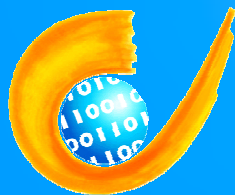


Using Legally Compliant Reputation Systems to Filter SPIT

Marit Hansen

Independent Centre for Privacy Protection
marit.hansen@datenschutzzentrum.de



Markus Hansen – Jan Möller
Thomas Rohwer – Carsten Tolkmitt
Henning Waack



Motivation

- Internet Telephony has developed, allows **cost-saving** use of VoIP technology.
- VoIP will affect audio communication as e-mail affected written communication.
- **Unsolicited calls** are already annoying PSTN customers.

=> SPAM over Internet Telephony (SPIT) will become a problem similar to e-mail SPAM.

Motivation

- SPIT is expected to increase dramatically with cheaper calls.
=> Privacy protection needed.
- Laws prohibiting such calls are most often effectless against calls from other countries.
=> Technical approach needed.
- Telecommunication is regulated by several laws. Sanctions are up to five years in prison.
=> Legal compliance needed.

The SPIT-AL Project

(“SPIT-Abwehr-Lösung” – funded by European Regional Development Fund)

- **White Paper**
German language, download at www.spit-filter.com
- **Prototype**
Implementation in progress <=
- **Test Run**
with 1,000 users by end of 2006
- **Open Source Project**
Public funding, public benefit!
- **Diploma Thesis**
at Dresden University of Technology

SPITting into your Ear

- **Calls from humans: e.g., call centres**
- **Calls from automated devices: e.g., SPAM Bots**
- **Ringtone SPIT**
- **Combinations**

- ***Simple(?) solution – requiring change in protocol:
Attaching money to calls and thereby
offering a surety (“Kaution”),***
*cf. M. Reichenbach, H. Damker, H. Federrath, K. Rannenber, "Individual Management of
Personal Reachability in Mobile Communication", in: Proceedings of the IFIP TC11 SEC 97,
13th International Information Security Conference, Copenhagen, May 1997.*

SPIT-AL: Technical Approach

- **E-mail SPAM: header & content analysis**
- **Content analysis of audio communication:**
 - **Synchronous** communication; impossible to conduct before call is established
 - Technically **complex**, binds resources
 - **Breaking of secrecy of telecommunication possible, in Germany: up to 5 years in prison**
 - **Not planned within SPIT-AL**
(would not prevent annoyance anyway)

SPIT-AL: Technical Approach

- Analyse **information about caller**:
 - Caller ID? (lacking authenticity with SIP)
 - Origin: PSTN / SIP (proxy, IP range)?
 - **White lists** / buddy lists / black lists
 - **Recursive lists** / Web of Trust
 - *Statistical Analysis (backbone)*
 - Analyse **information about call**:
 - “6am? Sorry, Mum.”
 - Weight results, sum up.
- ⇒ **Reachability management**

SPIT-AL: Technical Approach

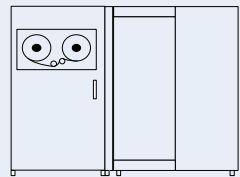
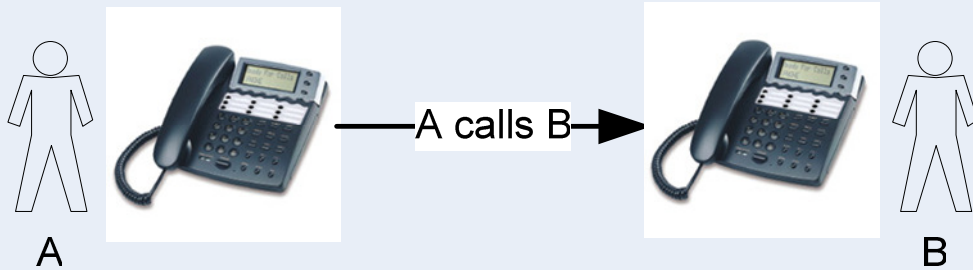
- Different **actions** according to results:
 - Establish call (implementation: easy)
 - “Busy” on first try (greylisting)
 - Challenge the caller:
 - “Please press *42#.” (simple voice menu)
 - “What is 10 divided by 2?”
 - *Voice box* => asynchronous
 - Announce alternate reachability

