

FFI Forsvarets
forskningsinstitutt

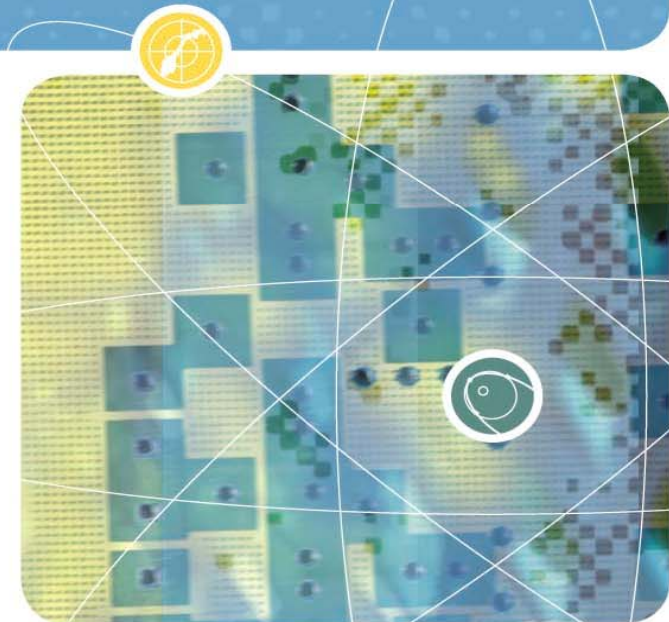
Norwegian Defence Research Establishment

Multi Level Security (MLS)

Eli Winjum, FFI

NISNETs Winterschool in
Information Security

Finse, May 3 – 8, 2009



1. Introduction and MLS models

- a. a model of military security classes
- b. MLS confidentiality
- c. MLS integrity
- d. compound MLS models
- e. MSL and MILS

2. Some problems and challenges of current MLS systems

- a. confidentiality and integrity as interdependent aspects
- b. how to classify
- c. lattice structure and scalability
- d. the number of security classes
- e. simpler class structures – simpler and scalable models



Outline

3. A multidimensional MLS model

- a. concept overview
- b. security classes
- c. simple verification of rights
- d. command & control systems
- e. sensor systems
- f. IP routing

4. Conclusive remarks

5. Further work at FFI



Introduction to multilevel security (MLS) (1:3)

- Both military and civil systems need to separate information into different levels of security and to control information flow between levels
- Military security policies have emphasized multilevel confidentiality
 - prevent information flow from higher to lower levels of confidentiality
- Financial businesses have emphasized multilevel integrity
 - prevent information flow from lower to higher levels of integrity
- There are models that combine confidentiality and integrity requirements, but
 - most current multilevel architectures classify information according to confidentiality only, and integrity properties may follow implicitly, so that high confidentiality classification implies high integrity



Introduction to multilevel security (MLS) (2:3)

- Multilevel security (MLS) describes an information system which is trusted to
 - contain information classified into different security levels
 - maintain separation between the levels
 - concurrent users may have different permissions with respect to the security levels
- During the 1970's, Denning, Bell, LaPadula and Biba developed lattice-based MLS models
 - core ideas are still valid
 - systems built from these models turned out to be complex, expensive and impractical



Introduction to multilevel security (MLS) (3:3)

- Current implementations
 - comprise a large number of security classes
 - verifying that operations between any two classes are secure is time consuming and costly
 - actual security policies deviate from the formal axioms
 - over-classification and cumbersome reclassification involve review and release functions, which even today may be manual.



Definitions

- *Confidentiality, integrity and availability* are the three basic aspects of information security

The literature provides numerous informal definitions

- A more formal definition:

Let X be a set of entities and I some information (or a resource).

Then:

I has the property of confidentiality with respect to X if no member of X can obtain information of I

I has the property of integrity with respect to X if all members of X trust I

I has the property of availability with respect to X if all members of X can access I



Military security levels (1:2)

Example:

{ UNCLASSIFIED, CONFIDENTIAL, SECRET, TOP SECRET }

Security level
TOP SECRET
SECRET
CONFIDENTIAL
UNCLASSIFIED

A simple hierarchical and linear ordering of security levels

Similar levels exist – formally or informally – in commercial organizations as well



Military security levels (2:2)

Example:

{ UNCLASSIFIED, CONFIDENTIAL (**NO**, **UK**), CONFIDENTIAL (**NO**, **US**), CONFIDENTIAL (**NO**, **UK**, **US**), ... , SECRET (**NO**, **UK**), SECRET (**NO**, **US**), ... , TOP SECRET (**NO**, **UK**), TOP SECRET (**NO**, **FR**), ... , TOP SECRET (**NO**, **FR**, **UK**),..., }

A not so simple
non-hierarchical
and non-linear
ordering of security
levels

Similar levels exist
– formally or informally –
in commercial
organizations as well



Denning's lattice model (1:3)

- Lattice properties permit concise formulations of the security requirements of information systems and facilitate mechanisms to enforce a security policy
- Denning proposed a model which derives the lattice structure from security classes
- $SC = \{A, B, \dots\}$ is a set of security classes corresponding to disjoint classes of information
- $\langle SC, \rightarrow, \oplus, \otimes \rangle$ forms a universally bound lattice iff:
 - $\langle SC, \rightarrow \rangle$ is a partially ordered set
 - SC is finite
 - SC has a lower bound L , such that $L \rightarrow A$ for all $A \in SC$
 - SC has an upper bound H
 - \oplus is a least upper bound operator on SC
 - \otimes is a greatest lower bound operator on SC
- $\langle SC, \rightarrow \rangle$ is a partially ordered set. That is, for any $A, B, C \in SC$
 - $A \rightarrow A$ (reflexive)
 - $A \rightarrow B$ and $B \rightarrow C \Rightarrow A \rightarrow C$ (transitive)
 - $A \rightarrow B$ and $B \rightarrow A \Rightarrow A = B$ (anti-symmetric)

Denning's lattice model (2:3)

Linear ordered lattice

$$SC = \{ A_1, \dots, A_n \}$$

$$A_i \rightarrow A_j \text{ iff } i \leq j$$

$$A_i \oplus A_j \equiv A_{\max(i, j)}$$

$$A_i \otimes A_j \equiv A_{\min(i, j)}$$

$$L = A_1$$

$$H = A_n$$

Description

 A_n
 \uparrow
 A_{n-1}
 \uparrow
 \cdot
 \cdot
 \uparrow
 A_2
 \uparrow
 A_1

Representation

Denning's lattice model (3:3)

Non-linear ordered lattice of subsets of $X = \{x, y, z\}$

SC = power set $\{ X \}$

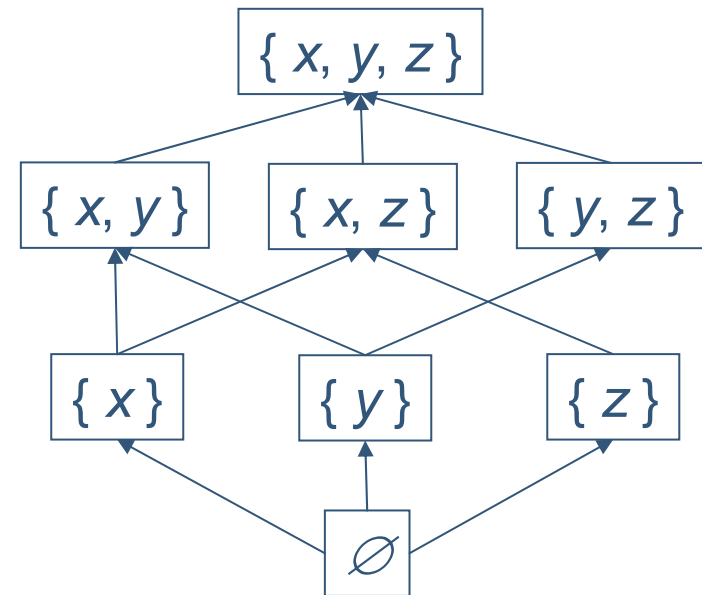
$A \rightarrow B$ iff $A \subseteq B$

$A \oplus B \equiv A \cup B$

$A \otimes B \equiv A \cap B$

$L = \emptyset$

$H = X$



Description

Representation

Lattice-based security models

- Still richer structures can be constructed as combinations of linear ordered and non-linear ordered lattices
- If the lattice properties are preserved during state transitions, insecure states can not be reached
- Such lattices are the foundation for classic MLS models, which current MLS-systems are based upon
- Lattice-based access control – mandatory access control – rule-based access control



The Bell – LaPadula (BLP) model (1:4)

- The BLP model describes a generic multilevel confidentiality policy
- The objects of the model have security (confidentiality) classifications,
 $L(O) = level_{object}$
- The subjects of the model have security (confidentiality) clearances,
 $L(S) = level_{subject}$
- Security labels may indicate the different levels
- The BLP model combines mandatory and discretionary access control
 - rules regulating read and write access enforce one-directional information flow
- Military MLS systems are based on the BLP model



The Bell – LaPadula (BLP) model (2:4)

The system is secure if the set of state transitions preserves:

- The *simple security condition*
 - a subject can read an object iff
 - confidentiality level_{subject} \geq confidentiality level_{object}
 - the subject has a discretionary read access to the object
- The **-property*
 - a subject can write an object iff
 - confidentiality level_{subject} \leq confidentiality level_{object}
 - the subject has a discretionary write access to the object



The Bell – LaPadula (BLP) model (3:4)

The BLP policy allows information flow from low confidentiality level to higher levels and disallows flow in the opposite direction

Security level	Subjects	Objects
TOP SECRET	Tracy, Thomas	Personnel files
SECRET	Sally, Sam	Electronic mail files
CONFIDENTIAL	Claire, Carl	Activity logs
UNCLASSIFIED	Ursula, Ulysses	Telephone list



The Bell – LaPadula (BLP) model (4:4)

- The set { UNCLASSIFIED, CONFIDENTIAL, SECRET, TOP SECRET } forms a linear ordering
- The model may be extended with *compartments* (or *categories*)
 - specified *areas of interest*
 - examples are the set of departments of an organization or the subset of information two nations agree to exchange
- Compartments
 - reflect a need-to-know-policy and restrict the subjects' access to information at levels for which they are cleared
 - lead to a lattice including the set of all subsets of the set of compartments, also called the power set of the set of compartments
 - read and write access rules are extended to encompass the combined lattice structure
- Solaris TE is an example of current implementation of the extended BLP model



The Biba model (1:3)

- The Biba model describes a generic multilevel integrity policy
- The subjects and objects are associated with integrity levels
- Integrity levels may be used as a measure of trustworthiness
- The higher the level, the more confidence is implied
 - that a program will execute correctly
 - that (user) data is authentic, not modified, accurate, reliable..
- Labels may indicate the different integrity levels
- “Integrity labels” are *not* “security (confidentiality) labels”
 - integrity labels aim at *inhibit the modification* of information
 - security (confidentiality) labels aim at *limit the flow* of information
 - should be assigned and maintained separately
 - (should be called *confidentiality labels* and *integrity labels*)



The Biba model (2:3)

- Rules regulating read and write access enforce one-directional information flow
- The model is a basis for different policies
- The strict integrity policy regulates read and write accesses as follows:
 - a subject can read an object iff
 - $\text{integrity level}_{\text{subject}} \leq \text{integrity level}_{\text{object}}$
 - a subject can write an object iff
 - $\text{integrity level}_{\text{subject}} \geq \text{integrity level}_{\text{object}}$





The Biba model (3:3)

- The Biba policy allows information flow from high integrity level to lower levels and disallows flow in the opposite direction
- Like the BLP model, the Biba model may be extended with compartments (or categories)
- A recent example of integrity classes is Windows Integrity Control (WIC) in which information and roles are fixed at predefined levels. Does not implement the Biba model!

