

Organizational Processes for Supporting Sustainable Security

Edited by

Lizzie Coles-Kemp¹, Carrie Gates², Dieter Gollmann³,
Sean Peisert⁴, and Christian Probst⁵

1 Royal Holloway University – London, GB

2 CA Labs – New York, US, carrie.gates@ca.com

3 TU Hamburg-Harburg, DE, diego@tu-harburg.de

4 University of California – Davis, US peisert@cs.ucdavis.edu

5 Technical University of Denmark, DK, probst@imm.dtu.dk

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 12501 “Organizational Processes for Supporting Sustainable Security” which ran from December 9 to 12, 2012 and was held in Schloss Dagstuhl – Leibniz Center for Informatics. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. We also ran a number of collaborative sessions designed to promote the development of design principles for sustainably secure organizational processes. The first section describes the seminar topics and goals in general. The following section contains abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper.

Seminar 9.–12. December, 2012 – www.dagstuhl.de/12501

1998 ACM Subject Classification K.6.5 Management of Computing and Information Systems: Security and Protection, D.4.6 Operating Systems: Security and Protection

Keywords and phrases Insider threat, Organizational Process, Resilience, Security Policy

Digital Object Identifier 10.4230/DagRep.2.12.37

1 Executive Summary

Lizzie Coles-Kemp

Carrie Gates

Dieter Gollmann

Sean Peisert

Christian Probst

License  Creative Commons BY-NC-ND 3.0 Unported license

© Lizzie Coles-Kemp, Carrie Gates, Dieter Gollmann, Sean Peisert and Christian Probst

The Dagstuhl seminar “Designing for process resilience to insider threats” was held on December 10–12th December, 2012 (Seminar #12501) to advance our understanding of ways of reducing insider threats through the design of resilient organizational processes.

The 2012 seminar built on the results of its predecessor from 2010 (Insider Threats: Strategies for Prevention, Mitigation, and Response, #10341, Seminar Homepage, Seminar Report). In this seminar we developed a shared, inter-disciplinary definition of the insider and a good formulation for a taxonomy or framework that characterizes insider threats. The



Except where otherwise noted, content of this report is licensed under a Creative Commons BY-NC-ND 3.0 Unported license

Organizational Processes for Supporting Sustainable Security, *Dagstuhl Reports*, Vol. 2, Issue 12, pp. 37–48

Editors: Lizzie Coles-Kemp, Carrie Gates, Dieter Gollmann, Sean Peisert, and Christian Probst



DAGSTUHL
REPORTS

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

seminar also began to explore how organizational considerations might better be incorporated into addressing insider threats.

The purpose of the 2012 seminar was to build on the understanding of the classification of the insider threat as a type of informed threat and the design requirements for tools and policies to respond to this category of threat that we had gained from the 2008 and 2010 Dagstuhl seminars on insider threats (Countering Insider Threats, #08302, and Insider Threats: Strategies for Prevention, Mitigation, and Response, #10341). Our goal was to explore what makes organizational processes resilient to insider threats. The exploration of organizational processes required us to consider the fluid set of informed actors against organizations whose processes and boundaries can be dynamic. It also required us to conceptualise threats and vulnerabilities as “emergent”. The conclusions from the previous seminars had resulted in the insight that resilient organizational processes are more resilient with respect to insider threats and more capable of limiting the damage from insider attacks. We also had the insight that resiliency appears to stem from usable, effective, and efficient security having been built into the organizational processes.

The seminar participants contained a carefully balanced mix of social and computer scientists and practitioners in order to explore the technological, organizational and social dimensions of the organizational process and its implementation. In order to productively combine the skills of the different disciplines and perspectives represented, the seminar started with a series of provocations. Debi Ashenden presented a provocation about the competing and sometimes conflicting uses of gamefication in the UK military setting. Kai-Uwe Loser presented a grounded example of personal data management practices and the conflicting perceptions of policy compliance that emerged within the example. Trish Williams presented a provocation about the value of big data in the case of electronic health data.

These design principles reflect a start point for future work on the design of organizational processes that are sustainably secure. Seminar organizers intend to produce a book that extends and explores these principles.

