Privacy-aware Access Control

Nicola Zannone
Access Control

- **Goal**: protect data and resources from unauthorized access
  - Confidentiality
  - Integrity
- **Policy**: define which actions a subject is allowed to perform on an object
- **Model**: define specification and enforcement of access control policies
  - DAC, MAC, RBAC, ABAC
Goal of this lecture

- Understanding how access control can be extended for privacy
Privacy-aware Access Control

Outline

- Privacy-aware Access Control
- Hippocratic Databases (Agrawal, 2002)
- Purpose-based Access Control (Byun and Li, 2008)
- Enterprise Privacy Authorization Language (IBM 2003)
Privacy

Privacy is an important issue today

- **Individuals wants**
  - Information about them protected

- **Enterprises need to**
  - Keep their customers feel safe
  - Comply with legal regulations
  - Protect themselves from any legal dispute
  - Maintain good reputations
Privacy Regulations

Impose stringent requirements on the collection, processing and disclosure of personal data

- Fair and lawful processing
- Purpose specification
- Consent
- Minimality
- Minimal disclosure
- Information quality
- Data subject’s control
- Sensitivity
- Information security

Purpose Specification

Personal data should be collected for specified, lawful and legitimate purposes and not processed in ways that are incompatible with the purposes for which data have been collected.
Privacy-aware Access Control

Introduction to Privacy-Aware Access Control

Beyond Access Control

- Traditional access controls focus on:
  - which users perform which actions on which data objects

- Privacy is more than confidentiality and integrity of data

- Privacy policies are concerned with which data object is used for which purposes:
  - “We will collect and use customer identifiable information for billing purposes and to anticipate and resolve problems with the service.”

- Notion of purpose must play a major role in access control:
  - Access decisions should be made based on purpose
Privacy Policy

- **Who**: user identities or roles
- **What**: resources or data
- **How**: actions
- **Why**: the reason for which data are processed
- **Conditions**: under which the access is granted/denied
- **Obligations**: mandatory requirements to be fulfilled
Privacy Policy

A sales agent is allowed to collect a customer’s data for processing the customer’s orders if the customer is older than 13 years of age. The data are stored for 3 years.
A sales agent is allowed to collect a customer’s data for processing the customer’s orders if the customer is older than 13 years of age. The data are stored for 3 years.
A sales agent is allowed to collect a customer’s data for processing the customer’s orders if the customer is older than 13 years of age. The data are stored for 3 years.

<table>
<thead>
<tr>
<th>subject</th>
<th>sales agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td></td>
</tr>
<tr>
<td>object</td>
<td></td>
</tr>
<tr>
<td>purpose</td>
<td></td>
</tr>
<tr>
<td>condition</td>
<td></td>
</tr>
<tr>
<td>obligation</td>
<td></td>
</tr>
</tbody>
</table>
A sales agent is allowed to collect a customer’s data for processing the customer’s orders if the customer is older than 13 years of age. The data are stored for 3 years.

<table>
<thead>
<tr>
<th>subject</th>
<th>sales agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>collect</td>
</tr>
<tr>
<td>object</td>
<td></td>
</tr>
<tr>
<td>purpose</td>
<td></td>
</tr>
<tr>
<td>condition</td>
<td></td>
</tr>
<tr>
<td>obligation</td>
<td></td>
</tr>
</tbody>
</table>
A sales agent is allowed to collect a customer’s data for processing the customer’s orders if the customer is older than 13 years of age. The data are stored for 3 years.

<table>
<thead>
<tr>
<th>subject</th>
<th>sales agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>collect</td>
</tr>
<tr>
<td>object</td>
<td>customer record</td>
</tr>
<tr>
<td>purpose</td>
<td></td>
</tr>
<tr>
<td>condition</td>
<td></td>
</tr>
<tr>
<td>obligation</td>
<td></td>
</tr>
</tbody>
</table>
A sales agent is allowed to collect a customer’s data for processing the customer’s orders if the customer is older than 13 years of age. The data are stored for 3 years.