SPIT-AL: Legal Aspects

- **Consequences for development:**
 - **User-controlled filtering!**
 - **Transparency and control of data processing and its consequences**
 - **Configuration presets for different types of users**
 - **Configuration options fine-grained**

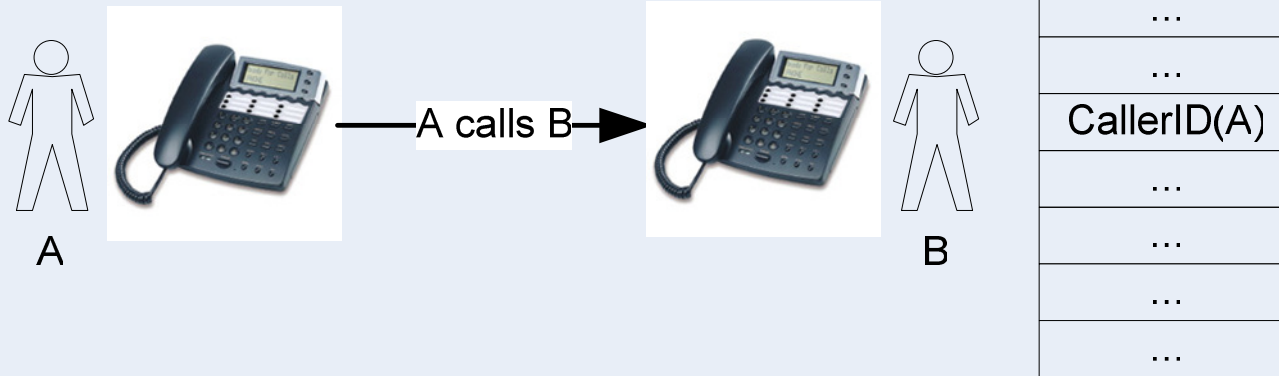
Problem: Recognising SPIT

**Problem:
How to enhance control
by the user?**



**Calling
Machine?**

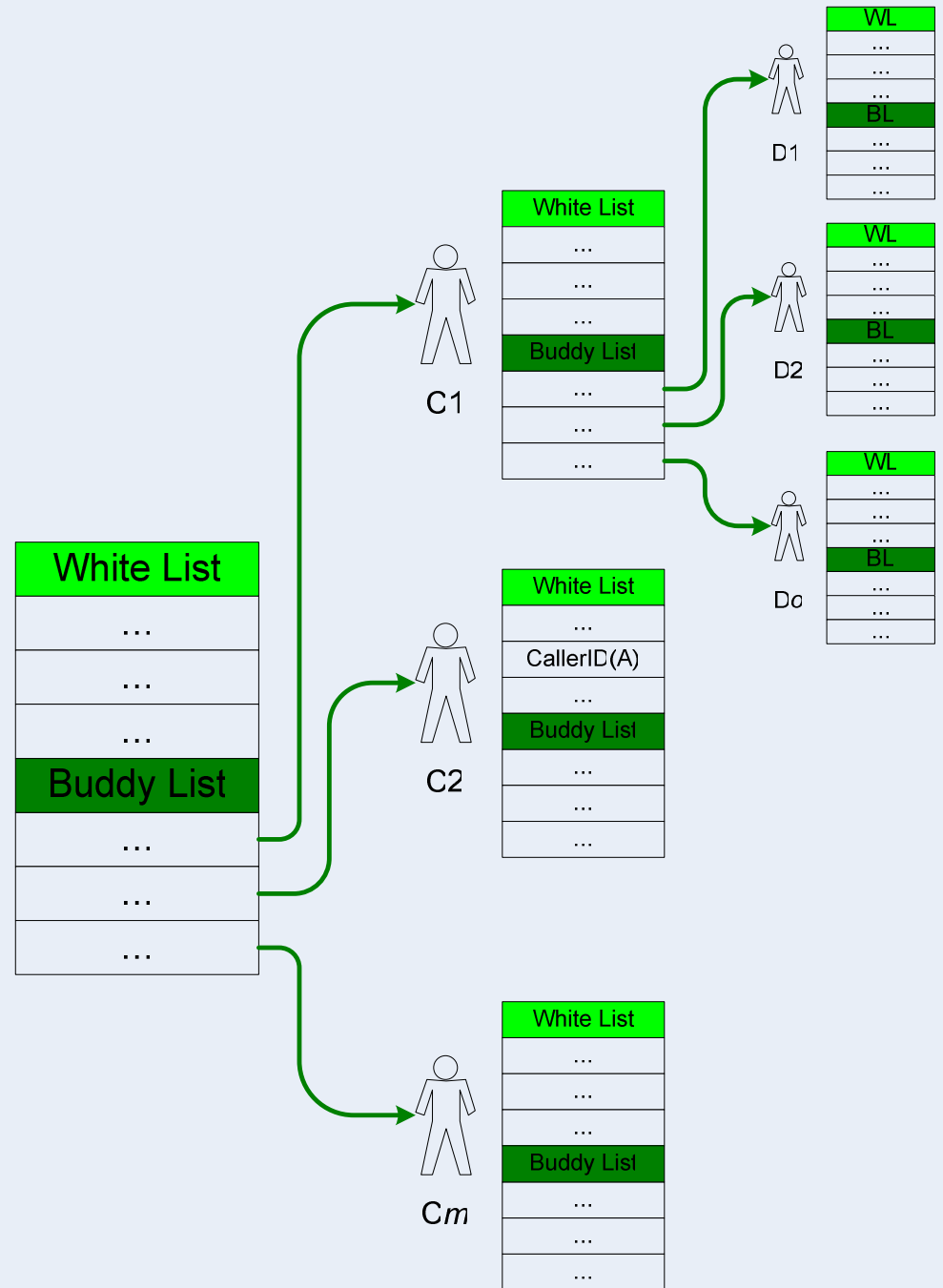
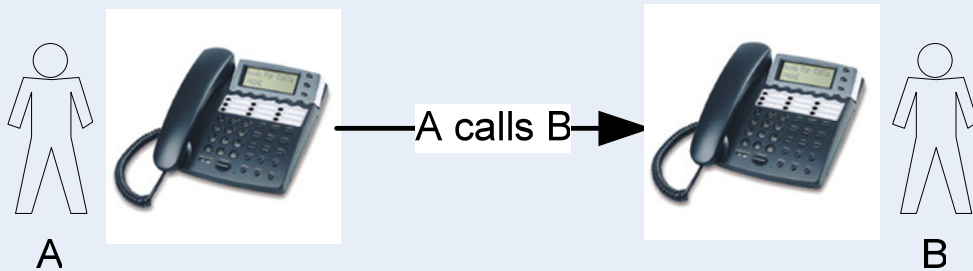
White List on the User's Side



