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
  o 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
    o Achieves notification and subscription confidentiality
  • Secure Routing Vector (SRV) Protocol
    o 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
  o Achieving higher scalability
  o Group management in CBPS