<table>
<thead>
<tr>
<th>subject</th>
<th>sales agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>collect</td>
</tr>
<tr>
<td>object</td>
<td>customer record</td>
</tr>
<tr>
<td>purpose</td>
<td>order processing</td>
</tr>
<tr>
<td>condition</td>
<td></td>
</tr>
<tr>
<td>obligation</td>
<td></td>
</tr>
</tbody>
</table>
Privacy Policy

A sales agent is allowed to collect a customer’s data for processing the customer’s orders if the customer is older than 13 years of age. The data are stored for 3 years.

<table>
<thead>
<tr>
<th>subject</th>
<th>sales agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>collect</td>
</tr>
<tr>
<td>object</td>
<td>customer record</td>
</tr>
<tr>
<td>purpose</td>
<td>order processing</td>
</tr>
<tr>
<td>condition</td>
<td>the customer is older than 13 years</td>
</tr>
<tr>
<td>obligation</td>
<td></td>
</tr>
</tbody>
</table>
Privacy Policy

A sales agent is allowed to collect a customer’s data for processing the customer’s orders if the customer is older than 13 years of age. The data are stored for 3 years.

<table>
<thead>
<tr>
<th>subject</th>
<th>sales agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>collect</td>
</tr>
<tr>
<td>object</td>
<td>customer record</td>
</tr>
<tr>
<td>purpose</td>
<td>order processing</td>
</tr>
<tr>
<td>condition</td>
<td>the customer is older than 13 years</td>
</tr>
<tr>
<td>obligation</td>
<td>delete data after 3 years</td>
</tr>
</tbody>
</table>
Access Control

- Subject
- Object
- Action
- Purpose
- Conditions
- Obligations
Usage Control

- Subject
- Object
- Action
- **Purpose**
- Conditions
- Obligations
  - pre-obligations
  - ongoing-obligations
  - post-obligations

Usage Control Policy
- Subject
- Object
- Action
- Conditions
- Obligations

Usage request
- Subject
- Object
- Action
Privacy-Aware Access Control

- Access decisions based on purpose
  - Purpose: the reasons for data collection and access

Challenges

- Purpose Management
- Purpose Determination
- Purpose Control (Verification)
Outline

- Privacy-aware Access Control
- Hippocratic Databases (Agrawal, 2002)
- Purpose-based Access Control (Byun and Li, 2008)
- Enterprise Privacy Authorization Language (IBM 2003)
Hippocratic Databases

- **Goal:** Incorporate privacy protection within DB systems
- Inspired by the Hippocratic Oath
  
  Hippocratic Oath
  
  “And about whatever I may see or hear in treatment, or even without treatment, in the life of human beings – things that should not ever be blurted out outside – I will remain silent, holding such things to be unutterable.”

- Establish a number of guiding principles
- Encompass an architecture that uses privacy metadata
- Use purpose as the central concept
Purpose Specification. For personal information stored in the database, the purposes for which the information has been collected shall be associated with the information.

Consent. The purposes associated with personal information shall have the consent of the data subject.

Limited Collection. Personal information shall be limited to the minimum necessary for accomplishing the specified purposes.

Limited Use. The database shall run only those queries that are consistent with the purposes for which the information has been collected.

Limited Disclosure. The personal information stored in the database shall not be communicated outside the database for purposes other than those for which there is consent from the data subject.
Privacy Principles (2)

▶ **Limited Retention.** Personal information shall be retained only as long as necessary for the fulfillment of the purposes for which it has been collected.

▶ **Accuracy.** Personal information stored in the database shall be accurate and up-to-date.

▶ **Safety.** Personal information shall be protected by security safeguards against theft and other misappropriations.

▶ **Openness.** A data subject shall be able to access all her information stored in the database.

▶ **Compliance.** A data subject shall be able to verify compliance with the above principles. Similarly, the database shall be able to address a challenge concerning compliance.
Privacy Metadata

- Purpose associated to each piece of information
- For each piece of information collected for that purpose:
  - Authorized-users: users who can access this information
  - External-recipients: whom the information can be disclosed to
  - Retention-period: how long the information is stored
- Privacy-policies table
  - privacy practices
- Privacy-authorization table
  - access control supporting privacy policy

<table>
<thead>
<tr>
<th>table</th>
<th>attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>privacy-policies</td>
<td>purpose, table, attribute, {external-recipients}, retention</td>
</tr>
<tr>
<td>privacy-authorizations</td>
<td>purpose, table, attribute, {authorized-users}</td>
</tr>
</tbody>
</table>
# Privacy Policy Table

<table>
<thead>
<tr>
<th>table</th>
<th>attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>customer</td>
<td>customer-id, name, shipping-address, email, credit-card-info</td>
</tr>
<tr>
<td>order</td>
<td>customer-id, transaction-id, book-info, status</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>purpose</th>
<th>table</th>
<th>attributes</th>
<th>external-recipients</th>
<th>retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>purchase</td>
<td>customer</td>
<td>name</td>
<td>{delivery-company, credit-card-company}</td>
<td>1 month</td>
</tr>
<tr>
<td>purchase</td>
<td>customer</td>
<td>shipping-address</td>
<td>{delivery-company}</td>
<td>1 month</td>
</tr>
<tr>
<td>purchase</td>
<td>customer</td>
<td>email</td>
<td>empty</td>
<td>1 month</td>
</tr>
<tr>
<td>purchase</td>
<td>customer</td>
<td>credit-card-info</td>
<td>{delivery-company}</td>
<td>1 month</td>
</tr>
<tr>
<td>purchase</td>
<td>order</td>
<td>book-info</td>
<td>empty</td>
<td>1 month</td>
</tr>
<tr>
<td>registration</td>
<td>customer</td>
<td>name</td>
<td>empty</td>
<td>3 years</td>
</tr>
<tr>
<td>registration</td>
<td>customer</td>
<td>shipping-address</td>
<td>empty</td>
<td>3 years</td>
</tr>
<tr>
<td>registration</td>
<td>customer</td>
<td>email</td>
<td>empty</td>
<td>3 years</td>
</tr>
<tr>
<td>recommendations</td>
<td>order</td>
<td>book-info</td>
<td>empty</td>
<td>10 years</td>
</tr>
<tr>
<td>purchase-circles</td>
<td>customer</td>
<td>shipping-address</td>
<td>empty, {aggregated-all}</td>
<td>1 years</td>
</tr>
<tr>
<td>purchase-circles</td>
<td>order</td>
<td>book-info</td>
<td>{aggregated-all}</td>
<td>1 years</td>
</tr>
</tbody>
</table>
# Privacy Authorization Table

<table>
<thead>
<tr>
<th>purpose</th>
<th>table</th>
<th>attributes</th>
<th>authorized-users</th>
</tr>
</thead>
<tbody>
<tr>
<td>purchase</td>
<td>customer</td>
<td>customer-id</td>
<td>all</td>
</tr>
<tr>
<td>purchase</td>
<td>customer</td>
<td>name</td>
<td>{shipping, charge, customer-service}</td>
</tr>
<tr>
<td>purchase</td>
<td>customer</td>
<td>shipping-address</td>
<td>{shipping}</td>
</tr>
<tr>
<td>purchase</td>
<td>customer</td>
<td>email</td>
<td>{shipping, customer-service}</td>
</tr>
<tr>
<td>purchase</td>
<td>customer</td>
<td>credit-card-info</td>
<td>{charge}</td>
</tr>
<tr>
<td>purchase</td>
<td>order</td>
<td>customer-id</td>
<td>all</td>
</tr>
<tr>
<td>purchase</td>
<td>order</td>
<td>transaction-id</td>
<td>all</td>
</tr>
<tr>
<td>purchase</td>
<td>order</td>
<td>book-info</td>
<td>{shipping}</td>
</tr>
<tr>
<td>purchase</td>
<td>order</td>
<td>status</td>
<td>{shipping, customer-service}</td>
</tr>
<tr>
<td>registration</td>
<td>customer</td>
<td>customer-id</td>
<td>all</td>
</tr>
<tr>
<td>registration</td>
<td>customer</td>
<td>name</td>
<td>{registration, customer-service}</td>
</tr>
<tr>
<td>registration</td>
<td>customer</td>
<td>shipping-address</td>
<td>{registration}</td>
</tr>
<tr>
<td>registration</td>
<td>customer</td>
<td>email</td>
<td>{registration, customer-service}</td>
</tr>
<tr>
<td>recommendations</td>
<td>order</td>
<td>customer-id</td>
<td>{mining}</td>
</tr>
<tr>
<td>recommendations</td>
<td>order</td>
<td>transaction-id</td>
<td>{mining}</td>
</tr>
<tr>
<td>recommendations</td>
<td>order</td>
<td>book-info</td>
<td>{mining}</td>
</tr>
<tr>
<td>purchase-circles</td>
<td>customer</td>
<td>customer-id</td>
<td>{olap}</td>
</tr>
<tr>
<td>purchase-circles</td>
<td>customer</td>
<td>shipping-address</td>
<td>{olap}</td>
</tr>
<tr>
<td>purchase-circles</td>
<td>order</td>
<td>customer-id</td>
<td>{olap}</td>
</tr>
<tr>
<td>purchase-circles</td>
<td>order</td>
<td>book-info</td>
<td>{olap}</td>
</tr>
</tbody>
</table>
Data Collection

- Matching privacy policy with user preferences
  - check whether the privacy policy is acceptable to the user
  - if not, database rejects the transaction

- Data insertion
  - Data inserted with the purpose for which it may be used
Data Processing

- Queries submitted to the database along with their purpose
  - e.g. SELECT name FROM customer FOR Marketing

- Before query execution:
  - check privacy-authorizations table for a match on purpose, attribute and user

- During query execution:
  - ensure that only records whose purpose attribute includes the query’s purpose will be visible to the query
Purpose Management

- Difficult policy refinement (Minimality)
  - Decompose purposes into sub-purposes and store them in DB
  - No logical relation between purposes

- Information relevant and complete wrt purpose? (Information Quality)
  - Purpose P decomposed in P1 and P2 (both needed to fulfill P)
  - Customer allows P1, but not P2
  - Cannot specify alternatives

- No support to verify whether a user was allowed to specify a certain purpose in the access request.
Outline

- Privacy-aware Access Control
- Hippocratic Databases (Agrawal, 2002)
- Purpose-based Access Control (Byun and Li, 2008)
- Enterprise Privacy Authorization Language (IBM 2003)
Purpose-based Access Control

- Definition of Purpose
- Purpose Compliance
- Access Purpose Determination
Definition of Purpose

- Describe the reason(s) for data collection and processing
- Organized in a tree structure
Definition of Purpose

- **Intended Purpose (IP)**
  - Regulate access to data
  - Associated with data

- **Access Purpose (AP)**
  - Purpose for accessing a particular data item
  - Associated with access requests
Intended Purpose

- Associated with data and regulate data processing

\[ IP = \langle AIP, PIP \rangle \]

- AIP – Allowed Intended Purposes
  - Data access for purposes in AIP is allowed
  - Translation of user preferences

- PIP – Prohibited Intended Purposes
  - Data access for purposes in PIP is never allowed
  - Restriction by organizational requirements or privacy laws
Ancestors and descendants

Given a set of purposes $P$

- $P^\uparrow = \text{Ancestors}(P)$
  - set of all purposes that are ancestors of the purposes in $P$
  - include purposes in $P$

- $P^\downarrow = \text{Descendants}(P)$
  - set of all purposes that are descendants of the purposes in $P$
  - include purposes in $P$

- $P^\leftrightarrow = P^\uparrow \cup P^\downarrow$
Intended Purpose – Entailment

- $IP = \langle \{Admin, Marketing\}, \{Third-Party\} \rangle$
- $AIP \downarrow = \text{Descendants}(Admin) \cup \text{Descendants}(Marketing)$

Diagram:
- General-Purpose
  - Admin
    - Profiling
    - Analysis
  - Purchase
  - Shipping
  - Marketing
    - Direct
      - D-Email
      - D-Phone
    - Third-Party
      - T-Email
      - T-Postal
    - Special-Offers
    - Service-Updates
Intended Purpose – Entailment

- \( IP = \langle \{\text{Admin, Marketing}\}, \{\text{Third-Party}\} \rangle \)
- \( PIP^\dagger = \text{Descendants}(\text{Third-Party}) \cup \text{Ancestors}(\text{Third-Party}) \)
Intended Purpose – Entailment

- $IP = \langle \{Admin, Marketing\}, \{Third-Party\} \rangle$
- $IP^* = AIP_{\downarrow} - PIP_{\uparrow}$
Access Purpose Compliance

