Authentication for E-Government in Developing Countries - With special focus on the North Africa Countries

Recently, many countries include both developed countries as well as developing countries have transformed paper based systems into electronic systems using ICT technologies in order to improve service delivery and reduce cost. Several researches and International Organizations in the field of e-Government reports that many countries over the world have not achieved transaction stages of government e-services and most of those countries are from developing countries. One of the main issues challenge government e-service inclusion is digital divide which barriers achieving principle of equal access and benefit of government e-service. Therefore, This thesis aims to investigate digital divide and IDM issues challenge government e-service in developing countries such as North Africa Countries (NAC) from achieving the priciple of equal access in a secure manner. To achieve this aim we, developed a framework that consists of two components include digital divide variables and a simple IDM model in order to assess the current state of government e-service in NAC. Moreover,we analyzed the existing IDM protocol's concept to understand whether those concepts consider disadvantaged user’s needs. Based on the identified challenges in NAC using the developed framework and the analysis of IDM protocol's concept we identify the requirements to be satisfied in order to allow large portion of citizens access and benefit of government e-service in equal and secure manner. One possible solution to improve e-Government inclusion is to consider vulnerable group needs such as the case in which users (citizens) do not have the ability either to read or write and as a result are excluded from e-services. Thus, a solution should enable such users to benefit from e-services. Introducing vulnerable group such as illiterate individuals might introduce new risks which have not existed in citizens-government face to face interaction. Thus, considering security property include confidentiality, integrity, non-repudiation and accountability for a proposed solution is needed. User authentication based on social relationship protocol is proposed in order to bridge digital divide. We formalized the proposed protocol as well as IDM protocol's concept using Open Source Fixed Point Model Checker tool (OFMC) To verify security properties include secrecy of exchanged information and authenticity of communication parties of the target protocols. OFMC is an automatic protocol security verification tool to identify the strengths of the verified protocol. Based on the verification result of OFMC tool, an attack is found against the existing IDM protocol's concept when considering vulnerable users while the proposed protocol has achieved the specified goals without ant attack at least in one session. We also, performed a simple usability comparison...
between the proposed protocol and public kiosk service delivery channel and the proposed protocol shows its effectiveness as well as efficient.

**General information**

State: Submitted
Organisations: Cyber Security, Department of Applied Mathematics and Computer Science
Authors: Elaswad, O. (Intern), Jensen, C. D. (Intern)
Number of pages: 130
Publication date: 2017

**Publication information**

Publisher: DTU Compute
Original language: English

Series: DTU Compute PHD-2017
Volume: 455
ISSN: 0909-3192
Main Research Area: Technical/natural sciences

**Relations**

Projects:

- Authentication for E-Government in Developing Countries - With special focus on the North Africa Countries
Publication: Research › Ph.D. thesis – Annual report year: 2017

**Enhancing Security and Privacy in Video Surveillance through Role-Oriented Access Control Mechanism**

Use of video surveillance has significantly increased in the last few decades. Modern video surveillance systems are equipped with techniques that automatically extract information about the objects and events from the video streams and allow traversal of data in an effective and efficient manner. Pervasive usage of such systems gives substantial powers to those monitoring the videos and poses a threat to the privacy of anyone observed by the system. Aside from protecting privacy from the outside attackers, it is equally important to protect the privacy of individuals from the inside personnel involved in monitoring surveillance data to minimize the chances of misuse of the system, e.g., voyeurism. In this context, several techniques to protect the privacy of individuals, called privacy enhancing techniques (PET) have therefore been proposed in the literature which detect and mask the privacy sensitive regions, e.g., faces, from the videos. However, very few research efforts have focused on addressing the security aspects of video surveillance data and on authorizing access to this data. Interestingly, while PETs help protect the privacy of individuals, they may also hinder the usefulness of video surveillance systems resulting in compromising the very purpose of such systems, i.e., public safety. Thus the challenge is to provide sufficient need-specific data to those monitoring the surveillance systems yet preserving the privacy of people as much as possible. This can be achieved through a dynamic access control mechanism that may provide proportionate access to data while allowing reversing the PETs whenever required. In this context, a summary of thesis contributions is given below.

In this thesis, we present an abstract model of video surveillance systems that helps identify the major security and privacy requirements in a video surveillance system. We study existing solutions against these requirements and point out practical challenges in ensuring the security of video surveillance data in all stages (in transit and at storage). Our study shows a gap, between the security requirements that we identified and the proposed security solutions, where future research efforts may focus in this domain. From the challenges that we outline regarding security in video surveillance, we focus on development of a dynamic access control mechanism.

We develop a general-purpose access control model that is suitable for video surveillance systems as well as other domains sharing similar requirements. As the currently dominant access control models – the role-based access control (RBAC) and the attribute-based access control (ABAC) – suffer from limitations while offering features complementary to each other, their integration has become an important area of research. Our access control model combines the two models in a novel way in order to unify their benefits while avoiding their limitations. Our approach provides a mechanism that not only takes information about the current circumstances into account during access control decision making, but is also suitable for applications where access to resources is controlled by exploiting the contents of resources in the access control policy. We evaluate our model against RBAC and ABAC and demonstrate that our model brings together the benefits offered by RBAC and ABAC while addressing the role- and permission-explosion issues faced in RBAC.

