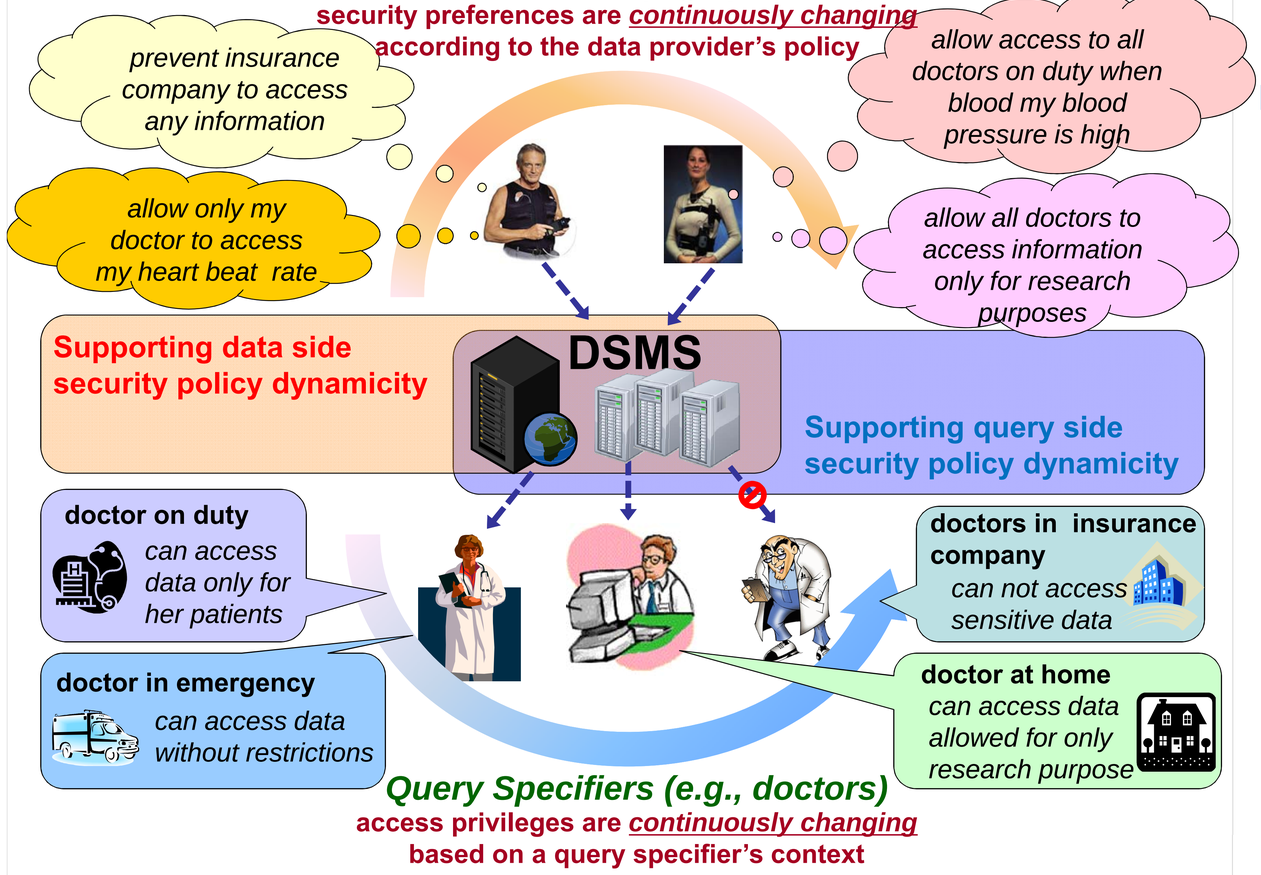
CERIAS

the center for education and research in information assurance and security

Continuous Security Policy Enforcement in Streaming Environments

Rimma V. Nehme, Hyo-Sang Lim, Elisa Bertino
CERIAS, Purdue University
rnehme@cs.purdue.edu, hslim@cs.purdue.edu, bertino@cs.purdue.edu

Motivating Example: Patient Monitoring



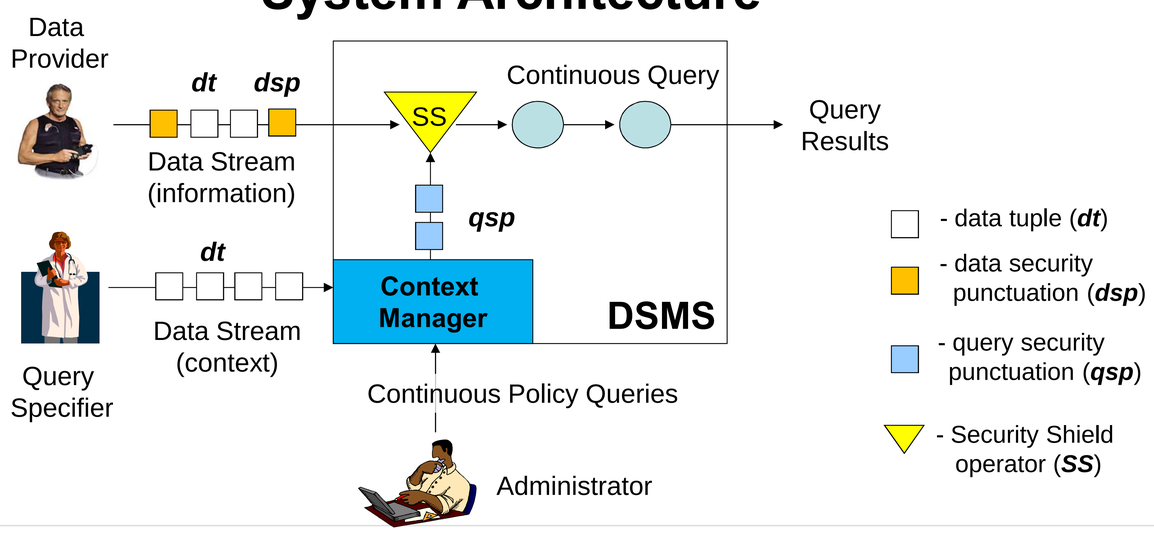
Continuous Security Policy Enforcement: Overview

