Data Security and Data Privacy
in Network Environments and Assistance Systems

Problem
Development of Methods for Secure Data Partitioning, Code Partitioning and Multi-Channel Communication

- Data security and secure communication are essential for the professional usage of information systems.*
- Inter alia, the usage of Cloud Computing Services needs a high level of reliability and trust in the Cloud provider’s security policies and security management processes **

Goals
- Improving data security and privacy in distributed information systems
- Enhancing trust and reliability between user and provider

Approach

Data Partitioning
1. Data Analysis based on specific data types and security criteria
2. Data Separation in different categories (e.g., private and public)
3. Data Distribution to different data sinks

Code Partitioning
1. Code Analysis at time of compilation (e.g., by using security code annotations) or as far as possible at run time with heuristics to find and distinguish sensitive and non-sensitive program parts
2. Code Separation by using distributed programming techniques (e.g., remote procedure calls (RPCs))
3. Code Distribution to public and private computing nodes

Multi-Channel Communication
- Usage of multiple independent communication channels and technologies
- Separation of original data streams into smaller data streams, weighted by the given network properties (e.g., bandwidth, latency, jitter)

Use Case: Smart Meeting Environment

Data Partitioning
- Mobile User do not want to share her/his private information with the Smart Environment (SE)
  ➔ Private Data = Mobile User’s data
  ➔ Public Data = Data gathered and computed by SE

Code Partitioning
- Mobile User accept the monitored execution of code on her/his own personal device ensemble
- Service-Agents migrate between SE and Mobile User’s devices and run in “Sandboxes” in which all accesses to private data are controlled

Multi-Channel Communication
- In case of Mobile User’s permission to share private information, she/he can transfer data by means of separate communication channels to the SE

Summary of expected results

✓ Novel techniques for establishing Data Security and Data Privacy in Distributed information Systems (e.g., Cloud Computing Systems, Smart Environments, etc.)
✓ Every User keeps control over her/his Private Data


Institute for Computer Science | Research Group Computer Architecture
University of Rostock | 18051 Rostock, Germany
Dipl.-Inf. René Leistikow | E-Mail: rene.leistikow@uni-rostock.de
Phone: +49 381 498 7554 | Facsimile: +49 381 498 7555