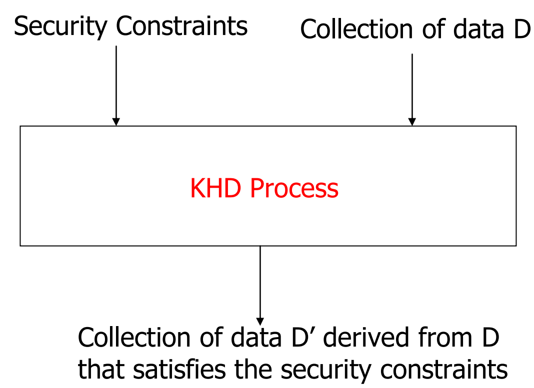
A Methodology for Hiding Knowledge in Databases

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".

ID	Fuel	Cyl	Power	Trans	Mileage
T1	Efi	4	High	Manu	Med
T2	Efi	6	High	Manu	Med
T3	2-bbl	6	High	Auto	Low
T4	Efi	6	Med	Manu	Med
…	…	…	…	…	…
T15	2-bbl	4	High	Auto	NULL (High)
T16	Efi	6	Med	Auto	NULL (Low)
T17	2-bbl	4	Low	Auto	NULL (Med)

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.

January 3, 2003 9

Class-Accuracy Set

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

January 3, 2003 10

Security Policies

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

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
   WHILE (exist descriptions to inspect)
      D = K level descriptions requiring inspection
      FOR (each description d in D)
         IF (d == zero description)
          append all specializations of d to zero description list
         ELSE IF (d == non-secure description)
            append d to non-secure description list
       END_FOR
       transform non-secure descriptions to secure descriptions
       by protecting subset of attribute values not belonging to
       target object
       K = K+1
    END_WHILE
UNTIL (no non-secure descriptions)
```

ID	Fuel	Cyl	Power	Trans	Mileage
T1	Efi	4	High	Manu	Med
T2	Efi	6	High	Manu	Med
T3	2-bbl	6	High	Auto	Low
T4	Efi	6	Med	Manu	Med
…	…	…	…	…	…
T15	2-bbl	4	High	Auto	NULL (High)
T16	Efi	6	Med	Auto	NULL (Low)
T17	2-bbl	4	Low	Auto	NULL (Med)

Tuple	Description	Class-Accuracy
T15	(Fuel = 2-bbl)	{(low, .25), (med, 0), (high, .75)}
T15	(Cyl = 4)	{(low, 0), (med, .375), (high, .625)}
T15	(Power = high)	{(low, .25), (med, .375), (high, .375)}
T15	(Cyl=4 & Power = high)	{(low, 0), (med, .5), (high, .5)}
T15	(Cyl = 4) & Tran = auto)	{(low, 0), (med, .5), (high, .5)}

ID	Fuel	Cyl	Power	Trans	Mileage
T1	Efi	**NULL**	High	Manu	Med
T2	Efi	6	High	Manu	Med
T3	2-bbl	**NULL**	High	**NULL**	Low
T4	Efi	6	Med	Manu	Med
…	…	…	…	…	…
T15	2-bbl	4	High	Auto	NULL (High)
T16	Efi	6	Med	Auto	NULL (Low)
T17	2-bbl	4	Low	Auto	NULL (Med)

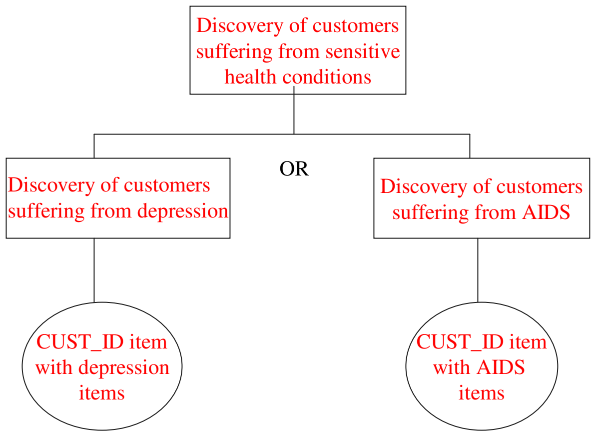
KHD: Association Mining

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 25

Formulate Security Policies

- Transform constructed fault-tree into appropriate security policies.
- Predefined set of templates.

January 3, 2003 26

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

January 3, 2003 29

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 $r \in A$.

January 3, 2003 30

Example

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

Data Integrity (X $\rightarrow$ 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:
  - [#($X \wedge Y$) / T,
    (#($X \wedge Y$) + P_MAX(X)) / T]
- Confidence:
  - [#($X \wedge Y$) / (#(X) + P_MAX(X)),
    (#($X \wedge Y$) + P_MAX(X)) / (#(X) + P_MAX(X))]

Data Integrity ($X \rightarrow Y$)

- Items belonging to right-hand side have been modified.
- Support:
  - [#($X \wedge Y$) / T,
    (#($X \wedge Y$) + P_MAX(Y)) / T]
- Confidence:
  - [#($X \wedge Y$) / #(X),
    (#($X \wedge Y$) + P_MAX(Y)) / #(X)]

Data Integrity ($X \rightarrow Y$)

- Items belonging to left- and right- sides have been modified
- Support:
  - $[\#(X \wedge Y) / T,$
    $(\#(X \wedge Y) + P\_MAX(X,Y)) / T]$
- Confidence:
  - $[\#(X \wedge Y) / (\#(X) + P\_MAX(X)),$
    $(\#(X \wedge Y) + P\_MAX(X,Y)) / (\#(X)+P\_MAX(X,Y))]$

Future Work

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