Using the IPSec Architecture for Secure Multicast Communication

Thorsten Aurisch
t.aurisch@fgan.de

Christoph Karg
chkarg@fgan.de

Research Establishment for Applied Science

Neuenahrer Straße 20

D-53343 Wachtberg, Germany

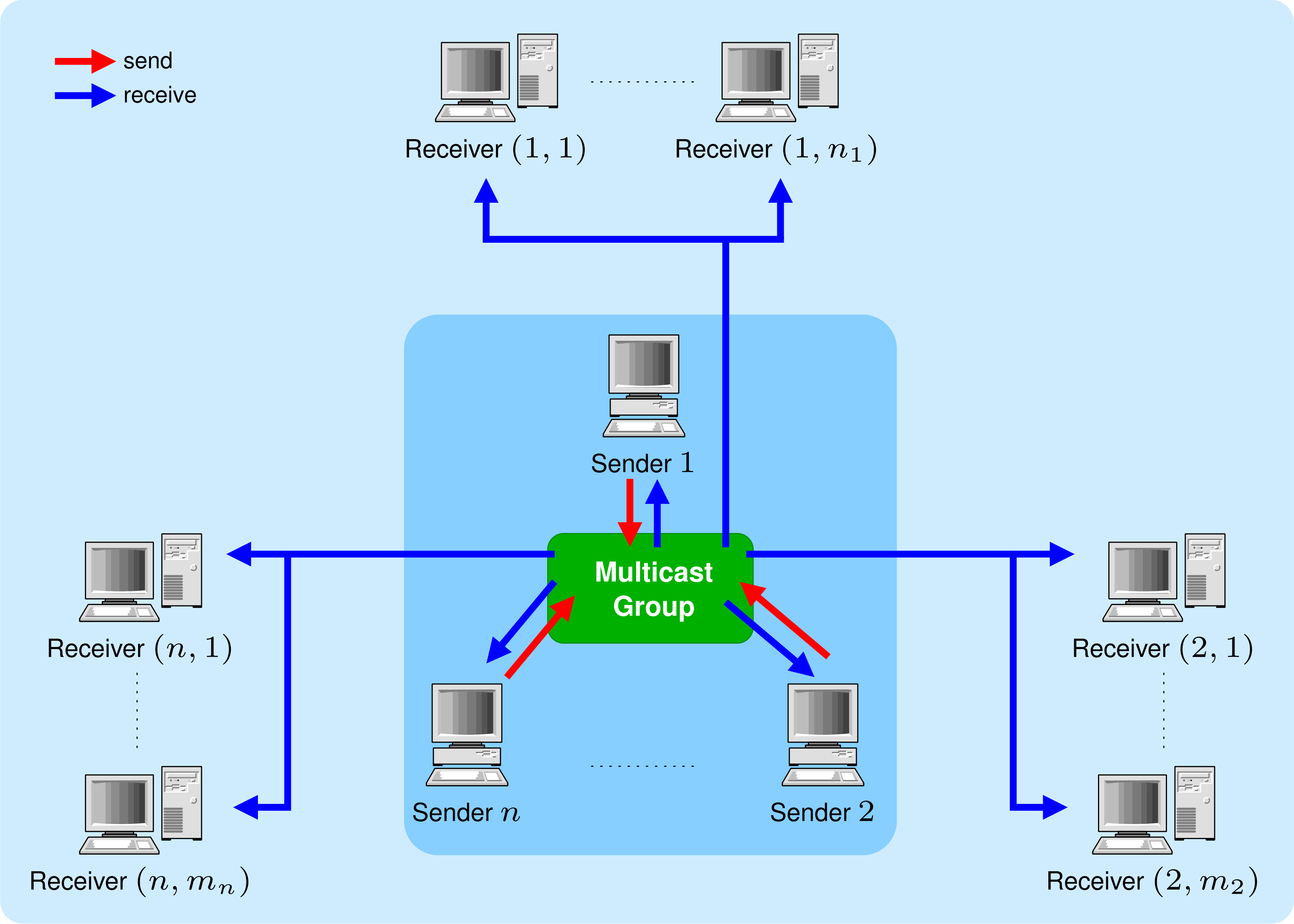
Multicast Communication

- Efficient data transmission from one sender to a group of receivers
- Examples of usage
  - ▷ Briefing sessions
  - ▷ Database replication
  - ▷ Audio/video conferencing
- Idea: send data once and duplicate it where necessary
- Requirement: sophisticated routing infrastructure
- Problem: How to secure the data traffic?