Based on our access control model, we then present an access control mechanism for video surveillance systems. Contrary to the existing approaches, the proposed access control mechanism is role-oriented and retains advantages associated with role-based access control, yet it allows specification of policies using the metadata associated with the objects as well as the attributes of users and environment. In addition to role hierarchies, the content-based permissions in our model allow derivation of several permissions from the explicitly stated ones due to the hierarchical relations between the attributes of different entities. We implement a prototype of the proposed mechanism and demonstrate that the access control policies using our approach may be specified via eXtensible Access Control Markup Language (XACML).
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.

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.
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 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.

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 complimentary 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
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.
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
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Authors: Mahmood Rajpoot, Q. (Intern), Jensen, C. D. (Intern)
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
Main Research Area: Technical/natural sciences
Electronic versions:
Video_Surveillance_Privacy_issues_and_legal_compliance.pdf
Source: PublicationPreSubmission
Source-ID: 110605574
Publication: Research - peer-review › Book chapter – Annual report year: 2015

Editorial: Thematic series on best articles from IFIPTM and PST

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, University of Malaga
Authors: Fernandez-Gago, C. (Ekstem), Jensen, C. D. (Intern)
Number of pages: 2
Publication date: 2014
Main Research Area: Technical/natural sciences

Publication information
Journal: Journal of Trust Management
Volume: 1
Issue number: 2
ISSN (Print): 2196-064X
Original language: English
Electronic versions:
Editorial.pdf
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.
Resilient Infrastructure and Building Security

Traditional authentication systems are considered persistent as they rarely limit the time the authentication is valid. Conversely, sensor-based authentication systems are considered transient as they allow continuous authentication of the users.

In this thesis we present a new approach to authentication that combines traditional access control systems with the sensing technologies and tracking capabilities offered by smart environments. Our approach is called Persistent Authentication for Location-based Services. Persistent authentication enables the secure provision of location-based services through non-intrusive authentication of mobile users in a smart environment. The objective is to shift the current authentication paradigm from a single discrete event to a continuous session. This is accomplished by utilising the contextual awareness provided by the smart environment to track principals from the point of initial authentication to the point where authorisation is requested by location-based services.

Facial recognition and appearance analysis are integrated in the persistent authentication system as remote biometric experts that operate at a distance and require no interaction from the users. The experts perform continuous authentication by processing samples of the biometric modalities as they become available.

Combining scores from multiple biometric experts is known as sensor fusion. A common challenge in this field is that the results from evaluating different biometric characteristic are usually incompatible, as they have different score ranges as well as different probability distributions. Error-rate-based fusion is presented as a novel fusion technique that transforms individual scores from different biometric systems into objective evidences and combine them using Bayesian inference.

Persistent authentication offers an effective integrated protection measure that is distributed directly in the facility and is non-intrusive to the public and affordable to the facility owners. Persistent authentication is suitable for security sensitive applications and can help protect the facility against terrorism and other types of crime.
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
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Authors: Mahmood Rajpoot, Q. (Intern), Jensen, C. D. (Intern)
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
Series: IFIP AICT - Advances in Information and Communication technology
Volume: 428
ISSN: 1868-4238
Main Research Area: Technical/natural sciences
Conference: 29th IFIP TC-11 International Information Security and Privacy Conference 2014, Marrakech, Morocco, 02/06/2014 - 02/06/2014
Video Surveillance, Security, Privacy, Monitoring, Storage, Access Control, Encryption
DOIs:
10.1007/978-3-642-55415-5_14
Source: PublicationPreSubmission
Source-ID: 101151347
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014


General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, University of Luxembourg
Authors: Mauw, S. (ed.) (Ekstern), Jensen, C. D. (ed.) (Intern)
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
Series: Lecture Notes in Computer Science
Volume: 8743
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
DOIs:
10.1007/978-3-319-11851-2
Publication: Research - peer-review › Book – Annual report year: 2014
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.

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.
Attacker Modelling in Ubiquitous Computing Systems

Within the last five to ten years we have experienced an incredible growth of ubiquitous technologies which has allowed for improvements in several areas, including energy distribution and management, health care services, border surveillance, secure monitoring and management of buildings, localisation services and many others. These technologies can be classified under the name of ubiquitous systems.

