

# **Communication Fraud Control Association 1999 Spring International Conference**

**4.-6. May 1999, Ismaning, Germany**

## **Modelling of Secure Interconnection**

**Matthias Kabatnik, Reiner Sailer**

# Structure

---

---

**Problem of interconnection: reliable information**

**Security mechanisms: a refined approach**

**Modelling of interconnection**

# Motivation

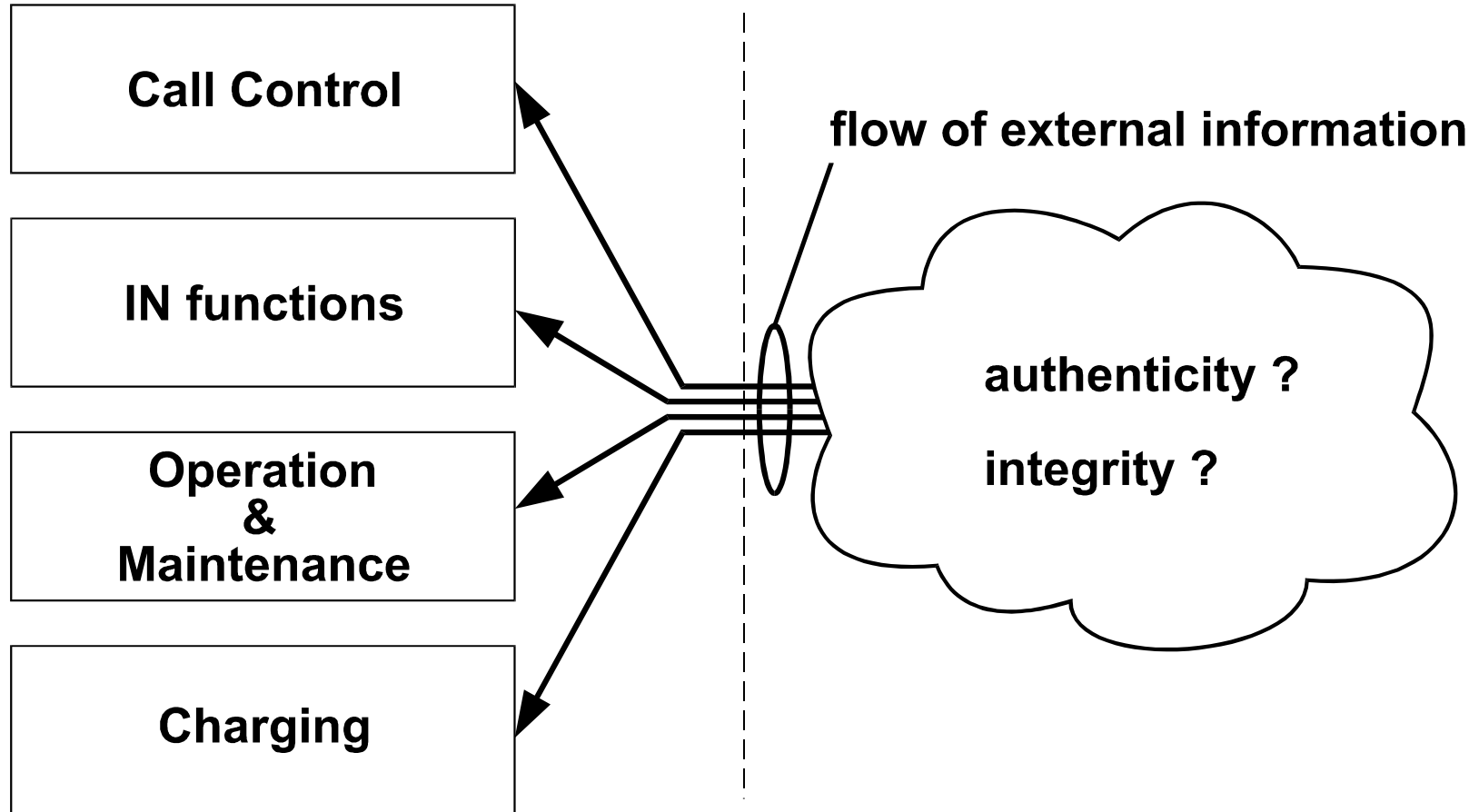
---

## **Situation at network borders is changing**

- **increasing number of interconnection partners**
- **equipment of different vendors**
- **different levels of skill**
- **new services across network borders**