Important Questions

- Which scenario for group communication?
- How to secure the multicast traffic?
- How to manage the security settings?

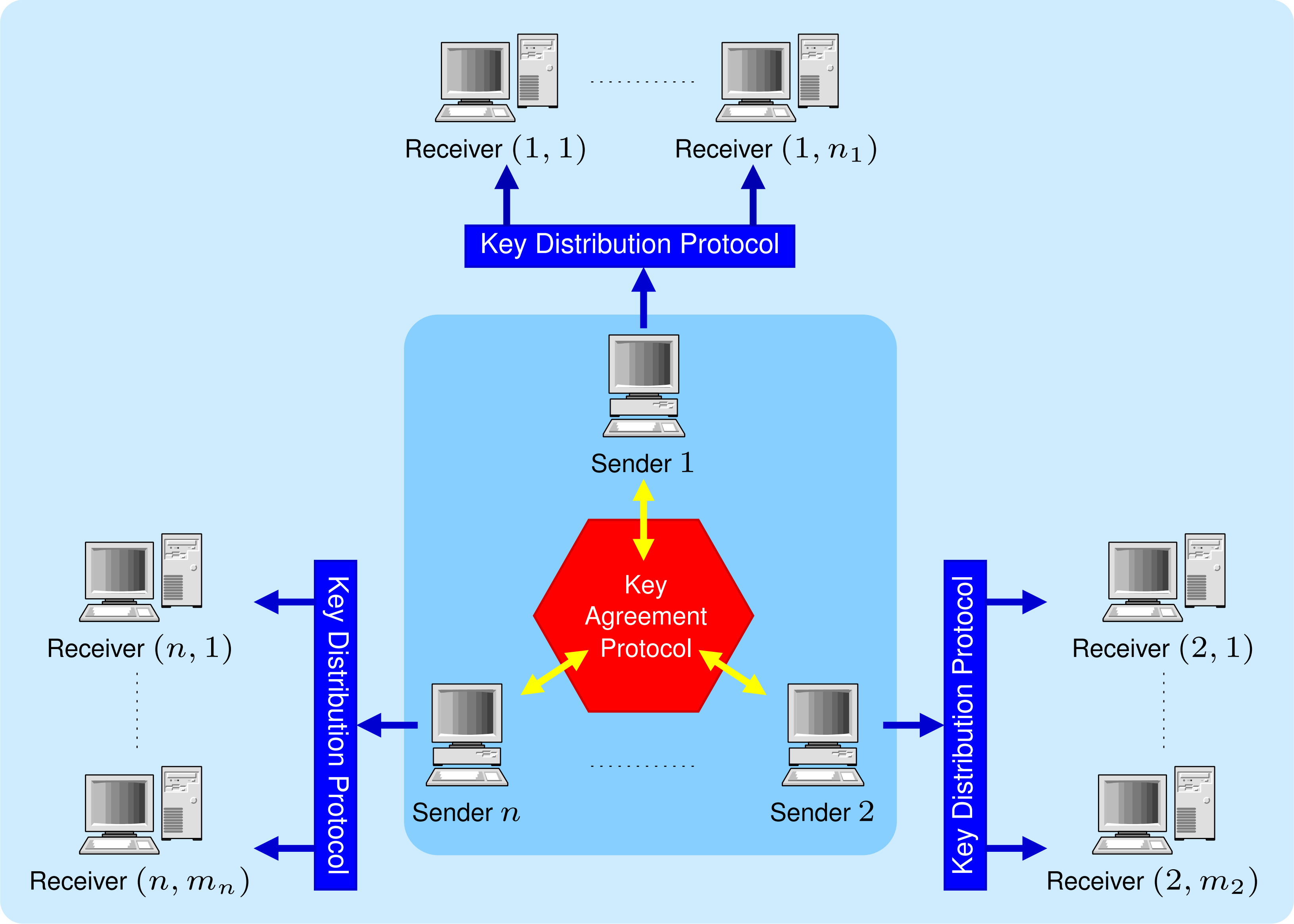
Scenario (Briefing Session)