The term Ubiquitous System dates back to 1991 when Mark Weiser at Xerox PARC Lab first referred to it in writing. He envisioned a future where computing technologies would have been melted in with our everyday life. This future is visible to everyone nowadays: terms like smartphone, cloud, sensor, network etc. are widely known and used in our everyday life. But what about the security of such systems. Ubiquitous computing devices can be limited in terms of energy, computing power and memory. The implementation of cryptographic mechanisms that comes from classical communication systems could be too heavy for the resources of such devices, thus forcing the use of lighter security measures if any at all. The same goes for the implementation of security protocols. The protocols employed in classical communication systems were not designed for the ubiquitous environment, hence their security has to be proven again, leading to the definition of new protocols designed specifically to address new vulnerabilities introduced by the ubiquitous nature of the system. Throughout the network security community this problem has been investigated for some time now and this has resulted in some lightweight cryptographic standards and protocols, as well as tools that make it possible for security properties of communication protocols which are typical of ubiquitous systems. However the abilities of the ubiquitous attacker remain somehow undemonstrated and still under extensive investigation.

This Thesis explores the nature of the ubiquitous attacker with a focus on how she interacts with the physical world and it defines a model that captures the abilities of the attacker. Furthermore a quantitative implementation of the model is presented. This can be used by a security analyst as a supporting tool to analyse the security of an ubiquitous system and identify its weak parts. Most importantly this work is also useful for system designers, who wish to implement an effective secure solution while developing their system.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Authors: Papini, D. (Intern), Sharp, R. (Intern), Jensen, C. D. (Intern)
Number of pages: 182
Publication date: 2012

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: IMM-PHD-2012
Number: 295
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions: Attacker_Modelling.pdf
Publication: Research - Ph.D. thesis – Annual report year: 2014

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
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering, Embedded Systems Engineering, Technical University of Denmark
Authors: Lindberg, K. (Ekstern), Jensen, C. D. (Intern)
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
BFI conference series: Conference on Privacy, Security and Trust (5000610)
Main Research Area: Technical/natural sciences
DOIs:
10.1109/PST.2012.6297938
Source: dtu
Source-ID: n::oai:DTIC-ART:inspec/370240457::19686
Publication: Research - peer-review › Article in proceedings – Annual report year: 2012

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
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering, Embedded Systems Engineering, Technical University of Denmark
Authors: Lindberg, K. (Ekstern), Jensen, C. D. (Intern)
Pages: 247-252
Publication date: 2012
Conference: 6th IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2012), Surat, India, 21/05/2012 - 21/05/2012
Main Research Area: Technical/natural sciences

Publication information
Journal: IFIP AICT - Advances in Information and Communication technology
Volume: 374
ISSN (Print): 1868-4238
Ratings:
Scopus rating (2016): CiteScore 0.33
BFI (2015): BFI-level 1
First Workshop on Incentives and Trust in E-Commerce (WIT-EC’12)

General information
State: 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
Main Research Area: Technical/natural sciences
Links:

Bibliographical note
Publication: Research › Book – Annual report year: 2012

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 session-less 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.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Computer Science and Engineering
Authors: Ahmed, N. (Intern), Jensen, C. D. (Intern)
Publication date: 2012

Host publication information
Title of host publication: Trust Management VI : 6th IFIP WG 11.11 International Conference, IFIPTM 2012, Surat, India, May 21-25, 2012. Proceedings
Publisher: Springer
ISBN (Print): 978-3-642-29851-6
Structured Intuition: A Methodology to Analyze Entity Authentication

Entity authentication is a process of verifying a claimed identity of a network party. It may appear to be a simple goal, but, depending on the application and context, it entails a number of modalities, such as whether the party is currently active on the network, whether the party is willing to communicate, and whether the party knows that it has been authenticated. Combining such goals in different ways leads to different flavours of entity authentication.

On an unauthenticated channel, an adversary can present a false claim of identity. Clearly, if the adversary succeeds, it may have serious consequences for the security of the system, e.g., private information of legitimate parties may be leaked or the security policy of a trusted system may be violated. At a corporate level, such a failure of authentication may result in loss of proprietary technology or customers' credit card information. Sometimes, a single failure of authentication affects the system for a long time, e.g., if an adversary is able to install a malicious program, such as a root kit, back door, key logger, bot, or other malware. Therefore, security protocols, which can resist a resourceful adversary, are used to authenticate network parties.

Verification of an authentication protocol to show that it is secure is a hard problem. Most of the reported flaws in authentication protocols are not due to some weakness in the cryptographic primitives used in these protocols. The usual problems lie in improper use of cryptographic primitives, and failure to unambiguously specify protocol assumptions and goals. Therefore, it is important that an authentication protocol is analysed with clear goals and explicitly stated assumptions.

There are many different formal definitions of authentication goals, and the decision of which definition is most appropriate depends on the requirements and constraints imposed by the larger system. Whether a reported flaw in a protocol is exploitable depends on the protocol goals and the environment in which the protocol is deployed. Whether a "secure" protocol is indeed secure depends on the security model and the level of abstraction used in the analysis. Thus, the goal of developing a high level methodology that can be used with different notions of security, authentication, and abstraction is worth considering.

In this thesis, we propose a new methodology, called the structured intuition (SI), which addresses the issues mentioned above. In the SI, we divide entity authentication into fine grained properties, which we call FLAGs (fine level authentication goals). FLAGs are protocol independent goals and represent one's expectations in an authentication-as-a-service paradigm. There is a single notion of security in our methodology, which is called canonicity, which is a weaker form of message authenticity. As compared to many contemporary analysis techniques, an SI based analysis provides detailed results regarding the design rationales and entity authentication goals of a protocol.
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.

