PrimeLife – Bringing sustainable privacy and identity management to future networks and services

Dudle – Privacy-Enhanced Event Scheduling

Event Scheduling

There is an endless list of Web 2.0 applications, which allow users to create web polls. (`doodle.com`, `moreganize.ch`, `whenisgood.net`, `agreeAdate.com`, `meetomatic.com`, etc...)

The most important use case of these applications is to schedule events. An initiator who wants to schedule some event creates a poll and sends the link to the poll to the potential participants. Each participant has to fill in his availability. From all availabilities, a meeting can be scheduled.

Privacy Threats

The so-called availability patterns often contain sensible information in at least two respects. First, it is possible to read information directly out of such a pattern (e.g., “Does my boss work after 3pm?”, “Will my husband vote for the date of our wedding anniversary?”).

Second, indirect inference arises from the fact that availability patterns contain much entropy and thus allow to (re-)identify individuals who would otherwise remain pseudonymous (e.g., “The participant, stating this particular availability pattern goes to lunch every day at 11:30. It therefore has to be Peter.”, “The availability pattern of user bunny23 looks suspiciously like the one of my employee John Doe!”).

The most existing applications for event scheduling allow at least some privacy settings. Therefore it is often possible to password-protect the polls, create so-called “hidden” polls where only the poll-initiator may see the results, or to conduct completely anonymous surveys. However, the other participants, the poll-initiator, or the server administrator are still able to see the availability patterns.

Security Threats

Apart from the privacy threats, all applications for event scheduling consist of security problems. In most of these applications, every participant may change the votes of each other participant. The problems of twice-voting and lying about ones identity are not solved in a satisfactory manner. Additionally, in case of the hidden polls at least the initiator might lie about the results.

The security problems get even worse when anonymous polls are performed, as an attacker may forge votes anonymously then.

Solutions

From a scientific point of view, e-voting solutions exist and in fact there are some of these solutions already implemented and available. The problem of these solutions is that they are too complex in terms of computation and communication to being implemented as a Web 2.0 application. All existing solutions therefore suit well in the field of academic protocols or as implementations for governmental elections with high security requirements.

PrimeLife’s Answer

To bring the opportunity of quick, easy, and secure web polls to everybody, a new voting protocol was developed within PrimeLife. This protocol has less requirements than existing e-voting solutions (i.e., it drops the property of coercion-resistance) but it is more efficient in terms of computation and communication complexity.

Derived from the protocol, a web application was created, which gives everybody the possibility to create privacy-enhanced web polls. No preconditions are required to use the application. After directing a browser to the web site, one can create a new poll, invite other participants, and schedule events or do web polls anonymously. After performing a poll, it is guaranteed that

- only the previously configured persons participated exactly once in the poll
- nobody is able to read single votes of the users

due to the cryptographic protocol.

Dudle

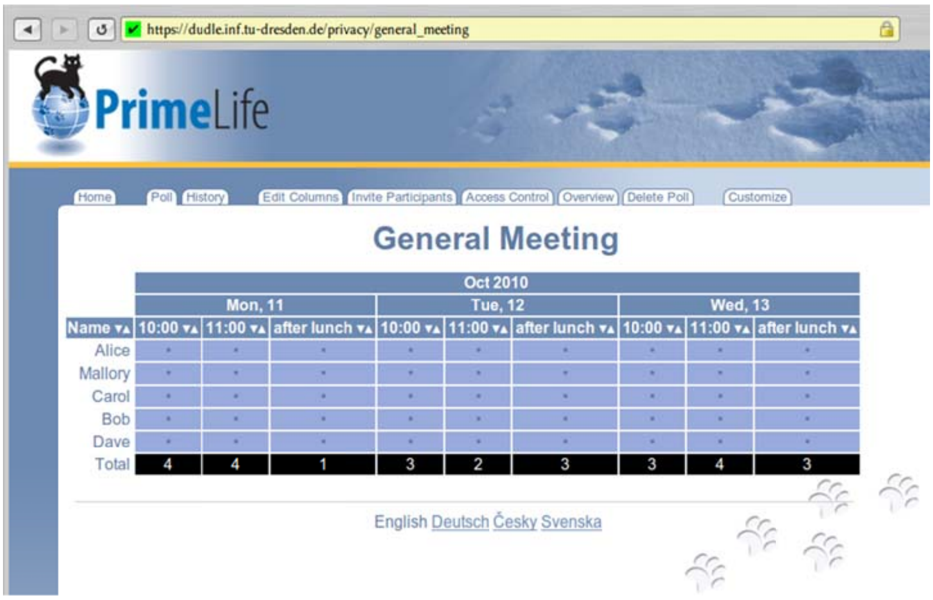
✓ **Secure**
impossible to forge others’ votes

✓ **Privacy-Friendly**
impossible to infer others’ preferences

✓ **Zero-Footprint**
no software-installation needed

`https://dudle.inf.tu-dresden.de`

On a more technical level: Every participant encrypts his vote with a homomorphic encryption. This encryption is realized in JavaScript within the users browser at client-side. Each of the participants will see the encrypted votes only and is able (due to the homomorphic property) to calculate the result from it without the need for decrypting each participants selection.



General Meeting

	Oct 2010								
	Mon, 11			Tue, 12			Wed, 13		
Name ▾▴	10:00 ▾▴	11:00 ▾▴	after lunch ▾▴	10:00 ▾▴	11:00 ▾▴	after lunch ▾▴	10:00 ▾▴	11:00 ▾▴	after lunch ▾▴
Alice	*	*	*	*	*	*	*	*	*
Mallory	*	*	*	*	*	*	*	*	*
Carol	*	*	*	*	*	*	*	*	*
Bob	*	*	*	*	*	*	*	*	*
Dave	*	*	*	*	*	*	*	*	*
Total	4	4	1	3	2	3	3	4	3

English Deutsch Česky Svenska

PrimeLife at a glance

Project reference:

IST-507591

PrimeLife's objective:

Development of a working prototype of a privacy enhancing Identity Management System and demonstration of novel solutions for managing identities

Project duration:

March 2008-June 2011

Partners:

20 partners from industry, academia, research centres and data protection authorities

Costs:

About € 15,5 Million

Funding:

The PrimeLife project receives research funding from the European Union's 7th Framework Program.

Contact:

Marit Hansen
t:+49-431-988-1214
f:+49-431-988-1223
primelife@datenschutzzentrum.de

Date of publication of this Primer:

January 2011

Want more info?

Various deliverables are available online: www.primelife.eu