CERIAS

An Efficient Time-bound Hierarchical Key Management Scheme for Secure Broadcasting of XML Documents

Elisa Bertino, Ning Shang, Samuel S. Wagstaff, Jr.

CERIAS, Purdue University, West Lafayette, IN

ABSTRACT A time-bound key management scheme for secure broadcasting of XML documents was proposed by E. Bertino, et al., in 2002, in which a method due to Tzeng was suggested. However this method was found insecure in 2004. We propose a new key assignment scheme for access control which is both efficient and secure.

Objectives:

- To find a key management scheme for secure broadcasting of XML documents
- To provide a general solution for other situations, e.g. Digital Rights Languages and RFID systems.

Tools:

- A temper-resistant device
- A secure hash function
- Elliptic curve cryptography

A Hierarchical Structure of the XML Source

Access control policies

↓

Policy configurations

↓

Classes of nodes of an XML source

Initiation

The vendor chooses an elliptic curve $E(F_q)$, a one-way hash function H, two random numbers *a* and *b*, a class key K (as a point on the elliptic curve) for each class of nodes.

The vendor computes and publishes on an authenticated board **values** (as points on the elliptic curve) which are determined by the partial order on the hierarchy.

Encrypting Key Generation

At any time granule *t* , the class with class key *K* is encrypted by a symmetric encryption algorithm with a temporal key $K_t=H(K_Y \oplus H^t(a) \oplus H^{Z-t}(b) \oplus ID)$, where $[1,Z]$ is the life time of the system and *ID* is the identity of the class.

The Key Management Scheme

User Subscription

A user is assigned to a certain class according to the access control policy he/she holds. A tamper-resistant device storing **proper information** for deriving the decryption key is issued to the user.

Decrypting Key Derivation

The user inputs his/her class key *K* or a combination of *K*, the identity of a lower class and a related public parameter found on the authenticated board to the tamper-resistant device to derive the temporal decrypting key.

March 21,2006 1:30-4:00 p.m.