CERIAS

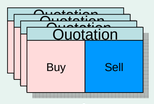
the center for education and research in information assurance and security

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
- ❑ > 10^5 quotes/sec

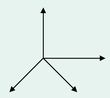
✓ Stock Market Surveillance

✓ Global Weather Update

0

Security Requirements

✓ Confidentiality
- ✓ Data Encryption
- ✓ Minimal Indirect Leakage
- ✓ Access Control



✓ Integrity (Content & Structural)

✓ Availability

✓ Completeness

1

Our Approach

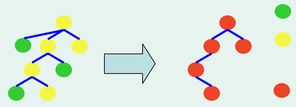
✓ XML Node level granularity for security enforcement

✓ Content based pub/sub system with a scalable architecture

✓ Efficient utilization of bandwidth through delta message transfer and multicasting

2

Content Encoding



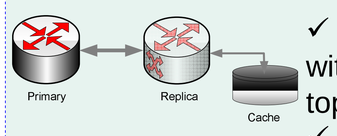
- Text Nodes
- Element Nodes before encoding
- Encoded element nodes

✓ Structural Identifiers based on XPath

For node x,
S(x) = <h(xpath(x.parent)), h(xpath(x)), r (x)>
I(x) = h(x.attr) || h(x.text)
E(x) = <S(x), I(x), K_s(K', K'(S(x), I(x), x.attr, x.text))>

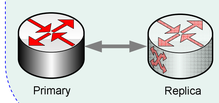
3

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

4

Efficient Bandwidth Utilization

✓ Delta Messaging

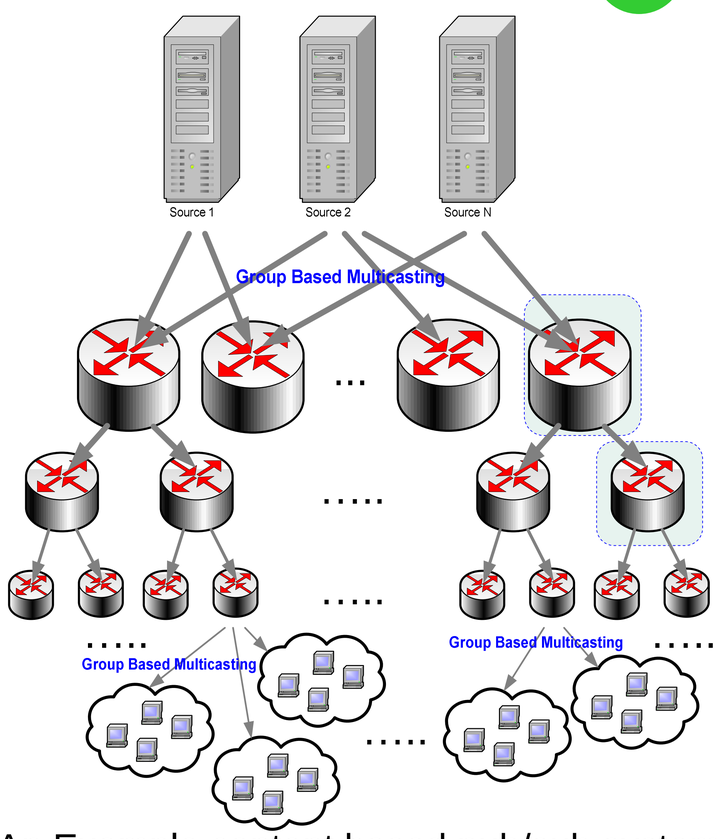
- Unchanged Nodes
- Changed Nodes

✓ **Enforcing security with delta messaging**

✓ Group Multicasting

✓ Content based Routing

5



An Example content based pub/sub system

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

6

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

7

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 h(xpath(x)) with h(xpath(x.parent))||h(/tagname(x))
If x is a right sibling of y, check r(x) > r(y)

8

Related Work

1. E. Bertino, B. Carminati, E. Ferarari, B.M. Thuraisingham, and A. Gupta. Selective and authentic third-party distribution of xml documents. *IEEE Trans. Knowl. Data Eng., 16(10):1263-1278, 2004.*
2. A. Kundu, E. Bertino. Secure dissemination of xml content using structure-based routing. In *Proceedings of the 10th IEEE international Enterprise Distributed Object Computing Conference (Edoc'06), pages 153-164, Washington, DC, USA, 2006.*

9

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center