Confidentiality and integrity – dual models

The strict integrity policy of the Biba model is the dual of the BLP model

	Bell - LaPadula	Biba
	Confidentiality policy	Integrity policy
	read down	read up
	write up	write down





Compound MLS models (1:3)

Composite multilevel models aim at combining confidentiality and integrity requirements

- Lipner augments confidentiality classifications with integrity classifications (1982)
- Sandhu describes a composite model with mutually independent confidentiality levels and integrity levels (1993)
 - The model applies BLP rules to confidentiality and Biba rules to integrity
 - A subject can read an object iff
$$\text{confidentiality level}_{\text{subject}} \geq \text{confidentiality level}_{\text{object}}$$
AND integrity level
$$\text{integrity level}_{\text{subject}} \leq \text{integrity level}_{\text{object}}$$
 - A subject can write an object iff
$$\text{confidentiality level}_{\text{subject}} \leq \text{confidentiality level}_{\text{object}}$$
AND integrity level
$$\text{integrity level}_{\text{subject}} \geq \text{integrity level}_{\text{object}}$$



Compound MLS models (2:3)

- Kang et al distinguish between reliable and unreliable OS processes by (2001)
 - extending the BLP model with integrity levels related to subjects (processes)
 - adding verification of process integrity to the BLP rules
 - low integrity level is associated with low confidentiality level
- Huang and Shen adopt both BLP and Biba (2004)
 - presume that confidentiality and integrity are interdependent
 - high confidentiality level implies high integrity level, but low confidentiality does not necessarily mean low integrity



Compound MLS models (3:3)

- Irvine et al combine BLP and Biba to enforce a unified access control policy (2004)
 - not quite clear how information objects are classified with respect to combined confidentiality and integrity, and whether such classifications are interdependent or not
- Liu and Li extend the lattice representation of a combined BLP and Biba model with a *concern degree* (2005)
 - enables a weighting of confidentiality versus integrity for a given subject or object



Some alternatives to MLS

- Multiple Single-Level (MSL) systems
 - each security level is isolated
 - the mechanism for isolation is usually physical separation in separate computers and networks
 - often used to support applications or OSs which have no possibility of supporting MLS, such as MS Windows.
- Multiple Independent Levels of Security (MILS)
 - an architecture
 - addresses the domain separation component of MLS
 - focus on the isolation, not the controlled interaction between domains
 - pursue the concept of MSL, often called “multiple independent domains of security”

1. Introduction and MLS models

- a. a model of military security classes
- b. MLS confidentiality
- c. MLS integrity
- d. compound MLS models
- e. MSL and MILS

2. Some problems and challenges of current MLS systems

- a. confidentiality and integrity as interdependent aspects
- b. how to classify
- c. lattice structure and scalability
- d. the number of security classes
- e. simpler class structures – simpler and scalable models



Outline

3. A multidimensional MLS model

- a. concept overview
- b. security classes
- c. simple verification of rights
- d. command & control systems
- e. sensor systems
- f. IP routing

4. Conclusive remarks

5. Further work

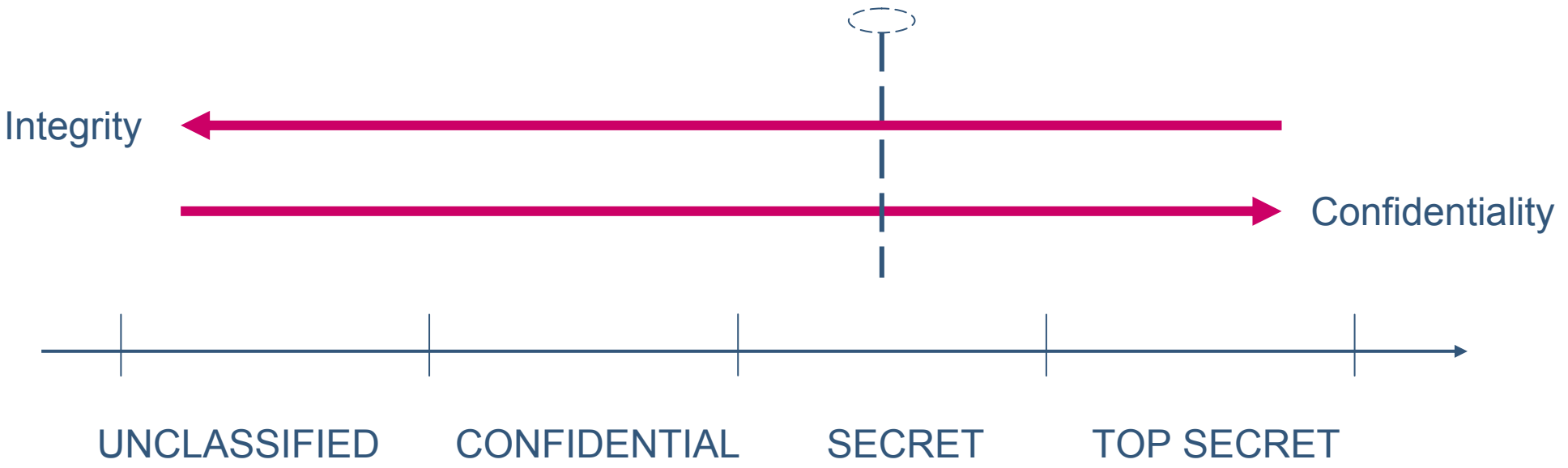


Confidentiality and integrity as interdependent aspects (1:2)

- Integrity aspects are not well appreciated in many organizations
 - that a program will execute correctly
 - that (user) data is authentic, not modified, accurate, reliable..
- Several current multilevel architectures classify information according to confidentiality only
- Integrity properties may follow implicitly, so that high confidentiality classification implies high integrity
- This assumption may, however, not be valid:
 - an unverified observation is probably less trustworthy than an observation reported by several independent and authenticated sources
 - such observations might have the same confidentiality classification, but might have different integrity classifications



Confidentiality and integrity as interdependent aspects (2:2)





How to classify (1:2)

	Confidentiality	Integrity	Availability
Very high	<p>disclosure to unauthorized can cause catastrophic harm</p> <p>enterprise critical and should be read by key personnel only</p> <p>controlled disclosure to authorized</p>	<p>faults may cause wrong decisions with fatal consequences</p>	<p>non-availability is catastrophic, even short disruptions</p>
High			
Medium			
Low	<p>disclosure causes no harm</p> <p>everyone can read</p> <p>owner may decide publishing policy</p> <p>anonymous can read</p>	<p>faults do not effect decision processes</p>	<p>non-availability has marginal impact on enterprise</p>



How to classify (2:2)

Example of integrity levels (?)

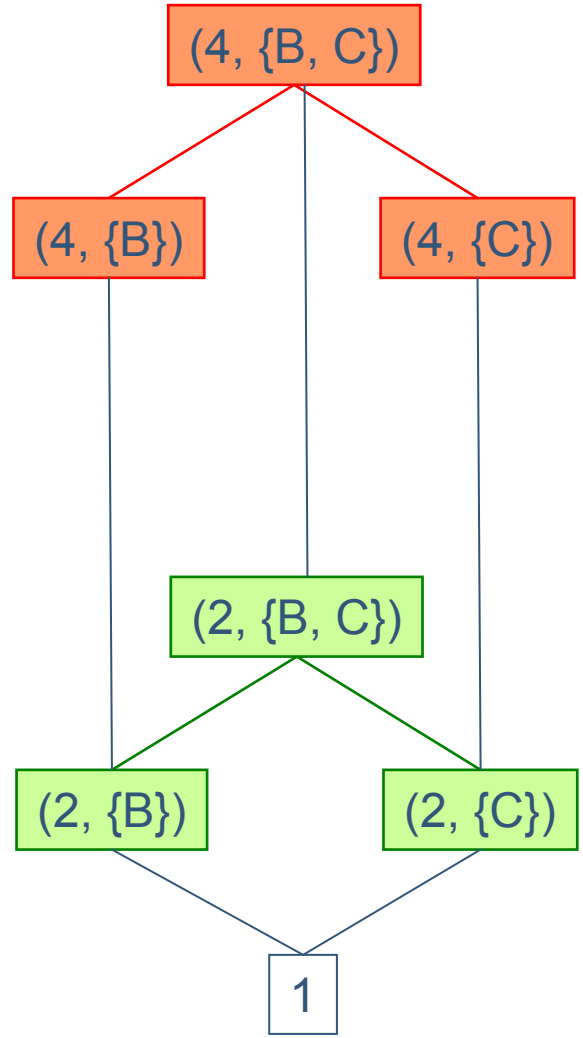
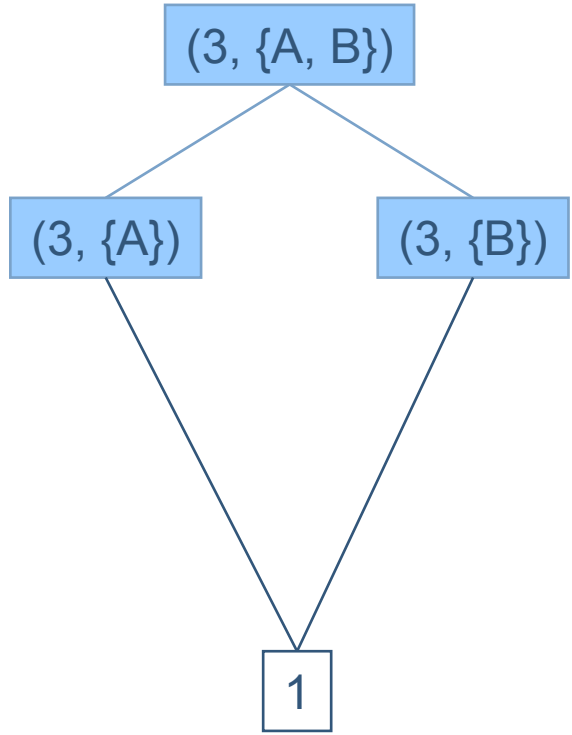
Common Criteria EAL	
7	formally verified design and tested
6	semiformally verified design and tested
5	semiformally designed and tested
4	methodically designed, tested and reviewed
3	methodically tested
2	structurally tested
1	functionally tested
0	unassured

Example of information types from the military domain that should be classified with regard to integrity:

- sensor data about enemy or other units
- single-source information collected by intelligence resources
- products from the intelligence service
- plans and orders
- reporting of own position
- reporting of own operational status
- logistics reporting
- distribution of warnings (e.g. about chemical warfare)
- maps