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Ahmed, N. (Intern), Jensen, C. D. (Intern)
Pages: 234-247
Publication date: 2011
Main Research Area: Technical/natural sciences

Publication information
Journal: Lecture Notes in Computer Science
Volume: 6542
ISSN (Print): 0302-9743
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 0.67 SJR 0.315 SNIP 0.552
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.328 SNIP 0.618 CiteScore 0.37
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.325 SNIP 0.678 CiteScore 0.42
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.329 SNIP 0.699 CiteScore 0.49
ISI indexed (2013): ISI indexed no
Web of Science (2013): Indexed yes
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.323 SNIP 0.708 CiteScore 0.49
ISI indexed (2012): ISI indexed no
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 1
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.
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.
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.

Towards Secure Intelligent Buildings

State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Ingwar, M. I. (Intern), Jensen, C. D. (Intern)
Publication date: 2011
Host publication information
Title of host publication: Proceedings of the 5th Nordic Workshop on Dependability and Security (NODES’11)
Main Research Area: Technical/natural sciences
Workshop: 5th Nordic Workshop on Dependability and Security, Copenhagen, Denmark, 28/06/2011
Links:
Source: orbit
Source-ID: 316295
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 that we keep designing new protocols due to 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, 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.

A Generic Access Control Model for Wind Power Systems

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Ahmed, N. (Intern), Jensen, C. D. (Intern)
Publication date: 2010

Publication information
Place of publication: Kgs. Lyngby, Denmark
Publisher: Technical University of Denmark, DTU Informatics, Building 321
Original language: English
Series: IMM-Technical Report-2010-17
Main Research Area: Technical/natural sciences
Electronic versions:
tr10_17.pdf
Source: orbit
Source-ID: 271425
Publication: Research › Report – Annual report year: 2010

A Generic Role Based Access Control Model for Wind Power Systems

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling, Technical University of Denmark
Authors: Nagarajan, A. (Ekstern), Jensen, C. D. (Intern)
Pages: 1-14
Publication date: 2010

Host publication information
Title of host publication: Workshop Proceedings of the Fourth IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2010) : Proceedings of the International Workshop on Infrastructure Assurance (iWiA 2010)
Main Research Area: Technical/natural sciences
Conference: Proceedings of the International Workshop on Infrastructure Assurance, 01/01/2010
Source: orbit
Source-ID: 270641
Publication: Research - peer-review › Article in proceedings – Annual report year: 2010

A Generic Role Based Access Control Model for Wind Power Systems

The electrical power infrastructure is facing a transition from a largely centralised distribution infrastructure with a few large power plants to an increasingly distributed infrastructure that must incorporate privately owned and operated power generation units based on fuel cells or sustainable energy sources, such as wind turbines, solar energy or wave energy. This introduces important new security challenges that are not adequately addressed by existing approaches to security in the electrical power distribution infrastructure. In this paper we examine some of the security challenges that may arise in 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
State: Published
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.
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.
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.
The Role of Trust in Persistent Authentication

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Jensen, C. D. (Intern)
Pages: 41-52
Publication date: 2010

Host publication information
Title of host publication: Workshop Proceedings of the Fourth IFIP WG 11.11 International Conference on Trust Management (IFIPTM 2010) : Proceedings of the Joint International Workshop on Trust in Location and Communications in Decentralized Computing (TruLoCo 2010)
Main Research Area: Technical/natural sciences
Conference: Proceedings of the Joint International Workshop on Trust in Location and Communications in Decentralized Computing, Morioka, Iwate, Japan, 01/01/2010
Source: orbit
Source-ID: 270639
Publication: Research - peer-review › Journal article – Annual report year: 2010

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 over all 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.

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Ahmed, N. (Intern), Jensen, C. D. (Intern)
Pages: 148-162
Publication date: 2009

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 methods 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.

General information
State: Published
Organisations: Embedded Systems Engineering, Department of Informatics and Mathematical Modeling
Authors: Ahmed, N. (Intern), Jensen, C. D. (Intern)
Publication date: 2009
Main Research Area: Technical/natural sciences
Security, Usability, Ubiquitous Computing, Nomadic Users, Authentication.
Electronic versions:
Links:
http://www.ep.liu.se/ecp/041/005/index.html
Source: orbit
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

Why Security is Bad for Trust
Main Research Area: **Technical/natural sciences**

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

**WRS Demonstration Posters**

**General information**
State: Published
Organisations: System Security, Department of Informatics and Mathematical Modeling
Authors: Jensen, C. D. (Intern)
Publication date: 2009
Event: Poster session presented at 3rd IFIP International Conference on Trust Management, West Lafayette, United States.
Main Research Area: **Technical/natural sciences**

**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
Publication: Research - peer-review › Poster – Annual report year: 2009

