Privacy and Processes

Ciarán Bryce

PRIAM

Saint Malo

May 22-23 2008

Definition of a Process

- "*A general method of doing something, involving steps or operations which are usually ordered and/or interdependent.*"
  - E.g., in manufacturing, organizations, software development, etc.
- "*A business process is a set of linked activities that create value by transforming an input into a more valuable output. Both input and output can be artifacts and/or information and the transformation can be performed by human actors, machines, or both*".

Why Processes are Important

- Information system is subject to technical, organizational and legal constraints
  - Organizational
    - *Applying patches and measuring effectiveness of patches,*
    - *Analyzing user behavior for application preferences and evolution of system*
    - *Ensuring people who need documents have access*
  - Legal
    - *Document archival for Sarbanes Oxley*
    - *Digital Restrictions Management (e.g., for software licensing)*
    - *Personal Data protection*

Why Processes are Important

- Technical solutions have less and less significance
  - E.g., Most effective anti-virus is coherent and rigorous patching policy
- Information system is an organizational bottleneck
  - To be agile, need to abstract IT to match roles and objectives of organization
  - IT Challenge is integration
    - Companies need architects, not programmers
- Written formal description of process permits
  - Comparison, optimisation and analysis (e.g., for business continuity, etc.)
  - Foundation for execution

Processes versus Applications

	Application	Process
Defined as	Code base	Set of activities working towards precise goal
Actors involved	Programmer, user	Programmer, manager, operator, certifier, client, user, etc.
Role in organization	Asset	Expresses business or organizational model
Reliability/Availability	Fault Tolerance (software and hardware faults)	Business Continuity (Bird flu, computer failure, stock market crash)
Security	Cryptography, access control, etc.	Employee screening, key management, SOX compliance, etc.
Efficiency	CPU cycles, memory space, etc.	Man-hours, cost, sales, business intelligence.

Processes in PRIAM

- CNIL and Garante directives
  - Implementing them and verifying them
- In functional model, the auditor is a role !
  - Who is permitted this role? What are associated rights? etc.
  - Knowledge Management is a process issue
    - Someone has to define ontologies - and someone has to define who that someone is
- TPM management is a process issue
  - Roles of privacy CA need to managed: security depends on this
- Software provider of functional model layer is a principal !

Example of Motivation for Process Support

… and challenges

The EDOS Project - improving the quality of an open source distribution.

Background

- *"Linux is not a product. Rather, Linux is a collection of software components, individually crafted by thousands of independent hands around the world, with each component changing and evolving on its own independent timetable. …. Linux is not a product. It is a process."*

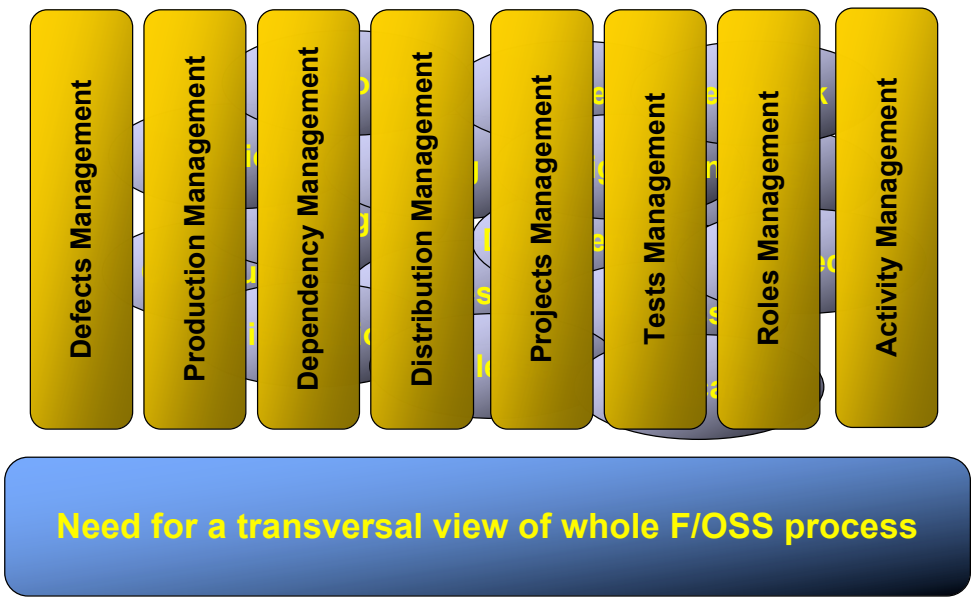
  Ian Murdock, founder of the Debian project.

- The more F/OSS users, the better! …. In principle.

