not require any modifications to the existing Wikipedia software. In this paper we examine the problem of reengineering a large and popular system, in this case the Wikipedia, in order to include a reputation system. We propose a recommendation system, which allows Wikipedia users to calculate a personalised rating for any article based on feedback (recommendations) provided by other Wikipedia users. The recommendation system developed for the Wikipedia is based on a general architecture, which we believe applies to many existing applications for online collaboration. The proposed recommendation system is implemented in a proxy placed between the user’s web-browser and the Wikipedia server, e.g., on the user’s own machine, so there is no need to modify Wikipedia servers or software. A simple prototype of the proposed recommendation system is presented in this paper along with a preliminary evaluation of the prototype.

General information
Publication status: Published
Organisations: System Security, Department of Informatics and Mathematical Modeling
Contributors: Korsgaard, T. R., Jensen, C. D.
Pages: 71-84
Publication date: 2008

Host publication information
Title of host publication: Proceedings of the 4th International Workshop on Security and Trust Management (STM 08)
Source: orbit
Source-ID: 220972
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2008 › Research › peer-review
Assessment of Privacy in Government IT-Systems

General information
Publication status: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Contributors: Peen, S., Jansen, T. W., Jensen, C. D.
Publication date: 2007

Host publication information
Title of host publication: First International Workshop on Sustaining Privacy in Autonomous Collaborative Environments (SPACE 2007) July 30, 2007
Source: orbit
Source-ID: 202545

Co-Authentication: An Authentication Paradigm for the Global Computing Infrastructure

General information
Publication status: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Contributors: Jónsson, E., Jensen, C. D.
Publication date: 2007

Host publication information
Title of host publication: NODES 07 - NOrdic workshop and doctoral symposium on Dependability and Security
Place of publication: Oslo, Norway
URLs:
http://www2.imm.dtu.dk/pubdb/views/publication_details.php?id=5498
Source: orbit
Source-ID: 205560

End-by-Hop Data Integrity

General information
Publication status: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Contributors: Jensen, C. D., Farrell, S.
Publication date: 2007
Integrity in Open Collaborative Authoring Systems

General information
Publication status: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Contributors: Jensen, C. D.
Pages: 399-402
Publication date: 2007

Resilia: a Safe and Secure Distributed Backup System for Small and Medium Enterprises

General information
Publication status: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Contributors: Jensen, C. D., Meira, F., Nittegaard-Nielsen, J.
Pages: 383-398
Publication date: 2007

Trust Management in Open Grid Systems

General information
Publication status: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Contributors: Jensen, C. D., Sharp, R.
Publication date: 2007
Trust Evolution Policies for Security in Collaborative Ad Hoc Applications

The vision of pervasive computing has introduced the notion of a vast, networked infrastructure of heterogeneous entities interact through collaborative applications, e.g., playing a multi-player online game on the way to work. This will require interactions between users who may be marginally known or completely unknown to each other, or in situations where complete information is unavailable. This introduces the problem of assigning access rights to such marginally known or unknown entities. Explicit trust management has emerged as a solution to the problem of dealing with partial information about other users and the context in which the interaction takes place. We have implemented an access control mechanism based on the human notion of trust, where recommendations or initial participation in low risk interactions will allow entities to slowly build trust in each other. As the trust between two entities grows, interactions that entail a higher degree of risk may be allowed to proceed. We have used this mechanism in a simple role-based access control mechanism that uses trust to assign roles to users in a distributed blackjack card game application. This application allows us to experiment with different policies for trust-based admission control and trust evolution. In this paper we present an evaluation of policies specifying trust dynamics, which shows that our prototype reacts appropriately to the behaviour of other users and that the system updates trust values and implements admission policies in a manner similar to what would be expected from human trust assessment. This indicates that trust evolution policies can replace explicit human intervention in application scenarios that are similar to the evaluated prototype.