## **⇒ new security problems**

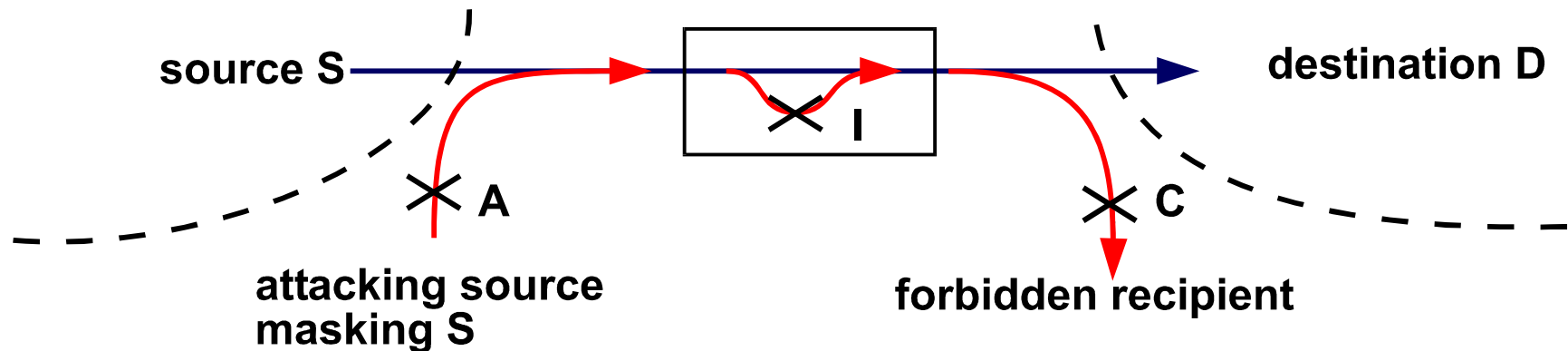
- **decreasing reliability**
- **faulty or no charging of services**
- **impact on customers**



**necessity of protection is obvious**

## Substantial security requirements for external information

- **Authenticity (A) or plausibility**  
assignment of information to the correct source
- **Integrity (I)**  
to maintain correctness of intended effect
- **Confidentiality (C)**  
to keep information flows limited to source and intended destination



**Potential attackers must be kept from**

- **inserting data**
- **deleting data**
- **manipulating data**

**This can be achieved by**

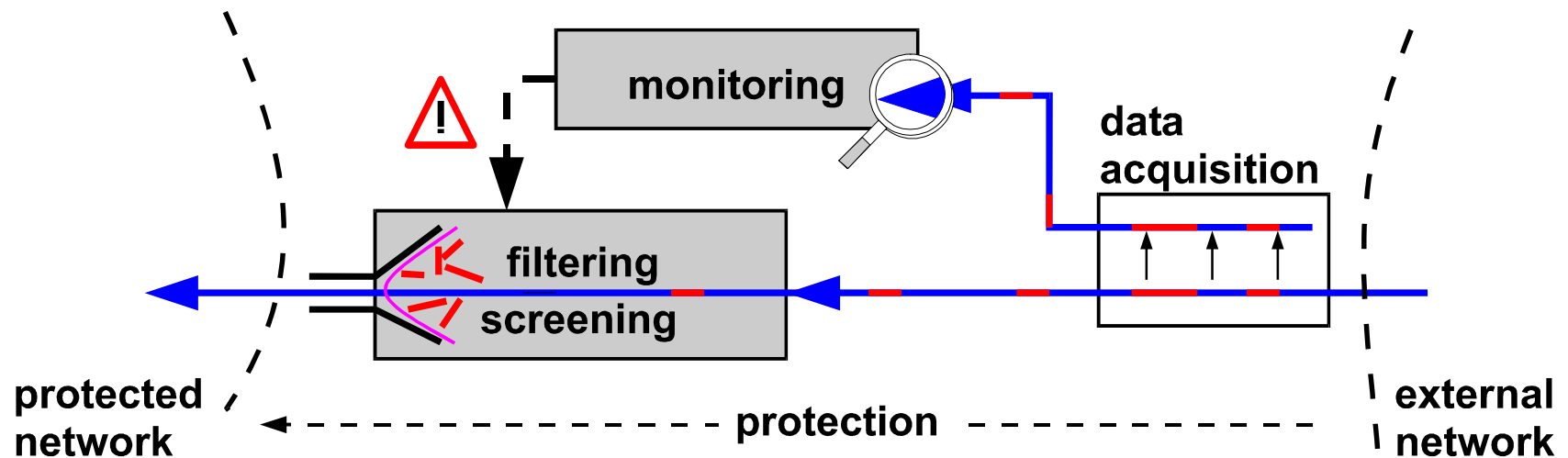
- **physical separation (structure of network between ICP)**
- **logical separation (orthogonal address spaces)**
- **cryptographic separation**