**WRS: The Wikipedia Recommender System**

**General information**
State: Published
Organisations: System Security, Department of Informatics and Mathematical Modeling
Authors: Lefèvre, T. (Ekstern), Jensen, C. D. (Intern), Thomas Rune, K. (Ekstern)
Number of pages: 322
Pages: 298-301
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
Series: IFIP Advances in Information and Communication Technology
Number: 300
ISSN: 1868-4238
Main Research Area: **Technical/natural sciences**
Conference: 3rd IFIP International Conference on Trust Management, West Lafayette, United States, 16/06/2009 - 16/06/2009

**Bibliographical note**
The two co-authors were one student and one former student.
Source: orbit
Source-ID: 246033
Publication: Research - peer-review › Conference abstract in proceedings – Annual report year: 2009

**Dynamics of Trust Evolution: Auto-configuration of dispositional trust dynamics**

**General information**
State: Published
Organisations: Department of Informatics and Mathematical Modeling, System Security
Authors: Jensen, C. D. (Intern), Korsgaard, T. R. (Ekstern)
Number of pages: 558
Pages: 509-518
Publication date: 2008
On the Need for Relaxed Security Models

General information
State: Published
Organisations: System Security, Department of Informatics and Mathematical Modeling
Authors: Jensen, C. D. (Intern)
Publication date: 2008

Publication information
Original language: English
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 222589
Publication: Research › Sound/Visual production (digital) – Annual report year: 2008

Persistent Authentication in Smart Environments

General information
State: Published
Organisations: System Security, Department of Informatics and Mathematical Modeling
Authors: Hansen, M. S. (Ekstern), Kirschmeyer, M. (Ekstern), Jensen, C. D. (Intern)
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)
Publisher: Technical University of Aachen
Main Research Area: Technical/natural sciences
Conference: 2nd International Workshop on Combining Context with Trust, Security and Privacy, Trondheim, Norway, 01/01/2008
Source: orbit
Source-ID: 220971
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

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
State: Published
Organisations: System Security, Department of Informatics and Mathematical Modeling
Authors: Peen, S. (Ekstern), Jansen, T. W. (Ekstern), Jensen, C. D. (Intern)
Number of pages: 462
Publication date: 2008

Host publication information
Title of host publication: Online Consumer Protection: Theories of Human Relativism
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
State: Published
Organisations: System Security, Department of Informatics and Mathematical Modeling
Authors: Korsgaard, T. R. (Ekstern), Jensen, C. D. (Intern)
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)
Main Research Area: Technical/natural sciences
Conference: 4th International Workshop on Security and Trust Management, Trondheim, Norway, 01/01/2008
Source: orbit
Source-ID: 220972
Publication: Research - peer-review › Article in proceedings – Annual report year: 2008

Trust Management II: Proceedings of the IFIPTM 2008 - Joint iTrust and PST Conferences on Privacy, Trust Management and Security

General information
State: Published
Organisations: SAP A.G., Stanford University, Norwegian University of Science and Technology, Technical University of Denmark
Pages: 368
Publication date: 2008
Main Research Area: Technical/natural sciences

Publication information
Journal: IFIP International Federation for Information Processing
Volume: 263
Original language: English
Source: orbit
Source-ID: 235843
Publication: Research › Editorial – Annual report year: 2008
Assessment of Privacy in Government IT-Systems

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Peen, S. (Ekstern), Jansen, T. W. (Ekstern), Jensen, C. D. (Intern)
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
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 202545
Publication: Research - peer-review › Article in proceedings – Annual report year: 2007

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

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Jónsson, E. (Ekstern), Jensen, C. D. (Intern)
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
Main Research Area: Technical/natural sciences
Links: http://www2.imm.dtu.dk/pubdb/views/publication_details.php?id=5498
Source: orbit
Source-ID: 205560
Publication: Research - peer-review › Article in proceedings – Annual report year: 2007

End-by-Hop Data Integrity

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Jensen, C. D. (Intern), Farrell, S. (Ekstern)
Publication date: 2007

Host publication information
Title of host publication: Lecture Notes in Computer Science
Volume: 4572
Publisher: Springer
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 202535
Publication: Research - peer-review › Book chapter – Annual report year: 2007

Integrity in Open Collaborative Authoring Systems

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Jensen, C. D. (Intern)
Pages: 399-402
Publication date: 2007
Resilia: a Safe and Secure Distributed Backup System for Small and Medium Enterprises

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Jensen, C. D. (Intern), Meira, F. (Ekstern), Nittegaard-Nielsen, J. (Ekstern)
Pages: 383-398
Publication date: 2007

Trust Management in Open Grid Systems

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Jensen, C. D. (Intern), Sharp, R. (Intern)
Publication date: 2007

User-centric Identity, Trust and Privacy

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Seigneur, J. (Ekstern), Jensen, C. D. (Intern)
Publication date: 2007
PayBAC: A Payment Based Access Control Mechanism

General information
State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Authors: Pajkovski, B. (Ekstern), Jensen, C. D. (Intern), Fåk, V. (ed.) (Ekstern)
Pages: 145-156
Publication date: 2006