2 Table of Contents

Executive Summary

Lizzie Coles-Kemp, Carrie Gates, Dieter Gollmann, Sean Peisert and Christian Probst 37


Overview of Talks

Gemini – New Approach to Data Leakage Prevention <i>Julie Boxwell Ard</i>	40
Attack Time Analysis for Insiders <i>Florian Arnold</i>	40
Bernie the Sheep as a Role Model for Changing Security Behaviour <i>Debi Ashenden</i>	41
Defining the Cloud Battlefield: Insider Threats in Cloud Computing <i>Soeren Bleikertz</i>	41
Measuring Access, Knowledge, and Trust: A Discussion <i>Sophie Engle</i>	41
“Insider Threats” and “Supporting Sustainable Security” – Adding the Dimension of Privacy and Data Protection <i>Marit Hansen</i>	42
Research interests and potential research questions to studying and understanding socio-technical attacks <i>Jean-Louis Huynen</i>	43
Participatory Designing Work Processes and Security Processes <i>Kai-Uwe Loser</i>	43
Outsourcing Democracy: Losing Control of e-Voting in the Netherlands <i>Anne-Marie Oostveen</i>	44
TREsPASS: the socio-technical attack navigator <i>Wolter Pieters</i>	44
From black and white to shades of grey – Static analysis of human behavior <i>Christian W. Probst</i>	45
Interconnecting Insider-Threat-Defense Responsibilities in Socio-Technical Ecosystems – A managerial perspective <i>Ingrid Schirmer</i>	45
Where to start with security in healthcare? Dealing with security, insider threat, and increasing mobility in healthcare <i>Trish Williams</i>	46
Problem Statement: System Design beyond Duress Passwords <i>Alf Zugenmaier</i>	46
Working Groups	47
Open Problems	47
Participants	48

3 Overview of Talks

3.1 Gemini – New Approach to Data Leakage Prevention

Julie Boxwell Ard (Glenn Dale, US)


License  Creative Commons BY-NC-ND 3.0 Unported license
© Julie Boxwell Ard

Joint work of Ard, Julie Boxwell; Gates, Carrie; Bishop, Matt

In this talk we present a new approach to potentially detecting information leakage or malicious activity, whether it be intentional or unintentional activity. Traditionally, security research has approached insider threat detection from the perspective of modeling human behavior, often at the individual level, and then applying anomaly detection techniques to those models to detect potentially malicious activity. We hypothesize that the workflow and handling of documents has characteristics that can be modeled and analyzed in a manner similar to human activity. That is, we hypothesize that “similar” documents, where similarity might be based on meta-data and/or content, will follow a similar path (or behavior) through an organization. For example, documents created by Alice with similar content might always be reviewed and modified by Bob within a week of creation, followed by editing and moving them to a particular server, etc. We further hypothesize that files that deviate from established patterns merit further investigation and could indicate malicious activity including data exfiltration or malware spreading.

3.2 Attack Time Analysis for Insiders

Florian Arnold (University of Twente, NL)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Florian Arnold

Attack trees are a widely popular graphical model to represent attack scenarios by defining a system’s vulnerabilities and their interdependences. Ray and Poolsapassit extended the basic model by considering attacks from authorized insiders. On the basis of the assumption that attack steps of an intruder might be perfect legitimate operations for an insider, they developed a trimming algorithm to efficiently evaluate an attack tree from the perspective of an insider. We aim to extend their static approach by including a notion of time and sequencing. The goal of this extended model is to derive a probability distribution for the time until the attacker succeeds. Each attack step is assumed to require a certain time which can be expressed by a acyclic phase-type distribution. The whole attack is then composed by using the maximum, minimum and convolution operation. Based on the work of Pulungan we present a method which can evaluate huge scenarios by compressing the phase-type representation of an attack and introduce an efficient tool chain.