Background

- Building a distribution involves
  - Producing and Collecting software
  - Configuring/compiling with respect to the dependencies
  - Quality Assurance (Testing)
  - Distributing to clients : boxes and download
- These activities are currently tackled separately
- List is not exhaustive, e.g.,
  - Training of developers
  - Scouting for clients
  - ….
- All part of the F/OSS process

F/OSS Environment



F/OSS Process

- Process
  - A community of actors who consume and produce resources
  - A multitude of activities and tools
  - A number of roles for activity organisation
- Lack of activity coordination and performance metering leads to process inefficiency
- Structured process management leads to improvement, e.g. in F/OSS,
  - Ontology activity that defines and binds attributes to actors and resources for more flexible look-up, e.g.,
    - *Find package that has been tested on Mandrivalinux 10.1 with Ethernet card enabled*
    - *Find developer with experience in cryptography and Java programming*
    - *Find someone willing to act as a secondary server administrator*

Process Reference Model (version 1)

- Represents the main data types used in a F/OSS process
- Represents content and community in a uniform manner
- Models management of any activity in the F/OSS Process
- Models evolution of projects, i.e., addition and integration of new activities
- The PRM provides a model of F/OSS artefacts and activities that manage these artefacts
- Current format of PRM: formal model and Java API

PRM Model

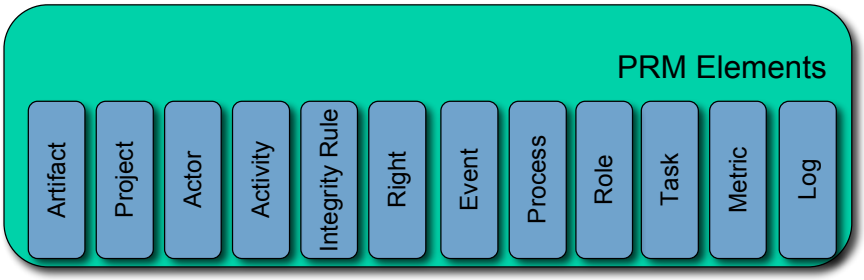
- The Information model binds meta-data (attributes) to artefacts
  - Used to lookup artefacts
    - *E.g., find Java packages with RSA implementations*
  - Lookup takes attribute Boolean algebra expressions
    - *E.g., find Java cryptography packages from official mirror servers or trusted peers*
  - Substitutability
    - "Best match" semantics in look-up
- The model also defines primitives to create and lookup artifacts based on attributes
  - These enable F/OSS activities to be coordinated
    - *E.g., pipeline all reported errors on package to competent developer*
  - Lookup blocks until create of artefact with matching attributes

Examples of Attributes

Actor	Unit of Content
Contact Information	License
Knowledge	Version
Competences	Type
Interests	Target architecture
	Dependencies
	Conflicts
	Et cetera

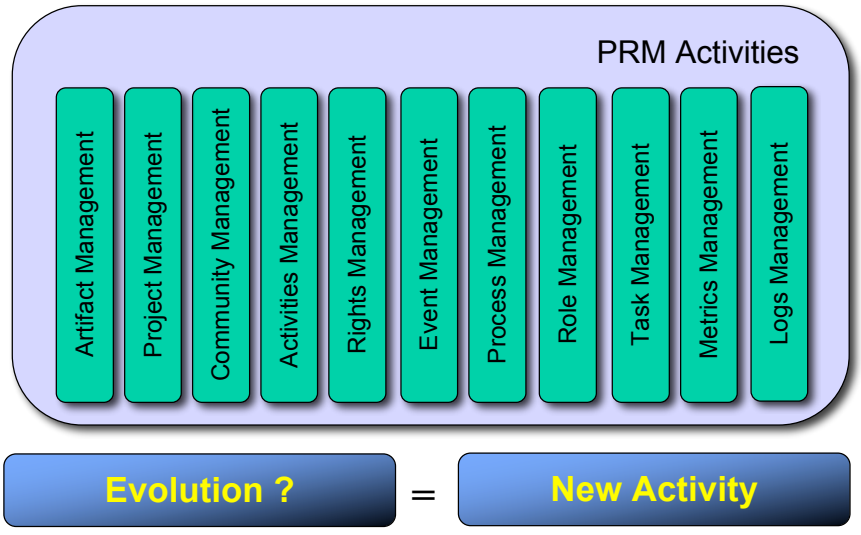
- Actors and content are equally important to process
- Code and documentation are equally important

PRM Elements



- Core PRM Elements represent the minimal set of Artifacts for handling
  - Community, Projects, Resources, Responsibilities, Measurement, Etc.
- Artifacts
  - Managed by PRM activities
  - Located via attributes