Host publication information
Title of host publication: Proceedings of the 11th Nordic Workshop on Secure IT-Systems (NordSec 2006)
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 200311
Publication: Research - peer-review › Article in proceedings – Annual report year: 2006

Program Partitioning using Dynamic Trust Models

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, System Security
Publication date: 2006

Host publication information
Title of host publication: Workshop on Formal Aspects in Security and Trust (FAST 2006)
Main Research Area: Technical/natural sciences
Conference: Workshop on Formal Aspects in Security and Trust, 01/01/2006
Links:
http://www2.imm.dtu.dk/pubdb/p.php?4745
Source: orbit
Source-ID: 191578
Publication: Research - peer-review › Article in proceedings – Annual report year: 2006

Trust-Based Route Selection in Dynamic Source Routin

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Jensen, C. D. (Intern), Connell, P. O. (Ekstern)
Pages: 150-163
Publication date: 2006

Host publication information
Title of host publication: 4th International Conference on Trust Management
Publisher: Springer Verlag
Main Research Area: Technical/natural sciences
Links:
http://www2.imm.dtu.dk/pubdb/p.php?4611
Source: orbit
Source-ID: 191547
Publication: Research - peer-review › Article in proceedings – Annual report year: 2006

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.
Trust Dynamics, Trust Formation, Trust Management

Security in open Grid systems

The Claim Tool Kit for ad hoc recognition of peer entities

Trust Evolution Policies for Security in Collaborative Ad Hoc Applications
Trust Transfer: Encouraging Self-Recommendations without Sybil Attack

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Seigneur, J. (Ekstern), Gray, A. (Ekstern), Jensen, C. D. (Intern)
Pages: 321-337
Publication date: 2005

Host publication information
Title of host publication: Third International Conference on Trust Management
Publisher: Springer Verlag
Main Research Area: Technical/natural sciences
Links:
http://www2.imm.dtu.dk/pubdb/p.php?3888
Source: orbit
Source-ID: 185744
Publication: Research - peer-review › Article in proceedings – Annual report year: 2005

Combating Spam with TEA (Trusted Email Addresses)

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Seigneur, J. (Ekstern), Dimmock, N. (Ekstern), Bryce, C. (Ekstern), Jensen, C. D. (Intern)
Publication date: 2004

Host publication information
Title of host publication: Second Annual Conference on Privacy, Security and Trust
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 154662
Publication: Research - peer-review › Article in proceedings – Annual report year: 2004

Security in Exotic Wireless Networks

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Farrell, S. (Ekstern), Seigneur, J. (Ekstern), Jensen, C. D. (Intern)
Pages: 101-114
Publication date: 2004

Host publication information
Title of host publication: Security and Privacy in Advanced Networking Technologies
Volume: NATO Computer and Systems Sciences Series III vol 193
Publisher: IOS Press
ISBN (Print): 1-58603-430-8
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 154723
Publication: Research - peer-review › Book chapter – Annual report year: 2004
The Role of Identity in Computational Trust

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Seigneur, J. (Ekstern), Jensen, C. D. (Intern)
Publication date: 2004

Host publication information
Title of host publication: Proceedings of The First Workshop on Security and Privacy at the Conference on Pervasive Computing
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 154663
Publication: Research - peer-review › Article in proceedings – Annual report year: 2004

Trading Privacy for Trust

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Seigneur, J. (Ekstern), Jensen, C. D. (Intern)
Publication date: 2004

Host publication information
Title of host publication: Proceedings of the 2nd International Conference on Trust Management
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 154664
Publication: Research - peer-review › Article in proceedings – Annual report year: 2004

Trust Enhanced Ubiquitous Payment without Too Much Privacy Loss

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Seigneur, J. (Ekstern), Jensen, C. D. (Intern)
Publication date: 2004

Host publication information
Title of host publication: Proceedings of the 19th Annual ACM Symposium on Applied Computing: Track on Ubiquitous Computing Applications
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 154665
Publication: Research - peer-review › Article in proceedings – Annual report year: 2004


General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Jensen, C. D. (Intern), Poslad, S. (ed.) (Ekstern), Dimitrakos, T. (ed.) (Ekstern)
Publication date: 2004

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

**General information**
State: Published
Organisations: Department of Photonics Engineering, Department of Informatics and Mathematical Modeling
Authors: Engberg, S. J. (Ekstern), Harning, M. B. (Intern), Jensen, C. D. (Intern)
Publication date: 2004

**Host publication information**
Title of host publication: Second Annual Conference on Privacy, Security and Trust
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 154610
Publication: Research - peer-review › Article in proceedings – Annual report year: 2004

A Unified Security Framework for Networked Applications

**General Information**
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Abendroth, J. (Ekstern), Jensen, C. D. (Intern)
Publication date: 2003

**Host publication information**
Title of host publication: Eighteenth ACM Symposium on Applied Computing
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 58496
Publication: Research - peer-review › Article in proceedings – Annual report year: 2003

Cryptographic Access Control in a Distributed File System

**General Information**
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Harrington, A. (Ekstern), Jensen, C. D. (Intern)
Pages: 158-165
Publication date: 2003

**Host publication information**
Title of host publication: 8th ACM Symposium on Access Control Models and Technologies
Main Research Area: Technical/natural sciences
Source: orbit
Source-ID: 58527
Publication: Research - peer-review › Article in proceedings – Annual report year: 2003
Risk Probability Estimating Based on Clustering

Ubiquitous 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.

