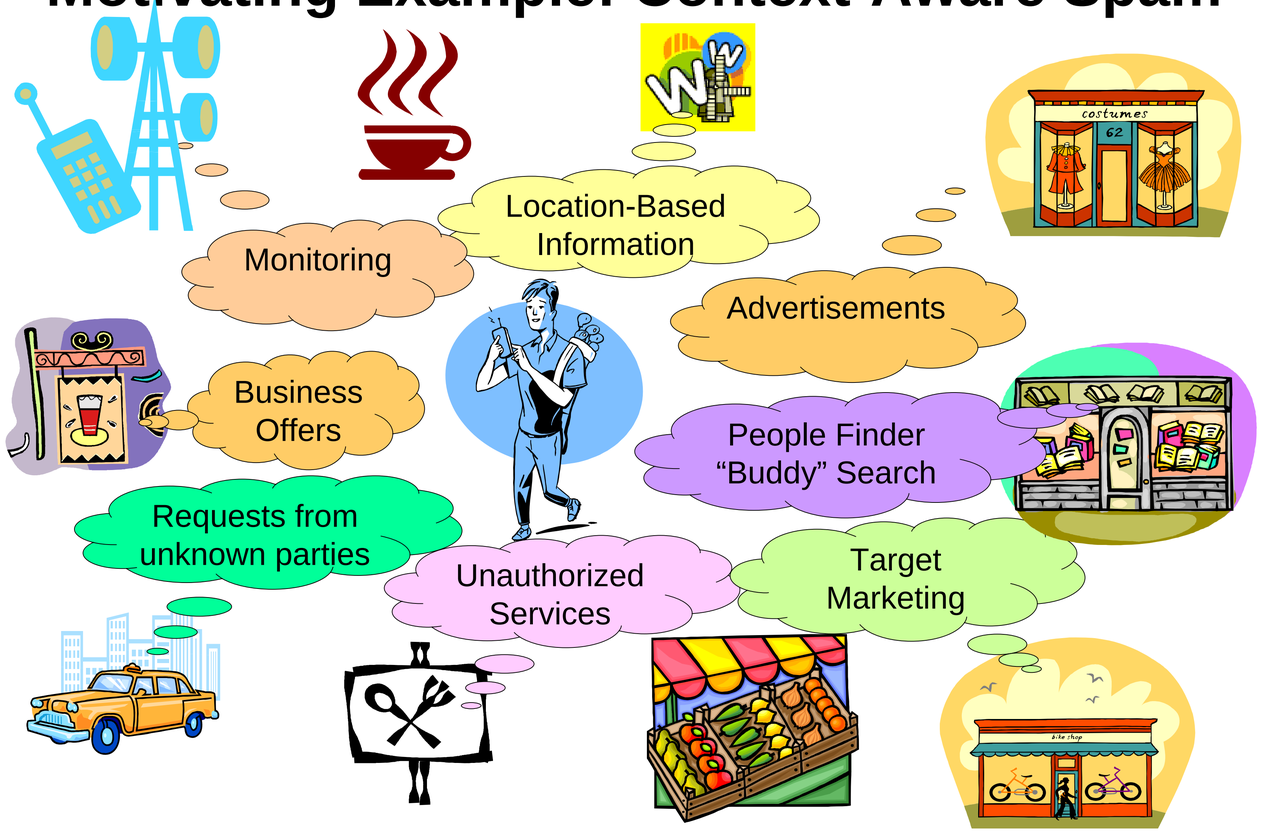
CERIAS

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

Rimma V. Nehme[1], Elke A. Rundensteiner[2], Elisa Bertino[1]
[1]CERIAS, Purdue University, [2]Worcester Polytechnic Institute
rnehme@cs.purdue.edu, rundenst@cs.wpi.edu, bertino@cs.purdue.edu

Motivating Example: Context-Aware Spam

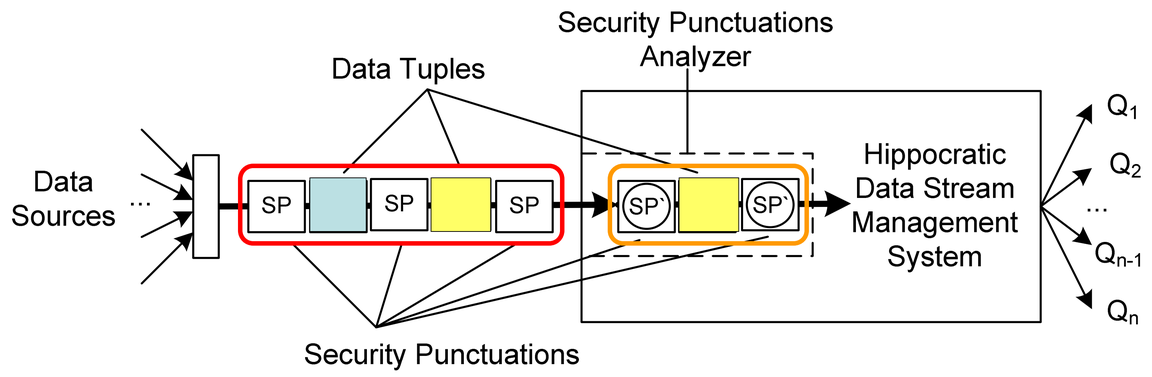


People can become targets of context-aware spam.
Streaming data (e.g., current location) is exposed to anyone.