The Goal: Enforce access control in dynamic streaming environments where
1) data provider's security preferences may *continuously change* and
2) query specifier's access privileges may *continuously change*

Proposed Solution:

- ***Security Punctuations*** : streaming security meta-data tuples describing *both* data and queries' security restrictions
- ***Continuous Policy Queries***: predefined logics for generating proper access privileges of query specifiers based on the context data streams

System Architecture



General Security Punctuation Schema

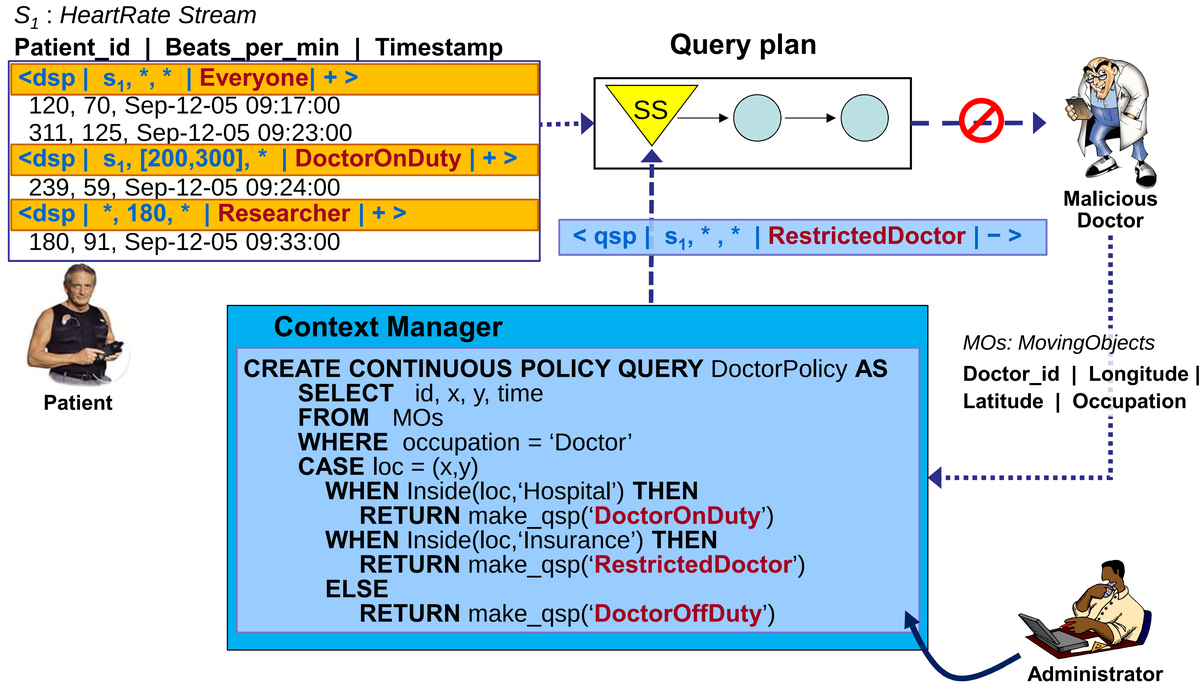
- **Data Security Punctuations (*dsp*)** : interleaved with data tuples in the information data streams from data providers
- **Query Security Punctuations (*qsp*)** : generated by CP-Queries based on the context data streams from query specifiers

Continuous Policy Queries (CP-Queries)

```
CREATE CONTINUOUS POLICY QUERY name AS
  --INPUT STREAM
    SELECT   select_clause
    FROM     from_clause
    WHERE    where_clause
  --OUTPUT STREAM
    CASE     expression
        WHEN value1 THEN
            RETURN query_security_punctuation_i
        WHEN value2 THEN
            RETURN query_security_punctuation_j
        ...
        WHEN valueN THEN resultN
            RETURN query_security_punctuation_k
        [ELSE query_security_punctuation_l]
    END
```

- **Input**: context data streams
- **Output**: meta streams, i.e., streams composed of **query security punctuations (*qsp*)**
- **Processing**: similar to traditional continuous queries
- ***QSPs*** are produced ***incrementally*** by CP-Query

Security-Aware Query Processing: An Example



Contributions:

- A mechanism for enforcing dynamic access control on streaming data
- Support both data-and-query-side dynamicity of access control policies
- Proposed a symmetric model to describe data-and-query side dynamicity

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center