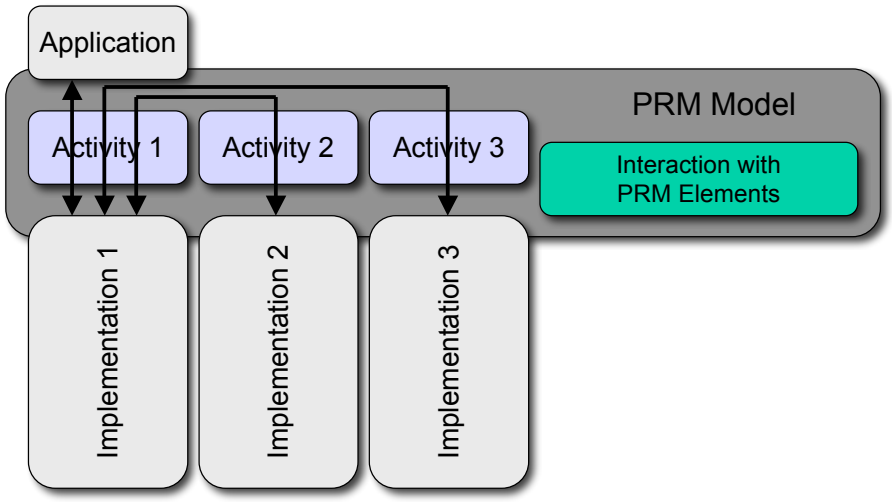
Core PRM Activities



- An activity defines a set of operations that manage artifacts and integrity rules
  - e.g., No version exists between old and new version for code artifacts

PRM Activity Interaction

- Challenge in implementing processes is handling legacy code
  - Applications and Activity implementations have to communicate through the interfaces provided by the Activities



Examples of PRM Operations

- Artifact Management
  - registerArtifactType(Type Directory, Valuation Directory, P IR, Project):Type
  - newArtifact(Type, Value Directory, Project):
  - lookup(Directory, Project):PArtifact
  - exists(Artifact):Boolean
  - substitutable(Artifact, Artifact):Boolean
- Activity Management
  - declareActivity(Name, P(lambda, P IR)):Activity
  - associateActivity(Activity, Project):void
  - lookup(Directory):PArtifact
  - exists(Activity):Boolean
  - isAssociated(Activity, Project):Boolean

Metrics handling

- Fundamental goal of process infrastructure is to measure and meter activities
- Individual activities can have metrics (e.g., number of bug reports per package)
  - Or are bound to specific implementation tools
- Challenge is to convert metrics to KPIs
  - Useful KPIs in PRIAM
    - Number of reported privacy violations
    - Relation of number of auditors to claimed violations
    - Relation of TPM use to reported violations
    - Ease of integration of functional architecture

Handling metrics through the PRM

- Creation
  - new Metric(description, viewpoint, metric set[], occurrence, execution)
- Lookup
  - find(directory) -> Metric[]
- Evaluation
  - evaluate(project, Metric) -> value
- Observation
  - observe(Project, Metric, Value) -> wait for event (metric value reached)

Current Work on the PRM

Ciaran Bryce (INRIA)

Olivier Abdoun (INRIA)

Chrislain Razafimahefa (Shared Object)

Stéphane Laurière (Mandriva)

Michel Pawlak (University of Geneva)