3.3 Bernie the Sheep as a Role Model for Changing Security Behaviour

Debi Ashenden (Cranfield Univ. – Swindon, GB)

License © © ⊖ Creative Commons BY-NC-ND 3.0 Unported license
© Debi Ashenden

How can we persuade end users to behave securely? Accepted approaches have traditionally relied on security awareness programmes, often delivered through computer-based training. Surely if we just give end users the right information in these programmes they'll make good security decisions? As Health Experts have realised this approach to changing behaviour is unlikely to work—otherwise “none of us would be obese, none of us would smoke and none of us would drive like lunatics” (Ian Potter, New Zealand Herald, 2007).

Social marketing, however, is a framework that is increasingly being used to deliver behavioural change for social good (such as healthcare initiatives). It could also offer a promising approach for changing security behaviours in organizations. Social marketing programmes use established marketing concepts such as “exchange” and “competition” to develop an in-depth understanding of the needs and motivations of end users. From this understanding interventions are designed that persuade end users to change their behaviour. “Bernie the Sheep” will be used to illustrate the key concepts of this approach.

3.4 Defining the Cloud Battlefield: Insider Threats in Cloud Computing

Soeren Bleikertz (IBM Research – Zürich, CH)

License © © ⊖ Creative Commons BY-NC-ND 3.0 Unported license
© Soeren Bleikertz

Joint work of Bleikertz, Sören; Masteli, Toni; Pape, Sebastian; Pieters, Wolter; Dimkov, Trajce
Main reference S. Bleikertz, T. Mastelic, S. Pape, W. Pieters, T. Dimkov, “Defining the Cloud Battlefield: Supporting Security Assessments by Cloud Customers,” in Proc. of the IEEE Int'l Conf. on Cloud Engineering (IC2E'13), 2013, to appear.

Cloud computing is becoming more and more popular, but security concerns over shadow its technical and economic benefits. In particular, insider attacks and malicious insiders are considered as one of the major threats and risks in cloud computing. As physical boundaries disappear and a variety of parties are involved in cloud services, it is becoming harder to define a security perimeter that divides insiders from outsiders, therefore making security assessments by cloud customers more difficult.

3.5 Measuring Access, Knowledge, and Trust: A Discussion

Sophie Engle (University of San Francisco, US)


License © © ⊖ Creative Commons BY-NC-ND 3.0 Unported license
© Sophie Engle

An insider is often defined as a user with access, knowledge, and trust. We propose a semi-automatable approach for a metric of “insiderness” for a user that takes into account all three of these attributes. Specifically, we approximate these attributes by examining access control configurations, access logs, and differences in security policies.

We will use the access control configuration to determine a ratio of configured versus possible access for a particular user, while using access logs to calculate a lower-bound for the amount of knowledge a user has of particular systems and resources. Finally, we will estimate trust by determining the amount of excess access a user has when comparing the configured and feasible levels of policy. This gives an intuitive, concise, semi-automated metric of insiderness that can be used for targeted auditing.

3.6 “Insider Threats” and “Supporting Sustainable Security” – Adding the Dimension of Privacy and Data Protection

Marit Hansen (ULD SH – Kiel, DE)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Marit Hansen


Privacy and data protection have many flavors: They may be considered as fundamental rights of data subjects, as legally demanded compliance issues, as valuable assets for individuals, for organizations or for the society. Or as an obstacle to security. So what does it mean to add the dimension of privacy and data protection to the discussion on insider threats and support of sustainable security?

First the bad news: The picture gets more complex if further demands and interests have to be considered. Adding the privacy dimension requires a thorough view on the needs, wishes and rights of all parties involved. The good news is that similar procedures and approaches that have proven to be useful in the information security context can be applied when adding, or better: weaving in, privacy and data protection. We will show similarities and differences of the concepts by complementing established security protection goals (confidentiality, integrity, availability) with specific privacy protection goals (unlinkability, transparency, intervenability). These protection goals have to be balanced against each other. Note that the traditional bias towards the organization and its security needs is overcome if the privacy protection goals are taken seriously.