Scaling an Interplanetary Internet

Towards security auto-configuration for smart appliances
Trajectory Based Addressing

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Farrell, S. (Ekstern), Jensen, C. D. (Intern)
Publication date: 2003

Host publication information
Title of host publication: 8th Cabernet Radicals Workshop
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 58516
Publication: Research - peer-review › Article in proceedings – Annual report year: 2003

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.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Gray, E. (Ekstern), Seigneur, J. (Ekstern), Chen, Y. (Ekstern), Jensen, C. D. (Intern), Nixon et al., P. (ed.) (Ekstern)
Pages: 239-254
Publication date: 2003

Host publication information
Title of host publication: The First International Conference on Trust Management : Lecture notes in computer science, vol. 2692
Publisher: Springer
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 58521
Publication: Research - peer-review › Article in proceedings – Annual report year: 2003

Using Trust for Secure Collaboration in Uncertain Environments

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Pages: 52-61
Publication date: 2003
Main Research Area: Technical/natural sciences
PEM3 - the Policy Enhanced Memory Management Model

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling
Authors: Andersson, J. (Ekstern), Jensen, C. D. (Intern), Weber, S. (Ekstern)
Publication date: 2002

Host publication information
Title of host publication: IEEE 3rd International Workshop on Policies for Distributed Systems and Networks
Place of publication: Monterey, CA, USA
Main Research Area: Technical/natural sciences
Links:
Source: orbit
Source-ID: 58429

Publication: Research - peer-review › Journal article – Annual report year: 2003
Secure Collaboration in Global Computing Systems

**General information**
- **State:** Published
- **Organisations:** Department of Informatics and Mathematical Modeling
- **Authors:** Jensen, C. D. (Intern)
- **Pages:** 34-35
- **Publication date:** 2002
- **Main Research Area:** Technical/natural sciences

**Publication information**
- **Journal:** ERCIM news
- **Issue number:** 49
- **Original language:** English
- **Links:**
- **Source:** orbit
- **Source-ID:** 58087

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**
- **State:** Published
- **Organisations:** Department of Informatics and Mathematical Modeling
- **Authors:** Jensen, C. D. (Intern)
- **Publication date:** 2002

**Host publication information**
- **Title of host publication:** First Internal iTrust Workshop on Trust Management in Dynamic Open Systems, Glasgow, September
- **Main Research Area:** Technical/natural sciences
- **Links:**
- **Source:** orbit
- **Source-ID:** 58239

Secure Ubiquitous Computing based on Entity Recognition

**General information**
- **State:** Published
- **Organisations:** Department of Informatics and Mathematical Modeling
- **Authors:** Seigneur, J. (Ekstern), Farrell, S. (Ekstern), Jensen, C. D. (Intern)
- **Publication date:** 2002

**Host publication information**
- **Title of host publication:** UBICOMP2002 Security Workshop, September, Gothenburg, Sweden
- **Main Research Area:** Technical/natural sciences
- **Links:**
- **Source:** orbit
- **Source-ID:** 58221

Publication: Research - peer-review › Article in proceedings – Annual report year: 2002
**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.

**General information**

State: Published
Organisations: Computer Science and Engineering, Department of Informatics and Mathematical Modeling
Projects:

**Context-Aware Access Control**

Technical University of Denmark  
Period: 01/02/2018 → 31/01/2021  
Number of participants: 3  
Phd Student:  
Sultan, Shizra (Ekstern)  
Supervisor:  
Meng, Weizhi (Intern)  
Main Supervisor:  
Jensen, Christian D. (Intern)

**Financing sources**

Source: Internal funding (public)  
Name of research programme: Institut stipendie (DTU)  
Project: PhD

**Cyber Resilience for the Shipping industry**

The CyberShip 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.

Department of Management Engineering  
Management Science  
Transport DTU  
Operations Management  
Department of Applied Mathematics and Computer Science  
Cyber Security  
Copenhagen Center for Health Technology  
Period: 01/09/2017 → 31/08/2019  
Number of participants: 4  
Acronym: CyberShip  
Project participant:  
Psaraftis, Harilaos N. (Intern)  
Jensen, Christian D. (Intern)  
Sepúlveda Estay, Daniel Alberto (Intern)  
Project Manager, organisational:  
Barfod, Michael Bruhn (Intern)

**Analysis and optimization of safety-critical real-time applications on interconnected networks**

Technical University of Denmark  
Period: 01/09/2015 → 31/10/2018  
Number of participants: 3  
Phd Student:
Gavrilit, Voica Maria (Intern)
Supervisor:
Jensen, Christian D. (Intern)
Main Supervisor:
Pop, Paul (Intern)