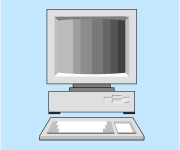
Multicast Security

- Mandatory requirements
  - ▷ Secrecy of the data traffic
  - ▷ Group authentication
  - ▷ Source authentication
  - ▷ Forward/backward security
- Group key exchange
  - ▷ Key agreement protocols
    ⇝ collaborative key negotiation
  - ▷ Key distribution protocols
    ⇝ generation & distribution via a key server

Scenario (Key Exchange)

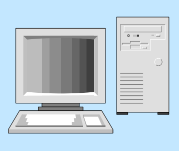


Scenario Details



Sender hosts

- Number $n \approx 25$
- Send and receive data
- Connected via broadband networks
- Key exchange via agreement



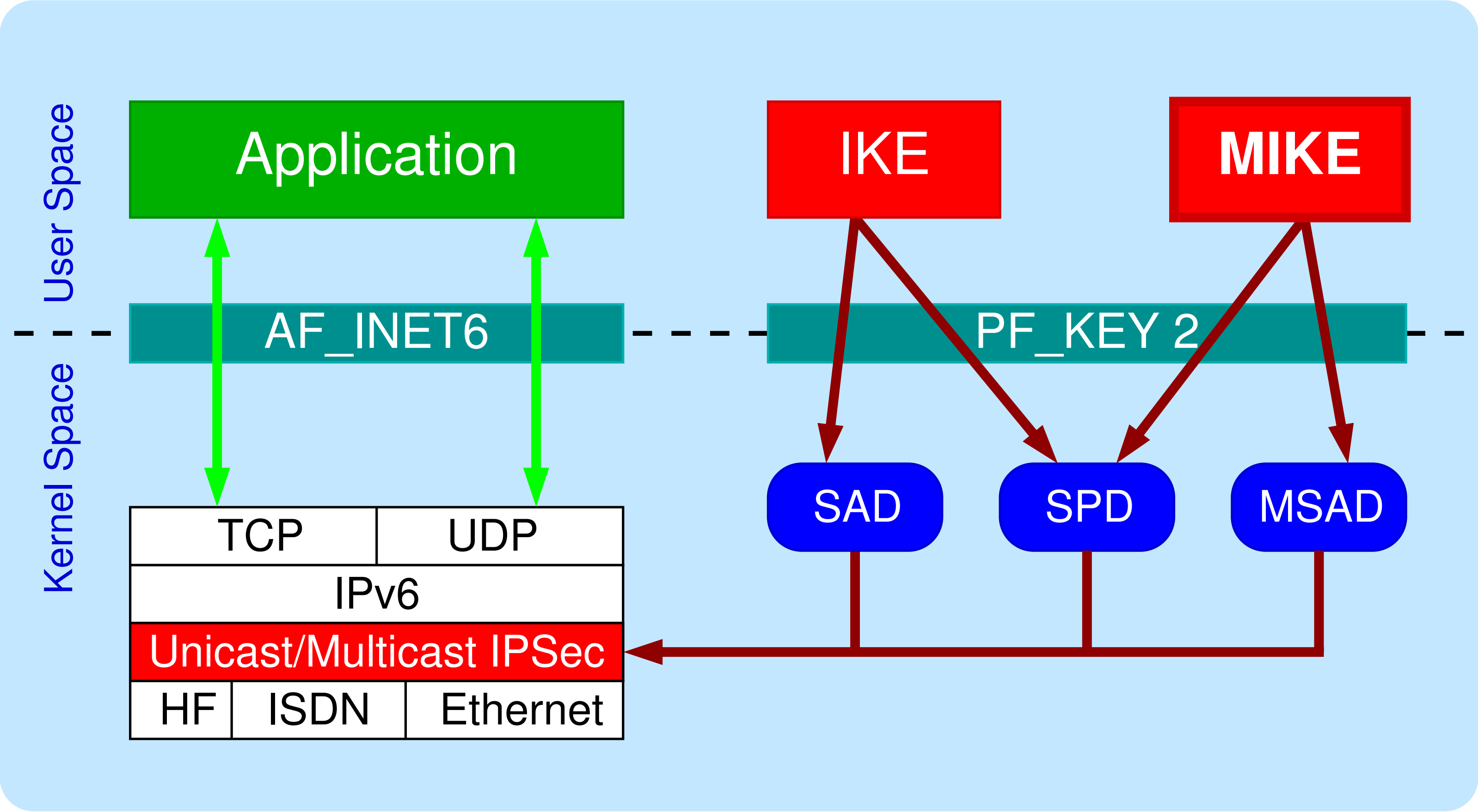
Receiver hosts

- Number $m_i \approx 10000$
- Only receive data
- Connected via networks with narrow bandwidth
- Key distribution from a designated sender

Security Concept

- Security: Usage of the IPSec protocol suite
  - ▷ Security at network layer
  - ▷ Multicast support
  - ▷ Algorithms for encryption and group authentication
  - ▷ But: No source authentication
    Hope: several IETF drafts (work in progress)
- To solve: Multicast Internet Key Exchange (MIKE)
  - ▷ Negotiation of IPSec settings
  - ▷ Key exchange functionality
- Goal: Development of a MIKE daemon

