A J2EE Syslog Aggregation and Reporting System

10th ICCRTS - June 14, 2005

Patrick C. Carroll

JTOGO

Jump Start Your Java™ Projects

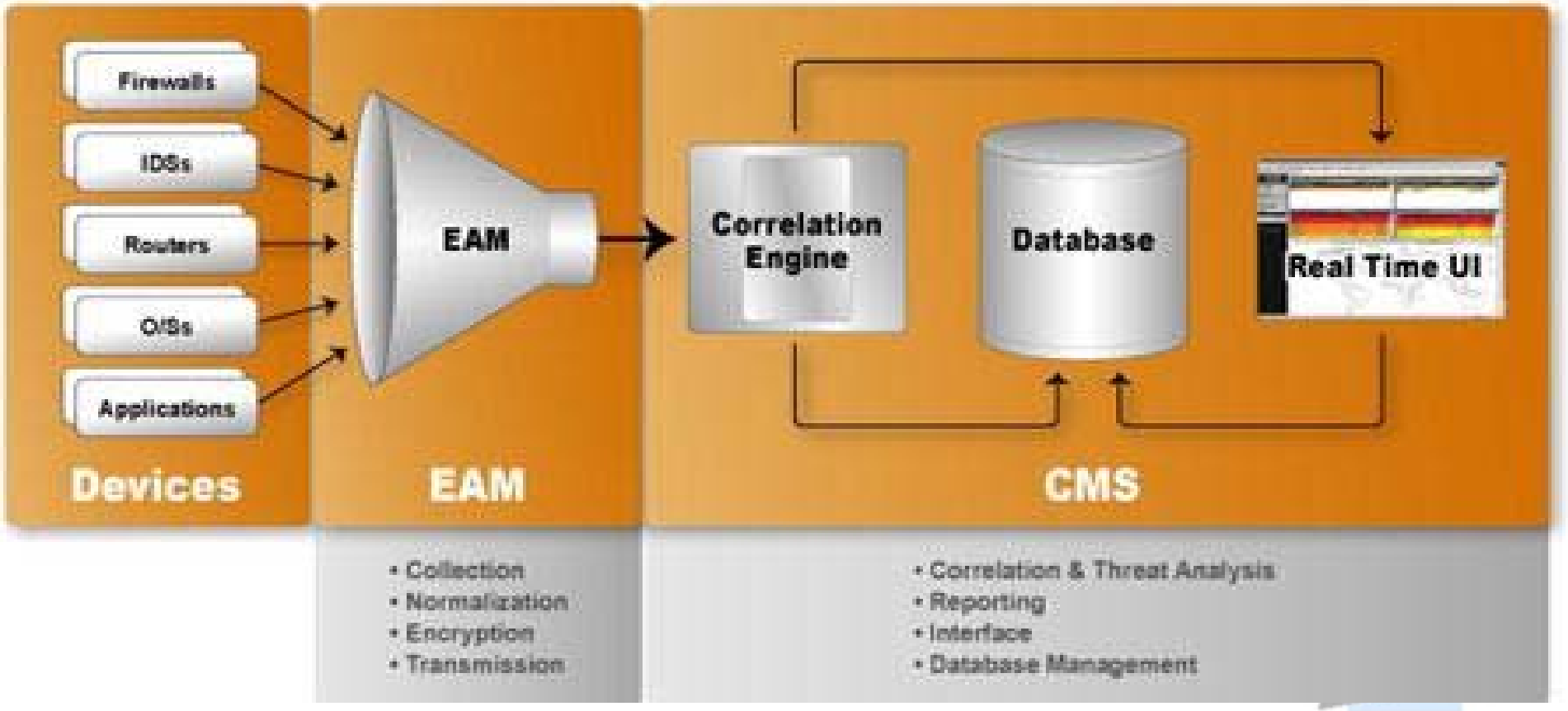
MOTIVATIONS

- Legislation, etc.
- State of the Practice
- Standards-based Open Source Development

LEGISLATION, ETC

- US Law
  - HIPAA/GLBA/Sarbox/California SB 1386
- It's a dangerous world
  - State-sponsored Information Warfare
  - Script Kiddies

