Galois Connection and Security (I) : Application to Secure Information Flow

Sakuraba, Taketoshi
Hitachi Yokohama Laboratory

出版情報：MI lecture note series. 53, pp.18-27, 2013-12-26. 九州大学マス・フォア・インダストリ研究所
バージョン：
権利関係：

Galois Connection and Security (I)

ガロア接続を用いた動的秘密情報の管理 (I)

Application to Secure Information Flow

SAKURABA, Taketoshi[1,a)]

Abstract: As the part I of the presentation, we introduce concept of the lattice, the technology called formal concept analysis (FCA) and show their relation with the system security models. FCA is an application of the lattice theory and has been proposed as a method for the knowledge analysis. The basis of FCA is the Galois connection in the lattice theory, which derives a lattice from a context table. In the system security area, the lattice theory also plays important roles. One of the classical facts is that any secure information flow systems form lattices. It was explained in an axiomatic argument on property of secure information flow. In this presentation, we show this classical result by applying FCA to an access control table derived from a security policy.

1. Lattices

For lattice theory, refer [1].

A partially ordered set is a set equipped with a order relation "$\leq$" which satisfies following for elements x, y and z.

$$x \leq x \quad x \leq y \text{ and } y \leq z \Rightarrow x \leq z \quad x \leq y \text{ and } y \leq x \Rightarrow x = y$$

A lattice is a partial ordered set with more properties that any two elements x, y have the least common upper bound (lub) $x \vee y$ and the greatest common lower bound (glb) $x \wedge y$.

$$x \leq x \vee y \text{ and } y \leq x \vee y \quad \text{if } x \leq z \text{ and } y \leq z \;\Rightarrow\; x \vee y \leq z$$
$$x \wedge y \leq x \text{ and } x \wedge y \leq y \quad \text{if } z \leq x \text{ and } z \leq y \;\Rightarrow\; z \leq x \wedge y$$

Replacing "any two elements" with "any subset", the notion of complete lattices is obtained. But, considering only finite lattices, completeness does not matter.

Well known example of a partially ordered set P is non empty set of sets ordered by inclusion. If P is finite, it can be embedded in a lattice L, the intersection closure of P:

$$L = \{\cap A \mid A \subseteq P\} \qquad x \vee y = \bigcap \{z \mid x \leq z \text{ and } y \leq z\}$$

2. Galois Connection

Let G and M are non empty sets, and I is a relation between G and M, i.e. $I \subseteq G \times M$. $K = (G, M, I)$ is called a context. From the context, define maps γ and μ as follows. %

$$g \,\mathrm{I}\, m \Leftrightarrow (g, m) \in I$$
$$g \,\mathrm{I}\, N \Leftrightarrow g \,\mathrm{I}\, m \quad (\forall\, m \in N) \quad H \,\mathrm{I}\, m \Leftrightarrow g \,\mathrm{I}\, m \quad (\forall\, g \in H)$$

$$\gamma(\emptyset) = M \qquad \mu(\emptyset) = G$$
$$\gamma(g) = \{m \mid g \,\mathrm{I}\, m\} \qquad \mu(m) = \{g \mid g \,\mathrm{I}\, m\}$$
$$\gamma(H) = \{m \mid H \,\mathrm{I}\, m\} \qquad \mu(M) = \{g \mid g \,\mathrm{I}\, M\}$$
$$\mu\gamma(H) = \mu(\gamma(H)) = \{g \in G \mid g \,\mathrm{I}\, \{m \in M \mid H \,\mathrm{I}\, m\}\}$$
$$\gamma\mu(N) = \gamma(\mu(N)) = \{m \in N \mid g \,\mathrm{I}\, \{g \in G \mid g \,\mathrm{I}\, N\}\}$$
$$\gamma K = \{\gamma(H) \mid H \subseteq G\} \qquad \gamma\mu K = \{\gamma\mu(N) \mid N \subseteq M\}$$
$$\mu K = \{\mu(N) \mid N \subseteq M\} \qquad \mu\gamma K = \{\mu\gamma(H) \mid H \subseteq G\}$$

Then we get a lattice associated with the context $K = (G, M, I)$

Theorem 1 (Galois Connection)**.** *$\gamma\mu K$, γK, $\mu\gamma K$ and μK are all identical lattices. To be precise, $\gamma\mu K = \gamma K$, $\mu\gamma K = \mu K$, and γK and μK are dual each other. γ and μ are the order reversing isomorphism between them*

3. Formal Concept Analysis

Formal Concept Analysis (FCA) is an application of Galois-Connection. It was proposed by Wille [2] as a tool for analyzing data and knowledge. The settings of FCA are as follows [3].