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



User-side policy specification

Server-side policy modification

- Client and server access control policies expressed in the form of security punctuations applicable to the same tuples are combined using *union* or *intersect* semantics.

Security Punctuation Schema

Data Description Part (DDP)	Security Restriction Part (SRP)	Sign	Immutable
Stream(s), Tuple(s), Attribute(s) …	RBAC, MAC, PBAC, DAC …	+ / -	T / F

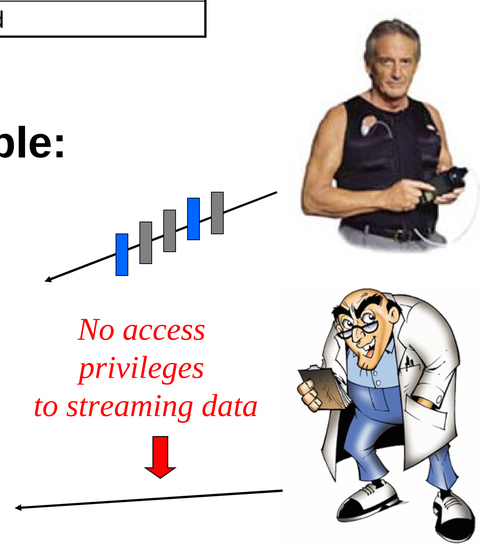
Data Patterns:

Punctuation attribute	Matches tuple attribute
`[x,y], (x,y)`	value in this range
`{x,y,z}`	value in this list
`x`	this value only
`*`	wildcard

Healthcare Application Example:

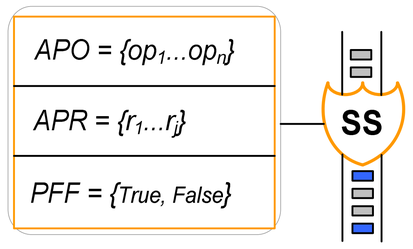
s_1: HeartRate Stream

Patient_id | Beats_per_min | Timestamp
*<s_1, * , * | {Physician, Nurse-On-Duty} | + | F >*
120 , 70 , Sep-12-05 9:17:00
311 , 125 , Sep-12-05 9:23:00
*<s_1, [200,300] , * | Nurse-On-Duty | - | F >*
289 | 59 | Sep-12-05 9:24:00
<, 180 , * | Cardiologist | + | T >*
180 , 91 , Sep-12-05 9:33:00
…



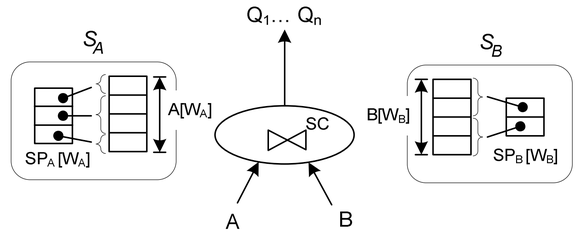
Security-Enhanced Query Processing

SS Operator State

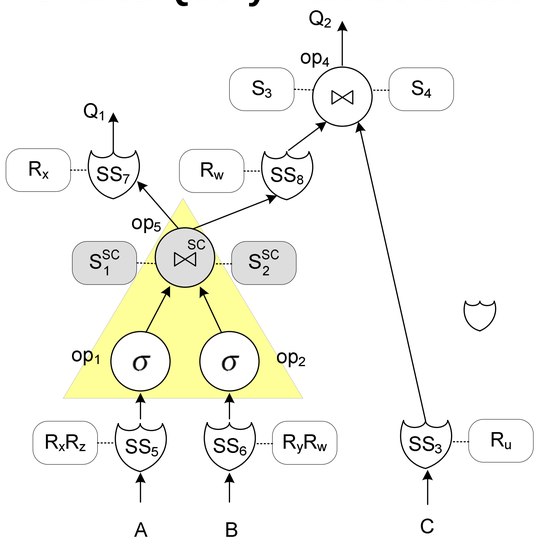


Security Shield (SS) Operator

Security Compliant Join (SCJoin)



Shared Query Plan Generation



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

PURDUE UNIVERSITY
PURDUE HOMELAND SECURITY INSTITUTE
CERIAS
REGENSTRIEF CENTER FOR HEALTHCARE ENGINEERING
Discovery Park e-Enterprise Center