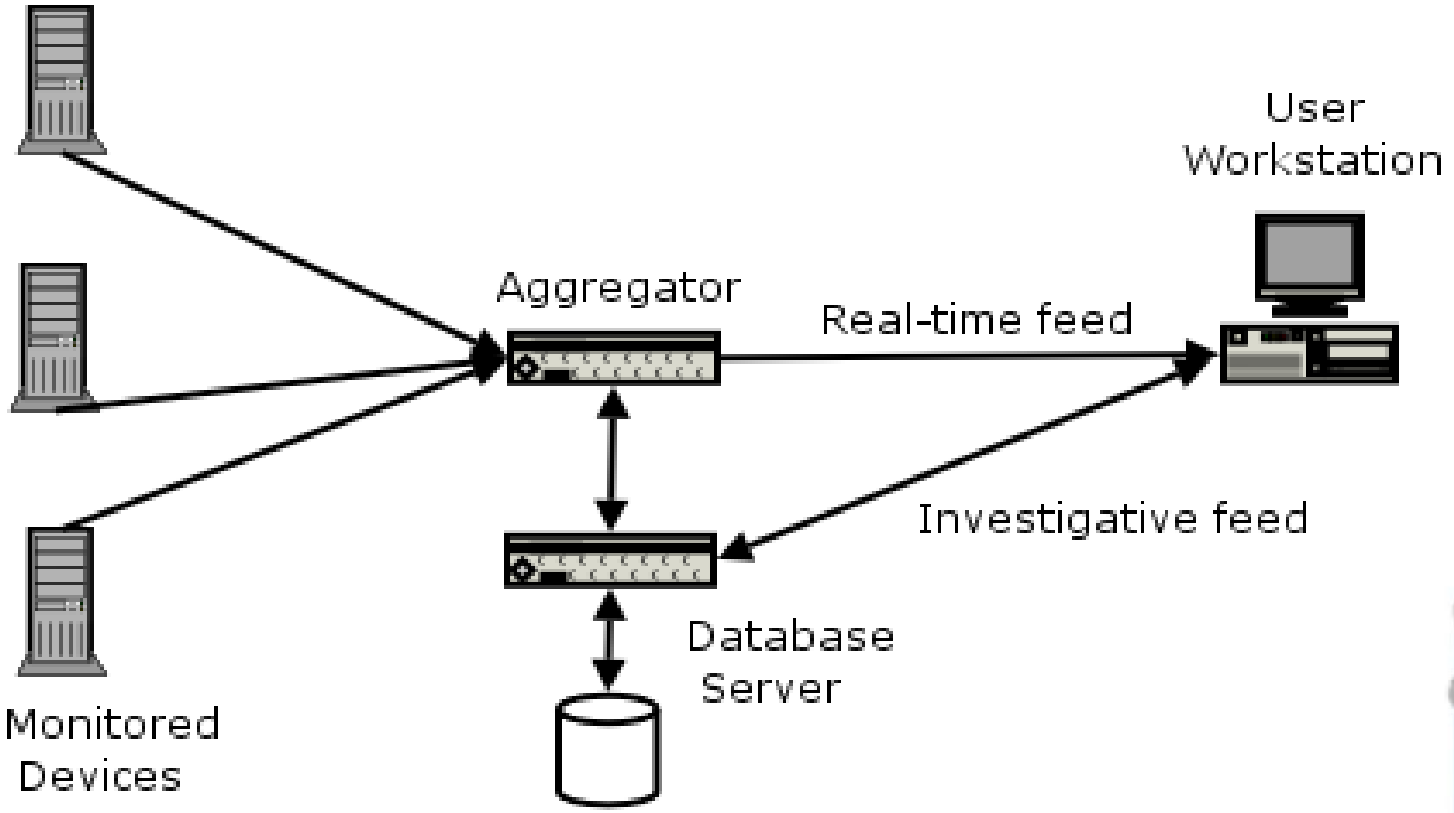
Example Security Information Management System (SIMS)



