Body:

Introduction

The protection of one’s digital privacy is largely based on the security of digital information. Hence, the users’ digital privacy is protected if they have the necessary control over their data or information. This implies that their data on the Internet is protected from unwanted and unauthorized access using appropriate safeguarding measures and that the user is actually able to interact with and apply these measures effectively. Therefore, investigating the usability of security measures is paramount to create effective digital privacy protection. In this context, usability of security and privacy comprises the integration of measures into daily workflows with reasonable effort while keeping complexity and adoption barriers low. Because security and therefore privacy are usually a secondary goal for users on the Internet, complex and costly measures will cause users to neglect security in order to reach primary goals.

Motivation

Research has neglected the usability aspects of security measures in the past. Most of the privacy protection mechanisms applied today were designed to comply with security goals while generally ignoring the users’ needs. Ignoring usability, however, usually causes the user to ignore or circumvent protection mechanisms, which in turn leads to ineffective privacy protection. Similarly, complicated APIs for security mechanisms cause developers to work around security measures.

Hence, a dedicated evaluation of existing security practices and support for the design of future privacy protection measures from the users’ and developers’ perspective is an important challenge for the future of the Internet. Our society can only continue to benefit from information technology, if new, usable security mechanisms are designed and not simply for their compliance with technical goals. Additionally, the need for end-user usability in security mechanisms needs to be recognized by software designers and developers as well. To this end, the following usable privacy and security challenges have been addressed in this project.

Challenges & Highlights

Perceptions and Acceptance of Security and Privacy Measures: The perceptions and needs of users concerning their digital security and privacy need to be assessed and analyzed in more detail. The level of security or privacy a user desires and needs is currently unknown. While perceptions depend on the individual and the context of use, it is important to inform future developments about the users’ needs. Usable privacy and security research has begun to explore this wide field, but more effort needs to be invested in order to create a comprehensive picture. The acceptance of new security or privacy technologies and features also needs considerable attention. A technology can always increase privacy, but users need a motivation to actually apply a mechanism.

Development of Validated Methods for the Evaluation of Usable Security Aspects: Existing methods for the investigation of usability aspects of security and privacy are frequently adopted from sociology or psychology research and general software usability. However, these methods are not sufficient to address specific questions. The usable privacy and security community currently relies on individual and non-standard methods that can differ for similar problems between researchers. This hinders the comparison of related studies and, therefore, human-centric digital privacy and usable security research needs specialized tools that are validated and accepted throughout the research community.

Analyzing Existing Security Mechanisms: To enhance future security mechanisms with respect to usability as well as security characteristics, a focus of current research is the analysis of existing solutions. Analyzing current practices enables us to extract deficiencies concerning the integration of usability and security/privacy from a developer’s side. Based on these investigations, models and requirements of usable and secure mechanisms can be created and current issues can be avoided in future mechanisms.

Usable Privacy and Security by Design: The development of security mechanisms often integrates usability as a downstream step in the development process. While usability engineering advises to consider usability issues throughout the complete development process, dealing with usability requirements in later stages often results in poor usability-security integration. Hence, the development of mechanisms to protect users’ security and privacy needs integrate usable privacy and security aspects as early as possible in order to create mechanisms that are usable by design.
Potential applications & future issues

A future issue is the users’ perception. While addressing the users’ needs in IT security and privacy, mechanism development is one important aspect in the overall process of improving digital privacy, another requirement is the education of users. Many security mechanisms are not used, because users either are not aware of possible security threats or do not have knowledge of alternative mechanisms to protect their privacy appropriately. In a first step, the users’ awareness for existing threats needs to be raised which is an unsolved challenge to date. After users are sensitized to threats, methods need to be found that allow us to enable users to deal with them on their own by using appropriate tools and mechanisms.

Project abstract:

The USECAP project investigates the usability of security and privacy measures as well as the users’ and developers’ perception of online security and its tools. Our efforts aim to raise users’ awareness of potential security and privacy tradeoffs in a sustainable way, in order to enable them to deal with the threats on their own by using appropriate tools and mechanisms.

Project duration:
01.01.2013 - 31.12.2013

Bibsonomy show project publications:
0
Bibsonomy use tabs to list publications:
0

Project manager:
Prof. Dr. Matthew Smith

Project research areas:
Privacy & Security

Project type:
E-Science

Research Area:
E-Science

Status of the Project: