Secure & Scalable Dissemination of XML Content with Frequent Incremental Updates

Elisa Bertino, Mohamed Nabeel, Ashish Kundu

Use cases
✓ Stock Market Quote Dissemination
✓ Thousands of Instruments
✓ > 10^6 quotes/sec
✓ Stock Market Surveillance
✓ Global Weather Update

Content Encoding
✓ Text Nodes
✓ Element Nodes before encoding
✓ Encoded element nodes
✓ Structural Identifiers based on XPath
For node x, S(x) = h(xpath(x.parent)) || h(xpath(x)) || h(x.text)
E(x) = S(x), I(x), r(x).

Efficient Bandwidth Utilization
✓ Delta Messaging
✓ Changed Nodes
✓ Group Multicasting
✓ Content based Routing

Security Requirements
✓ Confidentiality
✓ Data Encryption
✓ Minimal Indirect Leakage
✓ Access Control
✓ Integrity (Content & Structural)
✓ Availability
✓ Completeness

Our Approach
✓ XML Node level granularity for security enforcement
✓ Content based pub/sub system with a scalable architecture
✓ Efficient utilization of bandwidth through delta message transfer and multicasting

Availability
✓ Passive replication with disk caching for top-level routers
✓ Encoded messages are cached
✓ Routers rely on their parent to build the picture in case of a fail-over

Access Control & Minimal Leakage
✓ Make sure that access to data is strictly controlled
✓ Prevent indirect information leakage
✓ Minimal disclosure of structure of the rest of the document

Related Work

Completeness
✓ With delta messaging how do we make sure that clients get all the updates they are supposed to receive?
✓ Key Idea: Use a probability based approach while remaining oblivious to distributors and minimizing leakage

Content Decoding
✓ Two Level of Integrity
✓ Content Integrity
✓ Structural Integrity (Two levels)
✓ Compliance to Schema (w/o order)
✓ Child order preservation (may not need to check for some apps)
For node x, Check (I(x) with decrypted I(x)
Check xpath(x) with xpath(x.parent) turnaround(x)
If x is a right sibling of y, check r(x) > r(y)

An Example content based pub/sub system

XPath
Structural Identifiers based on distributors and minimizing leakage approach while remaining oblivious to the updates they are supposed we make sure that clients get all