G :	Set of objects (Gegenstände)
M :	Set of attributes (Merkmale)
I :	Context (Kontext)
$\gamma(H)$:	Intent of H, common attributes of all $g \in H \subseteq G$
$\mu(N)$:	Extent of N, objects satisfy attribute $m \in N \subseteq M$
(H, N) :	Formal concept of K, if $\gamma(H) = N$ and $\mu(N) = H$
$\mathfrak{B}(K)$:	Concept lattice, set of all formal concepts in K
	$(H_1, N_1) \leq (H_2, N_2) \;\Leftrightarrow\; H_1 \subseteq H_2 \;\Leftrightarrow\; N_1 \supseteq N_2$

Theorem 2 (Fundation of FCA)**.**

$$\bigwedge_t (H_t, N_t) = (\cap_t H_t, \gamma\mu(\cup_t N_t)) \qquad \bigvee_t (H_t, N_t) = (\mu\gamma(\cup_t H_t), \cap_t N_t)$$

As seen in the definition, an element of the concept lattice is

[1] Hitachi Yokohama Laboratory, Yokohama 244–0817, Japan
[a)] taketoshi.sakuraba.hc@hitachi.com

a pair of an intent and an extent, they are firmly related in the context K. Concrete but excessive concepts are reduced and included into the formal concepts. As the result of the construction, just enough formal concepts are remained. They are the essentially meaningful knowledge in the context K, and form a lattice.

4. Information Flow

A security model is a format of security policies. Information Flow Control (IFC) is one of the fundamental security model. Dividing users and information into some security classes, and monitoring and controlling flows of information and moves of information carriers. Let A and B are security classes. The order relation "$A \rightarrow B$" means that any information flow from A to B is permitted. The information flow relation can be seen as an order relation. Denning [4] showed that the security classes and secure information flow between them form a lattice. Thus this model also called the lattice model. Well known information flow policy is Bell-LaPadula model [6], which had been developed and used in US government. The lattice of BLP policy is simply linear-four-layers structure.

Important notions in IFC are NO-READ-UP and NO-WRITE-DOWN. the former means users in the lower security classes are not permitted to write anything into files of the upper security classes. This rule would be trivial. The latter means users of upper security classes are inhibited to write anything into files of the lower security classes, because upper secret may leak to the lower.

5. Application of FCA to IFC

A secresy security policy can be interpreted into an information flow control policy. As a consequence of the fact, one can see that, in a secure information flow policy, their security classes and the information flow relation form a lattice. These can be shown by using FCA as follows.

Define G as the set of users, and let M be the set of files. A file is considered as an attribute of a user, that means the user is permitted to access to the file by the security policy. This form of the security policy is called access control matrix (table). This information can be seen as a context of FCA. So, applying FCA to this context data, a concept lattice is derived. Each concept corresponds to a security class, and the order relation corresponds to the permitted information flow. In the access control theory, $\mu(m)$ is called access control list (ACL) of $m \in M$, and $\gamma(g)$ is called capability of $g \in G$. So, μK can be called ACL lattice, and γK can be called capability lattice.

Denning's explanation [4] was axiomatic, but in her another note [5], starting with partially ordered information flow models, and applying the intersection closure technic, she derived a lattice, which can be seen as a capability lattice in our argument.

6. Conclusion

The lattice and Galois connection thoery and FCA are introduced. Information flow and the lattice model of Denning are explained. Applying FCA to security policies, the lattice model is derived.

References

[1] Davey, B. A., Priestley, H. A.: *Introduction to Lattices and Order, second edition*, Cambridge University Press, Cambridge, UK, 2002.

[2] R. Wille, Restructuring lattice theory: an approach based on hierarchies of concept, D. Reidel, Ordered Sets (I. Rival eds.), pp.445–470, 1982

[3] Suzuki, O., Murofushi, T.: 形式概念分析 – 入門・支援ソフト・応用, 日本知能情報ファジイ学会, 知識と情報 vol.19, no. 2, pp. 103–142, 2007

[4] Denning, D. E. R.: A Lattice Model of Secure Information Flow, ACM, CACM, Vol.19, No.5, pp.236–243, 1976.

[5] Denning, D. E. R.: On the Derivation of Lattice Structures Information Flow Policies, Purdue University, CSD TR 180, 1976.

[6] Bell, D. E., LaPadula, J.: Secure Computer Systems: Unified Exposition and Multics Interpretation, MTR-2997, MITRE Corporation, ESD-TR-75-306, 1976.

[7] Sandhu, R. S., Coyne, E. J., Feinstein, H. L. and Youman, C. E.: Role-based access control models, IEEE Computer, Vol.29 No.2, pp.38–47, 1996.

HITACHI
Inspire the Next

IMI Workshop (2013/8/26—30)
安全・安心社会基盤構築のための代数構造
～サイバー社会の信頼性確保のための数理学～

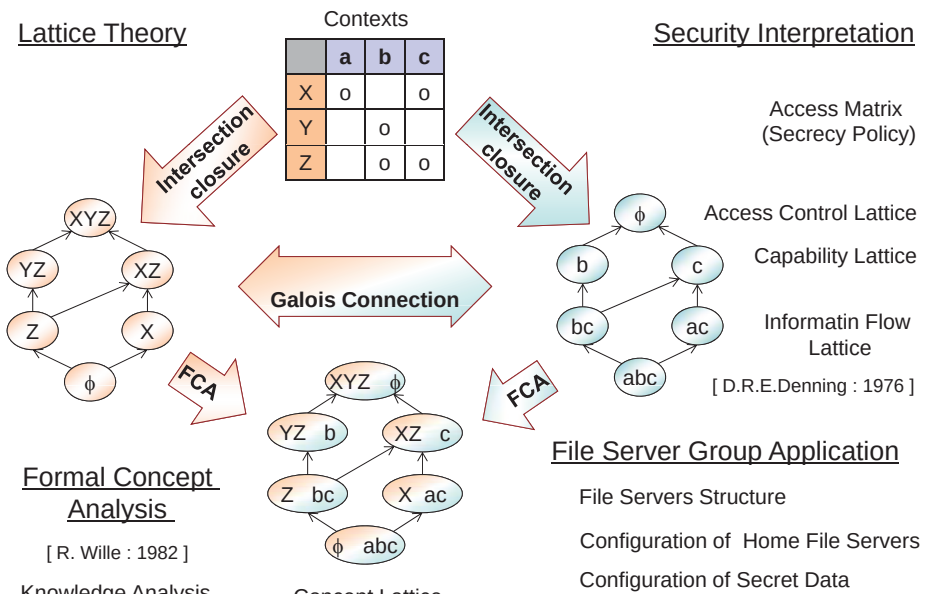
Galois Connection and Security (I)
ガロア接続を用いた動的秘密情報の管理 (I)
Application to Secure Information Flow

2013/08/27 Fukuoka, Japan

SAKURABA, Taketoshi Hitachi, Ltd.

Outline

HITACHI
Inspire the Next



 2

Agenda

HITACHI
Inspire the Next

- Galois Connection
  - Lattice Theory
  - Formal Concept Analysis
- Security
  - Information Flow Control
  - Lattice Model
- Application -- Hierarchical File Server Groups
  - Structure of HFSG
  - Security of HFSG
    - Information Flow Control,
    - Labeled Control without Labels,
    - RBAC
  - Management of HFSG
    - Comparison with Flat Structure
- Conclusions

Lattice

HITACHI
Inspire the Next

- Lattice
  - Partially Ordered Set (, not a subalgebra of Z x Z)
  - For any a and b in a lattice, they have both of
    lub [least upper bound, sup, join] of $\{a, b\}$, $= a \vee b$
    glb [greatest lower bound, inf, meet] of $\{a, b\}$, $= a \wedge b$
    - $a \vee b = b \vee a \quad a \vee (b \vee c) = (a \vee b) \vee c \quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ etc.
- Example