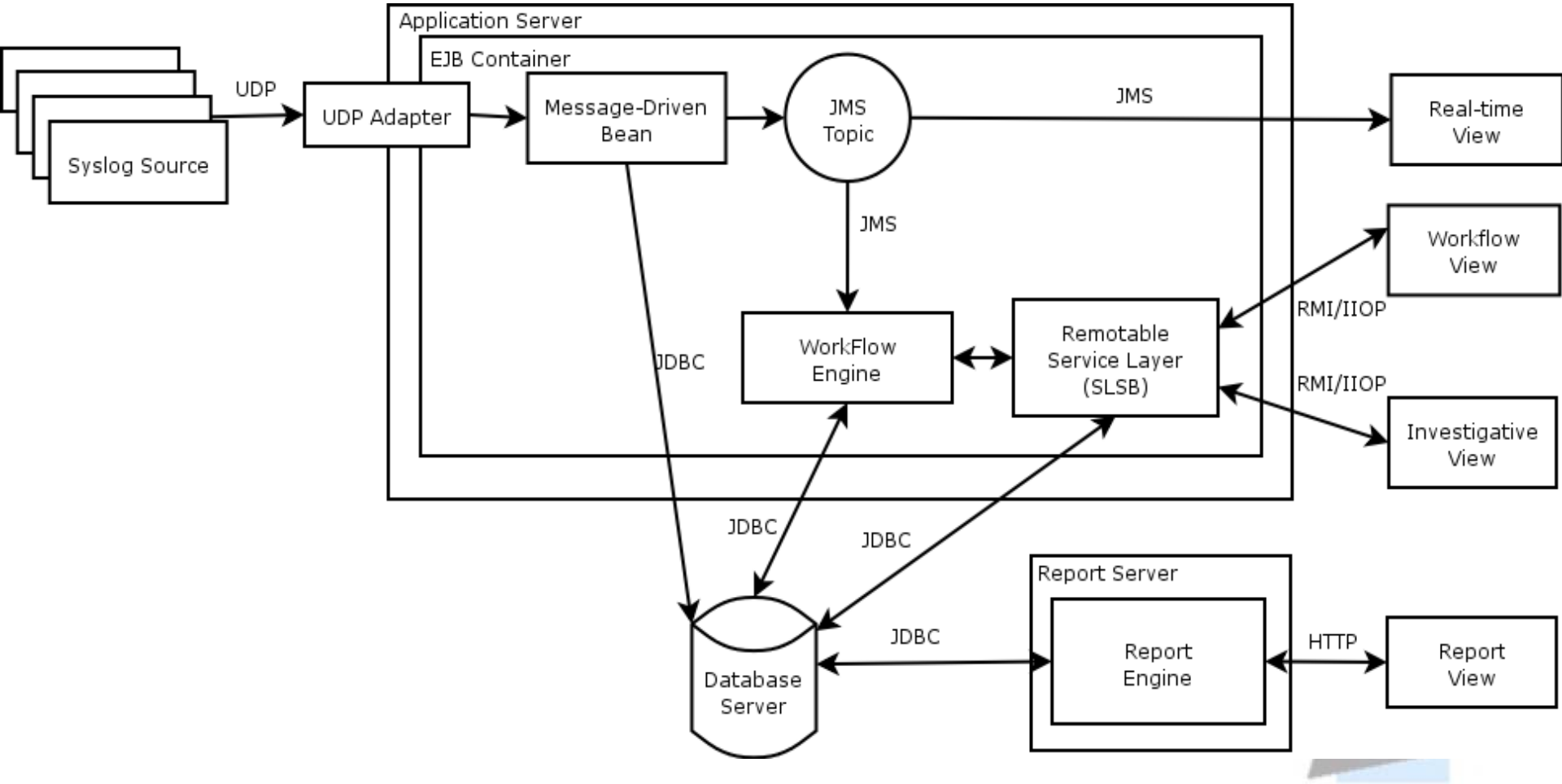
Top Concerns

- Immaturity
- Brittleness
- Scalability
- Total Cost of Ownership

SIMS in the Abstract



J2EE Equivalent SIMS



Technology Stack

- Java
- Open Source Application Server
- Hibernate O/R Mapping
- MySQL
- OpenReports
- Ant

Future Directions

- OpenReports 0.9+
- JESS – Recognize significant events
- jBPM – Ticketing, Escalation

Summary

- Legislation, etc.
- State of the Practice
- Standards-based Open Source Development

Contact

Patrick C. Carroll

JTOGO

Jump Start Your Java™ Projects

pcc@JTOGO.com

(404) 388-8620