



**Institute for Defense Analyses**  
1801 N. Beauregard Street • Alexandria, Virginia 22311-1772

## ***Management of Strong Access Control***

**Edward A. Schneider**  
**eschneider@ida.org**  
**26 September 2000**

03/16/99-1

© 2000 Edward A. Schneider. Permission to make digital or hard copies of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice.



## **Overview**

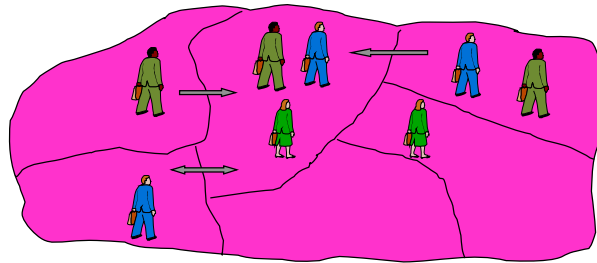
- **Information Families**
- **Flexible Policies**
- **Management issues**

03/16/99-2

© 2000 Edward A. Schneider. Permission to make digital or hard copies of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice.



## Information Families



Collection of data objects

- Subjects that can access it
- Security policy

03/16/99-3

© 2000 Edward A. Schneider. Permission to make digital or hard copies of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice.



## Strong Access Control

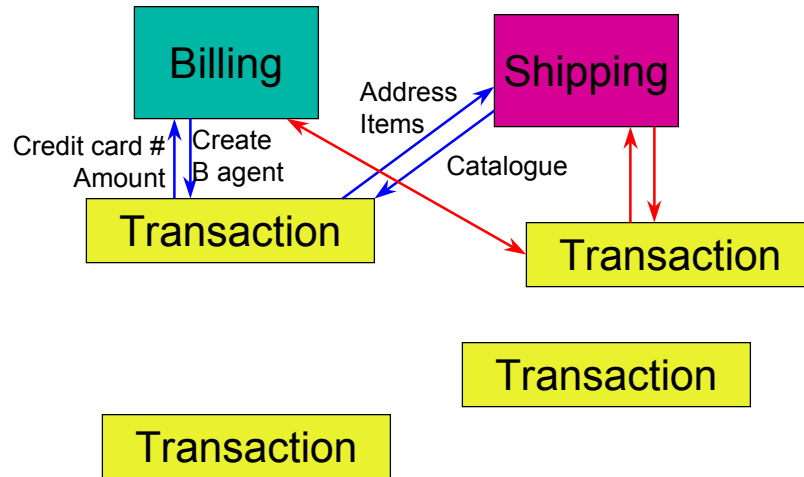
- **Usually discretionary within family**
  - Accesses defined by object types
  - No walls between subjects
- **Walls between families**
  - Includes network communications
  - VMs and VPNs
- **System-controlled transfers**
  - Data
  - Subject creation

03/16/99-4

© 2000 Edward A. Schneider. Permission to make digital or hard copies of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice.



## Mail Order Firm



03/16/99-5

© 2000 Edward A. Schneider. Permission to make digital or hard copies of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice.



## Flexibility

- **Add and delete families**
  - Transactions
  - Form coalition / virtual organization
  - New application with unique interactions
- **Change permitted flows**
  - Response to a threat
  - Resource failures

03/16/99-6

© 2000 Edward A. Schneider. Permission to make digital or hard copies of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice.



## Policy

### { Permissions, Prohibitions, Obligations }

- **Information Flow from F to F'**
  - Requires a subject **S** in both **F**, **F'**
  - **F**<sub>policy</sub> permits **S** export\_to **F'**
  - **F'**<sub>policy</sub> permits **S** import\_from **F**
- **B agent in Billing and Transaction families**

03/16/99-7 © 2000 Edward A. Schneider. Permission to make digital or hard copies of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice.



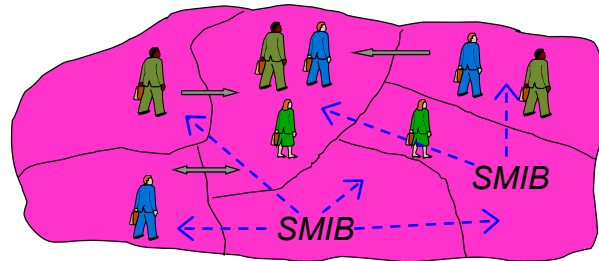
## Policy as Data

- **Security Management Information Base (SMIB)**
- **Separate from enforcement mechanisms**
- **Policy contained in some information families**
  - Protected according to access control policy of those families

03/16/99-8 © 2000 Edward A. Schneider. Permission to make digital or hard copies of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice.



## SMIBs



- **SMIB may define policy for its own family**
- **Transfers governed by SMIBs at both ends**

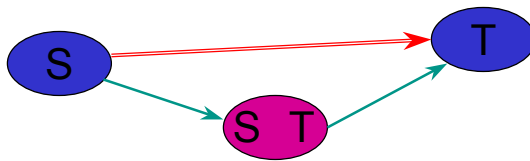
03/16/99-9

© 2000 Edward A. Schneider. Permission to make digital or hard copies of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice.



## Information Flows

- **Implicit flow from SMIB to family**
- **Policies such as Chinese Wall require flow from family to SMIB**
  - Policy updated by accesses
- **New family may circumvent prohibition**



03/16/99-10

© 2000 Edward A. Schneider. Permission to make digital or hard copies of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice.



## Strength of Mechanism

- **Access Control depends on**
  - Identification
  - Cryptography
  - Audit
  - Program correctness
- **Families may require a strength for each of these from the platforms which host them**

03/16/99-11

© 2000 Edward A. Schneider. Permission to make digital or hard copies of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice.