A Methodology for Hiding Knowledge in Databases

Tom Johnsten
Vijay Raghavan

Knowledge Hiding in Databases

- Non-trivial hiding of potentially sensitive knowledge in databases.
  - Maximize release data
  - Maintain data integrity
KHD Process

- Identify sensitive knowledge
- Identify data mining algorithms
- Formulate security policies
- Risk assessment
- Sanitize data
- Report generation
KHD vs. KDD

- Analyze a collection of data for its information content.
- Iterative processes
  - Information requirement, discovery phase, reporting phase.

KHD: Classification Mining
Identify Sensitive Knowledge

- “Junior engineers may not access mileage class of newly designed cars”.

<table>
<thead>
<tr>
<th>ID</th>
<th>Fuel</th>
<th>Cyl</th>
<th>Power</th>
<th>Trans</th>
<th>Mileage</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Efi</td>
<td>4</td>
<td>High</td>
<td>Manu</td>
<td>Med</td>
</tr>
<tr>
<td>T2</td>
<td>Efi</td>
<td>6</td>
<td>High</td>
<td>Manu</td>
<td>Med</td>
</tr>
<tr>
<td>T3</td>
<td>2-bbl</td>
<td>6</td>
<td>High</td>
<td>Auto</td>
<td>Low</td>
</tr>
<tr>
<td>T4</td>
<td>Efi</td>
<td>6</td>
<td>Med</td>
<td>Manu</td>
<td>Med</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>T15</td>
<td>2-bbl</td>
<td>4</td>
<td>High</td>
<td>Auto</td>
<td>NULL (High)</td>
</tr>
<tr>
<td>T16</td>
<td>Efi</td>
<td>6</td>
<td>Med</td>
<td>Auto</td>
<td>NULL (Low)</td>
</tr>
<tr>
<td>T17</td>
<td>2-bbl</td>
<td>4</td>
<td>Low</td>
<td>Auto</td>
<td>NULL (Med)</td>
</tr>
</tbody>
</table>
Class-Accuracy Set

- \{ (c_1, a_1), (c_2, a_2), \ldots, (c_n, a_n) \}

where
- \( c_i \) is the \( i \)th attribute in the domain of attribute containing the protected data element.
- \( a_i \) is the predicted accuracy (level of confidence) according to the classification algorithm of assigning to the protected object class label \( c_i \).

Class-Accuracy Set

- Class-accuracy set for tuple T15:
  - \{ (Mileage = low, a_{low}), (Mileage = med, a_{med}), (Mileage = high, a_{high}) \}
Security Policies

- Maximum threshold
  - All $a_i$ are less than some threshold value $\varepsilon$.
- Maximum range
  - $[\text{MAX}(a_1, ..., a_n) - \text{MIN}(a_1, ..., a_n)] < \varepsilon$

Security Policies

- Protected threshold
  - $a_i < \varepsilon$, ($a_i$ is predicted accuracy value associated with protected data element).
- Protected rank
  - Ranked position of protected data element is not within the non-secure range $[L, U]$. 
Risk Assessment

- Individual algorithm assessment
- Generic assessment

---

Risk Assessment

- Decision-Region Based Algorithms
  - Condition-1:
    - It is possible to identify a priori a finite set of descriptions, \( D \), in terms of the properties present in an object \( O \) such that the particular description \( d \) used by \( A \) to classify \( O \) is an element of \( D \).
Risk Assessment

- Decision-Region Based
  - Condition-2:
    - The predicted accuracy of assigning an object $O$ satisfying a description $d \in D$ to a class $C$ is dependent on the distribution of class label $C$ relative to all other class labels among the objects that satisfy $d$ in the training set.

Risk Assessment

- Given a description $d \in D$ the predicted accuracy of assigning the protected tuple $T$ the label $c$ is the ratio of the number of tuples assigned label $c$ and satisfy $d$ to the number of tuples that satisfy $d$. 
Risk Assessment

- Apply security policy to a particular description \( d \).
- Apply security policy to each description \( d \in D \).

