Report from Dagstuhl Seminar 19451

Biggest Failures in Security

Edited by

Frederik Armknecht[1], Ingrid Verbauwhede[2], Melanie Volkamer[3], and Moti Yung[4]

1 **Universität Mannheim, DE,** armknecht@uni-mannheim.de
2 **KU Leuven, BE,** ingrid.verbauwhede@esat.kuleuven.be
3 **KIT – Karlsruher Institut für Technologie, DE,** melanie.volkamer@kit.edu
4 **Columbia University – New York, US,** moti@cs.columbia.edu

Abstract

In the present era of ubiquitous digitalization, security is a concern for everyone. Despite enormous efforts, securing IT systems still remains an open challenge for community and industry. One of the main reasons is that the variety and complexity of IT systems keeps increasing, making it practically impossible for security experts to grasp the full system. A further problem is that security has become an interdisciplinary challenge. While interdisciplinary research does exist already, it is mostly restricted to collaborations between two individual disciplines and has been rather bottom-up by focusing on very specific problems.

The idea of the Dagstuhl Seminar was to go one step back and to follow a comprehensive top-down approach instead. The goal was to identify the "biggest failures" in security and to get a comprehensive understanding on their overall impact on security. To this end, the Dagstuhl Seminar was roughly divided into two parts. First, experienced experts from different disciplines gave overview talks on the main problems of their field. Based on these, overlapping topics but also common research interests among the participants have been identified. Afterwards, individual working groups have been formed to work on the identified questions.

Seminar November 3–8, 2019 – http://www.dagstuhl.de/19451
2012 ACM Subject Classification Security and privacy, Social and professional topics
Keywords and phrases Cryptography, Hardware, Security engineering, Software engineering, Usability, Human Computer interaction (HCI), Human and societal aspects of security and privacy, Usable security or human factors in security, Security evaluation and certification
Digital Object Identifier 10.4230/DagRep.9.11.1

1 Executive Summary

Frederik Armknecht
Ingrid Verbauwhede
Melanie Volkamer
Moti Yung

General Introduction

In the present era of ubiquitous digitalization, security is a concern for everyone. Consequently, it evolved as one of the most important fields in computer science. However, one may get the impression that the situation is hopeless. Nearly on a daily basis, reports of new security problems and cyberattacks are published. Thus, one has to admit that despite the huge

Biggest Failures in Security, *Dagstuhl Reports*, Vol. 9, Issue 11, pp. 1–23
Editors: Frederik Armknecht, Ingrid Verbauwhede, Melanie Volkamer, and Moti Yung
DAGSTUHL REPORTS Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

efforts continuously invested since many decades, securing IT systems remains an open challenge for community and industry.

One of the main reasons is that the variety and complexity of IT systems keeps increasing, making it practically impossible for security experts to grasp the full system. This results into the development of independent and isolated security solutions that at best can close some specific security holes. Summing up, security requires to solve an increasing number of inter- and intradisciplinary challenges while current approaches are not sufficiently effective. The aim of this seminar was to gain an interdisciplinary view on security and to identify new strategies for comprehensively securing IT systems.

Goals

The goals of the seminar was to address the following main challenges and to commonly discuss solution strategies:

Challenge 1: Interdisciplinarity The topic of security is getting more and more complex and already understanding the state-of-the-art within one discipline is highly challenging. This makes it practically impossible to understand the problems and constraints from other disciplines. Moreover, different disciplines often have their own methods and ”culture”. From our experience, working with colleagues from other disciplines requires at the beginning an enormous effort to understand each other. The complexity grows even further when more than two disciplines are involved.

Challenge 2: Variety of Problems In each discipline, a variety of problems do exist. Naturally, researchers have to single out specific problems that they work on instead of aiming for comprehensive solutions. The selection of problems usually depends on several factors, e.g., background of the researcher, topicality of the subject, etc. Most often, researchers aim for solving very specific problems rather than coming up with more comprehensive solutions. Moreover, the selection is driven by interdisciplinary factors.

For sure, interdisciplinary research does exist already. However, it is mostly restricted to address very few disciplines and has been rather bottom-up by focusing on very specific problems. Instead, the scope of the seminar was to aim for a *broad top-down approach.* To this end, the focus was on the following questions:

- What are the main recurring reasons within disciplines why security solutions fail, i.e., the biggest failures? (Top View)
- How do these failures impact solutions developed in other sub-disciplines? (Broad View)
- What are possible strategies to solve these problems?

Structure

The seminar was structured accordingly. Before the seminar, a survey was conducted where the participants have been asked, what they consider to be biggest failures in security. The list of participants was composed of experts from different, selected sub-fields who were encouraged to explain the main challenges in their field to the audience. Here, ample opportunities for discussions have been provided. That is, instead of having many different talks back-to-back, we had several overview talks from different fields within the first few days. Afterwards, the whole audience commonly identified three topics to be further investigated in separate working groups:

1. The process and role of certifications
2. The human factor in security
3. The education of the society in security

These subgroups met in parallel and worked on specific questions. The remaining days were composed of workgroup meetings and individual talks. At the end of the seminar, the workgroups reported to the whole audience their findings.

This report summarizes the finding of the survey (Section 3), the topics of the individual talks (Section 4), and also the findings of the individual workgroups (Section 5).