  For $M \subseteq \mathbf{P}(X)$ $\mathbf{P}(X)$: powerset of X
  - Intersection-closure of M (= $\underline{M}$)

    $= \{ (\cap A) \cap (\cup M) \mid A \subseteq M \}$ (N.B. $(\cap \phi) \cap (\cup M) = \cup M \in \underline{M}$)
  - Complete lattice ordered by inclusion including M
    - $A \wedge B = A \cap B$
    - $A \vee B = \cap \{ C \mid A \cup B \subseteq C \in \underline{M} \}$

Galois Connection

HITACHI
Inspire the Next

Definitions

- $\mathbf{K} = (G, M, \mathbf{I})$: G, M : sets, $\mathbf{I} \subseteq G \times M$: relation

$g\ \mathbf{I}\ m \Leftrightarrow (g, m) \in \mathbf{I}$ $\quad g\ \mathbf{I}\ N \Leftrightarrow \forall m \in N\ (g\ \mathbf{I}\ m)$ $\quad H\ \mathbf{I}\ m \Leftrightarrow \forall g \in H\ (g\ \mathbf{I}\ m)$

$\gamma(g) = \{m \in M \mid g\ \mathbf{I}\ m\}$ $\quad \gamma(H) = \{ m \in M \mid H\ \mathbf{I}\ m\} = \cap \{ \gamma(g) \mid g \in H\}$

$\mu(m) = \{g \in G \mid g\ \mathbf{I}\ m\}$ $\quad \mu(N) = \{ g \in G \mid g\ \mathbf{I}\ N\} = \cap \{ \mu(m) \mid m \in N\}$

$\mu\gamma(H) = \mu(\gamma(H)) = \{ g \in G \mid g\ \mathbf{I}\ \{m \in M \mid H\ \mathbf{I}\ m\}\}$

$\gamma\mu(N) = \gamma(\mu(N)) = \{ m \in M \mid \{g \in G \mid g\ \mathbf{I}\ N\}\ \mathbf{I}\ m\}$

$\gamma\mathbf{K} = \{ \gamma(H) \mid H \subseteq G\}$ $\quad \gamma\mu\mathbf{K} = \{ \gamma\mu(N) \mid N \subseteq M\}$ N.B. : $\gamma(\phi) = M \in \gamma\mathbf{K}$

$\mu\mathbf{K} = \{ \mu(N) \mid N \subseteq M\}$ $\quad \mu\gamma\mathbf{K} = \{ \mu\gamma(H) \mid H \subseteq G\}$ $\quad \mu(\phi) = G \in \mu\mathbf{K}$

Theorem

- $\gamma\mu\mathbf{K} = \gamma\mathbf{K}$, $\mu\gamma\mathbf{K} = \mu\mathbf{K}$. These are lattices . ($\because$) $\cap$-closures
- $\gamma\mathbf{K}$ and $\mu\mathbf{K}$ are dual (order reversed, isomorphic) to each other

($\because$) $H \subseteq K \subseteq G \Rightarrow \gamma(H) \supseteq \gamma(K)$, $N \subseteq L \subseteq M \Rightarrow \mu(N) \supseteq \mu(L)$, $H \subseteq \mu\gamma(H)$, $N \subseteq \gamma\mu(N)$

$\therefore \gamma(H) \supseteq \gamma\mu\gamma(H)$, $\gamma(H) \subseteq \gamma\mu(\gamma(H))$, $\therefore \gamma(H) = \gamma\mu\gamma(H) \in \gamma\mu\mathbf{K}$, $\therefore \gamma\mathbf{K} \subseteq \gamma\mu\mathbf{K}$, …