## Passive mechanisms

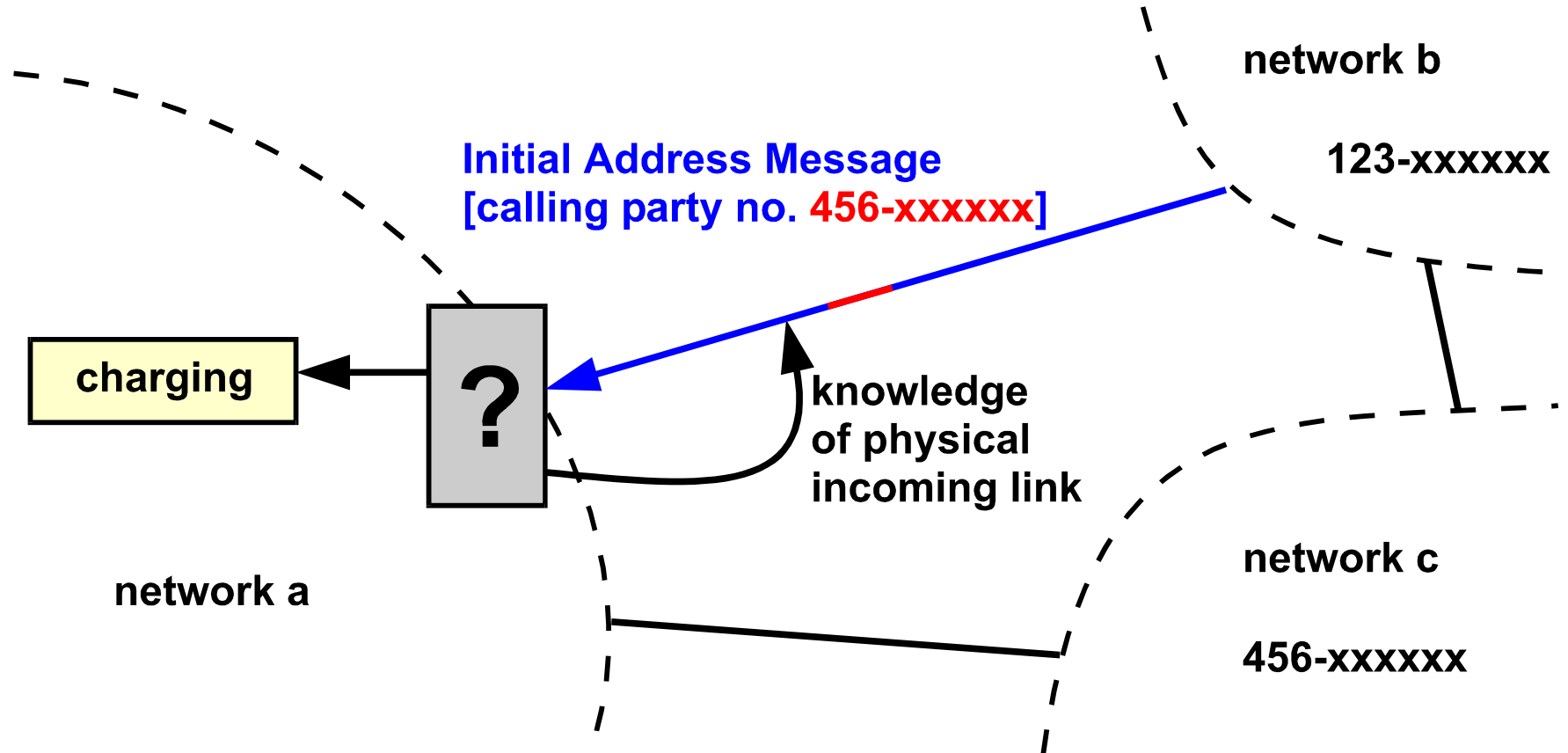
- monitoring (e. g. pattern recognition)