REPEAT
\[
K = 1 \\
\text{WHILE (exist descriptions to inspect)} \\
D = K \text{ level descriptions requiring inspection} \\
\text{FOR (each description } d \text{ in } D) \\
\quad \text{IF (} d \text{ == zero description)} \\
\quad \quad \text{append all specializations of } d \text{ to zero description list} \\
\quad \text{ELSE IF (} d \text{ == non-secure description)} \\
\quad \quad \text{append } d \text{ to non-secure description list} \\
\text{END\_FOR} \\
\text{transform non-secure descriptions to secure descriptions by protecting subset of attribute values not belonging to target object} \\
K = K+1 \\
\text{END\_WHILE} \\
\text{UNTIL (no non-secure descriptions)}
\]
<table>
<thead>
<tr>
<th>ID</th>
<th>Fuel</th>
<th>Cyl</th>
<th>Power</th>
<th>Trans</th>
<th>Mileage</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Efi</td>
<td>4</td>
<td>High</td>
<td>Manu</td>
<td>Med</td>
</tr>
<tr>
<td>T2</td>
<td>Efi</td>
<td>6</td>
<td>High</td>
<td>Manu</td>
<td>Med</td>
</tr>
<tr>
<td>T3</td>
<td>2-bbl</td>
<td>6</td>
<td>High</td>
<td>Auto</td>
<td>Low</td>
</tr>
<tr>
<td>T4</td>
<td>Efi</td>
<td>6</td>
<td>Med</td>
<td>Manu</td>
<td>Med</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>T15</td>
<td>2-bbl</td>
<td>4</td>
<td>High</td>
<td>Auto</td>
<td>NULL (High)</td>
</tr>
<tr>
<td>T16</td>
<td>Efi</td>
<td>6</td>
<td>Med</td>
<td>Auto</td>
<td>NULL (Low)</td>
</tr>
<tr>
<td>T17</td>
<td>2-bbl</td>
<td>4</td>
<td>Low</td>
<td>Auto</td>
<td>NULL (Med)</td>
</tr>
</tbody>
</table>

January 3, 2003

<table>
<thead>
<tr>
<th>Tuple</th>
<th>Description</th>
<th>Class-Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>T15</td>
<td>(Fuel = 2-bbl)</td>
<td>{(low, 0), (med, .5), (high, .5)}</td>
</tr>
<tr>
<td>T15</td>
<td>(Cyl = 4)</td>
<td>{(low, 0), (med, .375), (high, .625)}</td>
</tr>
<tr>
<td>T15</td>
<td>(Power = high)</td>
<td>{(low, .25), (med, .375), (high, .375)}</td>
</tr>
<tr>
<td>T15</td>
<td>(Cyl=4 &amp; Power = high)</td>
<td>{(low, 0), (med, .5), (high, .5)}</td>
</tr>
<tr>
<td>T15</td>
<td>(Cyl = 4) &amp; Tran = auto</td>
<td>{(low, 0), (med, .5), (high, .5)}</td>
</tr>
</tbody>
</table>

January 3, 2003
<table>
<thead>
<tr>
<th>ID</th>
<th>Fuel</th>
<th>Cyl</th>
<th>Power</th>
<th>Trans</th>
<th>Mileage</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Efi</td>
<td>NULL</td>
<td>High</td>
<td>Manu</td>
<td>Med</td>
</tr>
<tr>
<td>T2</td>
<td>Efi</td>
<td>6</td>
<td>High</td>
<td>Manu</td>
<td>Med</td>
</tr>
<tr>
<td>T3</td>
<td>2-bbl</td>
<td>NULL</td>
<td>High</td>
<td>NULL</td>
<td>Low</td>
</tr>
<tr>
<td>T4</td>
<td>Efi</td>
<td>6</td>
<td>Med</td>
<td>Manu</td>
<td>Med</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>T15</td>
<td>2-bbl</td>
<td>4</td>
<td>High</td>
<td>Auto</td>
<td>NULL (High)</td>
</tr>
<tr>
<td>T16</td>
<td>Efi</td>
<td>6</td>
<td>Med</td>
<td>Auto</td>
<td>NULL (Low)</td>
</tr>
<tr>
<td>T17</td>
<td>2-bbl</td>
<td>4</td>
<td>Low</td>
<td>Auto</td>
<td>NULL (Med)</td>
</tr>
</tbody>
</table>
Identify Sensitive Knowledge

- Analysis will only be as complete as the identified knowledge.
- “Fault-tree” to structure process.