General information
Publication status: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Pages: 95-111
Publication date: 2006
Peer-reviewed: Yes

Publication information
Journal: Electronic Notes in Theoretical Computer Science
Volume: 157
Issue number: 3
ISSN (Print): 1571-0661
Ratings:
Scopus rating (2006): SJR 0.386 SNIP 0.672
Original language: English
Keywords: Trust Dynamics, Trust Formation, Trust Management
DOIs:
10.1016/j.entcs.2005.09.038

Bibliographical note
Journal publication of STM 2005 paper
Source: orbit
Source-ID: 191461
Research output: Contribution to journal › Journal article – Annual report year: 2006 › Research › peer-review

Security in open Grid systems

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Jensen, C. D., Krogh, J.
Pages: 3
Publication date: 2005
Peer-reviewed: No

Publication information
Journal: Public Service Review: Nordic States
Original language: English
URLs:
The Claim Tool Kit for ad hoc recognition of peer entities

**General information**
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Seigneur, J., Jensen, C. D.
Pages: 49-71
Publication date: 2005
Peer-reviewed: Yes

**Publication information**
Journal: Science of Computer Programming
Volume: 54
Issue number: 1
Original language: English
URLs:
http://www2.imm.dtu.dk/pubdb/p.php?3407
Source: orbit
Source-ID: 185633
Research output: Contribution to journal › Journal article – Annual report year: 2005 › Research › peer-review

Trust Evolution Policies for Security in Collaborative Ad Hoc Applications

**General information**
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Publication date: 2005

**Host publication information**
Title of host publication: Proceedings of the 1st International Workshop on Security and Trust Management
URLs:
http://www2.imm.dtu.dk/pubdb/p.php?4091
Source: orbit
Source-ID: 185689
Research output: Contribution to journal › Journal article – Annual report year: 2005 › Research › peer-review

Trust Transfer: Encouraging Self-Recommendations without Sybil Attack

**General information**
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Seigneur, J., Gray, A., Jensen, C. D.
Pages: 321-337
Publication date: 2005

**Host publication information**
Title of host publication: Third International Conference on Trust Management
Publisher: Springer Verlag
URLs:
http://www2.imm.dtu.dk/pubdb/p.php?3888
Source: orbit
Source-ID: 185744
Research output: Contribution to journal › Journal article – Annual report year: 2005 › Research › peer-review
Trust Enhanced Ubiquitous Payment without Too Much Privacy Loss

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Seigneur, J., Jensen, C. D.
Publication date: 2004


General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Publication date: 2004

Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience

General information
Publication status: Published
Organisations: Department of Photonics Engineering, Department of Informatics and Mathematical Modeling
Contributors: Engberg, S. J., Harning, M. B., Jensen, C. D.
Publication date: 2004
A Unified Security Framework for Networked Applications

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Abendroth, J., Jensen, C. D.
Publication date: 2003

Host publication information
Title of host publication: Eighteenth ACM Symposium on Applied Computing
URLs:
Source: orbit
Source-ID: 58496

Cryptographic Access Control in a Distributed File System

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Harrington, A., Jensen, C. D.
Pages: 158-165
Publication date: 2003

Host publication information
Title of host publication: 8th ACM Symposium on Access Control Models and Technologies
URLs:
Source: orbit
Source-ID: 58527

End-to-end trust in pervasive computing starts with recognition

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Seigneur, J., Farrell, S., Jensen, C. D., Gray, E., Chen, Y.
Publication date: 2003

Host publication information
Title of host publication: First International Conference on Security in Pervasive Computing, March 12 - 14, in Boppard, Germany
URLs:
Source: orbit
Source-ID: 58560

Initial Investigation into Cross-Context Trust and Risk Assessment

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Gray, E., Chen, Y., Jensen, C. D.
Publication date: 2003

Host publication information
P2P with JXTA-Java pipes

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Seigneur, J., Biegel, G., Jensen, C. D.
Publication date: 2003

Host publication information
Title of host publication: 2nd International Conference on the Principles and Practice of Programming in Java
Publisher: ACM
URLs:
Source: orbit
Source-ID: 58558
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2003 › Research › peer-review

Partial Outsourcing: A New Paradigm for Access Control

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Abendroth, J., Jensen, C. D.
Pages: 134-141
Publication date: 2003

