

MILS-CORBA Status Report

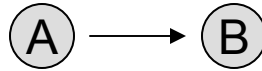
Jim Alves-Foss
Scott Harrison*
Paul Oman
and UI MILS-CORBA Student Team

University of Idaho

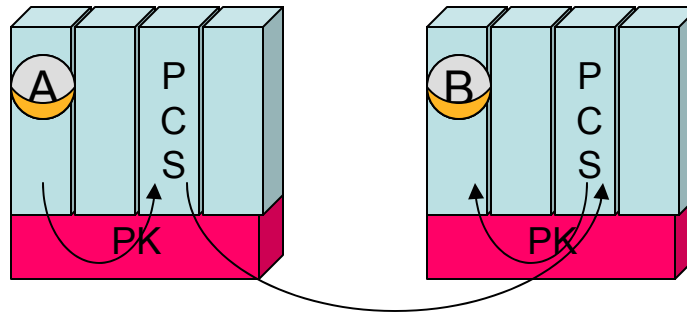
Tasks

- Protection Profile
- Formal Methods
 - ACL2 Model of Information Flow
 - model of secure message passing filter
 - Formal Model of Security Policy
 - developing model for distributed system
 - SPARK (Safe ADA subset)
 - code and proofs of secure message passing filter

Designer wants A to send
a message to B



Implementer maps A and B to partitions



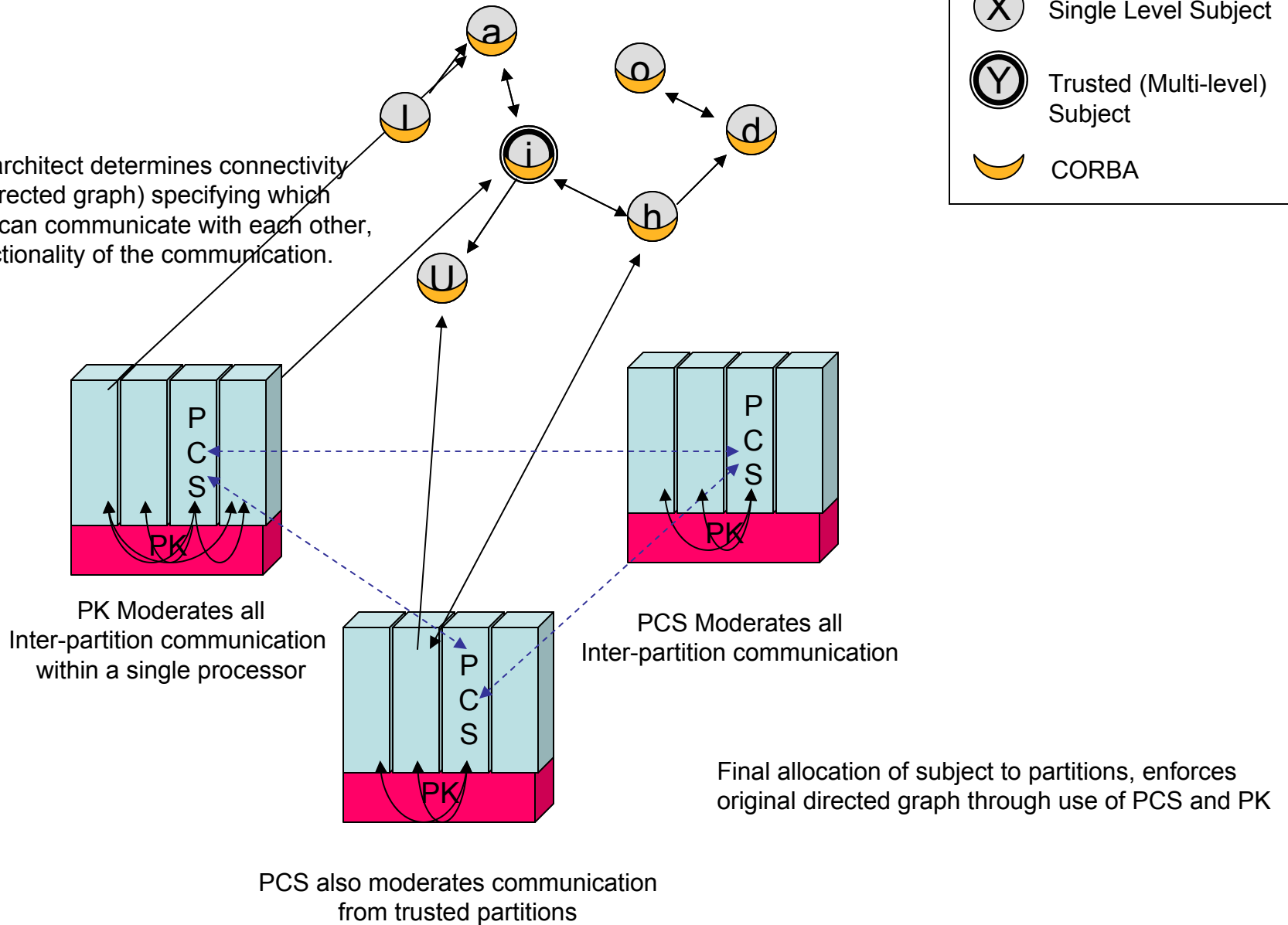
MILS CORBA, with help of
PCS, manages communication,
satisfying the security policy.