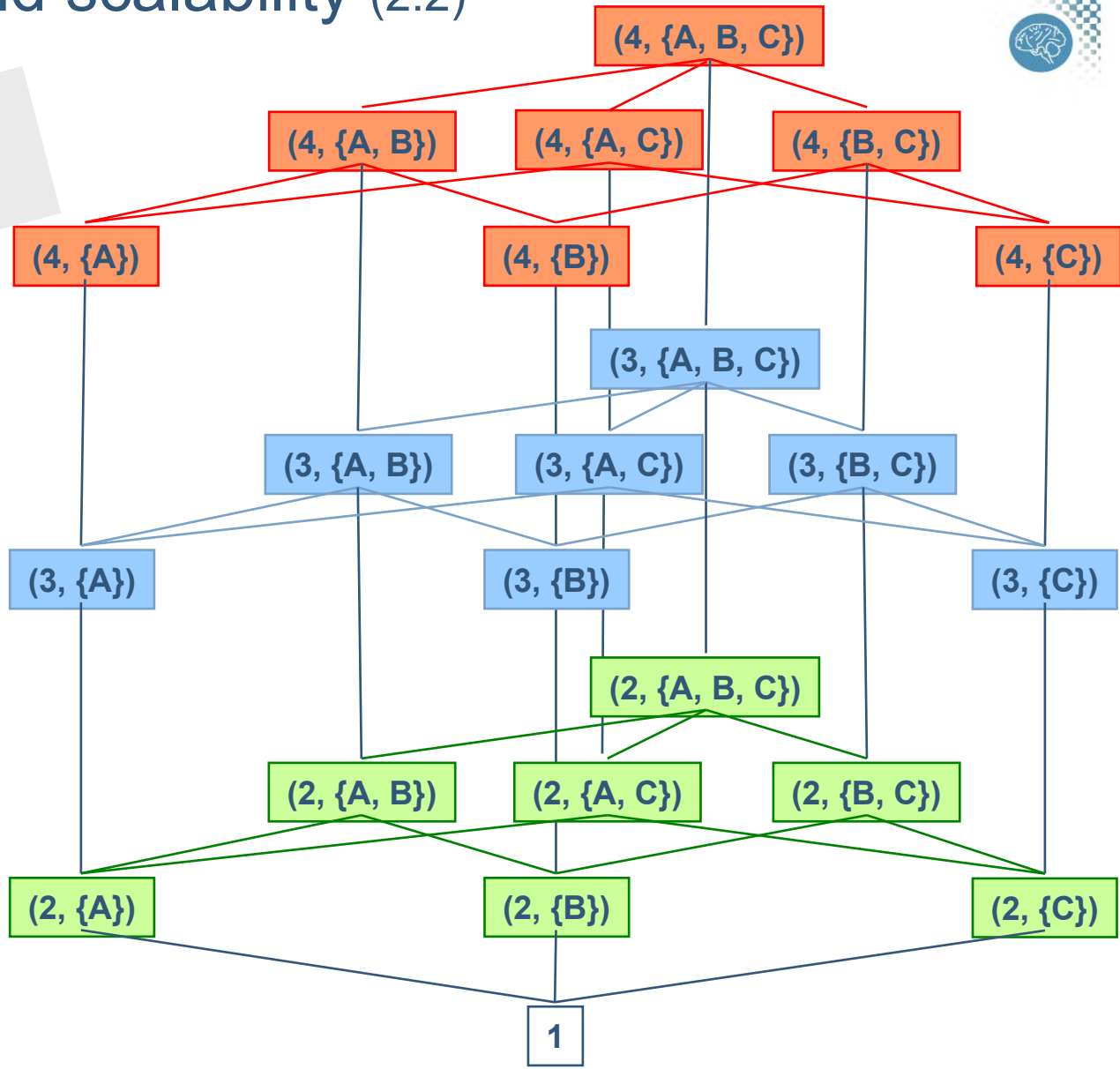
Ole-Erik Hedenstad, FFI

Lattice structure and scalability (1:2)

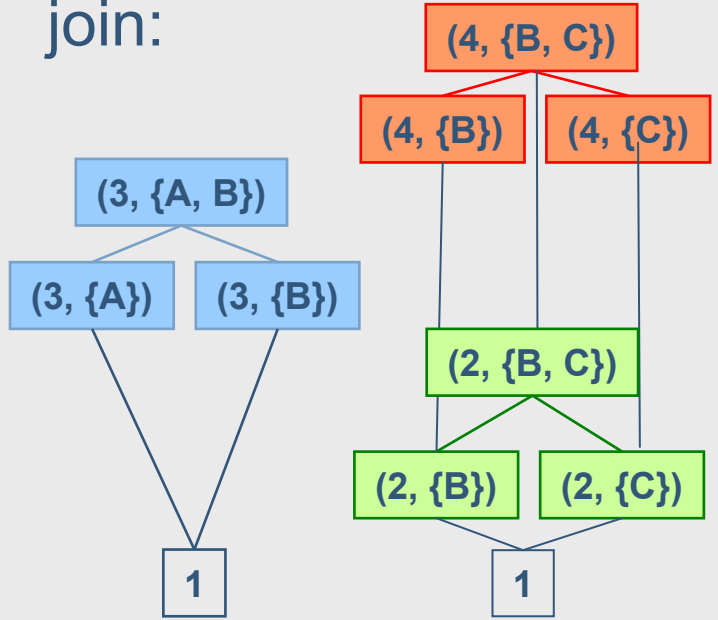


Lattice structure and scalability (2:2)

Models based on complex lattice structures do not scale well!



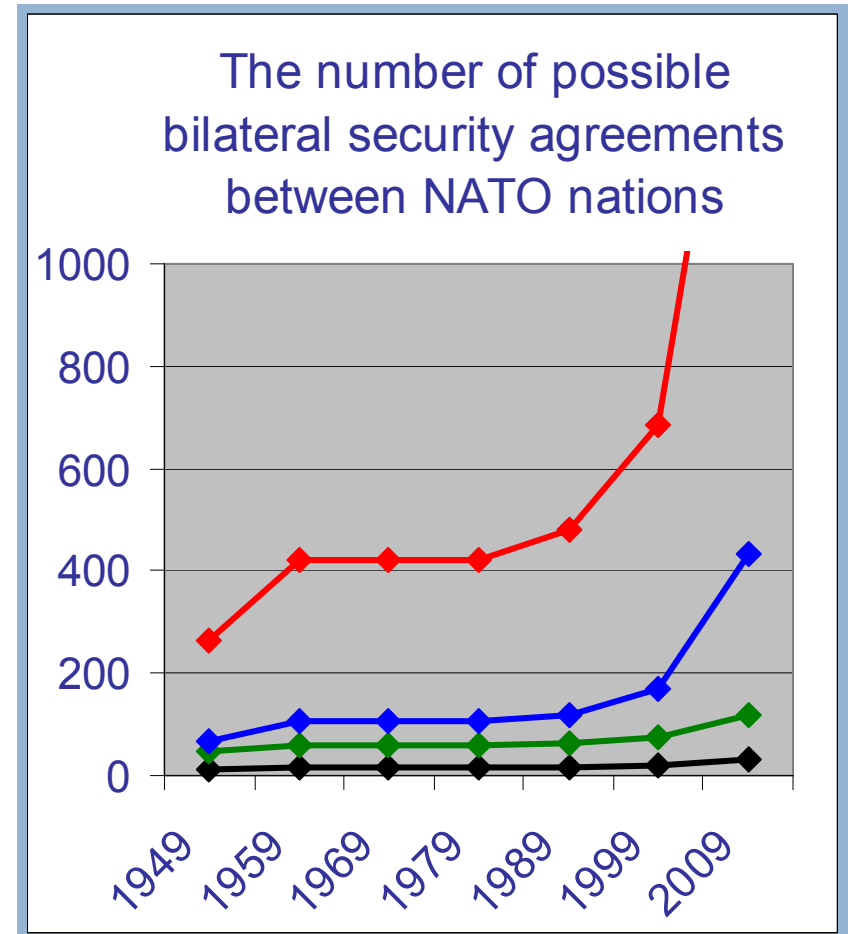
join:





The number of security classes

- The number of security classes in military systems – a threat against security?
- Nations' hierarchical levels may not be compatible
- Bilateral – multilateral agreements
- Commercial organizations?





Simpler class structures – simpler and scalable models

- Multilevel security is needed (confidentiality, integrity, availability..)
 - Is MSL an alternative?
- Are complex structures of security classes necessary?
- Can complex class structures be represented by scalable models?
- ..and implemented by scalable systems?
- How?
- Further research is needed!

- In many contexts, complex class structures are not needed and can be avoided
 - in specific, in environments where communications and processing resources are constrained!

1. Introduction and MLS models

- a. a model of military security classes
- b. MLS confidentiality
- c. MLS integrity
- d. compound MLS models
- e. MSL and MILS

2. Some problems and challenges of current MLS systems

- a. confidentiality and integrity as interdependent aspects
- b. how to classify
- c. lattice structure and scalability
- d. the number of security classes
- e. simpler class structures – simpler and scalable models



Outline

3. A multidimensional MLS model

- a. concept overview
- b. security classes
- c. simple verification of rights
- d. command & control systems
- e. sensor systems
- f. IP routing

4. Conclusive remarks

5. Further work

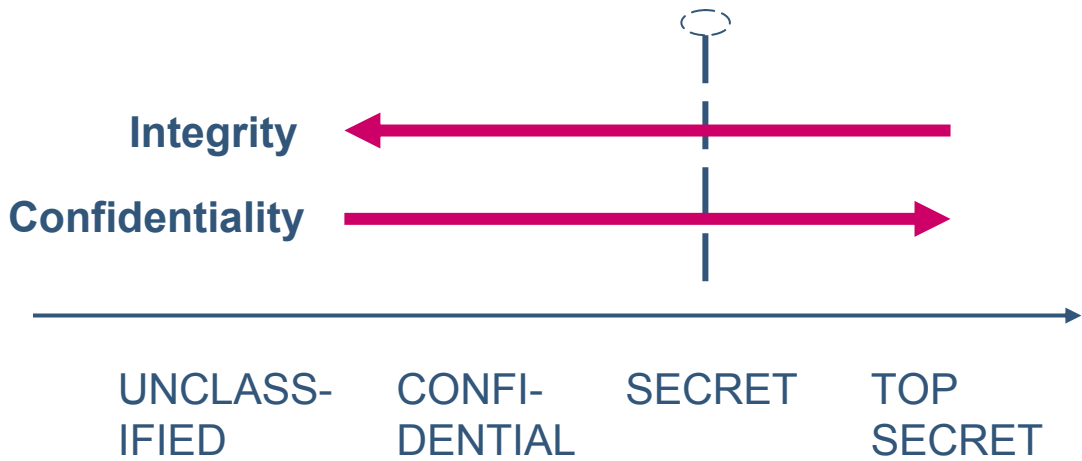


Assumptions

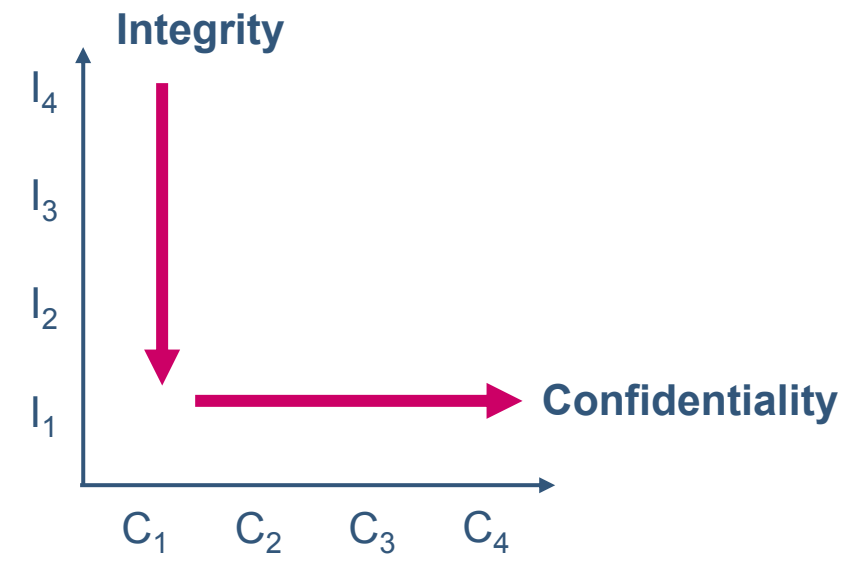
- Confidentiality, integrity and availability are *independent* properties of a generic information object
- Information in a MLS system is stored at its proper security level. For example, a high confidentiality level does not hold information that should be classified to a lower level
- Security labels are assigned to information objects and access labels to subjects (roles)
- RBAC enforces one-directional information flow as well as appropriate discretionary controls
- Procedures outside the model authenticate legitimate entities and check security and access labels for data integrity