- Intended purposes tell how data should be used
- Access purpose tells why data are requested

Purpose Compliance

- $AP \xleftarrow{PT} IP$ iff $AP \in IP^*$
  - $AP \notin PIP\uparrow$ and $AP \in AIP\downarrow$
- Data access is allowed only if $AP \xleftarrow{PT} IP$
Exercise

\[ IP = \langle \{ \text{General-Purpose} \}, \{ \text{Third-Party} \} \rangle \]

1. \( AP = \text{Marketing} \)
2. \( AP = \text{Admin} \)

Question: \( AP \leftarrow_{\mathcal{PT}} IP? \)
Solution

\[ IP = \langle \{ \text{General-Purpose} \}, \{ \text{Third-Party} \} \rangle \]

1. \( AP = \text{Marketing} \)
2. \( AP = \text{Admin} \)

1. \( AP \not\preceq_{PT} IP \) (\( \text{Marketing} \in \text{PIP}^\dagger \))
Solution

\[
IP = \langle \{\text{General-Purpose}\}, \{\text{Third-Party}\} \rangle
\]

1. \( AP = \text{Marketing} \)
2. \( AP = \text{Admin} \)

1. \( AP \not\in_{\mathcal{P}_T} IP \) (\( \text{Marketing} \in \text{PIP}^\downarrow \))
2. \( AP \in_{\mathcal{P}_T} IP \) (\( \text{Admin} \in \text{AIP}^\downarrow \) and \( \text{Admin} \notin \text{PIP}^\uparrow \))
Access Purpose – Definition

- **Access Purpose**
  - Purpose for accessing a particular data item
  - Associated with each data request (i.e., query)
  - e.g. SELECT name FROM customer **FOR Marketing**

- **How do we determine access purposes?**
  - That is, how does the access control system determine with what purpose a particular user is trying to access a particular data item?
Privacy-aware Access Control

Purpose-based Access Control

Access Purpose Determination

- Users explicitly state their access purposes in access request
  - Need to trust the users

- Register every application or procedure with an access purpose
  - Not applicable if they are complex

- Dynamically determined from the current context of the system
  - Difficult to capture all possibilities
Access Purpose Verification

- Users explicitly state the access purpose when querying
  - e.g., SELECT name FROM customer FOR Marketing

- Then, the system verifies if the stated access purpose is valid
  - i.e., the system checks if the user is indeed allowed to access data with the stated purpose for a given circumstances

- Verification done through roles (RBAC model)
Role Attributes

- Roles organized in hierarchies

- Role attributes
  - Every role $r$ is associated with a set of attributes
    - Defined directly for $r$
    - Inherited from the ancestor roles of $r$
  - When a user is assigned to a role $r$, the values for the role attributes of $r$ are specified for the user
  - Values of role attributes available to access control system
Role Attributes – Example

- Employee
  - Admin-Dept
  - Purchase-Dept
  - Shipping-Dept
  - Marketing-Dept
    - ManagerID
      - ExpLevel
    - TeamLeaderID
      - ServiceType
      - RegionID
        - Specialty
    - EmployeeID
      - Name
      - YearsInCompany
    - E-Marketing
      - E-Analysts
      - Writers
    - Tele-Marketing
      - T-Analysts
      - Operators
System Attributes

- Characterize the environment of the system
- Defined by system administrators for the application needs
- Available to access control system at all times
Conditional Roles

- A conditional role $cr$ is defined as a pair $\langle r, C \rangle$
  - $r \in \mathcal{R}$
  - $C$ is a finite propositional logic formula which may use the logical operators $\land$ and $\lor$, and each predicate is of the form $x \phi y$, where $x \in r.Attributes$ or $x \in S.Attributes$ and $y = \text{a constant}$, and $\phi \in \{<, \leq, >, \geq, =, \neq\}$.
  - e.g., $\langle E$-Marketing, $(time \geq 9am) \land (time \leq 5pm) \rangle$

- An activated role $r$ belongs to a conditional role $cr_i = \langle r_i, C_i \rangle$ in a system state $s$ iff
  1. $r \in \text{Descendants}(r_i)$
  2. Evaluation of $C_i$ under $r(u).Attributes$ and $S(s).Attributes$ is true
Access Purpose Verification