Host publication information
Title of host publication: 8th ACM Symposium on Access Control Models and Technologies
URLs:
Source: orbit
Source-ID: 58495
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2003 › Research › peer-review

Privacy Recovery with Disposable Email Addresses

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Seigneur, J., Jensen, C. D.
Pages: 35-39
Publication date: 2003
Peer-reviewed: Yes

Publication information
Volume: 1
Issue number: 6
ISSN (Print): 1540-7993
Ratings:
Web of Science (2003): Indexed yes
Original language: English
DOIs:
**Risk Probability Estimating Based on Clustering**

Biquitous computing environments are highly dynamic, with new unforeseen circumstances and constantly changing environments, which introduces new risks that cannot be assessed through traditional means of risk analysis. Mobile entities in a ubiquitous computing environment require the ability to perform an autonomous assessment of the risk incurred by a specific interaction with another entity in a given context. This assessment will allow a mobile entity to decide whether sufficient evidence exists to mitigate the risk and allow the interaction to proceed. Such evidence might include records of prior experiences, recommendations from a trusted entity or the reputation of the other entity. In this paper, we propose a dynamic mechanism for estimating the risk probability of a certain interaction in a given environment using hybrid neural networks. We argue that traditional risk assessment models from the insurance industry do not directly apply to ubiquitous computing environments. Instead, we propose a dynamic mechanism for risk assessment, which is based on pattern matching, classification and prediction procedures. This mechanism uses an estimator of risk probability, which is based on the automatic clustering of defining features of the environment and the other entity, which helps avoid subjective judgments as much as possible.

**General information**

Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Chen, Y., Jensen, C. D., Gray, E., Seigneur, J.
Publication date: 2003

**Host publication information**

Title of host publication: The 4th IEEE Annual Information Assurance Workshop, West Point, New York, USA., June

Source: orbit
Source-ID: 58510

Research output: Article in proceedings – Annual report year: 2003

**Scaling an Interplanetary Internet**

**General information**

Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Farrell, S., Jensen, C. D.
Publication date: 2003

**Host publication information**

Title of host publication: International Conference on Recent Advances in Space Technologies (RAST 2003)

Source: orbit
Source-ID: 58515

Research output: Article in proceedings – Annual report year: 2003

**Towards security auto-configuration for smart appliances**

**General information**

Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Seigneur, J., Farrell, S., Jensen, C. D., Gray, E., Chen, Y.
Publication date: 2003

**Host publication information**

Title of host publication: Proceedings of the Smart Objects Conference

Trust Propagation in Small Worlds

The possibility of a massive, networked infrastructure of diverse entities partaking in collaborative applications with each other increases more and more with the proliferation of mobile devices and the development of ad hoc networking technologies. In this context, traditional security measures do not scale well. We aim to develop trust-based security mechanisms using small world concepts to optimise formation and propagation of trust amongst entities in these vast networks. In this regard, we surmise that in a very large mobile ad hoc network, trust, risk, and recommendations can be propagated through relatively short paths connecting entities. Our work describes the design of trust-formation and risk-assessment systems, as well as that of an entity recognition scheme, within the context of the small world network topology.

Using Trust for Secure Collaboration in Uncertain Environments

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Pages: 52-61
Publication date: 2003
Peer-reviewed: Yes

Publication information
Journal: IEEE Pervasive Computing
Volume: 2
Secure Environments for Collaboration among Ubiquitous Roaming Entities
SECURE is a newly started IST project, which addresses secure collaboration among computational entities in emerging global computing systems. The properties of these systems introduce new security challenges that are not adequately addressed by existing security models and mechanisms. The scale and uncertainty of this global computing environment invalidates existing security models. Instead, new security models have to be developed along with new security mechanisms that control access to protected resources.