Financing sources
Source: Internal funding (public)
Name of research programme: Institut stipendie (DTU)
Project: PhD

Trusted Cryptography
Technical University of Denmark
Period: 01/07/2013 → 25/08/2016
Number of participants: 6
PhD Student:
Tiessen, Tyge (Intern)
Supervisor:
Knudsen, Lars Ramkilde (Intern)
Main Supervisor:
Rechberger, Christian (Intern)
Examiner:
Jensen, Christian D. (Intern)
Daemen, Joan (Ekstern)
Johansson, Thomas (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Eksternt finansieret virksomhed

Relations
Publications:
Secure Block Ciphers - Cryptanalysis and Design
Project: PhD

Graphical passwords user authentication
Technical University of Denmark
Period: 15/05/2013 → 11/05/2017
Number of participants: 5
PhD Student:
Elaswad, Othoman (Intern)
Main Supervisor:
Jensen, Christian D. (Intern)
Examiner:
Probst, Christian W. (Intern)
Kamala, Mumtaz A. (Ekstern)
Khajuria, Samant (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Privatist

Relations
Publications:
Authentication for E-Government in Developing Countries - With special focus on the North Africa Countries
Project: PhD

Security and privacy in Managed Video Systems
Technical University of Denmark
Period: 15/12/2012 → 25/05/2016
Number of participants: 5
Phd Student:
Mahmood Rajpoot, Qasim (Intern)
Main Supervisor:
Jensen, Christian D. (Intern)
Examiner:
Probst, Christian W. (Intern)
Coetzee, Marijke (Ekstern)
Fischer-Hübner, Simone (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Institut stipendie (DTU) Samf.
Project: PhD

Architecture of Managed Video Systems

Technical University of Denmark
Period: 15/11/2012 → 31/03/2015
Number of participants: 6
Phd Student:
Bayyapu, Karunakar Reddy (Intern)
Supervisor:
Jensen, Christian D. (Intern)
Main Supervisor:
Fischer, Paul (Intern)
Examiner:
Jensen, Peter Arendt (Intern)
Grunwaldt, Jan-Dierk (Intern)
Østberg, Martin (Intern)

Financing sources
Source: Internal funding (public)
Name of research programme: Institut stipendie (DTU) Samf.
Project: PhD

Resilient Infrastructure and Building Security

Technical University of Denmark
Period: 15/12/2010 → 21/09/2015
Number of participants: 5
Phd Student:
Ingwar, Mads Ingerslew (Intern)
Main Supervisor:
Jensen, Christian D. (Intern)
Examiner:
Probst, Christian W. (Intern)
Moelslund, Thomas (Ekstern)
Terzis, Sotirios (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Anden EU-finansiering
Project: PhD

Attacker Models for Ubiquitous Computing

Department of Informatics and Mathematical Modeling
**Device Centric Authentication for Ubiquitous Computing**

*Department of Informatics and Mathematical Modeling*

**Period:** 15/06/2009 → 28/09/2012  
**Number of participants:** 6  
**PhD Student:** Ahmed, Naveed (Intern)  
**Supervisor:** Zenner, Erik (Intern)  
**Main Supervisor:** Jensen, Christian D. (Intern)  
**Examiner:** Knudsen, Lars Ramkilde (Intern)  
Knapskog, Svein Johan (Ekstern)  

**Financing sources**  
*Source:* Internal funding (public)  
*Name of research programme:* Institut stipendie (DTU)  
*Project:* PhD

**Programming Models and Tools for Intelligent Embedded Systems**

*Department of Informatics and Mathematical Modeling*

**Period:** 01/03/2006 → 29/09/2010  
**Number of participants:** 5  
**PhD Student:** Sørensen, Peter Verner Bojsen (Intern)  
**Main Supervisor:** Madsen, Jan (Intern)  
**Examiner:** Jensen, Christian D. (Intern)  
Jerraya, Ahmed Amine (Ekstern)  
Svensson, Bertil (Ekstern)  

**Financing sources**  
*Source:* Internal funding (public)  
*Name of research programme:* DTU-lønnet stipendie  
*Project:* PhD

**Cryptographic Access Control**

*Department of Informatics and Mathematical Modeling*
Number of participants: 2
Phd Student:
Frank, Kristine (Ekstern)
Main Supervisor:
Jensen, Christian D. (Intern)

**Financing sources**
Source: Internal funding (public)
Name of research programme: DTU-lønnet stipendie
Project: PhD

Security in Grid Systems
Department of Informatics and Mathematical Modeling
Period: 01/02/2004 → 31/03/2005
Number of participants: 3
Phd Student:
Kampfeldt, Jesper (Intern)
Supervisor:
Jensen, Christian D. (Intern)
Main Supervisor:
Sharp, Robin (Intern)

**Financing sources**
Source: Internal funding (public)
Name of research programme: DTU, Samfinansiering
Project: PhD