**Goal**
To provide a comprehensive framework for securing XML data

**Benefits**
Ensuring security allowing at the same time:
- Flexibility
- Scalability
- Portability

**Scenarios**
Information dissemination systems, such as digital libraries, mailing lists, intracompany employee information systems

**Two different dissemination modes**
- Information pull
- Information push

**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

**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**
  - Providing all mechanisms for ensuring the stated security policies in disseminating XML data

**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

**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

**Author-X: the system**
A system for ensuring the satisfaction of both access control policies, through
- Traditional view-based techniques for pull mode
- Broadcast encryption for push mode, using XML encryption standard
- Signature policies, by using digital signature technology, adopting XML signature format

**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, broadcasted to all the subjects.
  - Each subject only receives the keys and signatures of the portions he/she is enabled to access
- **Key Management**
  - **Naive solution:** Each access control policy configuration is associated with a different key: $N$ policies $\Rightarrow 2^N$ secrets in the worst case
  - **Innovative solution:** A symmetric key assignment scheme based on temporal constraint specified in access control policies:
    - Linear number of $N$ in the number of policies

**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, B. Carminati and L. Parasiliti Provenza
  - Signature and Access Control policies for XML Documents
  - A Temporal key management scheme for broadcasting XML Documents