Both technical and organizational measures have to reflect the found balance between the various protection goals. Concerning insider threats, fairness among all parties involved may be achieved by introducing escalating processes that minimize privacy infringements as far (and as long) as possible. Within an organization, checks and balances can be implemented via a staff council and/or an internal data protection officer whose roles in the escalation processes are clearly defined. Sustainable security as well as sustainable privacy and data protection require a regular monitoring of an information security management system (ISMS) and a corresponding, but separate data protection management system. Both systems have to interact to achieve acceptable results.

3.7 Research interests and potential research questions to studying and understanding socio-technical attacks


Jean-Louis Huynen (University of Luxembourg, LU)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Jean-Louis Huynen

My PhD project is about investigating socio-technical aspects of computer security to enrich existing model of security protocols. Kahneman and Tversky's Dual process theory could be a good candidate to better define which triggers are used in socio-technical attacks. Using this theory as a starting point, the purpose of the talk was to ask questions about ways to build experiments to identify these triggers.

3.8 Participatory Designing Work Processes and Security Processes


Kai-Uwe Loser (Ruhr-Universität Bochum, DE)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Kai-Uwe Loser
Joint work of Loser, Kai-Uwe; Nolte, Alexander

Information Security processes are designed processes and they are sociotechnical. As well they are processes of work like other organizational processes. Trust, power, practicability, motivational aspects—like the basic question of who does the work and who has the benefit—or the transparency of rationale behind design decisions are highly relevant here, when it comes to human decision in such a context. Participatory design is an approach that is successful in other contexts, but which is not widely adopted in security processes. One method for the development and reflection of this kind of processes can be supported with the field-tested method of the sociotechnical walkthrough (STWT). Within a project of raising security standards for a university administration infrastructure, STWT was combined with common ISMS methodology. During this project we found indicators for improvement by employing the STWT: technical and organizational measures can be specified in a single effort; contingent relationships can be taken into account as well as vulnerability resulting from characteristics of social structures. Participatory design respects the grounded knowledge of all workers in processes and creates more realistic processes. Descriptions of work processes are supposed to be more realistic instead of abstract ideas of process designers. The earned respect, the joint decisions, the transparent rationale and the more useable processes should contribute to the motivation to obey to the rules of the processes.

3.9 Outsourcing Democracy: Losing Control of e-Voting in the Netherlands

Anne-Marie Oostveen (University of Oxford, GB)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Anne-Marie Oostveen


Main reference A.-M. Oostveen, “Outsourcing Democracy: Losing Control of e-Voting in the Netherlands,” *Policy and Internet*, 2(4), pp. 201–220, 2010.

URL <http://dx.doi.org/10.2202/1944-2866.1065>

Contracting out IT services is a common practice for many governments. This case-study shows that outsourcing is not without risk, especially where elections are concerned. Studying electronic voting in the Netherlands through documents obtained with Freedom of Information requests, we see that government agencies at both local and national level lacked the necessary knowledge and capability to identify appropriate voting technology, to develop and enforce proper security requirements and to monitor performance. Furthermore, over the twenty years that e-voting was used in the Netherlands, the public sector became so dependent on the private sector that a situation evolved where Dutch government lost ownership and control over both the e-voting system and the election process.

3.10 TRESPASS: the socio-technical attack navigator

Wolter Pieters (TU Delft, NL)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Wolter Pieters

Joint work of The TRESPASS consortium

URL <http://www.trespass-project.eu/>

Information security threats to organizations have changed completely over the last decade, due to the complexity and dynamic nature of infrastructures and attacks. Successful attacks cost society billions a year, impacting vital services and the economy. Examples include Stuxnet, using infected USB sticks to sabotage nuclear plants, and the DigiNotar attack, using fake digital certificates to spy on website traffic. New attacks cleverly exploit multiple organizational vulnerabilities, involving physical security and human behaviour. Defenders need to make rapid decisions regarding which attacks to block, as both infrastructure and attacker knowledge change rapidly.

Current risk management methods provide descriptive tools for assessing threats by systematic brainstorming. Attack opportunities will be identified and prevented only if people can conceive them. In today’s dynamic attack landscape, this process is too slow and exceeds the limits of human imaginative capability. Emerging security risks demand tool support to predict, prioritise, and prevent complex attacks systematically.


