Exploiting Security Punctuations to Enforce Security and Preserve Privacy in Data Stream Management Systems

Rimma V. Nehme¹, Elke A. Rundensteiner², Elisa Bertino¹
¹CERIAS, Purdue University, ²Worcester Polytechnic Institute
rnehme@cs.purdue.edu, rundenst@cs.wpi.edu, bertino@cs.purdue.edu

Motivating Example: Context-Aware Spam

People can become targets of context-aware spam. Streaming data (e.g., current location) is exposed to anyone.

Security Punctuations: Conceptual View

The Goal: real-time, flexible, low-overhead access control mechanism on streaming data with wide range of protection object granularities

Proposed Solution: Security Punctuations - meta-knowledge with security semantics embedded inside data streams

Security Punctuation Schema

<table>
<thead>
<tr>
<th>Data Description Part (DDP)</th>
<th>Security Restriction Part (SRP)</th>
<th>Sign</th>
<th>Immutable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream(s), Tuple(s), Attribute(s)</td>
<td>RBAC</td>
<td>MAC</td>
<td>MAC</td>
</tr>
</tbody>
</table>

Punctuation attribute | Matches tuple attribute
--- | ---
[x, y] | value in this range
[x, y, z] | value in this list
x | this value only
* | wildcard

Security-Enhanced Query Processing

SS Operator State

SS Compliant Join (SCJoin)

Contributions:

• A mechanism for enforcing access control on streaming data
• Support both user-and-server-specified access control policies
• Context/data-aware security mechanism
• Fine-grained access control on streaming data
• Support access right delegation on data streams
• Proposed SQL extensions to support security punctuations
• Proposed and implemented continuous queries execution mechanism compliant with security punctuations

Healthcare Application Example:

s₇: HeartRate Stream

Patient|Beats_per_min|Timestamp
---|---|---
<=20, 70 | Sep-12-05 8:1700
311–125, Sep-12-05 9:2300
<=289, 59 | Sep-12-05 9:2400
<=180, 91 | Sep-12-05 9:3300
...