Confidentiality and integrity as interdependent aspects

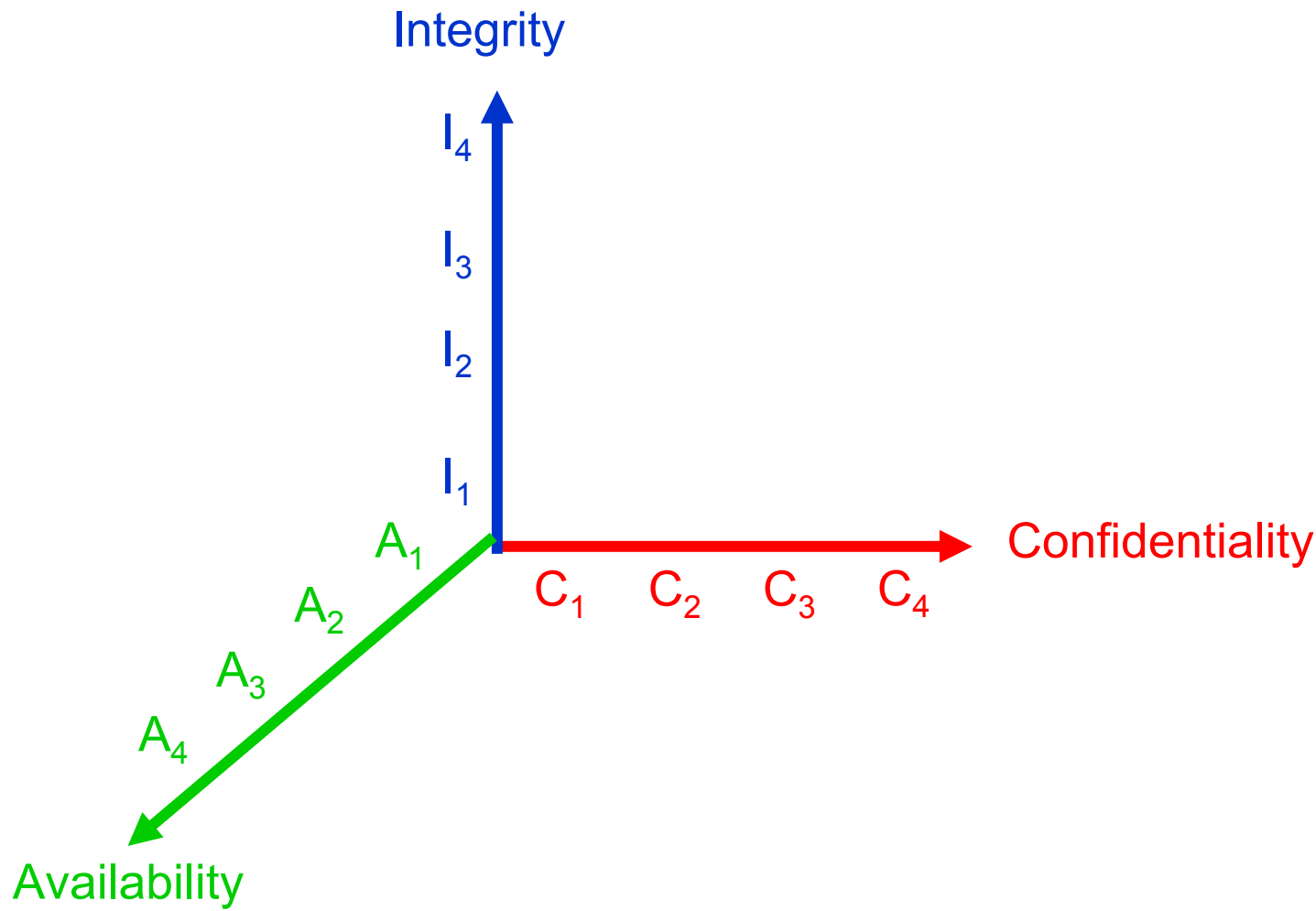


Confidentiality and integrity as independent aspects





Concept overview (1:7)





Concept overview (2:7)

Access rules regarding **confidentiality**

- to enforce one-directional information flow for confidentiality protection, we use the BLP rules on a linear ordered lattice
- using Denning's notation:
 - $SC = \{ C_1, \dots, C_p \}$, where a higher index means more confidentiality (1)
 - The flow operator " \rightarrow " is defined by $C_i \rightarrow C_j$ iff $i \leq j$ (2)
 - The class combining operator \oplus is defined by $C_i \oplus C_j = C_{\max(i, j)}$ (3)
- the rules are satisfied by separate *read* and *write* access
 - *create*, *destroy* and *execute* commands may be regarded as read or *write* commands



Concept overview (3:7)

Access rules regarding integrity

- to enforce one-directional information flow for integrity protection, we use the Biba rules on a linear ordered lattice
- using Denning's notation:

$SC = \{ l_1, \dots, l_q \}$, where a higher index means more integrity (4)

The flow operator " \rightarrow " is defined by $l_i \rightarrow l_j$ iff $i \geq j$ (5)

The class combining operator \oplus is defined by $l_i \oplus l_j = l_{\min(i,j)}$ (6)

- the rules are satisfied by separate *read* and *write* access



Concept overview (4:7)

Access rules regarding **availability**

- we base availability rules on the confidentiality rules (BLP)
- to enforce one-directional information flow for availability, we use the BLP rules on a linear ordered lattice

• using Denning's notation:

$SC = \{ A_1, \dots, A_r \}$, where a higher index means more restrictions (7)

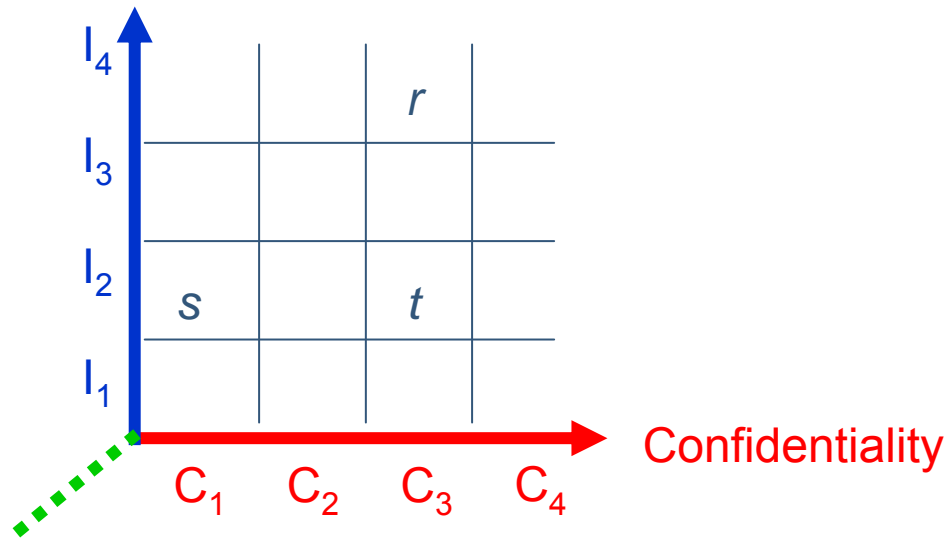
The flow operator " \rightarrow " is defined by $A_i \rightarrow A_j$ iff $i \leq j$ (8)

The class combining operator \oplus is defined by $A_i \oplus A_j = A_{\max(i, j)}$ (9)

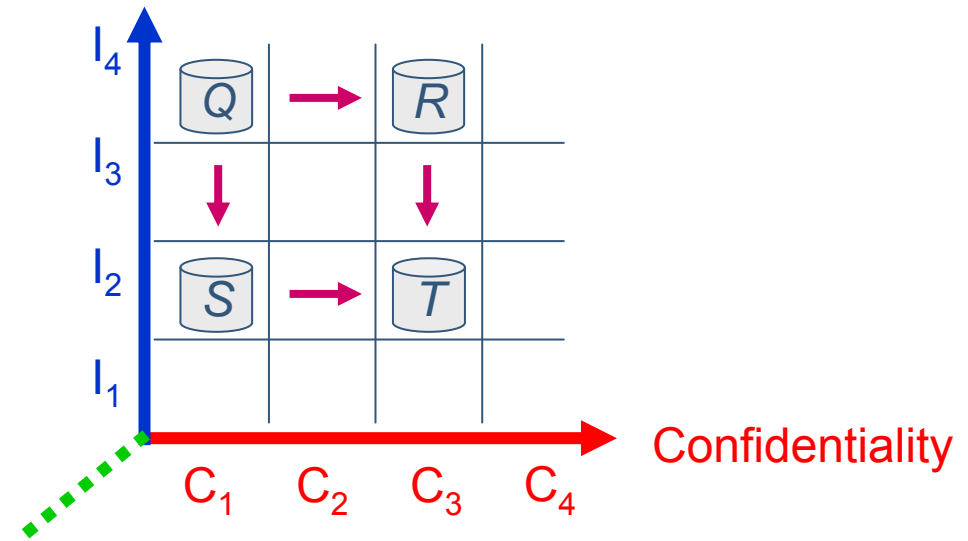
- the rules are satisfied by separate *read* and *write* access

Concept overview (5:7)

Integrity



Integrity



Concept overview (6:7)

The model forms a universally bound lattice, and can as such, not reach an undefined state

Consider two linear ordered lattices:

$(\underline{X}, \rightarrow_x, \oplus_x)$ and $(\underline{Y}, \rightarrow_y, \oplus_y)$

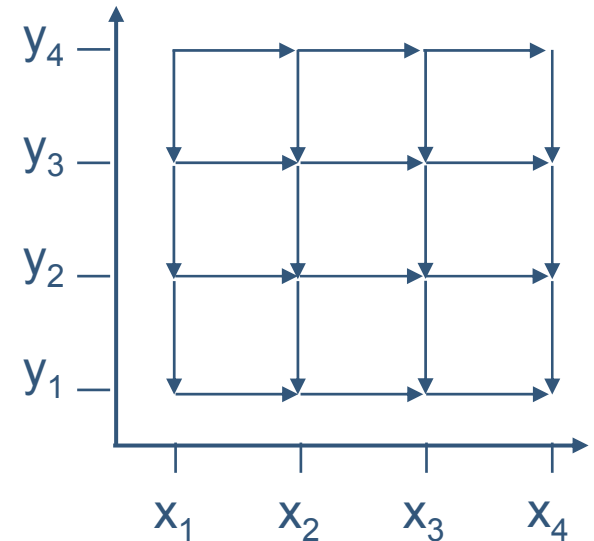
where $\underline{X} = \{x_1, \dots, x_m\}$ and $\underline{Y} = \{y_1, \dots, y_n\}$.

The two-dimensional lattice is described by:

i. $[x_i, y_j] = x_i \cap y_j$

ii. $[x_i, y_j] \rightarrow [x_i', y_j'] = [x_i \rightarrow_x x_i', y_j \rightarrow_y y_j']$

iii. $\oplus = [\oplus_x, \oplus_y]$



$$m = n = 4$$

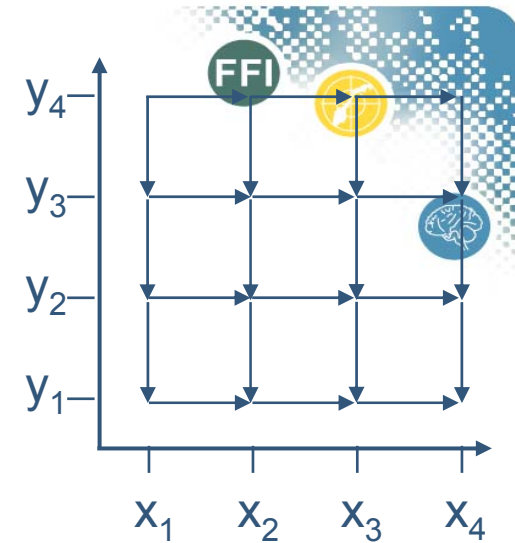
Concept overview (7:7)

Since $(\underline{X}, \rightarrow_x)$ and $(\underline{Y}, \rightarrow_y)$ are partially ordered sets,
then $([\underline{X}, \underline{Y}], \rightarrow)$
is a partially ordered set

Since $(\underline{X}, \rightarrow_x, \oplus_x)$ and $(\underline{Y}, \rightarrow_y, \oplus_y)$ satisfy the lattice properties,
then $([\underline{X}, \underline{Y}], \rightarrow, \oplus)$
must satisfy the lattice properties