Identify Sensitive Knowledge

- “Employees may not have knowledge of customers suffering from sensitive health conditions”.

January 3, 2003
Discovery of customers suffering from sensitive health conditions

- Discovery of customers suffering from depression
  - CUST_ID item with depression items

- Discovery of customers suffering from AIDS
  - CUST_ID item with AIDS items

Formulate Security Policies

- Transform constructed fault-tree into appropriate security policies.
- Predefined set of templates.
TYPE-1: Specific Item -> Specific Item
TYPE-2: Specific Item -> Any Item
TYPE-3: Any Item -> Specific Item
TYPE-4: Specific Item -> Any Subset of Items
TYPE-5: Any Subset of Items -> Specific Item
TYPE-6: Specific Item -> Specific Concept
TYPE-7: Specific Concept -> Specific Item
TYPE-8: Any Item -> Specific Concept
TYPE-9: Specific Concept -> Any Item
TYPE-10: Any Subset of Items -> Specific Concept
TYPE-11: Specific Concept -> Any Subset of Items
TYPE-12: Specific Concept -> Specific Concept

All templates include user-defined support and confidence threshold values.

Risk Assessment

- Each template is expanded into one or more association rules.
  - Each association rule is evaluated.
Sanitize Data

- Remove items from database
  - Maintains data integrity
- Modify item values
  - Maximize available data

Remove Items

- Minimum Coverage Item Set (MCIS)
  - Given a set of association rules $A$, a MCIS is a minimum set of items in which at least one of the items in the set is included in each rule $r \in A$. 
Example

- Given the non-secure sensitive association rules:
  - I1 -> I2
  - I1 -> I3 ∧ I4
  - I5 -> I6
  - I2 -> I7 ∧ I6
  - I6 -> I2 ∧ I1
- MCIS = {I1, I6}
  - Concealment of items I1 and I6 guarantees that the rules have no accuracy and strength.

Data Integrity (X → Y)

- Contains no items whose values have been modified.
  - Same level of support and confidence as with respect to unsanitized data.
Data Integrity ($X \rightarrow Y$)

- Items belonging to left-hand side have been modified.
- Support:
  - $[\frac{\#(X \land Y)}{T}, \frac{\#(X \land Y) + P_{\text{MAX}}(X)}{T}]$
- Confidence:
  - $[\frac{\#(X \land Y)}{\frac{\#(X) + P_{\text{MAX}}(X)}}]$

Data Integrity ($X \rightarrow Y$)

- Items belonging to right-hand side have been modified.
- Support:
  - $[\frac{\#(X \land Y)}{T}, \frac{\#(X \land Y) + P_{\text{MAX}}(Y)}{T}]$
- Confidence:
  - $[\frac{\#(X \land Y)}{\frac{\#(X) + P_{\text{MAX}}(Y)}}]$

January 3, 2003
Data Integrity \((X \to Y)\)

- Items belonging to left- and right- sides have been modified
- Support:
  \[
  \left[ \frac{\#(X \land Y)}{T}, \frac{\#(X \land Y) + P_{\text{MAX}}(X,Y)}{T} \right]
  \]
- Confidence:
  \[
  \left[ \frac{\#(X \land Y)}{(\#(X) + P_{\text{MAX}}(X)), \frac{\#(X \land Y) + P_{\text{MAX}}(X,Y))}{(#(X)+P_{\text{MAX}}(X,Y))}} \right]
  \]

January 3, 2003

Future Work

- Formal models to specify sensitive knowledge.
- Risk assessment procedures.
- Sanitization procedures.
- Data Integrity (Intra and Inter).