System architect maps subjects to partitions.

Key

- (X) Single Level Subject
- (Y) Trusted (Multi-level) Subject
- ☾ CORBA

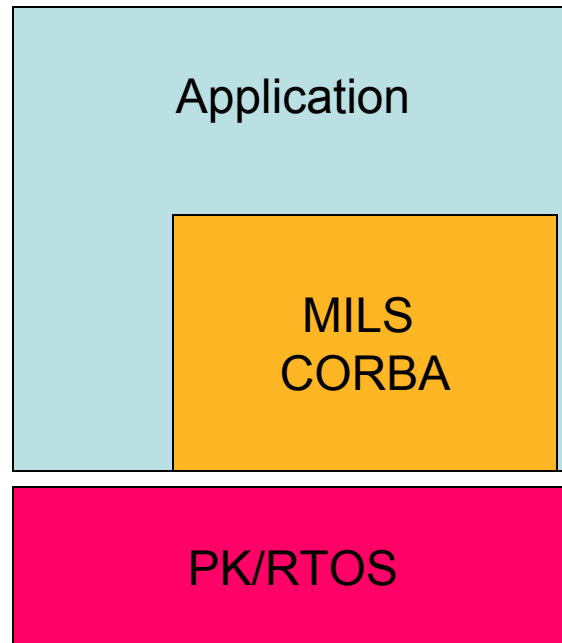
System architect determines connectivity graph (directed graph) specifying which subjects can communicate with each other, and directionality of the communication.

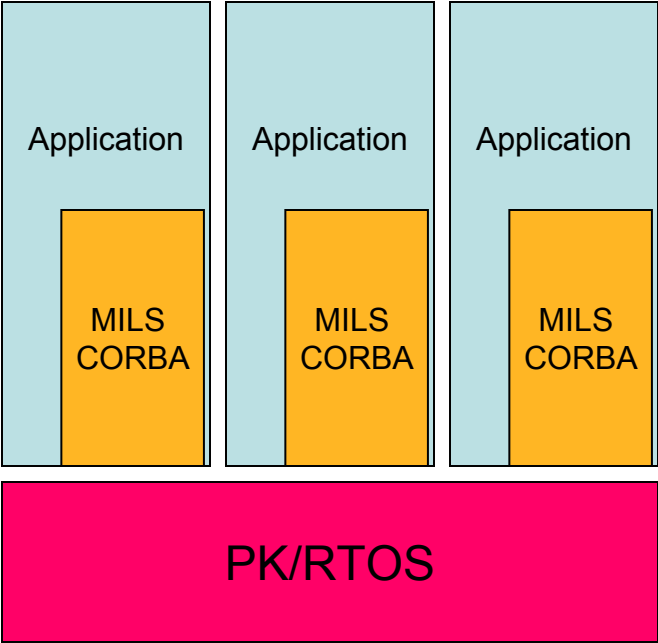


MILS CORBA

A verified library that provides a subset of CORBA functionality to support MLS applications.

- Processes application requests correctly
- Protects itself and app from incoming message





(Draft) MILS CORBA Protection Profile

Definitions/Descriptions

- 7 Security Policies
- 4 Working Assumptions (mostly about the PK)
- 23 Threats
- 13 Security Objectives
- 21 Functional Requirements
- 33 Assurance Requirements

(Draft) MILS CORBA Protection Profile

Security Policies

Consistent with the PK PP

- P.UNIQUE_PARTITION
- P.DATA_ISOLATION
- P.INFO_FLOW
- P.CLEAR_RESIDUAL

Consistent with DOD DCID 6-3

- P.CONFIDENTIALITY
- P.INTEGRITY
- P.AVAILABILITY

(Draft) MILS CORBA Protection Profile Mappings

- Security Policies X Security Objectives
- Threats X Security Objectives
- Objectives X Assumptions
- Objectives X Functional Requirements
- Objectives X Assurance Requirements