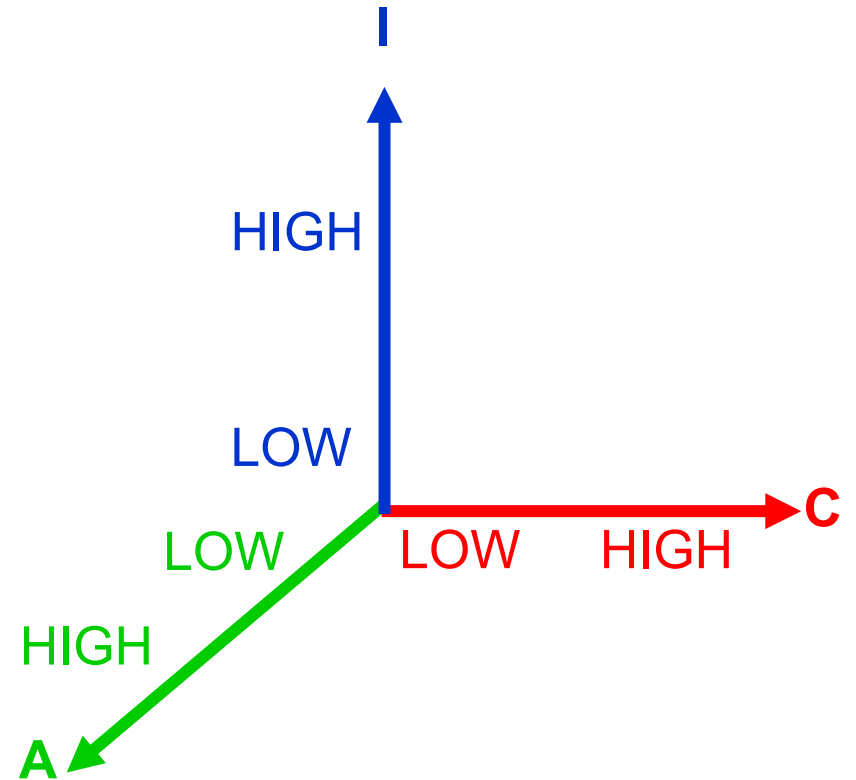
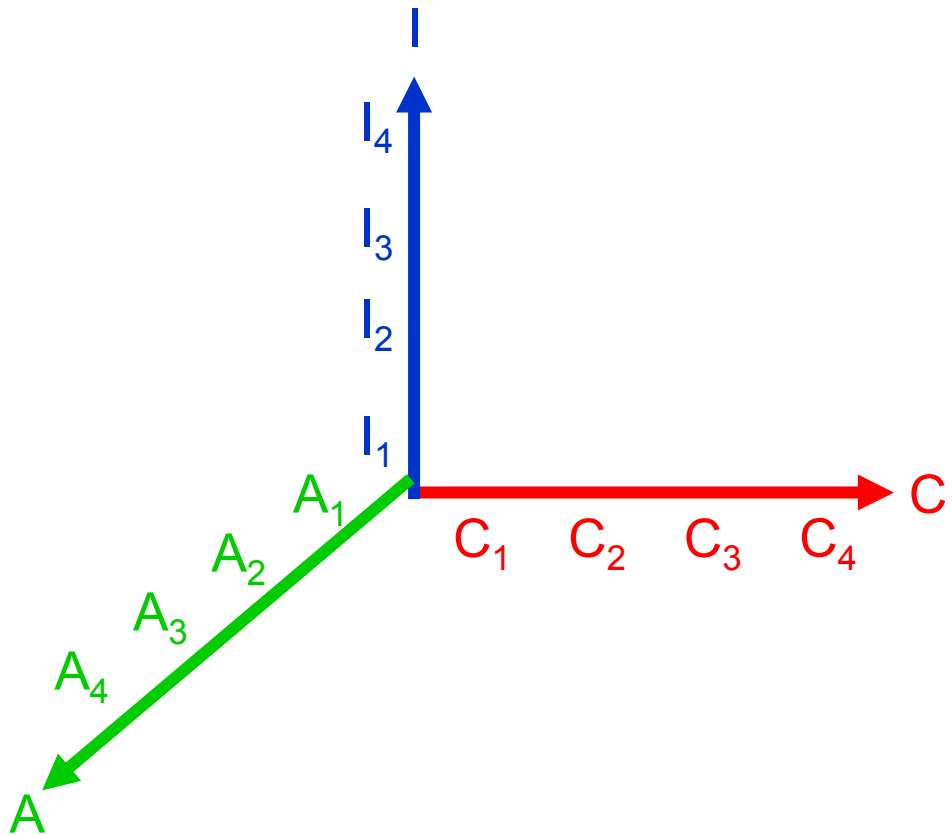
By extension, this holds for any finite number of disjoint linear ordered lattices

Thus, proven techniques for verification and certification of computer processes utilizing the lattice properties may be employed



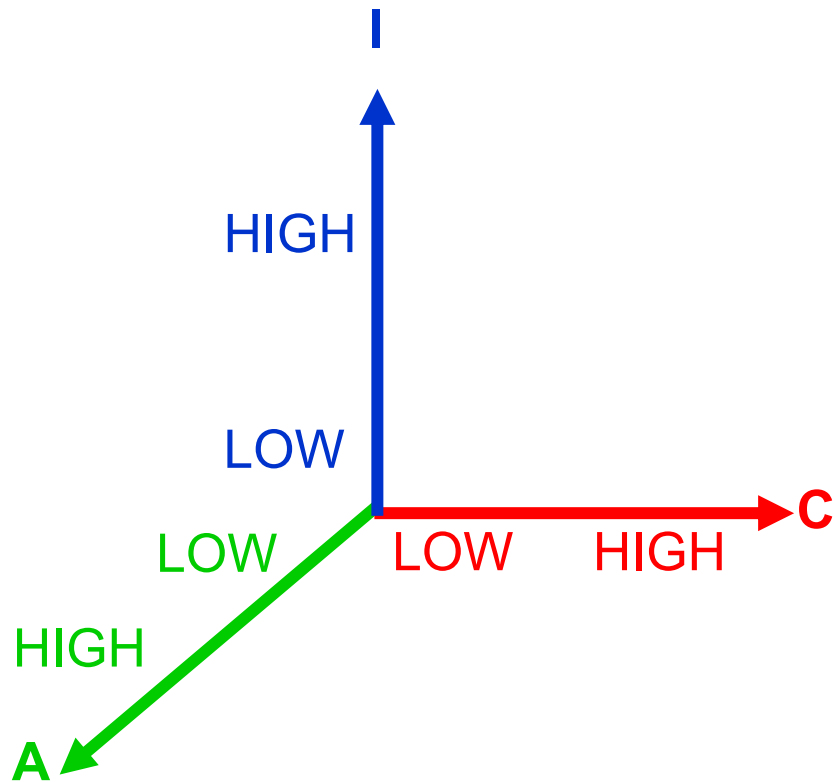


Security classes (1:2)





Security classes (2:2)



Conceptual security classes			
	C	I	A
LLL	LOW	LOW	LOW
LLH	LOW	LOW	HIGH
LHL	LOW	HIGH	LOW
LHH	LOW	HIGH	HIGH
HLL	HIGH	LOW	LOW
HLH	HIGH	LOW	HIGH
HHL	HIGH	HIGH	LOW
HHH	HIGH	HIGH	HIGH



Simple verification of access rights (1:4)

Conceptual security classes

	C	I	A
LLL	LOW	LOW	LOW
LLH	LOW	LOW	HIGH
LHL	LOW	HIGH	LOW
LHH	LOW	HIGH	HIGH
HLL	HIGH	LOW	LOW
HLH	HIGH	LOW	HIGH
HHL	HIGH	HIGH	LOW
HHH	HIGH	HIGH	HIGH

Conceptual access control matrix (read access)

		CLASSIFICATIONS (objects)							
		LLL	LLH	LHL	LHH	HLL	HLH	HHL	HHH
CLEARANCES (subjects)	LLL	r		r					
	LLH	r	r	r	r				
	LHL			r					
	LHH			r	r				
	HLL	r		r		r		r	
	HLH	r	r	r	r	r	r	r	r
	HHL			r				r	
	HHH			r	r			r	r



Simple verification of access rights (2:4)

- Since axes are treated independently, checking read and write access according to clearances is simple
- Separate testing of
 - confidentiality clearance against confidentiality levels,
 - integrity clearance against integrity levels
 - availability clearance against availability levels

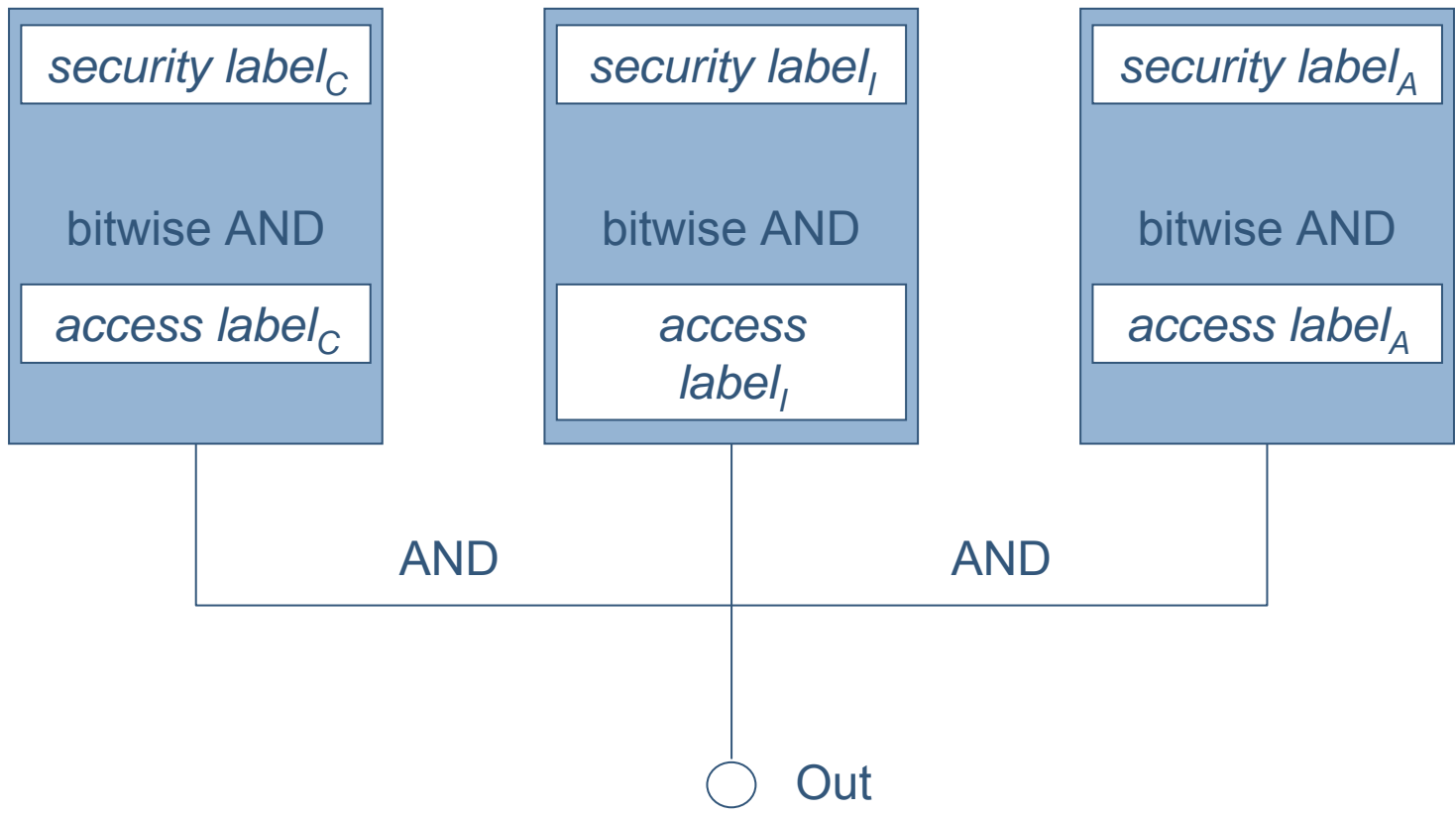
Read access is granted iff {(confidentiality read access)
AND (integrity read access) AND (availability read access)}

Write access is granted iff {(confidentiality write access)
AND (integrity write access) AND (availability write access)}

- Enables an efficient verification algorithm based on simple logical or binary operations



Simple verification of access rights (3:4)



