Carnival

An Application Framework for Enforcement of Privacy Policies

Ragni Arnesen, Jerker Danielsson and Bjørn Nordlund

Norwegian Computing Center (Norsk Regnesentral)

Nordsec 2004
5 November 2004
Carnival

- A means for organizations to achieve customer privacy
- Provides mandatory enforcement of organizations’ privacy policies through privacy access control
- Provides audit functionality
- Supports automated enforcement of customer preferences
- An application framework
- Implemented in Java
Customer privacy

► Customer privacy concerns organizations that collect and use personal data, and that:
  ▪ Have a legitimate need for personal data
  ▪ Wish to protect the privacy of their customers from threats from insiders and outsiders

► A privacy policy documents how personal data can be used in the organization. It is based on:
  ▪ Legislation
  ▪ The organization's needs and preferences
  ▪ Customers’ preferences
Customer privacy

► Carnival provides one part of the solution

► Organizations should:
  ▪ Analyze the need for collecting personal data
  ▪ Analyze the need for using personal data
  ▪ Develop a privacy policy
  ▪ Enforce the privacy policy
  ▪ Design for privacy
Privacy access control

- The purpose of the information access must coincide with the purpose stated when the requested information was collected (purpose binding)
- Access can lead to obligations that must be fulfilled
- Need for taking individual/customer preferences into account
Design goals

► Capture the user’s purpose of access
► Enforcement of application independent policies
► Support for domain specific obligations
► Support for replaceable access evaluation logic and condition evaluation logic
► Easy to integrate with applications
Carnival Framework

Application

Services / Interface

Carnival Framework

Rule Engine

Condition Evaluators

Data Subject Finders

Obligation Router

Obligation Executors

Logger

Application Logic and Data

Purpose selection

Privacy Manager

Managed Personal Data Object
Carnival deployment

Carnival Server
- Management
- Purpose Service
- Log Service
- Repository

Diagram showing the integration of Carnival Server with other components.
Information that Carnival extracts from the application

- The **roles** of the requesting user
- The **action** requested
- The **purpose** of the requested access
- The **type of data** requested
- The identity of the **data subject**
- Other information needed for evaluating domain specific conditions
Determining purpose, the problem

► Privacy policies, and the purpose statements they contain, are often rather abstract to be manageable and accessible to humans.

► Privacy policies state that personal data can only be accessed for specific purposes

► Computer applications are generally only aware of what the user wants to do (i.e. the requested operation), not why (i.e. for which purpose)

► The access control mechanism and the user must have the same understanding of what the user’s purpose is

► The interruption to users’ workflow should be minimized
Determining purpose, the Carnival way

► Refinement of possibly abstract purpose specifications
► A user’s current purpose is determined as a function of the user’s roles and the methods invoked by the user
► The application should provide methods that are called when the user moves from one purpose to another
► The application should provide Carnival with GUI callbacks, that Carnivals uses to display its understanding of the user’s current purpose
► The user is provided with the possibility to override the purpose selected by Carnival
Conclusions

► Privacy access control should be mandatory
► Access control and audit must be combined in the privacy domain
► Carnival fulfills the listed design goals
  ▪ Capture the user’s purpose of access
  ▪ Enforcement of application independent policies
  ▪ Support for domain specific obligations
  ▪ Support for replaceable access evaluation logic and condition evaluation logic
  ▪ Easy to integrate with applications
Thank you

Questions?

jerker@nr.no