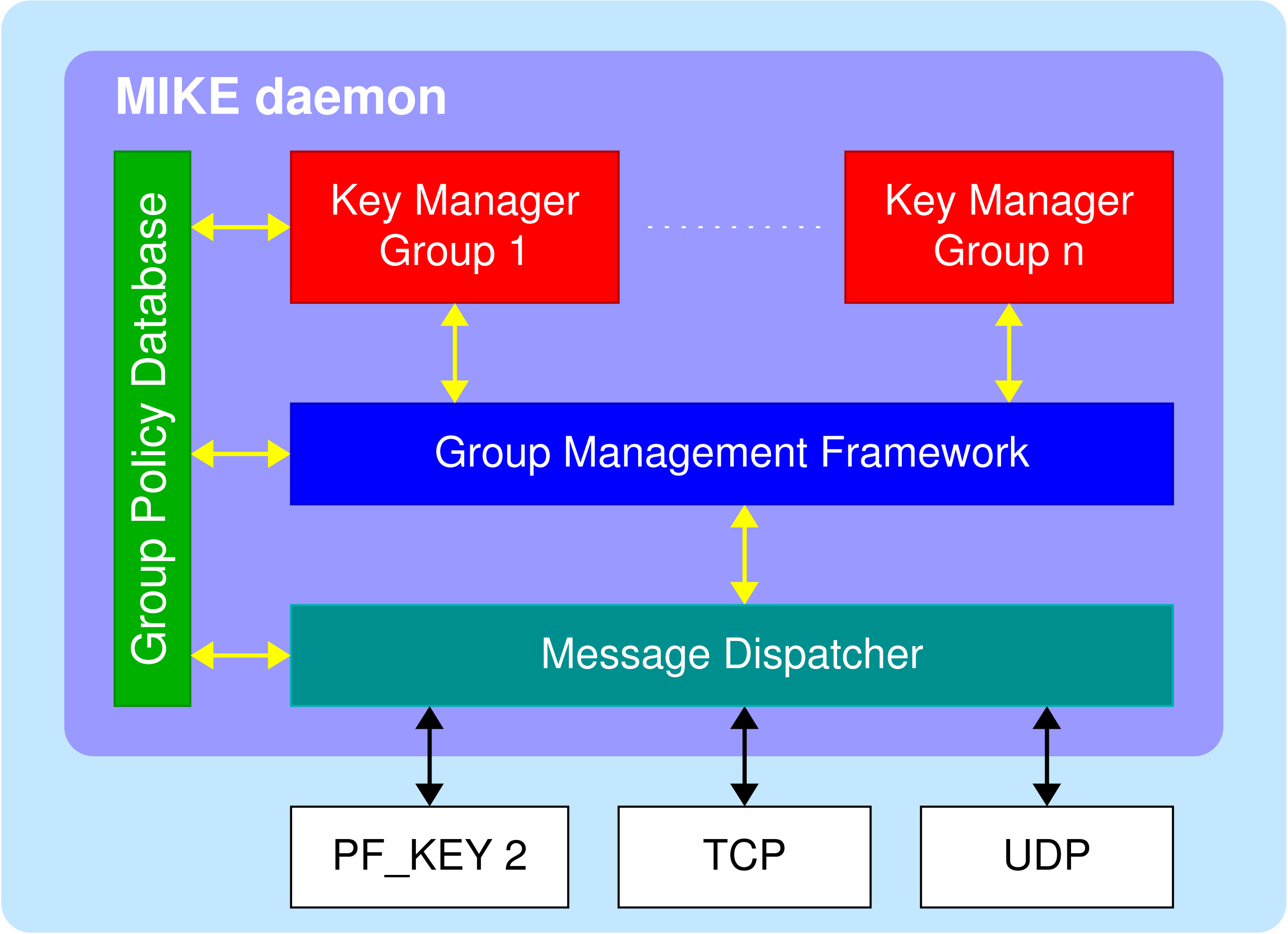
MIKE as part of the IPSec framework



MIKE Design Goals

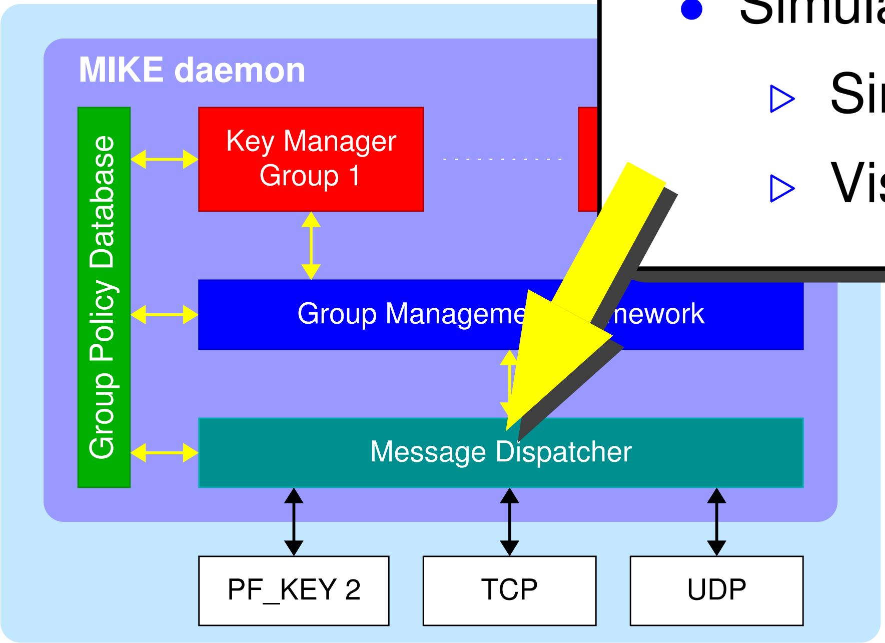
- Two objectives:
  - ▷ Prototypical implementation
  - ▷ Simulation environment
- Special focus on military environments
  - ▷ Narrow bandwidth (wireless communication)
  - ▷ Emission control (EMCON)
- Design criteria
  - ▷ Separation of key management and application
  - ▷ Robust exchange protocols
  - ▷ Extensibility
  - ▷ Independency from multicast routing mechanisms
  - ▷ Usage of existing standards as far as possible

MIKE Architecture



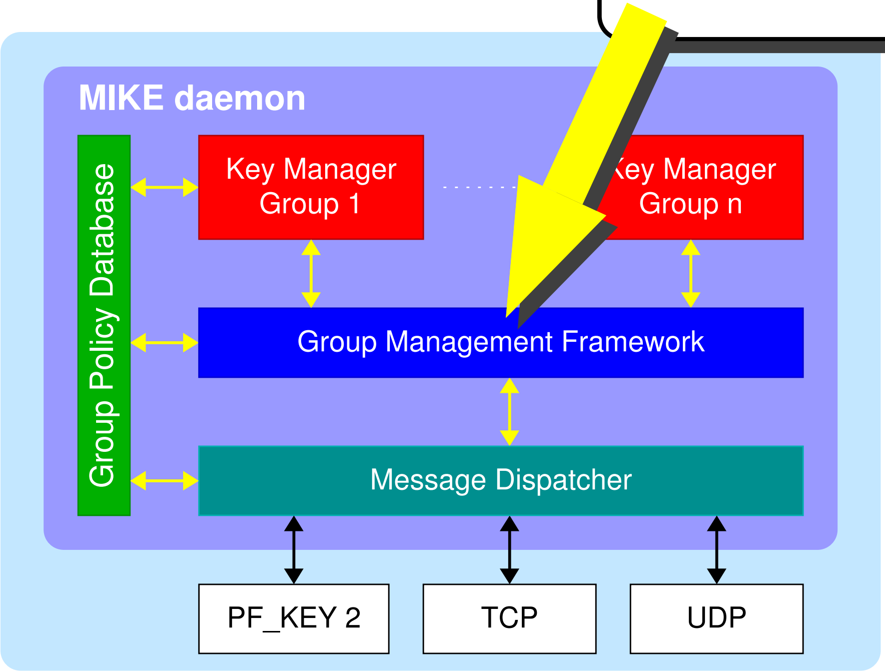
Message Dispatcher

- Task: transmission of key exchange messages
- Prototypical implementation
  - ▷ Connection to the Internet
  - ▷ Configuration of IPSec kernel module
- Simulation environment
  - ▷ Simulation of packet loss, delays, etc.
  - ▷ Visualization of key exchange protocols