The TRESPASS project will make this possible, by building an “attack navigator”. This navigator makes it possible to say which attack opportunities are possible, which of them are the most urgent, and which countermeasures are most effective. To this end, the project combines knowledge from technical sciences (how vulnerable are protocols and software), social sciences (how likely are people to succumb to social engineering), and state-of-the-art industry processes and tools.

By integrating European expertise on socio-technical security into a widely applicable and standardised framework, TRESPASS will reduce security incidents in Europe, and allow organizations and their customers to make informed decisions about security investments.

This increased resilience of European businesses both large and small is vital to safeguarding the social and economic prospects of Europe.

3.11 From black and white to shades of grey – Static analysis of human behavior

Christian W. Probst (Technical University of Denmark, DK)


License  Creative Commons BY-NC-ND 3.0 Unported license
© Christian W. Probst

Static analysis is a useful tool. It can, for example, compute properties of a system that hold for every possible execution of the system. These characteristics make static analysis very useable for the analysis of systems, and completely unusable for human behavior. This is caused by the fact that static analysis must assume that a system will perform every possible action in a given state; clearly analysing and predicting human behavior requires much more subtle approaches.

We start from modeling systems and analysing them for insider threats. After this we discuss the problem of applying static analysis to human behaviour, and present two solutions, one based on probabilities, the other on simulation.

3.12 Interconnecting Insider-Threat-Defense Responsibilities in Socio-Technical Ecosystems – A managerial perspective

Ingrid Schirmer (Universität Hamburg, DE)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Ingrid Schirmer


The management of insider threat defense requires integration with IT-Governance processes of an organization based on knowledge of the enterprise architecture. Whereas this integration is a challenge in itself, it is not sufficient.

Today's organizations are acting within socio-technical/business ecosystems with evolving interconnections of organizations, systems, cross-organizational processes, business models with a rapidly growing number of digitally empowered individuals / customers.

Transforming socio-technical ecosystems as a whole by applying IT-innovation (e.g., introducing private clouds) requires in parallel security concepts and their stepwise realization and cultivation within the whole socio-technical ecosystems blurring the insider-focused threat perspective, yet using its achievements. We propose the identification and interconnection of insider threat defense responsibilities in individual organizations as part of a decentralized and long-term security governance in socio-technical ecosystems based on concepts of business ecosystems architectures.

3.13 Where to start with security in healthcare? Dealing with security, insider threat, and increasing mobility in healthcare


Trish Williams (Edith Cowan University – Joondalup, AU)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Trish Williams

Drawing on the progression of the Dagstuhl seminars, the definition of insider threat needs to evolve and keep pace with the changing environment. This is presented as a necessity with the context of healthcare as its overarching use-case. The challenges are four fold: integrating security with workflow; influence of trust; a broadening field; and blurring of healthcare devices and software. In addition, there are four assertions to address in relation to mobile health (mHealth) and BYOD, and its impact on the insider threat. In essence, mHealth alters the definition of what constitutes an insider threat. Further, social media, geo-location data and big data are all unaddressed considerations. Before we can do any design it is essential to understand the context and agree (or disagree) on what the impact and effects of the evolution of mobile, social media and the increasing lack of control are. Organizational processes, at this juncture for healthcare, are mature however they do not address the basic security issues regardless of the desire for resilient and sustainable practices. This is compounded by a more fundamental problem of the design-reality gap in incorporating security into health information systems development and the healthcare environment. Whilst those in security appreciate what should be done, we do not “sell” security very well, and thus it is not as effective as we would like or anticipate. The design-reality gap stems from a lack of understanding and engagement with the target environment and a lack of appreciation of its changing nature in light of mobile health. Thus, the issues have to be addressed from the two opposing ends the security continuum: the initial design of security in healthcare systems and the end-user experience, use and consumption of information in health. What problems should be addressed first and how do we prioritise these? How can, or in fact are we able to, address both problems at the same time?