## Active mechanisms

- filtering decisions based on tables
- screening decisions based on tables and context



## Screening of “called party number”



## Definition

Filtering determines whether information has to be  
**passed** or **discarded**

**Basis of decision:** (part of) the information itself is index for a table  
no further information is used

**Result:** information is passed or discarded

**Examples:** destination filtering (DPC, SI, SSN)  
filtering of national parameters (ISUP Q.763)

**Conclusion:** filtering is applicable with authentic or  
destination-oriented information

## Definition

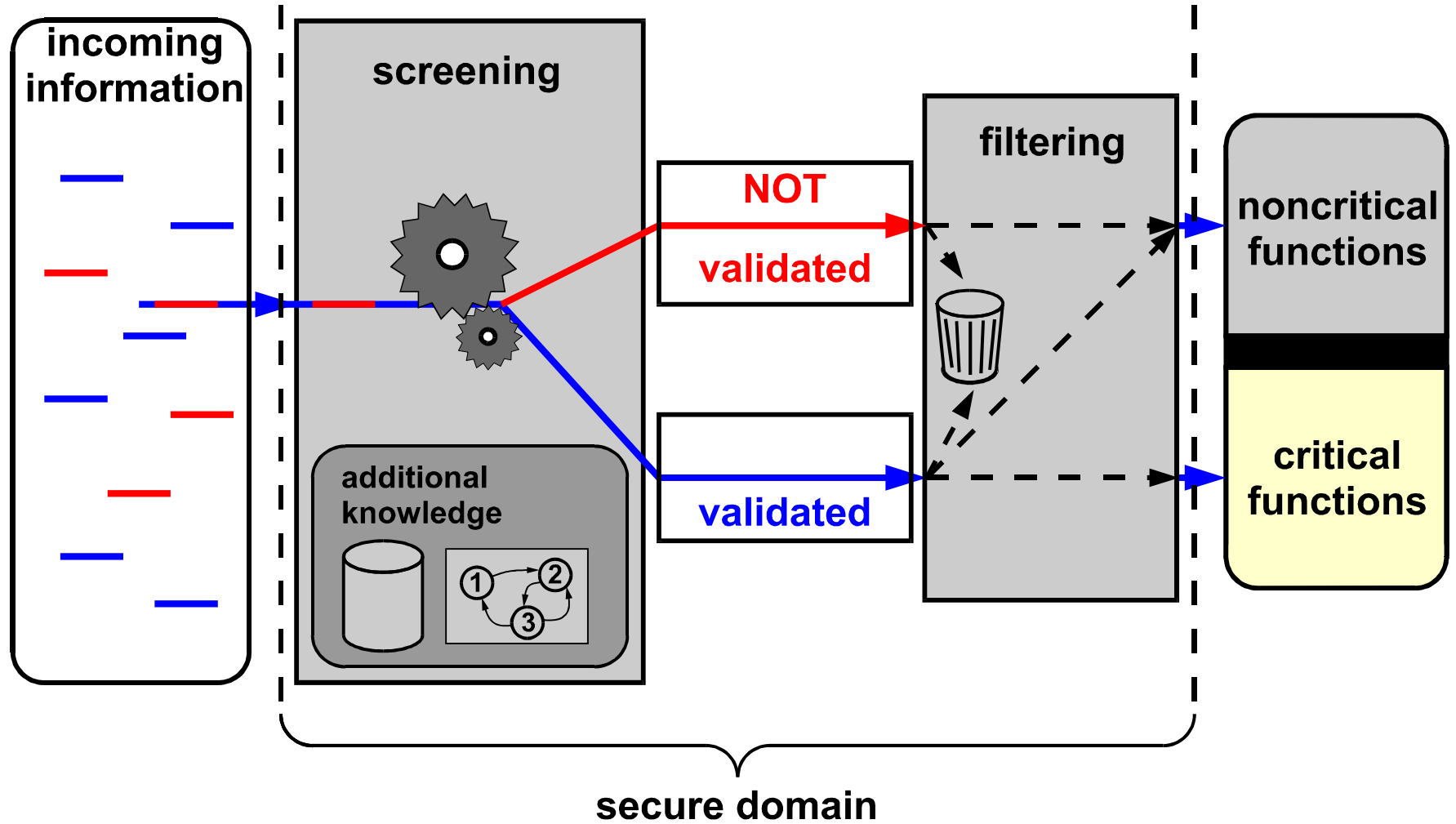
Screening denotes the classification of information  
in **valid** or **invalid**