(Draft) MILS CORBA Protection Profile

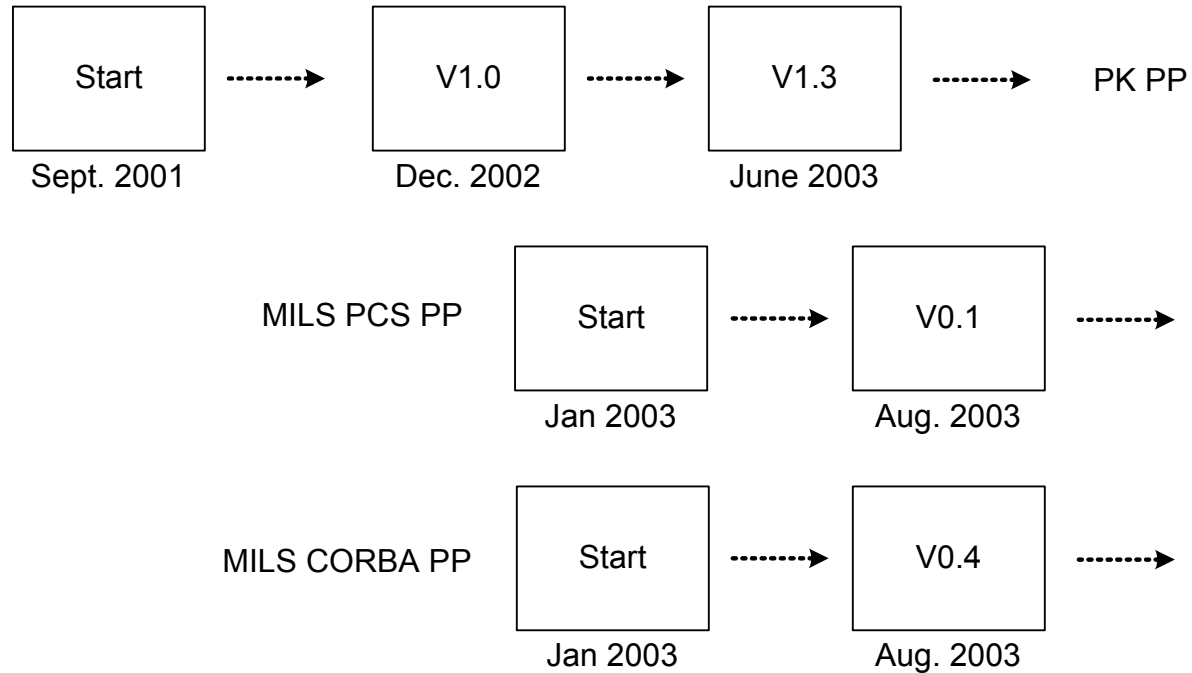
Threats

- T.O_ACCESS_TOE
- T.O_AUDIT_CONF_TOE
- T.O_AUDIT_CORRUPTED_TOE
- T.O_ORB_CORRUPT
- T.O_CRASH_TOE
- T.O_DOS
- T.O_FLOOD
- T.O_INSTALL
- T.O_NAMING_CORRUPT
- T.O_LOADED
- T.O_RECORD_EVENT_TOE
- T.O_REPOSITORY_CORRUPT
- T.O_RESOURCES_TOE
- T.O_TIMING_LEAK
- T.O_TRACEABLE_TOE
- T.O_UNAUTHORIZED_ACCESS
- T.O_UNSANITIZED
- T.O_WRONG_CODE
- T.O_PLATFORM_FAILURE
- T.O_MASQUERADE_SYSTEM
- T.O_MASQUERADE_REQUEST
- T.O_MASQUERADE_OWNER
- T.O_EXPLOIT_VULNERABILITY

(Draft) MILS CORBA Protection Profile Requirements X Security Matrix (Excerpt)

	U N I Q U E	D A T A	N O N	N O N				V A L I D A T E D		S E C U R E
	P A R T I T I O N	I S O L A T I O N	I N T E R F E R E N C E	M A S Q · I N F O F L O W	A U D I T	K N O W N	I N F O F L O W	C O M M	C O N F I G	L O A D
FAU_ARP.1					X		X	X		
FAU_GEN.1					X					
FAU_SAA					X					
FAU_SAR.1					X					
FCO_NRO.2				X		X	X	X		
FDP_ACC.2		X					X	X		
FDP_ACF.1								X		
FDP_DAU.1			X	X						
FDP_IFC.2				X			X			

Protection Profile Timeline



Proposed Timeline