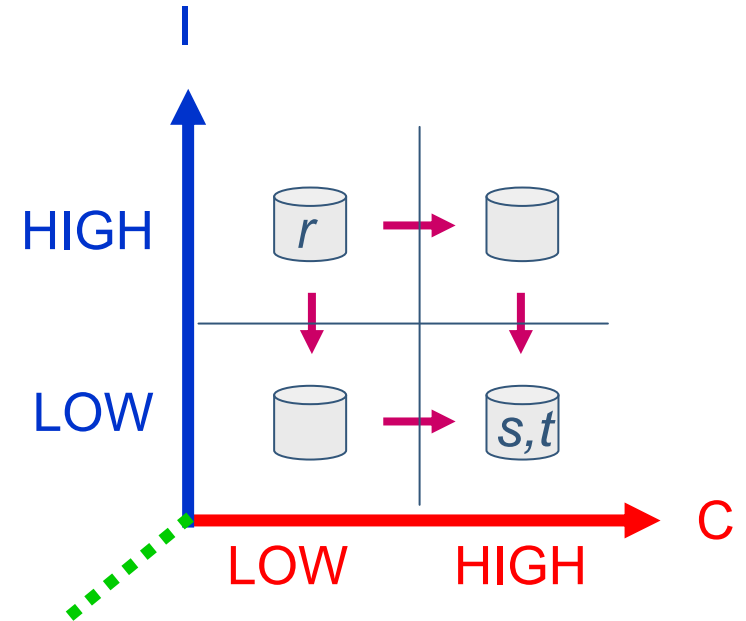
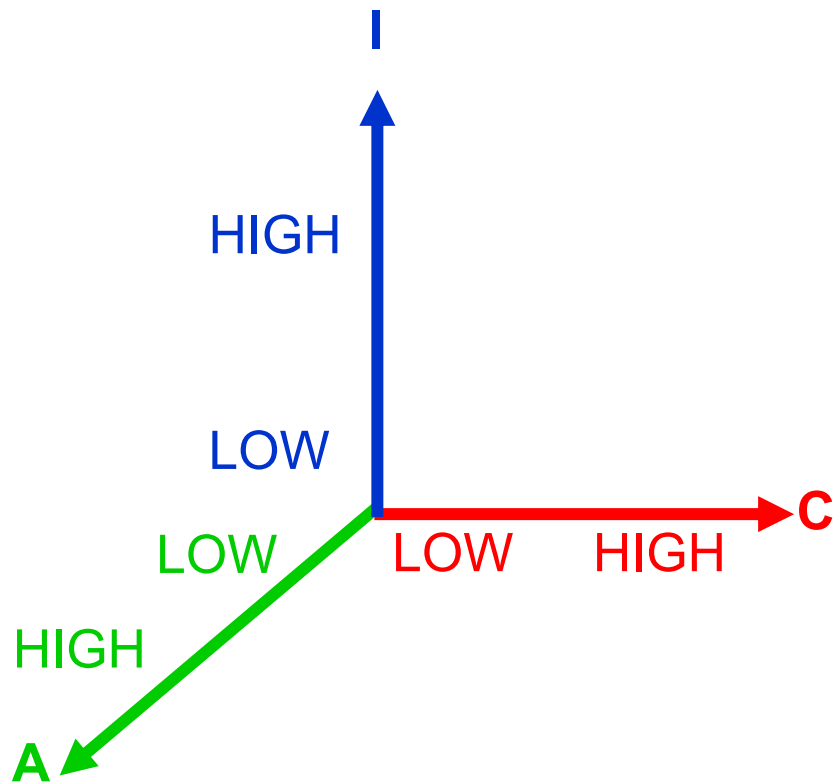


Simple verification of access rights (4:4)

	UNCLASSIFIED	CONFIDENTIAL	SECRET	TOP SECRET
Security label _C	0001	0010	0100	1000
Access label _C	0011	0011	0011	0011
bitwise AND	0001	0010	0000	0000
Evaluates to	TRUE	TRUE	FALSE	FALSE



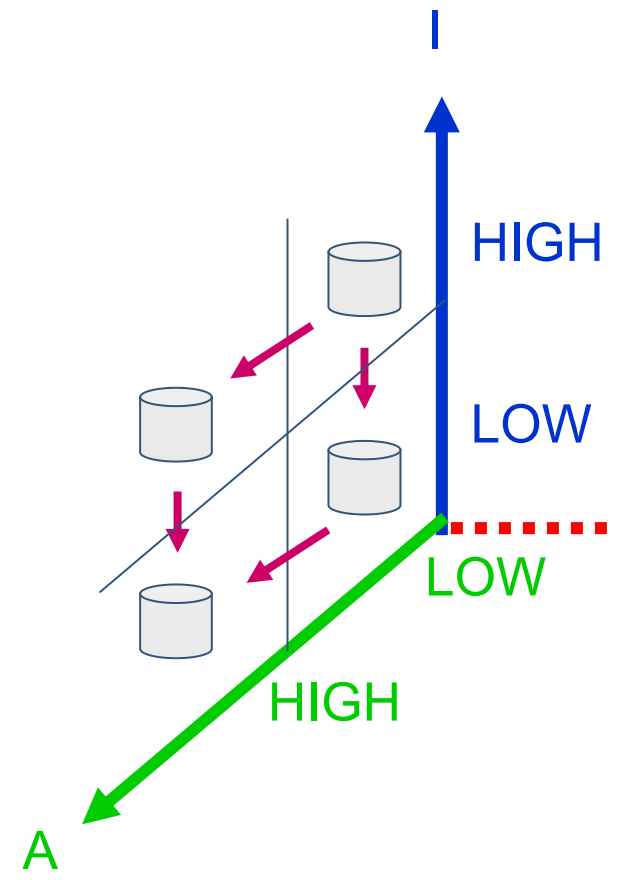
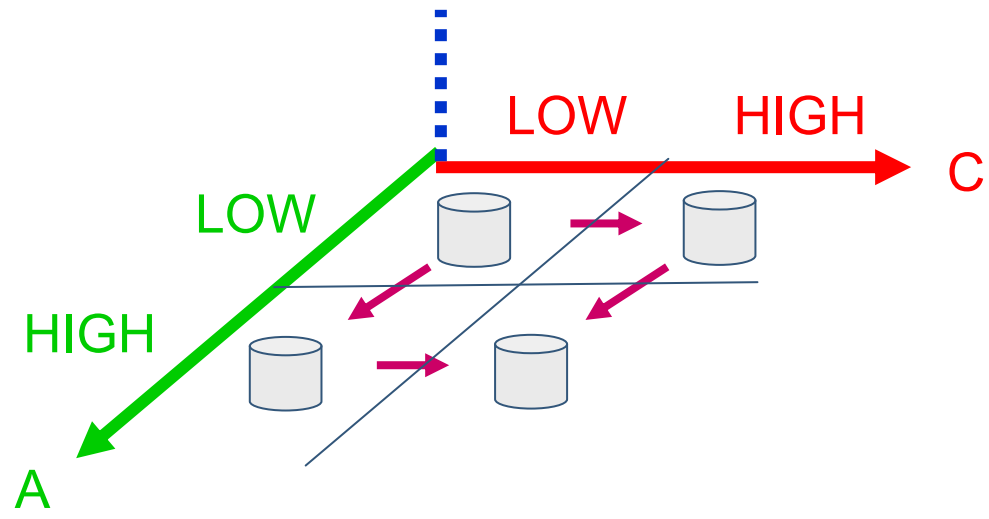
MLS in command & control systems (1:3)



$$Class_{object} = [C_i, I_j, A_k], \quad i, j, k \in \{ LOW, HIGH \}$$



MLS in command & control systems (2:3)





MLS in command & control systems (3:3)

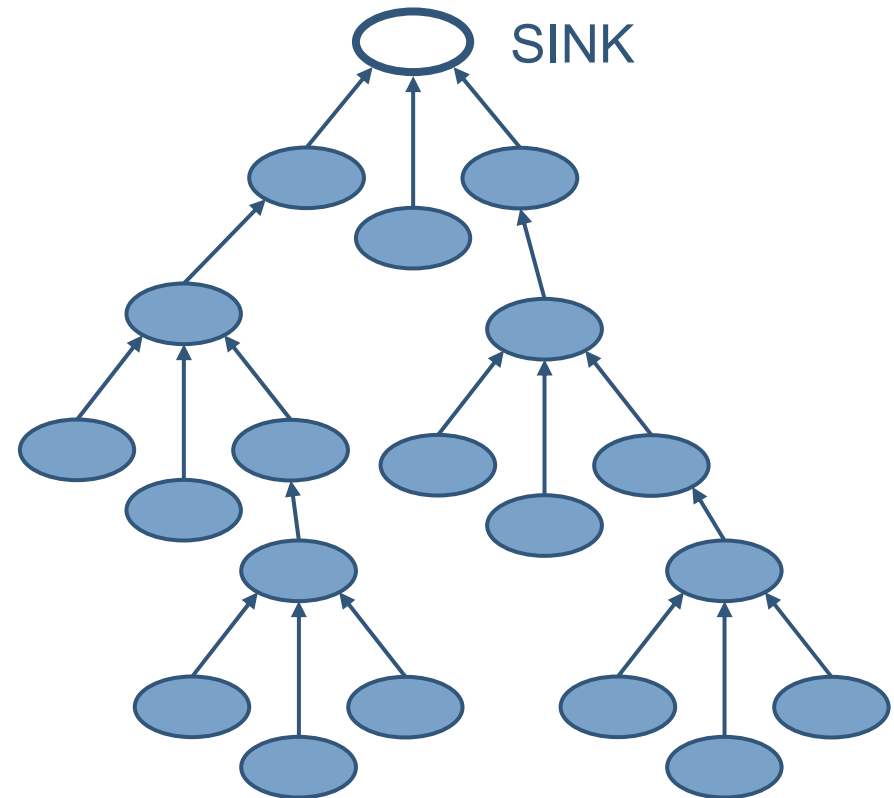
Advantages:

- Increase the quality of battle field information by adding multilevel integrity and availability requirements
- Linearly independent security dimensions facilitates
 - integrity (trustworthiness) of information objects can be handled independently of confidentiality facets
 - integrity requirements and protection of an information objects can be handled independently of confidentiality requirements and protection of that information
 - more automation in decision making
 - clearance for integrity levels is independent of confidentiality clearance
- Ease information sharing in coalition operations
 - multiple levels of availability may be an alternative to the full-blown extended BLP model

MLS in sensor systems (1:4)

Aspects of integrity:

- **Authenticity of origin:**
 - It can be proved that an observation originates from an authorized sensor
- **Authenticity of content:**
 - It can be proved that an observation is not changed by unauthorized
- **Trustworthiness:**
 - Observations reported by several sensors are more trustworthy than observations reported by one single sensor



MLS in sensor systems (4:4)

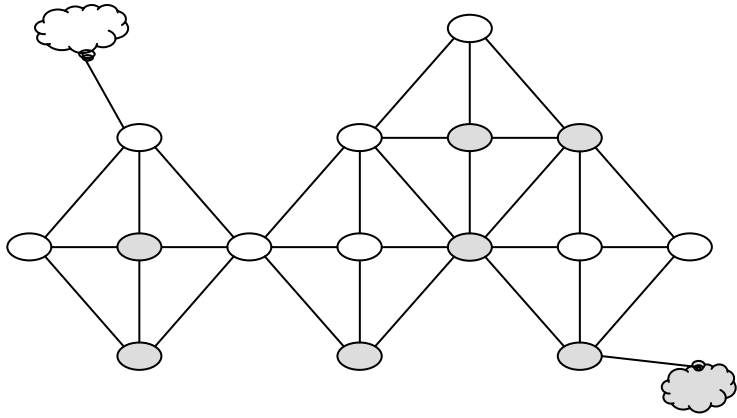
Advantages:

- Distributed evaluation of the trustworthiness of incoming information
- Reduces the cost of information protection by adapting protection mechanisms to the actual consequence of a security breach
- Reduces the cost of information transfer by letting one classified value replace $(I(v_j) * K)$ unclassified values
- Reduces bottle necks close to the sink
- Makes traffic analysis more difficult

