Poster: Understanding and Using Anonymous Credentials

Zinaida Benenson
Friedrich-Alexander-University Erlangen-Nuremberg
Erlangen, Germany
zinaida.benenson@cs.fau.de

Ioannis Krontiris and Kai Rannenberg
Goethe University Frankfurt
Frankfurt, Germany
{name.surname}@m-chair.net

Dominik Schröder
Friedrich-Alexander-University Erlangen-Nuremberg
Erlangen, Germany
dominik.schroeder@informatik.stud.uni-erlangen.de

Alexander Schopf
Friedrich-Alexander-University Erlangen-Nuremberg
Erlangen, Germany
alexander.schopf@phil.stud.uni-erlangen.de

Yannis Stamatiou and Vasia Liagkou
Computer Technology Institute
Patras, Greece
{stamatiu, liagkou}@cti.gr

1. INTRODUCTION

Today, people use the Internet in a great multitude of settings, from information search to shopping to social media participation, and in doing so, leave various digital tracks that are being used for profiling and identification [5].

Usable privacy-enhancing techniques should be complementary to the ongoing legislation efforts for online privacy protection [7]. In this work we report the first results of the empirical evaluation of understandability and usability of such techniques. The evaluation was conducted within the scope of the FP7 European project ABC4Trust (Attribute-based Credentials for Trust) [1].

The concept of Privacy Attribute-Based Credentials, called the *Privacy-ABCs* in the following, has evolved in the past decades [2] and its variants were implemented by IBM in the Idemix system [4] and by Microsoft in the U-Prove system [6]. In general, Privacy-ABCs are issued just like ordinary cryptographic credentials (e.g., X.509 credentials) using a digital (secret) signature key. However, Privacy-ABCs allow their holder to transform them into a new token, called *presentation token*, in such a way that the privacy of the user is protected. Still, these transformed tokens can be verified similarly to ordinary cryptographic credentials (using the public verification key of the issuer) and offer the same strong security.

The project ABC4Trust is comparing the available Privacy-ABC technologies in terms of functionality, security and efficiency and bringing them under one unified architecture. Using this architecture, several applications have been developed and are being tested in a series of pilot deployments. We used the first pilot deployment to explore the understanding and acceptance of the technology by the end users.

2. THE PATRAS PILOT

The first pilot was conducted at the university of Patras in winter term 2012. A course evaluation system was developed with the following properties:

- *Pseudonymity:* A student can authenticate to the system under a pseudonym. No one else (including a malicious Issuer) can present a matching pseudonym to hijack the user's identity.
- *Selective Disclosure:* The student is able to prove the desirable properties, e.g. verify her enrollment to the course she has registered for, without disclosing more information.
- *Untraceability:* The evaluation system cannot connect the evaluation of two different courses back to the same student.
- *Unlinkability:* The system cannot connect a presentation token with the issuance of any of the underlying credentials issued to the students by the institute.
- *Consumption Control:* Students cannot submit more than one evaluation for the same course.

For the pilot, we selected the course "Distributed Systems I" at the Computer Science Department. The 80 enrolled students were given an introductory lecture on the concepts of Privacy-ABCs and 48 of them decided to take part in the trial. These students were given smartcards and corresponding readers, as well as supporting material (manual, videos, etc.). The participants obtained a credential that contained their name and the course enrollment proof. During the term, the students were able to anonymously collect course attendance points with their smartcard. At the end of the term, they could anonymously evaluate the course, provided that they could prove to the system that they attended more than 50% of the lectures.

At the end of the semester, all 80 course participants could anonymously fill in our evaluation questionnaire, and 54 of them (23 years old on average, 36 male, 18 female) actually did so. 41 respondents (28 male, 13 female) had used the system, and 13 (8 male, 5 female) had not used the system.

3. PRELIMINARY RESULTS

3.1 Understanding of Privacy-ABCs

Understanding of the concepts underlying the Privacy-ABCs was tested using six knowledge statements that refer to different aspects of the concept, such as pseudonymity, minimal disclosure or untraceability. The statements could be marked with *true / false / don't know*.