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Jensen, C. D.
Publication date: 2002
Secure Ubiquitous Computing based on Entity Recognition

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Seigneur, J., Farrell, S., Jensen, C. D.
Publication date: 2002

Capability File Names: Separating authorisation from User Management in an Internet File System

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Regan, J., Jensen, C. D.
Pages: 221-234
Publication date: 2001

Computer security research in the Department of Computer Science, TCD

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Jensen, C. D.
Pages: 187-187
Publication date: 2001
Peer-reviewed: Unknown

Publication information
Journal: The Irish Scientist 2001 year book
Original language: English
URLs:
Source: orbit
Source-ID: 57809
Research output: Contribution to journal › Journal article – Annual report year: 2001 › Communication
Fingerprinting Text in Logical Markup Languages

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Jensen, C. D.
Pages: 433-445
Publication date: 2001

Host publication information
Title of host publication: 2001 Information Security Conference Malaga, Spain October 1-3
Publisher: Springer
URLs:
Source: orbit
Source-ID: 57844
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2001 › Research › peer-review

Kaffemik - A distributed JVM featuring a single Address Space Architecture

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Andersson, J., Weber, S., Cecchet, E., Jensen, C. D., Cahill, V.
Publication date: 2001

Host publication information
Title of host publication: USENIX JVM'01, Monterey, CA, April 23-24
URLs:
Source: orbit
Source-ID: 57820
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2001 › Research › peer-review

kaffemik - A distributed JVM on a single Address Space Architecture

General information
Publication status: Published
Organisations: Department of Informatics and Mathematical Modeling
Contributors: Andersson, J., Weber, S., Cecchet, E., Jensen, C. D., Cahill, V.
Publication date: 2001

Host publication information
Title of host publication: SCI Europe 2001 conference. Dublin 06 August
URLs:
Source: orbit
Source-ID: 57819
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2001 › Research › peer-review

Adaptability in CORBA: The Mobile Proxy Approach

Adaptability is one of the most important challenges in modern distributed systems. It may be defined as the ease with which a software application satisfies the different system constraints and the requirements of users and other applications. Adaptability is needed because distributed systems are inherently open, heterogeneous, and dynamic environments integrating a wide range of platforms, operating systems and applications from a number of different sources. In this paper, we propose to use mobile proxies to provide adaptability in distributed applications integrated using the CORBA technology. Downloading stubs and skeletons at runtime allows the adaptation of either client or server interfaces as well as the protocol linking the two.
CryptoCache: A Secure Sharable File Cache for Roaming Users

Small mobile computers are now sufficiently powerful to run many applications, but storage capacity remains limited so working files cannot be cached or stored locally. Even if files can be stored locally, the mobile device is not powerful enough to act as server in collaborations with other users. Conventional distributed file systems cache everything locally or not at all; there is no possibility to cache files on nearby nodes. In this paper we present the design of a secure cache system called CryptoCache that allows roaming users to cache files on untrusted file hosting servers. The system allows flexible sharing of cached files among unauthenticated users, i.e. unlike most distributed file systems CryptoCache does not require a global authentication framework. Files are encrypted when they are transferred over the network and while stored on untrusted servers. The system uses public key cryptography, which allows roaming users to selectively grant read and write access to others by entrusting them with respectively the public key or the private key.

CyberShip: Cyber Resilience for the Shipping Industry (CyberShip)

The shipping industry has become more vulnerable to cyber-attacks in recent years, because of its dependence on information technology and increasingly complex networks. Cyber systems are incorporated into almost every facet of maritime operations, such as financial and human resources management, security systems, navigation (Global Navigation Satellite Systems (GNSS), Automatic Identification System (AIS), Electronic Chart Display Systems (ECDIS), etc.), communications, electronic certificates, cargo tracking, pre-arrival processing and other key systems and equipment. All maritime structures (including ships and offshore facilities) as well as the connected infrastructure (e.g. offices of shipping companies, ports etc) are vulnerable. Currently, the awareness regarding cyber security aspects is either at a very low level or completely disregarded. The issue of cyber security has been brought into the attention of the International Maritime Organization (IMO), and industry associations such as BIMCO and others. As a result of this guidelines for tackling cyber security problems have been developed. This project is aimed at providing shipping companies and regulators with a reference framework and decision support model to better cope with disruptions originating from a cyber-attack.

Barfod, M. B., Project Manager, Department of Management Engineering, Management Science, Transport DTU, Operations Management
Psaraftis, H. N., Project Participant, Department of Management Engineering, Management Science, Transport DTU, Operations Management
Jensen, C. D., Project Participant, Department of Applied Mathematics and Computer Science, Cyber Security, Copenhagen Center for Health Technology
Sepúlveda Estay, D. A., Project Participant, Department of Management Engineering, Management Science, Transport DTU, Operations Management
Sahay, R., Project Participant, Department of Applied Mathematics and Computer Science, Cyber Security
Context-Aware Access Control
Sultan, S., PhD Student, Department of Mathematics
Jensen, C. D., Main Supervisor
Meng, W., Supervisor
Technical University of Denmark
01/02/2018 → 31/01/2021
Award relations: Context-Aware Access Control
Project: PhD

Statistical Tools for Cybersecurity
Vejre, P. S., PhD Student, Department of Mathematics
Bogdanov, A., Main Supervisor
Knudsen, L. R., Supervisor
Jensen, C. D., Examiner
Leander, G., Examiner
Johansson, T., Examiner
Technical University of Denmark
01/02/2016 → 12/12/2018
Award relations: Statistical Tools for Cybersecurity
Project: PhD

Analysis and optimization of safety-critical real-time applications on interconnected networks
Gavrilut, V. M., PhD Student, Department of Mathematics
Pop, P., Main Supervisor
Jensen, C. D., Supervisor
Madsen, J., Examiner
Behnam, M., Examiner
Gruian, F., Examiner
Technical University of Denmark
01/09/2015 → 14/01/2019
Award relations: Analysis and optimization of safety-critical real-time applications on interconnected networks
Project: PhD

Graphical passwords user authentication
Elaswad, O., PhD Student, Department of Mathematics
Jensen, C. D., Main Supervisor
Probst, C. W., Examiner
Khajuria, S., Examiner
Kamala, M. A., Examiner
Privatist
15/05/2013 → 11/05/2017
Award relations: Graphical passwords user authentication
Project: PhD

Trusted Cryptography
Tiessen, T., PhD Student, Department of Mathematics
Security and privacy in Managed Video Systems
Mahmood Rajpoot, Q., PhD Student, Department of Mathematics
Jensen, C. D., Main Supervisor
Probst, C. W., Examiner
Coetzee, M., Examiner
Fischer-Hübner, S., Examiner
Technical University of Denmark
15/12/2012 → 25/05/2016
Award relations: Security and privacy in Managed Video Systems
Project: PhD

Programming Models and Tools for Intelligent Embedded Systems
Serensen, P. V. B., PhD Student, Department of Informatics and Mathematical Modeling
Madsen, J., Main Supervisor
Jensen, C. D., Examiner
Jerraya, A. A., Examiner
Svensson, B., Examiner
DTU-lønnnet stipendie
01/03/2006 → 29/09/2010
Award relations: Programming Models and Tools for Intelligent Embedded Systems
Project: PhD

Attacker Models for Ubiquitous Computing
Papini, D., PhD Student, Department of Informatics and Mathematical Modeling
Sharp, R., Main Supervisor
Jensen, C. D., Supervisor
Mödersheim, S. A., Examiner
Skou, A. J., Examiner
Technical University of Denmark
01/10/2009 → 24/05/2013
Award relations: Attacker Models for Ubiquitous Computing
Project: PhD

Device Centric Authentication for Ubiquitous Computing
Ahmed, N., PhD Student, Department of Informatics and Mathematical Modeling
Jensen, C. D., Main Supervisor
Zenner, E., Supervisor
Knudsen, L. R., Examiner
Crampton, J., Examiner
Knapskog, S. J., Examiner
Technical University of Denmark
15/06/2009 → 28/09/2012
Award relations: Device Centric Authentication for Ubiquitous Computing
Project: PhD

Resilient Infrastructure and Building Security
Ingvar, M. I., PhD Student, Department of Mathematics
Jensen, C. D., Main Supervisor
Probst, C. W., Examiner
Moeslund, T. B., Examiner
Terzis, S., Examiner
EU-finansieret
15/12/2010 → 21/09/2015
Award relations: Resilient Infrastructure and Building Security
Project: PhD