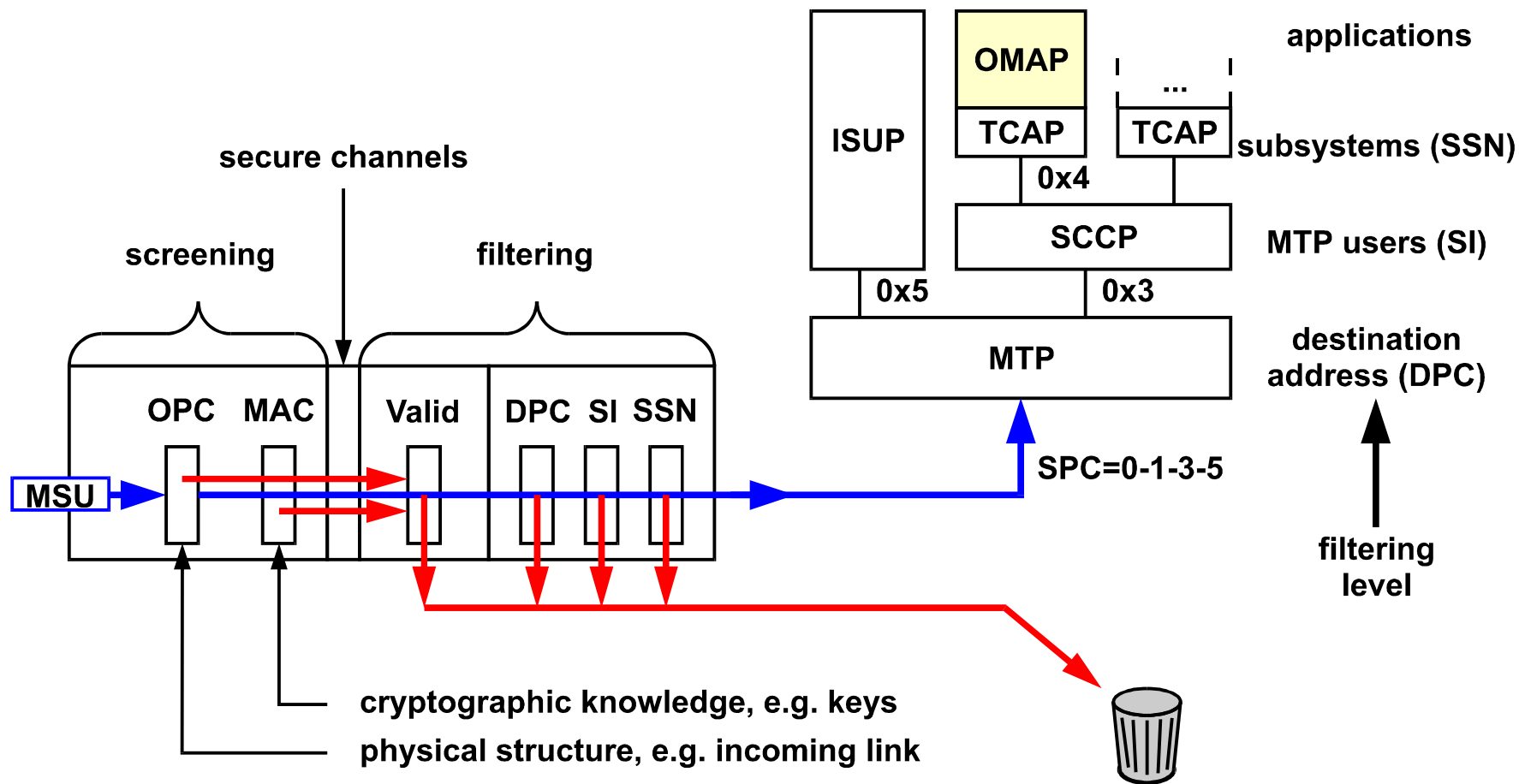
**Basis of decision:** combination of received information with  
related additional knowledge

