XML Security

University of Milan

E. Bertino, E. Ferrari, B. Carminati and L. Parasiliti Provenza

University of Insubria

Goal

To provide a comprehensive framework for securing XML data

Benefits

Ensuring security allowing at the same time:

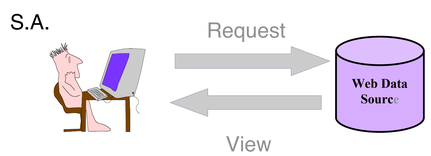
- Flexibility
- Scalability
- Portability

1 Scenarios

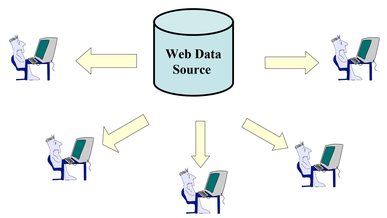
Information dissemination systems, such as digital libraries, mailing lists, intra-company employee information systems

Two different dissemination modes:

Information pull



Information push



2 Main security requirements

Confidentiality
data protection against unauthorized readings

Integrity
data protection against unauthorized modifications

Authenticity
ensuring both the truth of declared source and integrity of distributed data

for both the receiving subjects and information owners

3 What is needed ?

✓ Model

for specifying the security policies stating

- WHO can READ WHAT
- WHO can MODIFY WHAT
- WHO has to ensure authenticity to WHAT

✓ System

providing all mechanisms for enforcing the stated security policies in disseminating XML data

4 Author-X : the model

A model for specifying security policies on XML documents providing :

- ✓ selective protection both at intensional and extensional level
- ✓ temporal constraints
- ✓ flexible qualification of subjects through the notion of subject credential
- ✓ an XML formalism for specifying both access control and signature policies

X - Sec

ACCESS CONTROL vs SIGNATURE POLICIES

- an access control policy expresses the possibility of exercising a privilege on a document portion
- a signature policy states the duty of signing a document portion

5 Author-X : the system

A system for ensuring the satisfaction of both

- ✓ access control policies, through
  - traditional view-based techinques for pull mode
  - broadcast encryption for push mode, using XML ENCRYPTION standard
- ✓ signature policies, by using
  - digital signature technology, adopting XML SIGNATURE format

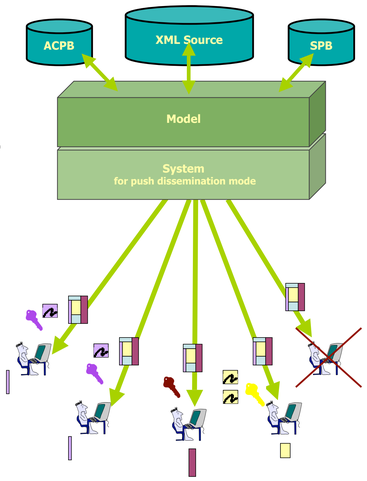
6 Secure push dissemination

✓ Access control mechanism: well-formed encryption

all the document portions to which the same access control policy configuration applies are encrypted with the same key

✓ Authenticity mechanism: correct signature

different portions of the same document are signed with different signatures according to the specified signature policies.



The same (encrypted and signed) copy is, then, broad-casted to all the subjects.

Each subject only receives the keys and signatures of the portions he/she is enabled to access

✓ Key Management

Naïve solution: each access control policy configuration is associated with a different key:

N policies ⇒ 2^N secret  in the worst case

Innovative solution: a symmetric key assignment scheme based on temporal constraint specified in access control policies:

Linear number of  in the number of policies

7 Future Work

- ✓ Model extension for supporting a large variety of signature policies
- ✓ Development of protocols and algorithms for the management of policy update

References

E. Bertino, E. Ferrari, L. Parasiliti Provenza.
Signature and Access Control policies for XML Documents.
In Proceedings of 8th European Symposium on Research in Computer Security, Springer-Verlag.

E. Bertino, E. Ferrari, B. Carminati.
A Temporal key management scheme for broadcasting XML Documents,
In Proc. of the 9th ACM Conference on Computer and Communications Security (CCS'02), ACM Press.