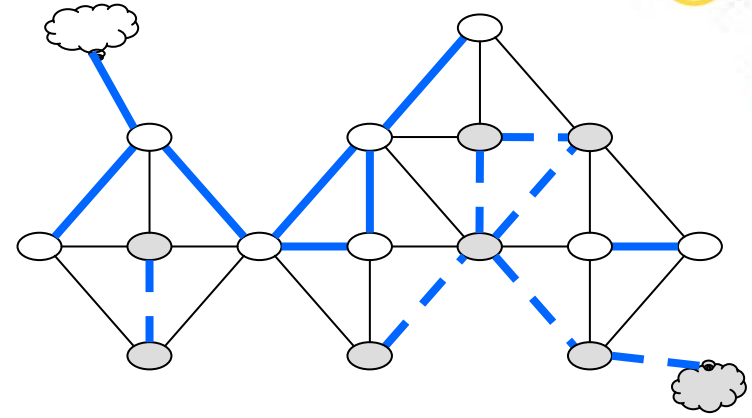


MLS in IP routing (1:7)

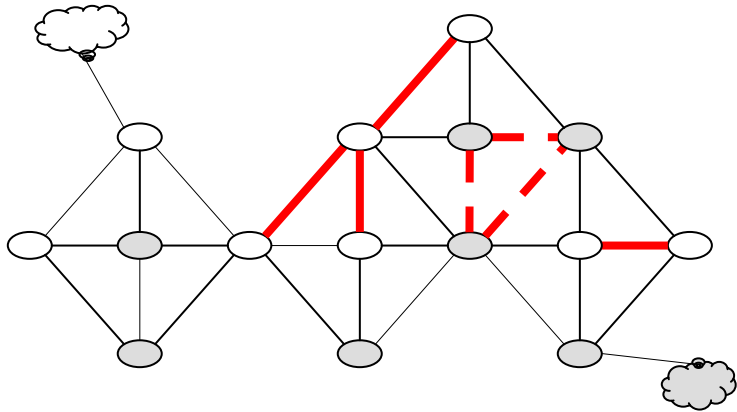
- Setting:
 - coalition IP network
- Enable each partner to:
 - calculate routes from security metrics to know, and partly control, the risk of utilizing a particular route across the unprotected coalition network
 - route packets according to partner-specific security policy. The payload of the IP packet or other security concerns may dictate the selection of routes
- The proposed scheme:
 - does not explicitly provide extra security to the payload
 - intends to provide a safer and more trustworthy packet transport across an unprotected IP network



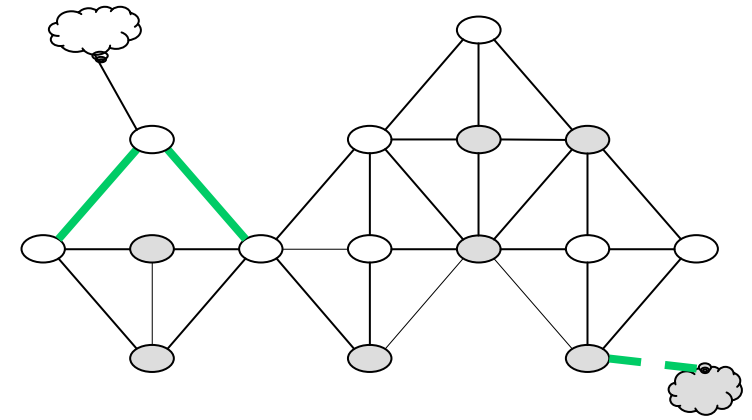
Coalition network of two partner networks (unprotected)



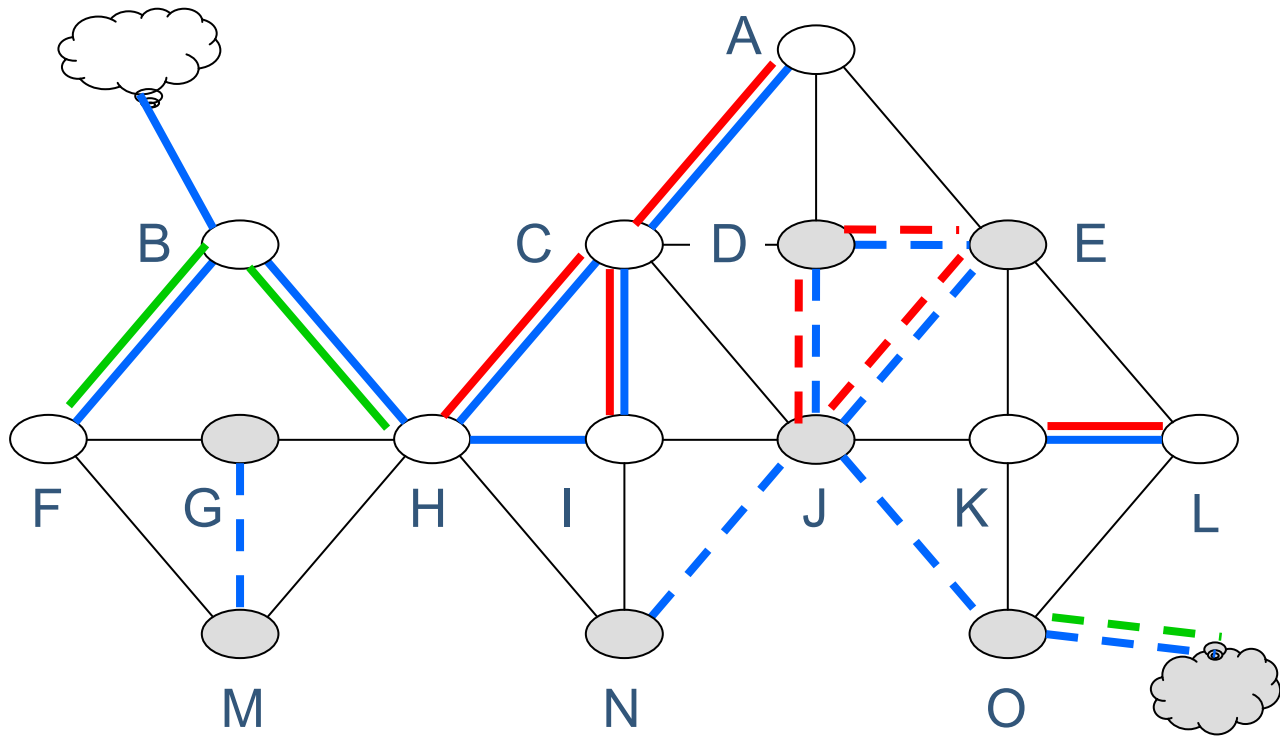
partner-specific logical networks classified to high integrity



partner-specific logical networks classified to high confidentiality



partner-specific logical networks classified to high availability



user information	Access label: H H H	Source: A	Destination: B
------------------	--	-----------	----------------



user information	Access label: L L L	Source: J	Destination: B
------------------	--	-----------	----------------



user information	Access label: L L L	Source: C	Destination: N
------------------	--	-----------	----------------

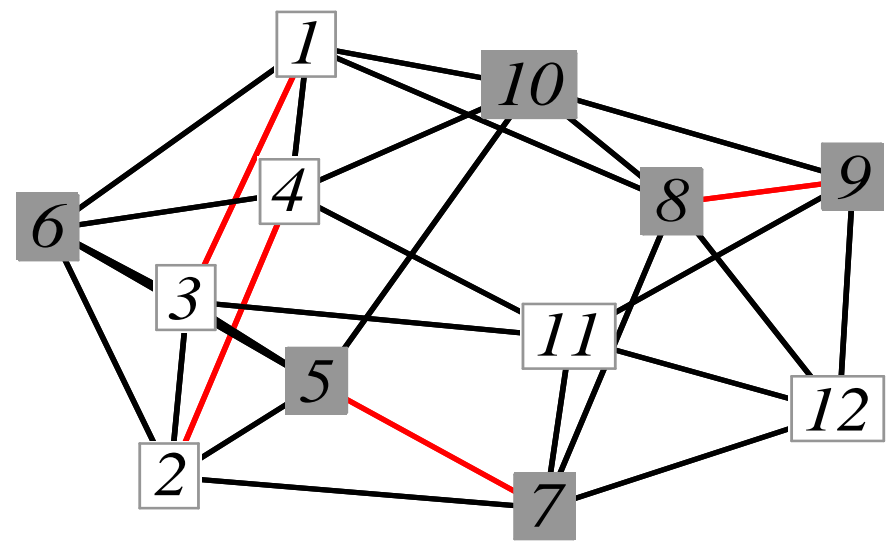
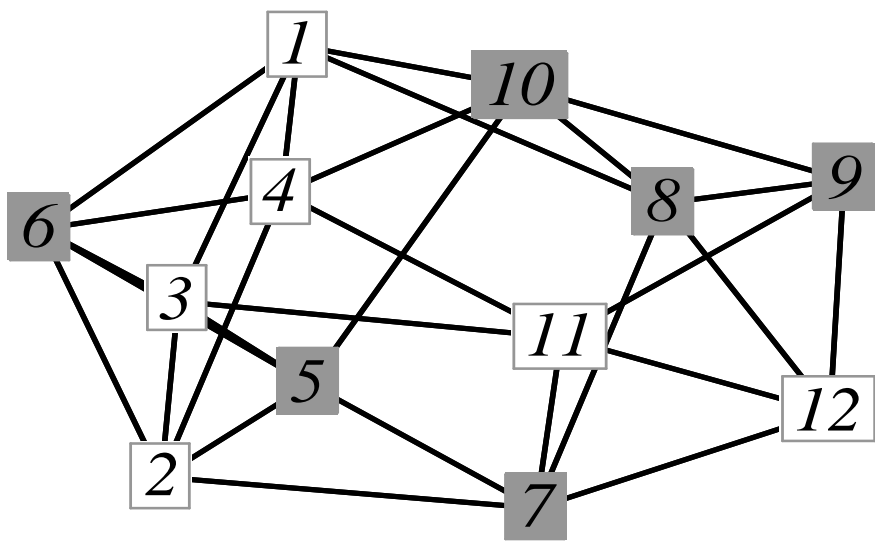


user information	Access label: H L H	Source: B	Destination: L
------------------	--	-----------	----------------



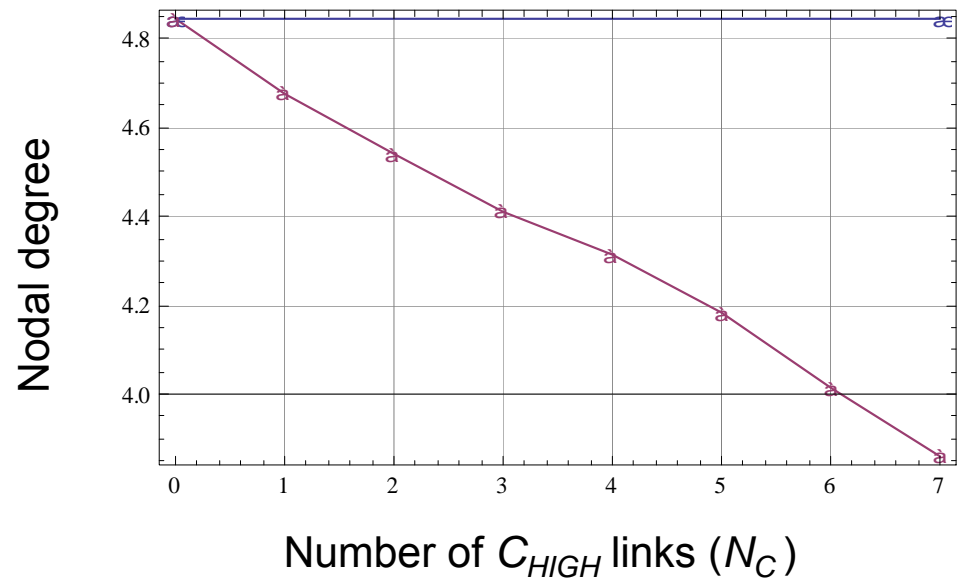
MLS in IP routing (3:7)

Confidentiality classification, an example (I:II)