**Related  
knowledge:** physical structure, cryptographic keys

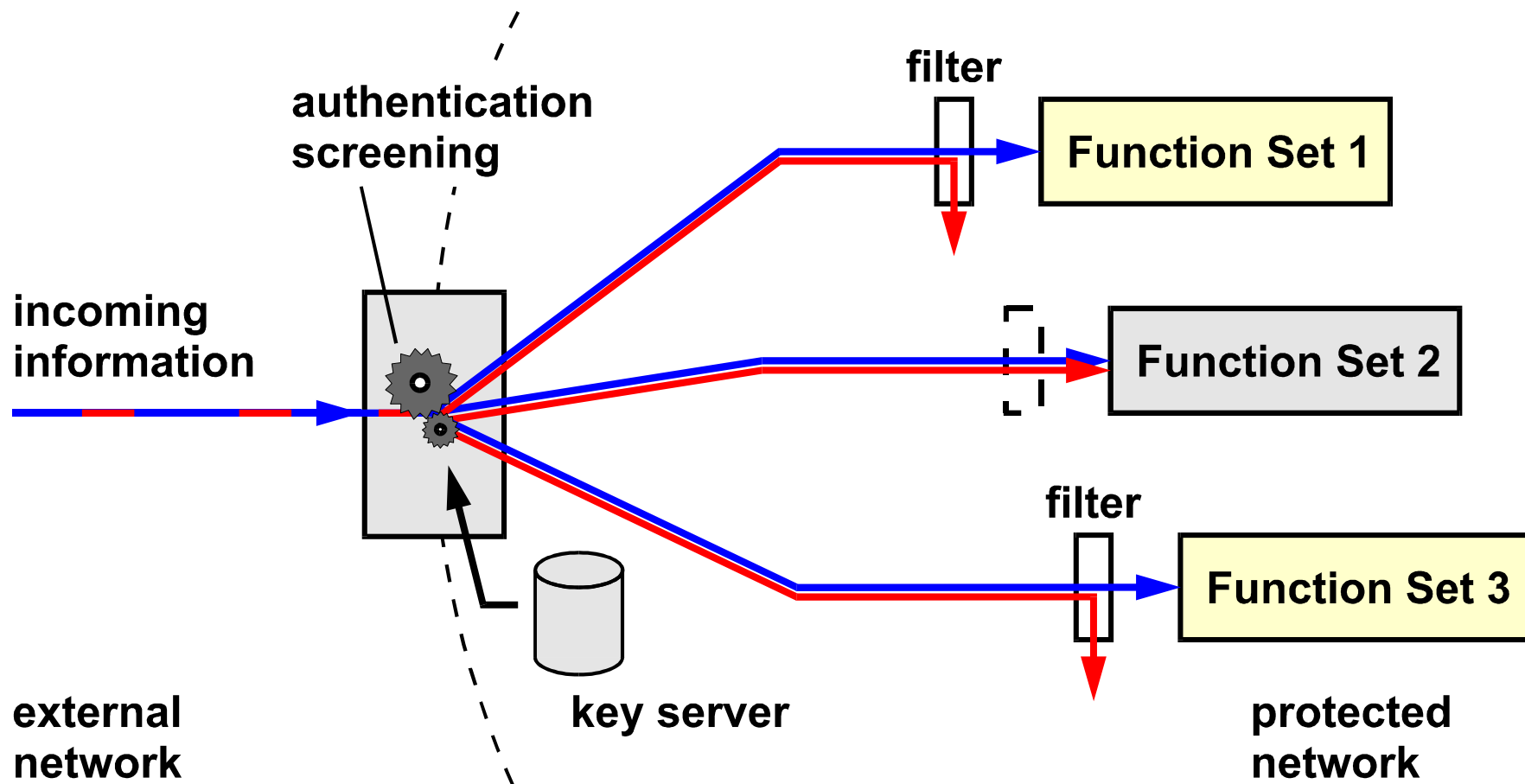
**Result:** information is marked valid or invalid

**Examples:** network indicator validation  
incoming link validation  
subscriber number validation  
cryptographic authentication





## Centralized authenticity screening with distributed filtering



# Summary

---

---

- **Refined approach to security mechanisms for interconnection**
- **High degree of flexibility by separating screening and filtering functions**
  - independent implementation of screening and filtering
  - screening and filtering may be distributed
  - centralised screening function is possible
- **Approach supports migration to secure interconnection**