3.14 Problem Statement: System Design beyond Duress Passwords

Alf Zugenmaier (Hochschule München, DE)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Alf Zugenmaier

Joint work of Zugenmaier, Alf; Coles-Kemp, Lizzie

Currently, most security system designs assume that, after successful authentication, all actions in the system represent the will of the authenticated principal. However, this view does not take into account coercion. Coercion is the threat of a coercer to bring a certain unpleasant consequence upon a coercee, unless the coercee performs (or doesn't perform) a specified action. A coercion attack would be very powerful, as it could be used to turn any attacker into an insider. Thus, it is necessary to define system design principles such that the system becomes resilient to coercion. Coercion resistance mechanisms available in the literature today are mainly limited to e-voting and to duress passwords. We will study the design space framed within the universal credit system for benefit in the UK, which will be digital by default. In this system, citizens will need to obtain an online identity from one of the different online identity assurance providers to participate. Coercion in this system would lead to increased cost in order to provide the required support to the citizens in need.

4 Working Groups

In order to promote a synthesis of the different perspectives represented, the seminar was structured as a combination of collaborative working groups focused on the development of design principles for organizational processes that are sustainably secure and talks. The abstracts from the talks are presented in the next section and reflect the breadth of the disciplines represented at the seminar. Each collaborative working group selected a theme and a scenario from the provocations and explored the organizational processes at work within the scenario. Each group produced their outputs in poster format and presented these outputs to the seminar. In the concluding session on working group work, we used a panel discussion format and the following design principles for organizational processes that are sustainably secure were co-produced:

- Transparency. In the working groups' scenarios transparency in organizational processes and an honest presentation of the values underpinning those processes was deemed necessary to encourage the desired data handling practices,
- Minimisation. In a number of the working groups, the need for minimisation of data handling practices was an emergent theme. Minimisation as a theme emerged in a number of ways: the need to reduce the number of data handling practices, the need to design simple data handling practices and the need to restrict the number of variants of a particular data handling practice.
- Consent. The theme of consent was reflected in a number of the working groups' conclusions. A spectrum of consent was considered ranging from consent to collect data about staff through to buy in from staff to support a particular organizational process.
- Lawfulness. It was agreed that there needs to be a clear alignment between the legal and regulatory framework in which the organization operates and the organizational processes that are implemented.

5 Open Problems

The design principles require investigation and as such the list of principles produced from the conclusions of the working groups present a set of open problems that require further exploration.

Participants

- Julie Boxwell Ard
Glenn Dale, US
- Florian Arnold
University of Twente, NL
- Debi Ashenden
Cranfield Univ. – Swindon, GB
- Arshid Bashir
RHUL – London, GB
- Sören Bleikertz
IBM Research – Zürich, CH
- Rainer Böhme
Universität Münster, DE
- Lizzie Coles-Kemp
RHUL – London, GB
- Sophie Engle
University of San Francisco, US
- Vaibhav Garg
Indiana University –
Bloomington, US
- Carrie Gates
CA Labs -New York, US
- Dieter Gollmann
TU Hamburg-Harburg, DE
- Marit Hansen
ULD SH – Kiel, DE
- Cormac Herley
Microsoft Res. – Redmond, US
- Michael Huth
Imperial College London, GB
- Jean-Lous Huynen
University of Luxembourg, LU
- Dan Ionita
University of Twente, NL
- Florian Kammüller
Middlesex University, GB
- Ana Margarida Leite de
Almeida Ferreira
University of Luxembourg, LU
- Makayla Miranda Lewis
RHUL – London, GB
- Kai-Uwe Loser
Ruhr-Universität Bochum, DE
- Anne-Marie Ostveen
University of Oxford, GB
- Wolter Pieters
TU Delft, NL
- Joachim Posegga
Universität Passau, DE
- Marco Prandini
University of Bologna, IT
- Christian W. Probst
Technical Univ. of Denmark, DK
- Ingrid Schirmer
Universität Hamburg, DE
- Sven Übelacker
TU Hamburg-Harburg, DE
- Sam Weber
NSF – Arlington, US
- Sean Whalen
Columbia University, US
- Trish Williams
Edith Cowan University –
Joondalup, AU
- Alf Zugenmaier
Hochschule München, DE

