IPA Herfstdagen on Security

21–25 November 2005, Zwartsluis

*Program:* Pieter Hartel, Bart Jacobs, Sjouke Mauw

*Organisation:* Tijn Borghuis, Sonja Joosten
Security is *hot*.

**Reasons:**
- Societal relevance.
- Interesting research questions.
- Research funding (Sentinels, NVSO, ...).
- Focus at national and international level (NOAG-ICT, ...).

**Within IPA:** 7 research groups work (partly) on security.

**One of four main application areas of IPA.**
Purpose

- Introduce basic research questions and approaches.
- In-depth knowledge on selected topics (foundations).
- Societal context, industrial experiences, practical problems, real-world applications.
- Competition.
- But also: informal meetings and discussions.
Security dilemma’s

- Security vs. user-friendliness.
- Cost vs. gain.
- Decentralization of computer maintenance vs. lack of security awareness and knowledge by users.
- Theoretical security vs. practical security.
- Identification vs. privacy.
- Vulnerabilities vs. resilience (not really a dilemma).
Structure

For each of the topics:

- Identification vs. privacy.
- Vulnerabilities vs. resilience.

We have three types of sessions:

- Technology session.
- Theory session.
- Application session.

Plus occasionally:

- Tutorial session.
Teams of up to 5 people (inform Tijn).
Teams work outside the scheduled program, and deliver their solutions to Tijn before lunch on Thursday (paper or pdf).
Jury selects best solutions (coffee break Thursday afternoon).
Presentations (5 minutes) of best solutions on Thursday evening.
Jury will announce winner.
The blind membership testing problem

- Server $S$ and a client $C$.
- Server maintains a set $P \subseteq A$, for some set of items $A$.
- Contents of $P$ is not known to the client.
- For a given item $x \in A$, which is not known to the server, the client wants to know whether $x \in P$.

Develop a protocol describing the communication between client and server, after execution of which the client knows if $x \in P$.

Requirements:
1. The server learns as little as possible about which value $x$ is being queried by the client.
2. The total size of the communications is minimal.
Two extreme solutions

Cheap, but no privacy.
- Client sends message $\textit{query}(x)$.
- Server replies $\textit{reply}(\text{yes})$ if $x \in P$ and $\textit{reply}(\text{no})$, otherwise.

Private, but expensive:
- Client sends the message $\textit{query}$.
- Server replies $\textit{reply}(P)$.
- Client tests whether $x \in P$. 