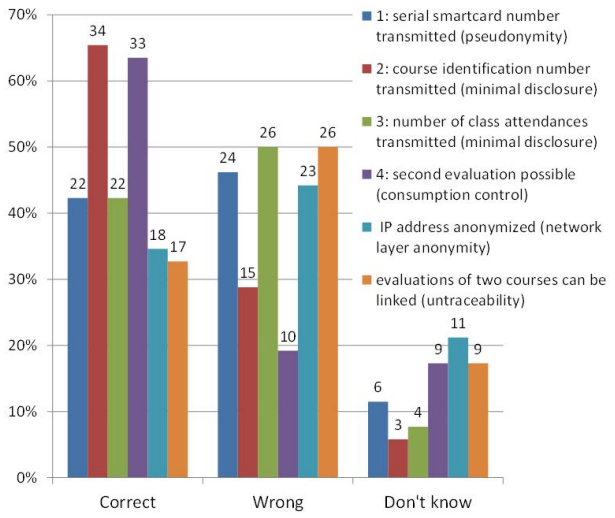

Figure 1: Answers to the knowledge statements about the underlying concepts of Privacy-ABCs.

For example, the statement *When I authenticate to the system, the smart card transmits its unique serial number* was designed to test the understanding that interaction with the system are pseudonymous, that is, the system *cannot* identify the user (and her card), and thus no serial number can be transmitted.

According to the results (see Fig. 1), most participants had difficulties with understanding of the underlying concepts, as more than 50% of them answered 4 out of 6 questions wrong or indicated that they do not know the right answer. There are no significant differences in understanding between students that used the system and students that did not use the system. Also gender differences are not significant.

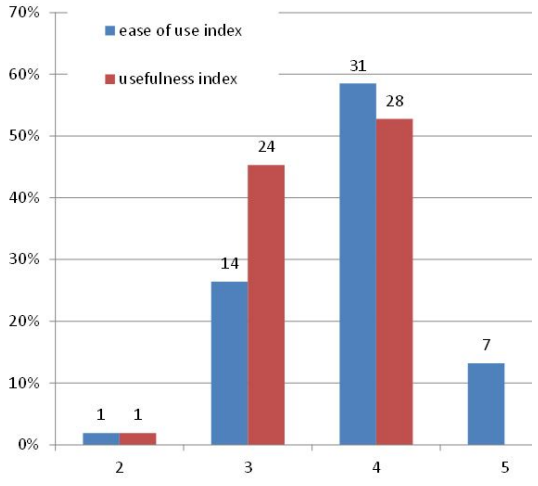

Figure 2: Rankings for Perceived Usefulness and Perceived Ease of use, 1 is the lowest rank, 5 is the highest.

3.2 Usefulness and Ease of Use

We used the 6-item scales for *perceived usefulness* and *perceived ease of use* developed by Davis [3]. We adopted the perceived usefulness scale to our case and asked the participants about the usefulness of the system for protecting their online privacy. The highest rank is 5, the lowest rank is 1. Most participants found the system easy to use and quite useful for protecting their online privacy (see Fig. 2).

4. DISCUSSION AND FUTURE WORK

This work has several limitations that make it difficult to generalize results. For example, all participants are computer science students, meaning that they are technically savvy and interested in technology. With other user groups, especially the results on ease of use might be quite different. Moreover, the pilot system was not actually designed with usability in mind. Better usability might have improved the understanding of system properties, as showed by Wästlund et al. [8].

In this poster, we present the first descriptive statistical results on users' understanding and usage of anonymous credentials. We actually also measured many other variables, such as privacy awareness and concerns, or patterns of the Internet usage. We plan to analyze statistical relationships between these variables more deeply, for example using regression. Moreover, as there are going to be more pilot deployments in the future, we are going to expand this research using the gained experience and lessons learned.

5. ACKNOWLEDGMENTS

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 257782 for the project Attribute-based Credentials for Trust (ABC4Trust).

6. REFERENCES

[1] ABC4Trust EU-Project, `https://abc4trust.eu`.

[2] J. Camenisch, I. Krontiris, A. Lehmann, G. Neven, C. Paquin, K. Rannenberg, and H. Zwingelberg. D2.1 Architecture for Attribute-based Credential Technologies – Version 1. ABC4Trust Deliverable D2.1, December 2011.

[3] F. D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, pages 319–340, 1989.

[4] IBM Research Zurich. Idemix: `http://www.zurich.ibm.com/security/idemix`.

[5] J. Mayer and J. Mitchell. Third-party web tracking: Policy and technology. In *Security and Privacy (SP), 2012 IEEE Symposium on*, 2012.

[6] Microsoft Research. U-Prove: `http://research.microsoft.com/en-us/projects/u-prove`.

[7] S. Spiekermann and L. Cranor. Engineering privacy. *Software Engineering, IEEE Transactions on*, 35(1), 2009.

[8] E. Wästlund, J. Angulo, and S. Fischer-Hübner. Evoking comprehensive mental models of anonymous credentials. In *Open Problems in Network Security*, pages 1–14. Springer, 2012.