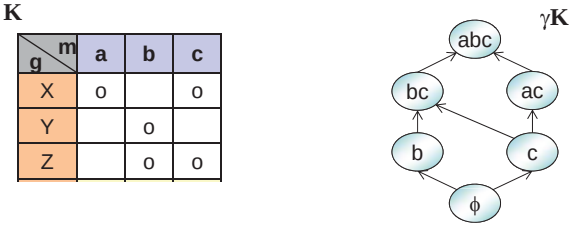
Example

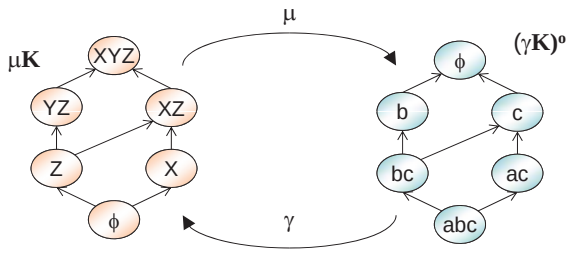
HITACHI
Inspire the Next

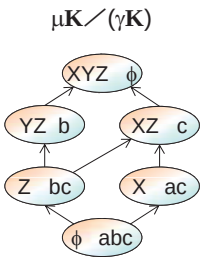
- $\mathbf{K} = (G, M, \mathbf{I})$ G, M : Sets, $\mathbf{I} \subseteq G \times M$
- $\gamma\mu\mathbf{K} = \gamma\mathbf{K}$, $\mu\gamma\mathbf{K} = \mu\mathbf{K}$: lattices. $\mu\mathbf{K} \equiv$ dual of $\gamma\mathbf{K}$

$\mathbf{K}$

g \ m	a	b	c
X	o		o
Y		o	
Z		o	o







ab denotes set {a, b}

FCA : Formal Concept Analysis

HITACHI
Inspire the Next

- **K**=(G, M, **I**)
  - G: Set of Objects, M: Set of Attributes, **I** (⊆G×M): “Formal” context
- γ(H) : Intent (H⊆G) μ(N) : Extent (N⊆M)
- (H, N) : “Formal” concept (H⊆G, N⊆M) ⇔ N=γ(H) and H=μ(N)
- **B**={(H,N) | (H,N) is a concept} : Concept Lattice

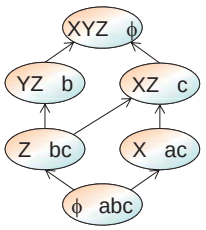
  (H1,N1)≦(H2, N2) ⇔ H1⊆H2 ⇔ N1⊇N2

  ⋀(Hi , Ni) = (∩Hi, γμ(∪Ni)) ⋁(Hi , Ni) = (μγ(∪Hi), ∩Ni))

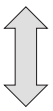
Context Table

g \ m	a	b	c	Intents	
X	o		o	ac	ϕ
Y		o		b	c
Z		o	o	bc	abc
Extents	X	YZ	XZ		
	ϕ	Z	XYZ		

Concept Lattice



Universal concept



Specific concept

Applications of FCA

HITACHI
Inspire the Next

- Rudolf Wille (1982).
  - “Restructuring lattice theory: an approach based on hierarchies of concepts”
- Data Analysis
- Healthcare
- Linguistics
- Software Design
- Security Models

- References

Davey, Priestley: Introduction to Lattices and Order, second edition, Ch.3, and Ch.7, Cambridge University Press (1990, 2002)

Suzuki, Murofushi: (in Japanese) Formal Concept Analysis – Introduction, Support Softwares and Applications –, **知識と情報** Vol.19, No.2 (2007)

Information Security

HITACHI
Inspire the Next

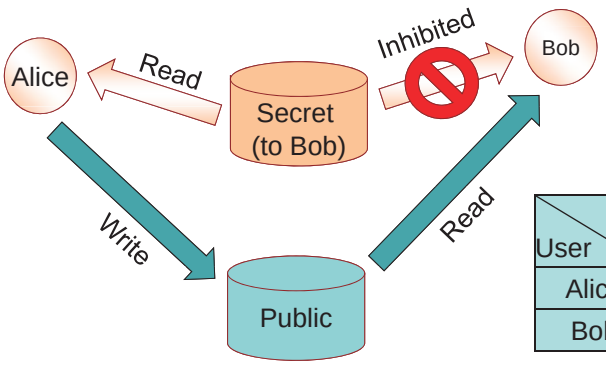
Technology for Protecting and Controlling “CIA”

- Confidentiality / Secret
  - Threats: Unauthorized access to information,
  - Measures: Information Flow Control, Cryptography, …
- Integrity / Consistency
  - Threats: Unauthorized modification of information
  - Measures: Rules for modification, Signature, …
- Availability
  - Threats: Unauthorized use of resources
  - Measures: Limiting resource allocation, Monitoring, …