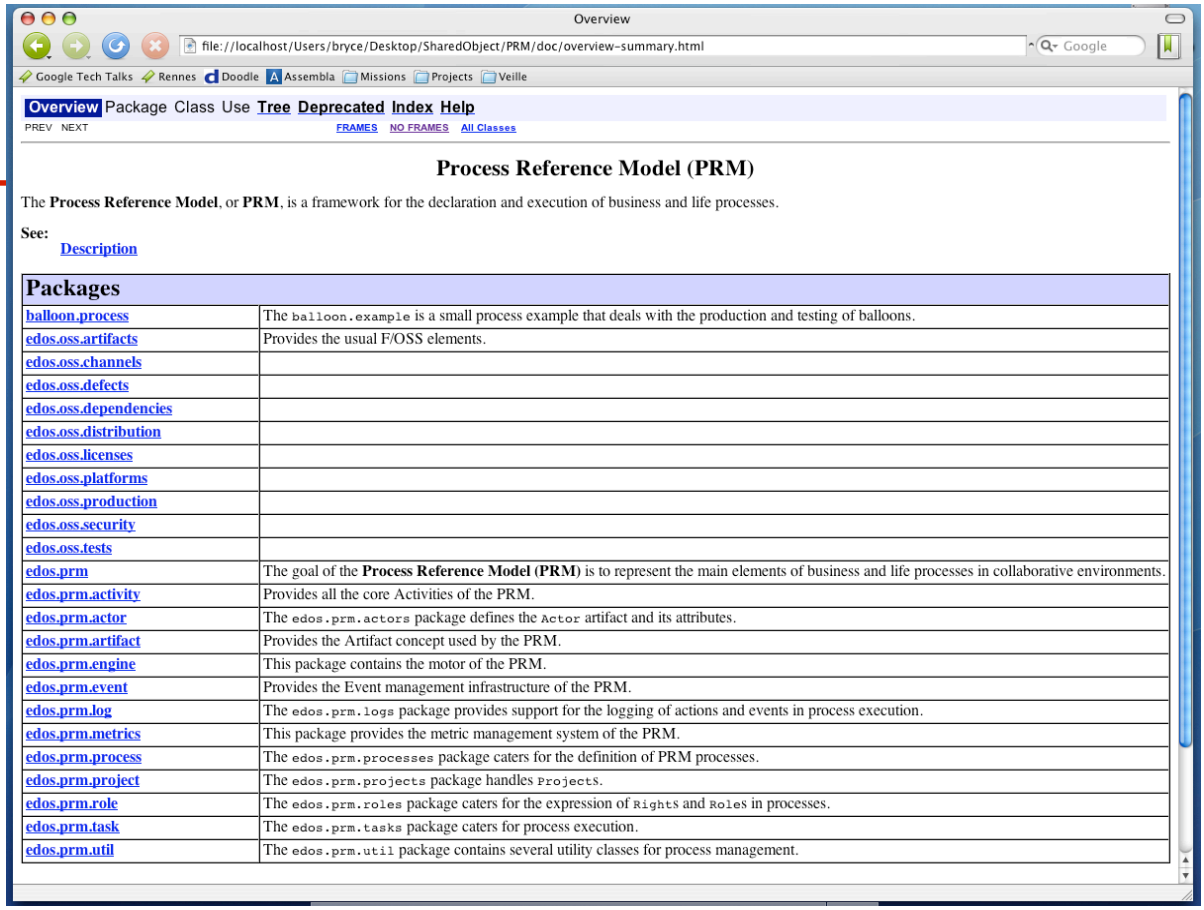
Current Work

- Separate core process support from F/OSS support
- Development of process language and (JavaCC) compiler

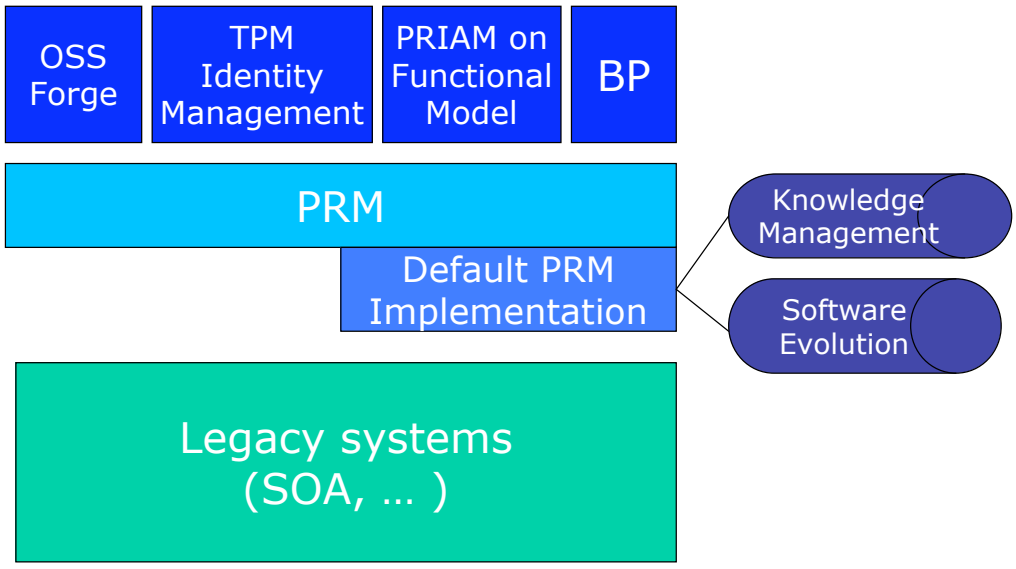
- SOA/BPM Project
  - Mapping PRM to SOA infrastructure

- Qualipso
  - Refining OSS part of PRM

- Code, code, code
  - Aiming for release in July (Apache 2 License)



Architectural Overview



Apache Licence 2, except for BP parts

Abstract Architecture