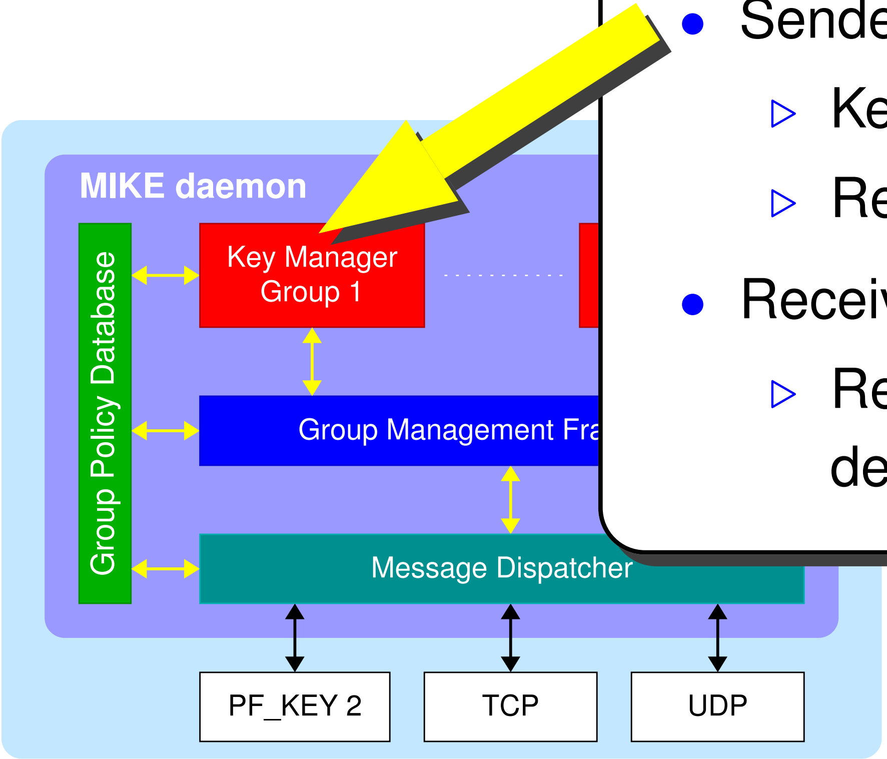


Group Management Framework

- Task: Multicast IPSec management of the host
- Group access control
- Invocation/termination of key managers
- Key exchange message distribution

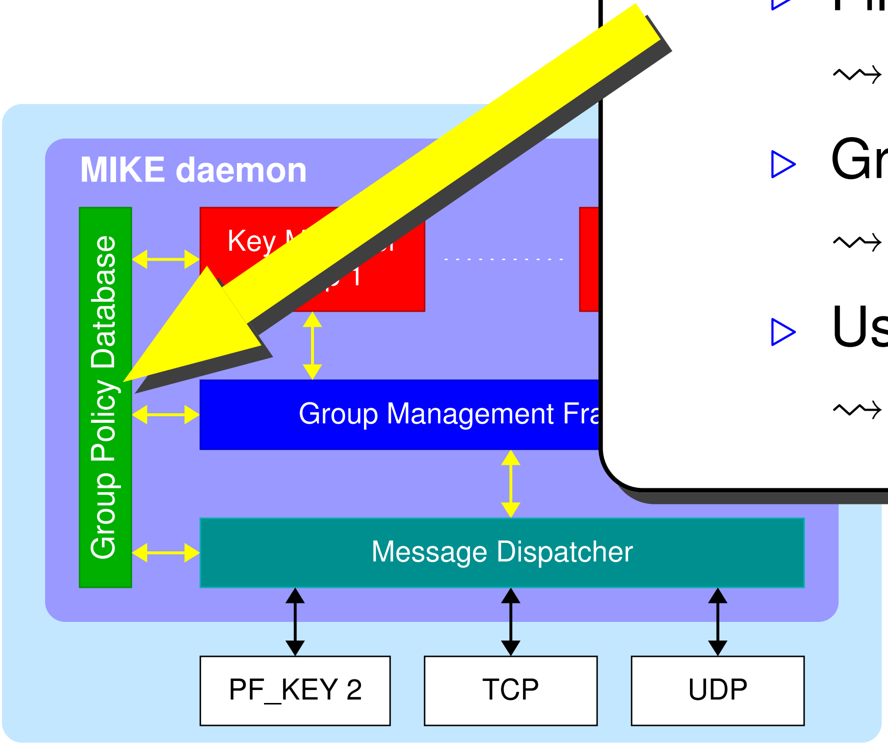


Key Manager



- Task: negotiation of IPSec settings for one multicast group
- Host authentication and digest validation
- Sender mode
  - ▷ Key agreement with other senders
  - ▷ Receiver management
- Receiver mode
  - ▷ Requesting IPSec settings from the designated sender

Group Policy Database



- Task: provision of security relevant information
- Type of information dependent on the accessing component
  - ▷ Filtering rules
    ⇝ message dispatcher
  - ▷ Group access policy
    ⇝ group management framework
  - ▷ User access control, authentication data
    ⇝ key manager

Implementation Details

- Object oriented approach (C++)
- Open source operating system
  - ▷ Debian Linux
  - ▷ USAGI IPv6/IPSecurity kernel patch
- Development tools
  - ▷ GNU Tools (gcc, make, etc.)
  - ▷ Standard Template Library
  - ▷ Crypto++ Library
- Roadmap:
  - ▷ First prototype at the end of 2003
  - ▷ Simulation environment in 2004

Conclusion

- Scenario: Briefing sessions
- Security via IPSec architecture
- Setup via Multicast Internet Key Exchange