Hierarchical Access Control

Dr. Ashok Kumar Das

IEEE Senior Member
Associate Professor
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad

E-mail: *ashok.das@iiit.ac.in*
URL: http://www.iiit.ac.in/people/faculty/ashokkdas

Hierarchical Access Control

Hierarchical Access Control

Overview of Hierarchical Access Control

- Hierarchical access control is a fundamental problem in computer and network systems.
- In a hierarchical access control, a user of higher security level class has the ability to access information items (such as message, data, files, etc.) of other users of lower security classes.
- A user hierarchy consists of a number n of disjoint security classes, say, SC_1, SC_2, ..., SC_n. Let this set be $SC = \{SC_1, SC_2, \ldots, SC_n\}$.
- A binary partially ordered relation $\geq$ is defined in SC as $SC_i \geq SC_j$, which means that the security class SC_i has a security clearance higher than or equal to the security class SC_j.

Overview of Hierarchical Access Control

- In addition the relation $\geq$ satisfies the following properties:
  - **[Reflexive property]** $SC_i \geq SC_i, \forall SC_i \in SC$.
  - **[Anti-symmetric property]** If $SC_i, SC_j \in SC$ such that $SC_i \geq SC_j$ and $SC_j \geq SC_i$, then $SC_i = SC_j$.
  - **[Transitive property]** If $SC_i, SC_j, SC_k \in SC$ such that $SC_i \geq SC_j$ and $SC_j \geq SC_k$, then $SC_i \geq SC_k$.
- If $SC_i \geq SC_j$, we call SC_i as the predecessor of SC_j and SC_j as the successor of SC_i. If $SC_i \geq SC_k \geq SC_j$, then SC_k is an intermediate security class. In this case SC_k is the predecessor of SC_j and SC_i is the predecessor of SC_k.
- In a user hierarchy, the encrypted message by a successor security class is only decrypted by that successor class as well as its all predecessor security classes in that hierarchy.

Hierarchical Access Control

Overview of Hierarchical Access Control

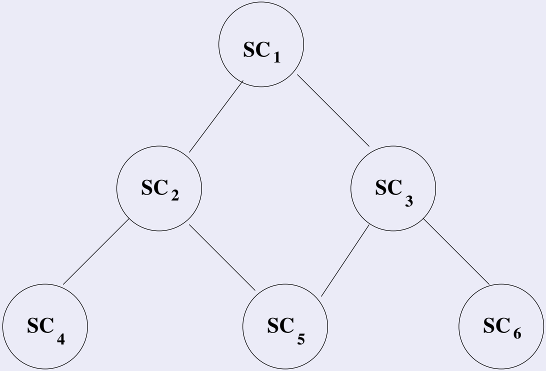

Figure: A small sample of poset in a user hierarchy.

Hierarchical Access Control

Applications of Hierarchical Access Control

- Military
- Government schools and colleges
- Private corporations
- Computer network systems
- Operating systems
- Database management systems

Chung et al.'s User Hierarchical Access Control Scheme

Reference

- Y. F. Chung, H. H. Lee, F. Lai and T. S. Chen, "Access control in user hierarchy based on elliptic curve cryptosystem", Information Sciences (Elsevier), vol. 178, no. 1, pp. 230-243, 2008 (2018 SCI Impact Factor: 5.524).

Chung et al.'s User Hierarchical Access Control Scheme

Relationship Building Phase

- CA (central authority) builds a hierarchical structure for controlling access according to the relationships among the nodes in the hierarchy.
- Let $U = \{SC_1, SC_2, \ldots, SC_n\}$ be a set of n security classes in the hierarchy. Assume that SC_i is a security class with higher clearance and SC_j a security class with lower clearance, that is, $SC_i \geq SC_j$.
- A legitimate relationship $(SC_i, SC_j) \in R_{i,j}$ between two security classes SC_i and SC_j exists in the hierarchy if SC_i can access SC_j.

Chung et al.'s User Hierarchical Access Control Scheme (Continued...)

Key Generation Phase

CA performs the following steps:

- **Step 1:** Randomly selects a large prime p.
- **Step 2:** Selects an elliptic curve $E_p(a, b)$ defined over Z_p such that the order of $E_p(a, b)$ lies in the interval $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$.
- **Step 3:** Selects a one-way function $h(\cdot)$ to transform a point into a number and a base point G_j from $E_p(a, b)$ for each security class SC_j $1 \leq j \leq n$.
- **Step 4:** For each security class SC_j $(1 \leq j \leq n)$, selects a secret key sk_j and a sub-secret key s_j.
- **Step 5:** For all $\{SC_i | (SC_i, SC_j)\} \in R_{i,j}$, computes the followings:
  $s_i G_j = (x_{j,i}, y_{j,i})$,
  $h(x_{j,i} || y_{j,i})$, where $||$ is a bit concatenation operator.

