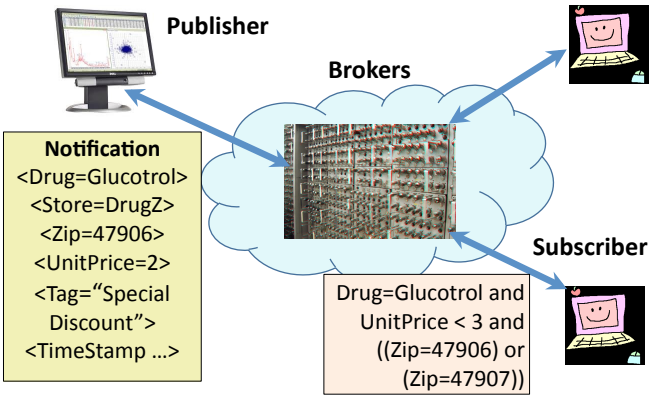
CERIAS

the center for education and research in information assurance and security

v-CAPS: A Confidential and Anonymous Routing Protocol for Content-Based Publish-Subscribe Networks

Amiya Kumar Maji and Saurabh Bagchi
Purdue University, West Lafayette, IN



Problem Statement

- Baseline CBPS *relies* on Brokers
  - What if a broker is compromised?
- Can we build an *efficient* CBPS system where brokers cannot see message content?
- Can we hide subscribers' interests from curious brokers and subscribers?
- Can we guarantee path anonymity?
- If so, then how and at what cost?

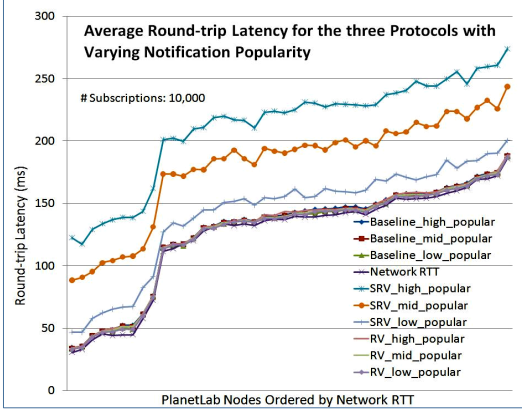
Our Approach

- Computation on encrypted data is costly
- Filter matching in plaintext is much faster
- Relax some decoupling properties of CBPS
- Extract routing *information* before encrypting messages
- Allow brokers to route using this information
- Threat model: trusted publisher, honest-but-curious broker

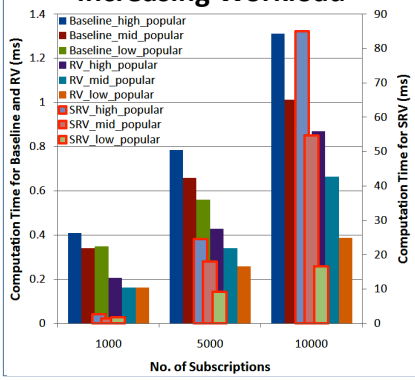
Solution

- Designed two protocols based on Siena CBPS system
- Routing Vector (RV) Protocol
  - Achieves notification and subscription confidentiality
- Secure Routing Vector (SRV) Protocol
  - Encrypt the RV further to guarantee anonymity

Implementation and Results



Computation Time with Increasing Workload



Conclusion and Future Work

- RV has similar latency as Baseline
- Notification popularity have large impact on SRV computation cost
- Future directions
  - Achieving higher scalability
  - Group management in CBPS

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center