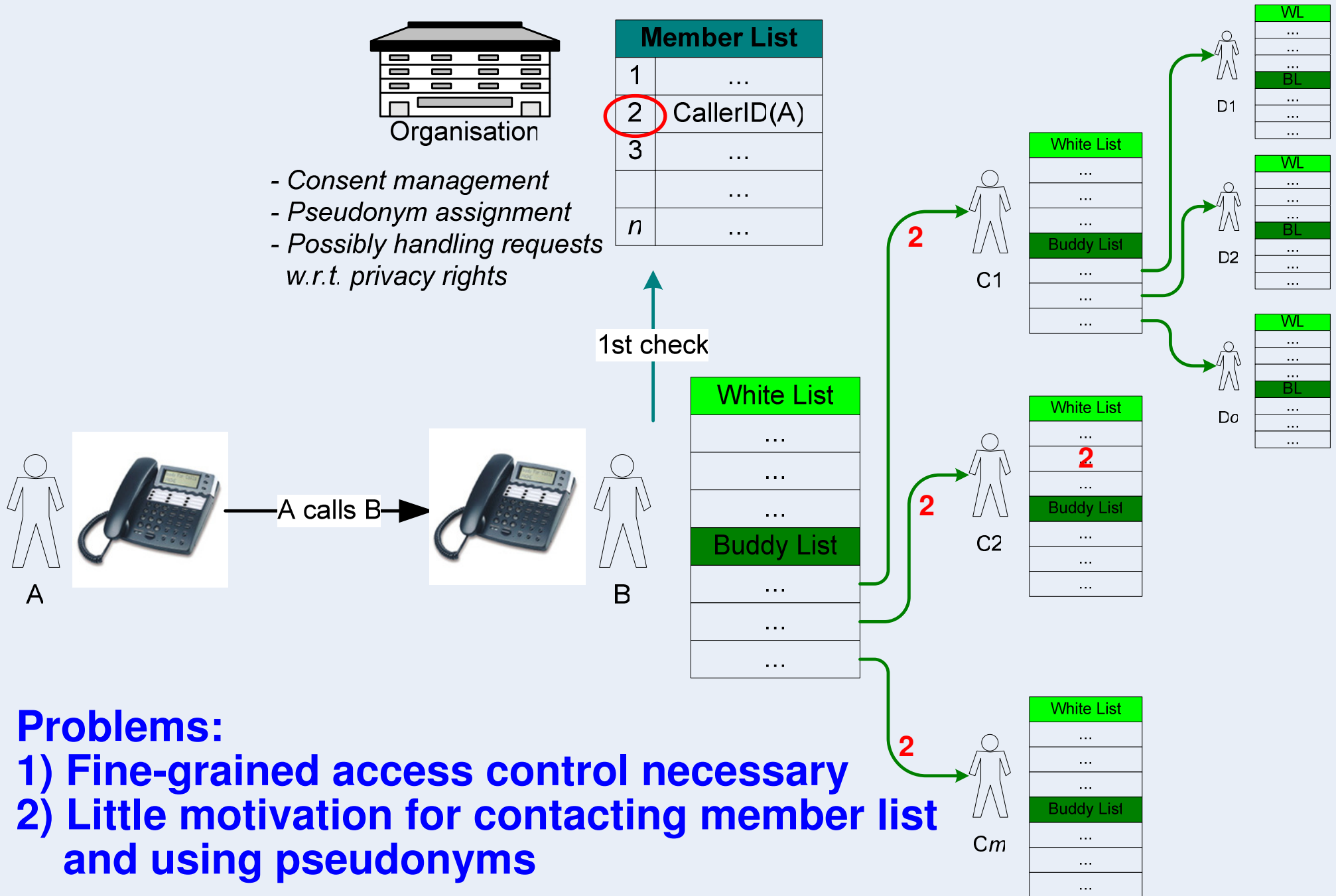
Problem:
Data base too small

Distributed White Lists

Problem:
Legal grounds for handling
A's personal data?



Central Party for Consent Mgmt



Problems:

- 1) Fine-grained access control necessary
- 2) Little motivation for contacting member list and using pseudonyms

Current Research Topics I – Interests of Callers –

- All privacy problems from **scoring systems!**
- How to handle **unfair discrimination?**
 - Complaint handling?
 - Default settings?
- Does **withdrawal of consent** work?
- How to **inform** users about data processing?
How to offer them **right to access?**
 - Log all requests?
 - Possibility for “active information” (sending messages to users without storage)?

Current Research Topics II

– Interests of Peers Providing Infos

- Protecting members from **undesired requests**
 - Protecting information about **social network**
 - Do **peers** have to fulfil the same **obligations** as organisations?
 - Responsibility for integrity etc.?
 - Guarantees of availability?
 - Handling complaints?
- ⇒ **Motivation** of peers to provide information?
Critical mass?

Current Research Topics III

– Other Real Life Problems –

- **“Wrong” entries**
 - Intentional, e.g., by hackers
 - Unintentional, e.g., by role switches (friend being an insurance agent)
 - Figuring out where they come from
 - ⇒ **Informing** source peer
 - ⇒ **Cutting link** to source peer
- **Efficiency**: What if real-time requests do not scale?
 - ⇒ **Crawler** to collect all data, being stored centrally
 - ⇒ **“Short cut requests”** possible
 - **Central knowledge of social networks!**
 - ⇒ **Possibility to partition data?**
 - ⇒ **How to balance** centralised and decentralised components?

Conclusions

- **Legal requirements** for reputation systems are neither fully described nor solved:
 - Privacy-enhancing reputation systems currently don't deal with **user rights to access** etc.
 - **Law addresses organisations** differently than natural persons: What about “organisations” / “communities” formed by peers?
- In the case of SPIT **data avoidance is difficult.**
- **Balances** sought:
 - Centralised vs. decentralised components
 - Rights vs. obligations ...

References

- www.spit-filter.com
- Markus Hansen, Marit Hansen, Jan Möller, Thomas Rohwer, Carsten Tolkmit, Henning Waack: *Developing a Legally Compliant Reachability Management System as a Countermeasure against SPIT*; Third Annual VoIP Security Workshop, 1-2 June, 2006, Berlin



- **PRIME Research on “Multilateral Interactions”**
- **Diploma Thesis at TU Dresden to come**