Chung et al.'s User Hierarchical Access Control Scheme (Continued...)

Key Generation Phase (Continued...)

- **Step 6:** Finally, computes the public polynomial $f_j(x)$ using the values of $h(x_{j,i}||y_{j,i})$ as

$$f_j(x) = \prod_{SC_i \geq SC_j} (x - h(x_{j,i}||y_{j,i})) + sk_j \pmod{p}$$

- **Step 7:** Sends sk_j and s_j to the security class SC_j via a secret channel.
- **Step 8:** Announces $p, h(\cdot), G_j, f_j(x)$ as public.

Chung et al.'s User Hierarchical Access Control Scheme (Continued...)

Key Derivation Phase

In order to compute the secret keys sk_j of all successors, SC_j, the predecessor SC_i, for which the relationships $(SC_i, SC_j) \in R_{i,j}$ between SC_i and SC_j hold, proceeds as follows:

- Step 1: For $\{SC_i | (SC_i, SC_j)\} \in R_{i,j}$, computes the followings:
  $s_i G_j = (x_{j,i}, y_{j,i})$,
  $h(x_{j,i} || y_{j,i})$.
- Step 2: Computes the secret key sk_j using $h(x_{j,i} || y_{j,i})$ as follows:

$$\begin{aligned} f_j(x) &= \prod_{SC_i \geq SC_j} (x - h(x_{j,i} || y_{j,i})) + sk_j \pmod{p}, \\ f_j(h(x_{j,i} || y_{j,i})) &= sk_j \pmod{p}. \end{aligned}$$

Chung et al.'s User Hierarchical Access Control Scheme (Continued...)

Key Derivation Phase (Continued...)

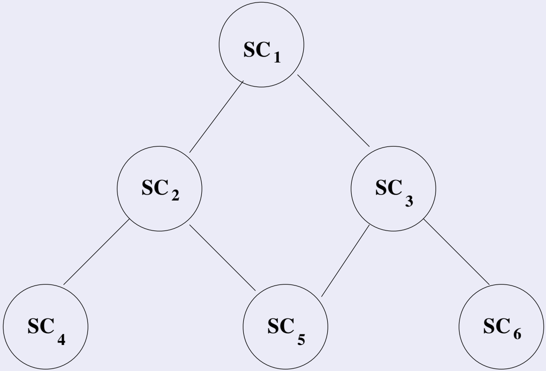

Figure: A small sample of poset in a user hierarchy.

Chung et al.'s User Hierarchical Access Control Scheme (Continued...)

Key Derivation Phase (Continued...)

$$
\begin{aligned}
f_j(x) &= \prod_{SC_i \geq SC_j} [x - h(x_{j,i}||y_{j,i})] + sk_j \pmod{p}, \\
SC_1 : f_1(x) &= [x - h(x_{1,0}||y_{1,0})] + sk_1 \pmod{p}, \text{ where } s_0 \text{ is given} \\
&\quad \text{by CA} \\
SC_2 : f_2(x) &= [x - h(x_{2,1}||y_{2,1})] + sk_2 \pmod{p}, \\
SC_3 : f_3(x) &= [x - h(x_{3,1}||y_{3,1})] + sk_3 \pmod{p}, \\
SC_4 : f_4(x) &= [x - h(x_{4,1}||y_{4,1})][x - h(x_{4,2}||y_{4,2})] + sk_4 \pmod{p}, \\
SC_5 : f_5(x) &= [x - h(x_{5,1}||y_{5,1})][x - h(x_{5,2}||y_{5,2})][x - h(x_{5,3}||y_{5,3})] \\
&\quad + sk_5 \pmod{p}, \\
SC_6 : f_6(x) &= [x - h(x_{6,1}||y_{6,1})][x - h(x_{6,3}||y_{6,3})] + sk_6 \pmod{p}
\end{aligned}
$$

Chung et al.'s Scheme (Continued...)

Key Derivation Phase (Continued...)

To derive the secret key sk_5 of SC_5 by its predecessor class SC_2, SC_2 needs to do following:

- Computes $s_2 G_5 = (x_{5,2}, y_{5,2})$ and then $h(x_{5,2}||y_{5,2})$.
- Determines sk_5 using $h(x_{5,2}||y_{5,2})$ from the public polynomial $f_5(x) = [x - h(x_{5,1}||y_{5,1})][x - h(x_{5,2}||y_{5,2})][x - h(x_{5,3}||y_{5,3})] + sk_5 \pmod p$ as $sk_5 = f_5(h(x_{5,2}||y_{5,2})) \pmod p$.