Information Flow

HITACHI
Inspire the Next

- Information Flow
  - Secret ⇒Alice ⇒ Public ⇒ Bob
    - Against “the security Policy”



Secret may be known by Bob …

Access Matrix

User \ File	Secret	Public
Alice	Read	Write
Bob	-	Read

Security Policy Models

HITACHI
Inspire the Next

Format of Security Policy

- Access Matrix Model (Access Control Table)

		Objects			
		Secret A	Secret B	TopSecret	Public
Subjects	Alice	Read, Write			Read
	Bob		Read, Write		Read
	Chris	Read	Read	Read, Write	Read
	David				Read,Write

Alice's Capability

ACL of B

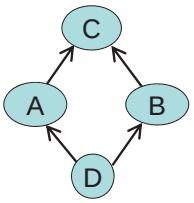
- Information Flow Model

A ∋ Alice、SecretA

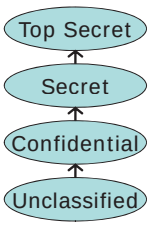
B ∋ Bob、SecretB

C ∋ Chris、TopSecret

D ∋ David、Public



Multi Level Security



 11

Order and Information Flow

HITACHI
Inspire the Next

A, B, … : security classes

≒ Set of "logical storage objects" sharing same information∋user, file, …

- A＝B : (members of) A and B share same information
- A⇒B : Information flow from A to B is permitted
  - Reflexive : A⇒A [may not be inhibited]
  - Transitive : A⇒B, B⇒C then A⇒C [B cannot keep secret]
  - Anti-Symmetric : A⇒B, B⇒A then A＝B
- Bell-LaPadula Model
  - A⇒B and A ≠ B then …
    - Read B by A : inhibited : No-Read-Up Read A by B : permitted
    - Write to A by B : inhibited : No-Write-Down Write to B by A : permitted
- Set of security classes forms partially ordered set furthermore, it becomes a Lattice [Denning,1976].

 12

FCA proof of Information Flow Lattice

HITACHI
Inspire the Next

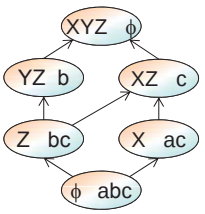
- Access Control Table ⇔ Context
- Information Flow : → ⇔ ≦ : Order Relation
- Security Classes ⇔ Concepts
- Structure of Security Classes ⇔ Lattice
- Access Control List (ACL) ⇔ Extent
- Capability ⇔ Intent

Access Matrix Model

file / user	a	b	c	Capability	
X	X can read a		o	ac	ϕ c ab
Y		o		b	
Z		o	o	bc	
ACL	X	YZ	XZ		
	ϕ Z XYZ				

⇔

Information Flow Model
Lattice Model



 13

Role Based Access Control

HITACHI
Inspire the Next

- RBAC
  - The most successful security model
  - Introduce Roles to describe Permission assignment rules
    - Subject ∈ Role ⇒ Permission, then Permission is assigned to Subject
      - Subject's actual/current role is determined dynamically [e.g. logon as an Admin]
      - Dr. Foo ∈ DOCTORS ⇒ May access his patient's medical record
  - Merits
    - Divide Permission Management into 2 parts, one is stable, another is easy
    - A subject may play different role in different context.
      - Dr. Foo on his day off, cannot access hospital's resource, except in emergency
- Modeling RBAC by using FCA
  - Dyadic Formal Context : Role-Permission relation
    ⇒ Role-lattice (Role hierarchy)
  - Triadic Formal Context :
    - K (R, D, P, **I**) ⇒ **I** ⊆ R × D × P = (R × D) × P
    - Roles, Documents, Permissions
      ⇒ Document types, classified by security point of view

 14

Conclusions (I)

HITACHI
Inspire the Next

- Galois Connection is a theorem of the Lattice theory
  $I \subseteq G \times M \Rightarrow$ derived two lattices are dual each other
- FCA is an application of Galois Connection for Knowledge Analysis
  considers extent lattice and intent lattice at once
- Security policy can be analyzed by FCA
  - Concept Lattice of given Security Policy represents appropriate Information Flow Policy
  - Another proof of Denning's theorem
- FCA is gathering attention from security point of view