- Access purpose authorization is a pair $\langle ap, cr \rangle$
  - $ap \in \mathcal{P}$
  - $cr$ is a conditional role

**Definition**

Let $ap$ be an access purpose and $r$ a role activated by a user $u$. $ap$ is valid for $u$ under $r$ if there exists an access purpose authorization $\langle ap_i, cr_j \rangle$ where $ap_i \in \mathcal{P}$ and $cr_j = \langle r_j, C_j \rangle$ is a conditional role defined over $\mathcal{R}$ and $\mathcal{S}$, satisfying the following conditions:

1. $ap \in \text{Descendants}(ap_i)$
2. $u$ belongs to the conditional role $cr_j$ either explicitly or implicitly
Purpose-based Access Control

Access Decision

User
access request for object \( o \):
\((u, o, ap)\)

Service provider
privacy policy:
\((o, \langle AIP, PIP \rangle)\)

Access purpose verification
\((ap, r)\)

access purpose authorization:
\(\langle ap', \langle r', C \rangle \rangle\)

\( r \in \langle r', C \rangle \)
\( r \in \text{Descendants}(r') \)
\( C \) is true
\( ap \in \text{Descendants}(ap') \)

Purpose compliance
\( ap \leftarrow_{PT} \langle AIP, PIP \rangle \)
\( ap \notin \text{PIP} \)
\( ap \in \text{AIP} \)

Privacy-aware Access Control
1. Define an access purpose authorization such that only users who activate role *E-Marketing* with *YearsInCompany* equal or greater than 5 and *ExpLevel* greater than 7 can access the data with purpose *Service-Update* between 9am and 5pm.

2. Determine if a user with role *Marketing-Dept*, *ExpLevel* equal to 8 and *YearsInCompany* equal to 10 can access the data for purpose *Service-Update* at 2pm. Justify the answer.
Solution

1. Define an access purpose authorization such that only users who activate role  *E-Marketing* with  *YearsInCompany* equal or greater than 5 and  *ExpLevel* greater than 7 can access the data with purpose  *Service-Update* between 9am and 5pm.

2. Determine if a user with role  *Marketing-Dept*,  *ExpLevel* equal to 8 and  *YearsInCompany* equal to 10 can access the data for purpose  *Service-Update* at 2pm.

Access purpose authorization

\[\langle Service-Update, \langle E-Marketing, (YearsInCompany \geq 5) \land (CurrentTime \geq 9am) \land (CurrentTime \leq 5pm) \land (ExpLevel > 7) \rangle \rangle\]
Solution

1. Define an access purpose authorization such that only users who activate role E-Marketing with YearsInCompany equal or greater than 5 and ExpLevel greater than 7 can access the data with purpose Service-Update between 9am and 5pm.

2. Determine if a user with role Marketing-Dept, ExpLevel equal to 8 and YearsInCompany equal to 10 can access the data for purpose Service-Update at 2pm.

1. Access purpose authorization
   
   ▶ \( \langle \text{Service-Update}, \langle \text{E-Marketing}, (\text{YearsInCompany} \geq 10) \wedge (\text{CurrentTime} > 9) \wedge (\text{CurrentTime} < 17) \wedge (\text{ExpLevel} > 7) \rangle \rangle \)

2. No. Marketing-Dept \( \notin \) Descendants(E-Marketing)
Summary

- Access control vs. Privacy
  - Protect information from unauthorized access
  - No control on how and why information is used
- Privacy-aware access control
  - Extend access control with the notion of purpose
- Hippocratic Databases
  - Metadata for the specification of privacy policy and privacy authorization tables
  - No purpose management
  - No purpose determination
- Purpose-based access control
  - Purpose management
  - Access purpose determination
  - No purpose control
References

Define the purpose hierarchy, role hierarchy, and access purpose authorizations in Purpose-based Access Control for the following scenario.

- A loan origination process consists of checking the financial information of the customer, making an offer and approving the loan.
- The loan origination process can only be performed during office hours.
- Bank employees (both managers and clerks) can verify financial information of customers.
- Any clerk can offer a loan of 1000$ or lower.
- Loans greater than 1000$ can be offered only by senior clerks.
- A senior clerk is a clerk with at least five years experience.
- Managers can approve a loan.