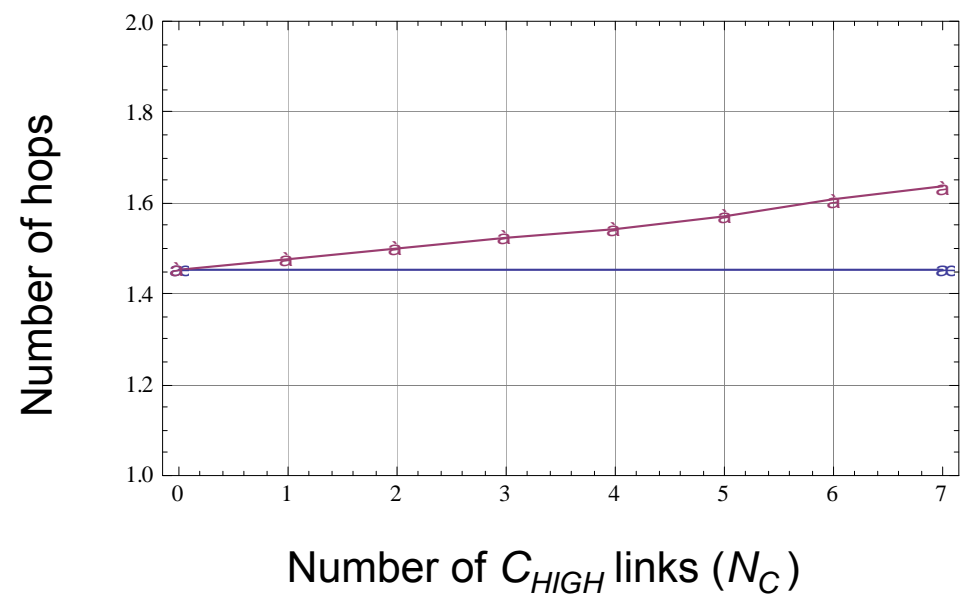


nodal degree: 5
network size: 2 x 6

MLS in IP routing (4:7)



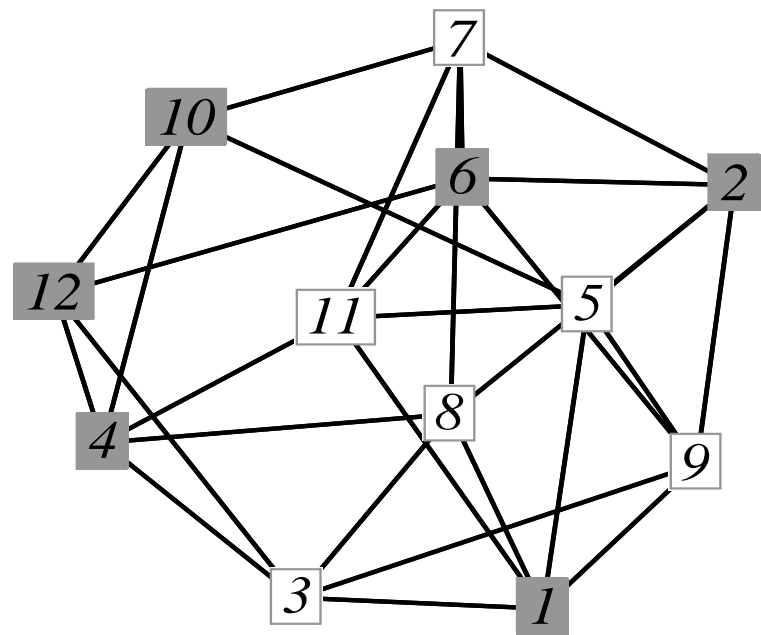
Confidentiality classification, an example (II:II)



MLS in IP routing (5:7)

Availability classification,
an example (I:II)

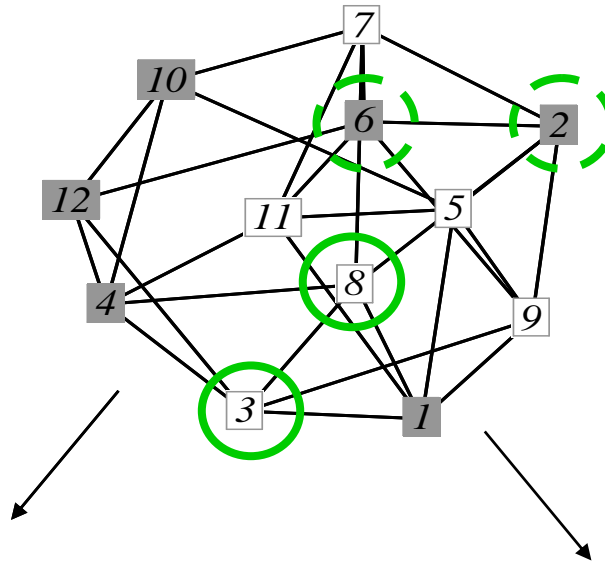
Unclassified



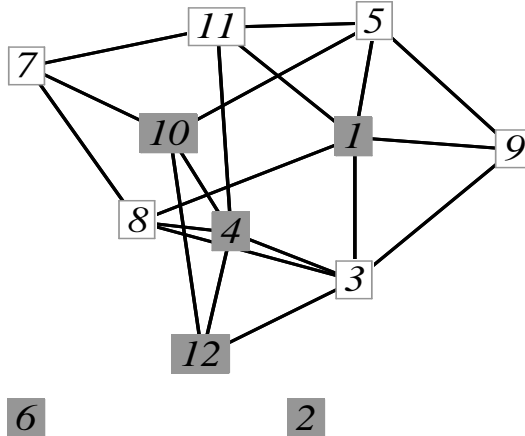
nodal degree: 5
network size: 2 x 6

MLS in IP routing (6:7)

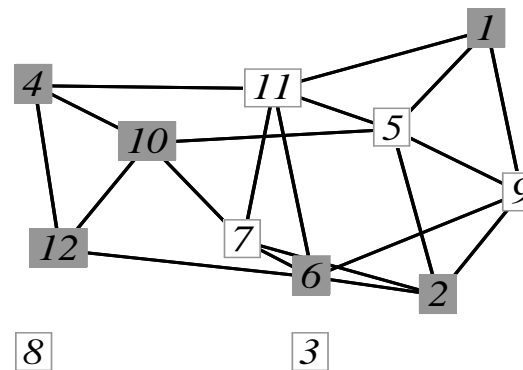
Availability classification, an example (II:II)



The network seen by those not cleared for the grey partners A_{HIGH} links.



The network seen by those not cleared for the white partners A_{HIGH} links.





MLS in IP routing (7:7)

Advantages:

- An alternative to multiple physically separated networks, by enabling:
 - levels of integrity
 - establish routes that exclusively involve a partner's routers
 - levels of confidentiality
 - make traffic analysis of network topology inconvenient
 - levels of availability
 - restrict the use of specific network resources, independently of integrity and confidentiality clearances.
- Partner specific classifications of links and routes versus coalition network connectivity:
 - integrity classification does not affect connectivity
 - confidentiality classification seems to have minor impact on connectivity
 - availability classification may have major impact on connectivity



Conclusive remarks (1:2)

- MLS is needed in military (and commercial) ICT systems
- Systems built from classic MLS models turned out to be complex, expensive and impractical, but the core ideas are still valid
- Some applications benefit from more security dimensions and fewer security levels than traditional MLS models can support
 - different security aspects (dimensions) can be handled as mutual independent properties of information
 - in specific, compartments/categories of traditional MLS models may be modeled as one or more linearly ordered availability classes



Conclusive remarks (2:2)

- The proposed multidimensional MLS concept does not provide the richness and granularity of traditional MLS-systems, but may adapt better to practical lightweight applications
- Verification of rights can be simplified, by requiring each security dimension to be a simple linear ordered lattice
 - the concept enables a scheme that verify allowed information flow along several axes within a few clock cycles
 - logical port circuits may implement the method
- Possible applications of multidimensional MLS include databases, OS security, information flow control on programs, file systems, file servers, secure access to web services and MLS for IP routing



Further work at FFI

- Formal in-depth studies of potential applications in databases, operating systems, communications networks, sensors
- Ongoing work
 - Study on multilevel integrity
 - MLS in IP routing
 - MLS in sensor systems
 - MLS file servers
- Do you want to cooperate in this work?



References (1:2)

- Bell, D.E. and LaPadula, L.J. (1975), "Secure Computer Systems, Mathematical Foundations", *Mitre Corp. Report No. MTR-2547*, Bedford, Mass., USA.
- Biba, K.J. (1977), "Integrity Considerations for Secure Computer Systems", *Mitre Corp. Report No. MTR-3153*, Bedford, Mass., USA.
- Bishop, M. (2003), "Computer Security: Art and Science", ISBN 0-201-44099-7, Addison-Wesley, pp 95-99.
- Denning, D.E. (1976), "A Lattice Model of Secure Information Flow", *Communications of the ACM*, vol. 19, No. 5, pp. 236-243.
- Galik, D. and Tretick, B. (1991), "Fielding Multilevel Security into Command and Control Systems", *Proceedings of the 7th Annual Computer Security Applications Conference*, pp. 202-208.
- Hoffman, P. (Ed.) (1999), "Enhanced Security Services for S/MIME", *Internet Engineering Task Force (IETF) rfc 2634*.
- Housley, R. (1993) "Security Label Framework for the Internet", *Internet Engineering Task Force (IETF) rfc 1457*.
- Huang, Q. and Shen, C. (2004), "A New MLS Mandatory Policy Combining Secrecy and Integrity Implemented in Highly Classified Secure Level OS", *Proceedings of the 7th International Conference on Signal Processing (ICSP'04)*, vol. 3, pp. 2409-2412.
- Irvine, C.E., Levin, T.E., Nguyen, T.D., Shifflett, D., Khosalim, J., Clark, P.C., Wong, A., Afinidad, F., Bibighaus, D. and Sears, J. (2004), "Overview of a High Assurance Architecture for Distributed Multilevel Security", *Proceedings of the 2004 IEEE Workshop on Information Assurance and Security*, pp. 38-45.
- Kang, J.-M., Shin, W., Park, C.-G. and Lee, D.-I. (2001), "Extended BLP Security Model Based on Process Reliability for Secure Linux Kernel", *Proceedings of the 2001 Pacific Rim International Symposium on Dependable Computing*, IEEE Computer Society, pp. 299-303.
- Kuhn, D.R. (1998), "Role Based Access Control on MLS Systems Without Kernel Changes", *3rd ACM Workshop on Role-Based Access Control*.



References (2:2)

- Landwehr, C.E., Heitmeyer C.L. and McLean, J.D. (1984), "A Security Model for Military Message Systems", *ACM Transactions on Computer Systems*, vol. 2, No. 3, pp. 198-222.
- Lipner, S. (1982), "Non-Discretionary Controls for Commercial Applications", *Proceedings of the 1982 IEEE Symposium on Security and Privacy*, pp. 2-10.
- Liu, Y. and Li, X. (2005), "Lattice Model Based on a New Information Security Function", *Proceedings of the Eight International Symposium on Autonomous Decentralized Systems (ISADS 2005)*, pp. 566-569.
- Neugent, B. (1994), "Where We Stand in Multilevel Security (MLS): Requirements, Approaches, Issues, and Lessons Learned", *Proceedings of the 10th Annual Computer Security Applications Conference*, pp. 304-305.
- Osborne, S., Sandhu, R. and Munawer, Q. (2000), "Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies", *ACM Transactions on Information and System Security*, vol. 3, No. 2, pp 85-106.
- Sandhu, R.S. (1993), "Lattice-Based Access Control Models", *IEEE Computer*, vol. 26, No. 11, pp. 9-19.
- Sandhu, R.S., Ferraiolo, D., Gavrila, S., Hu, V. and Kuhn, R. (2000), "The NIST Model for Role-Based Access Control: Towards A Unified Standard", *Proceedings of the 5th ACM Workshop on Role Based Access Control*.
- Shirey, R.W. (2000), "Internet Security Glossary", *Internet Engineering Task Force (IETF) rfc 2828*.
- Winjum, E. and Mølmann, B.K (2008), "A Multidimensional Approach to Multilevel Security", *Information Management & Computer Security*, vol. 16, issue 5, 2008.
- Winjum, E. and Berg, T.J. (2008), "Multilevel Security for IP Routing", *Proceedings of the IEEE Military Communications Conference 2008 (MILCOM 2008)*, San Diego, California, USA, November 2008.