PrimeLife – Privacy and Identity Management in Europe for Life

Dudle – Privacy-Enhanced Event Scheduling

Event Scheduling

There is a huge list of Web 2.0 applications which allow users to create web polls (e.g., 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 potential participants. Each participant has to fill in his availability. By analyzing the availabilities of all participants, a meeting can be scheduled that fits best.

Privacy Threats

The so-called availability patterns often contain sensitive 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 often 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!").

Most existing applications for event scheduling offer at least some privacy-related settings. For instance it is often possible to protect the polls by password against unauthorized access, 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, and the server administrator providing the service are still able to see the availability patterns.

Security Threats

Apart from privacy threats, all applications for event scheduling suffer from security problems: Most existing applications don't prevent that participants change the votes of other participants. The problems of twice-voting and lying about one's identity are not solved in a satisfactory manner. Additionally, in case of the hidden polls at least the initiator might lie about the re-sults.

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

Academic Solutions

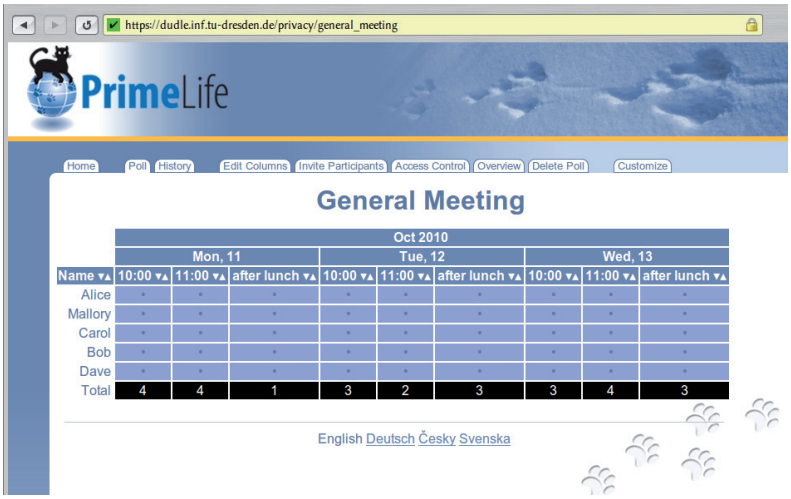
In the academic field, e-voting solutions have been developed in the last years, and meanwhile a few implementations are available. However, these solutions are still too complex in terms of computation and communication to being implemented as a simple Web 2.0 application. Thus, current e-voting solutions may 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 the PrimeLife project. This protocol fulfills fewer requirements than existing e-voting solutions (in particular it drops the property of coercion resistance), but it is more efficient in terms of computation and communication complexity.

On the basis of the developed protocol, a web application called "Dudle" was created that can be used by every interested user to create privacy-enhanced web polls. No preconditions are required to use the application. When accessing the Dudle website, a user can create a new poll, invite other participants, and schedule events or conduct web polls anonymously. The cryptographic protocol of Dudle guarantees that after performing a poll ...

- only the previously determined per-sons have participated maximal once in the poll and
- nobody is able to see single votes of the participants in clear text.



On a more technical level: Each participant encrypts his vote with a homomorphic encryption. This encryption is implemented in JavaScript within the user's browser at the client side. Each participant will see the encrypted votes only and is able (due to the homomorphic property) to calculate the result of the poll without the need for decrypting the other participants' votes.

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

- **Secure**
  impossible to forge others' votes
- **Privacy-Friendly**
  impossible to infer others' preferences
- **Zero-Footprint**
  no software-installation needed
- **Set up dudle on your own server**
  http://www.primelife.eu/results/opensource/63-dudle/

PrimeLife at a glance

Project reference:

216483

PrimeLife's objective:

Bring sustainable privacy and identity management to the web and develop tools for privacy-friendly identity management

Project duration:

March 2008 - June 2011

Partners:

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

Total cost:

About € 15.5 Million

Total EC funding:

€ 10.2 Million

Funding:

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

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:
http://www.primelife.eu/

PrimeLife