An Object-Oriented ISAKMP Implementation

Sanna Liimatainen

Helsinki University of Technology

Contents

- What is ISAKMP
- What is Jacob Framework
- How ISAKMP can be implemented with help of Jacob

Internet Security Architecture

- The Internet is based on TCP/IP protocols - no security

- IP Security Protocol (IPSEC) provides authentication, confidentiality and integrity

- IPSEC does not provide key exchange and management

Internet Security Association and Key Management Protocol

- RFC 2408 (November 1998)
- Authentication and Key Management
- ISAKMP is a framework
- Internet Key Exchange (IKE)

ISAKMP

- Two phases
- Security Association (SA)
- 13 Payloads
- 5 Exchanges
- Cookie

ISAKMP Header

<table>
<tr><td colspan="5">Initiator
Cookie</td></tr>
<tr><td colspan="5">Responder
Cookie</td></tr>
<tr><td>Next Payload</td><td>MjVer</td><td>MnVer</td><td>Exchange Type</td><td>Flags</td></tr>
<tr><td colspan="5">Message ID</td></tr>
<tr><td colspan="5">Length</td></tr>
</table>

Exchange Types

- Base Exchange (4 msgs)

- Identity Protection Exchange (6 msgs)

- Authentication Only Exchange (3 msgs)

- Aggressive Exchange (3 msgs)

- Informational Exchange (1 msg)

Base Exchange

Alice						Bob
	HDR	SA	Proposal	Transform	Nonce	→
←	HDR	SA	Proposal	Transform	Nonce	
	HDR	KE	IDii	AUTH		→
←	HDR	KE	IDir	AUTH		

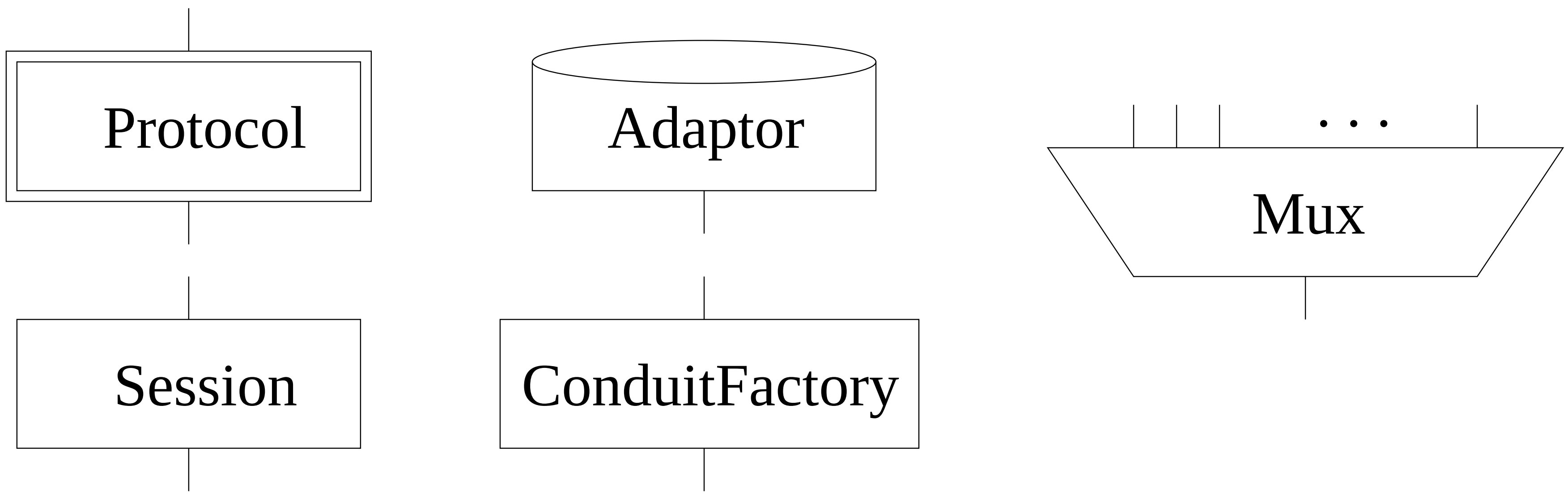
Java Conduits Framework (Jacob)

- Jacob is based on Hueni's, Johnson's and Engel's Conduits+ framework

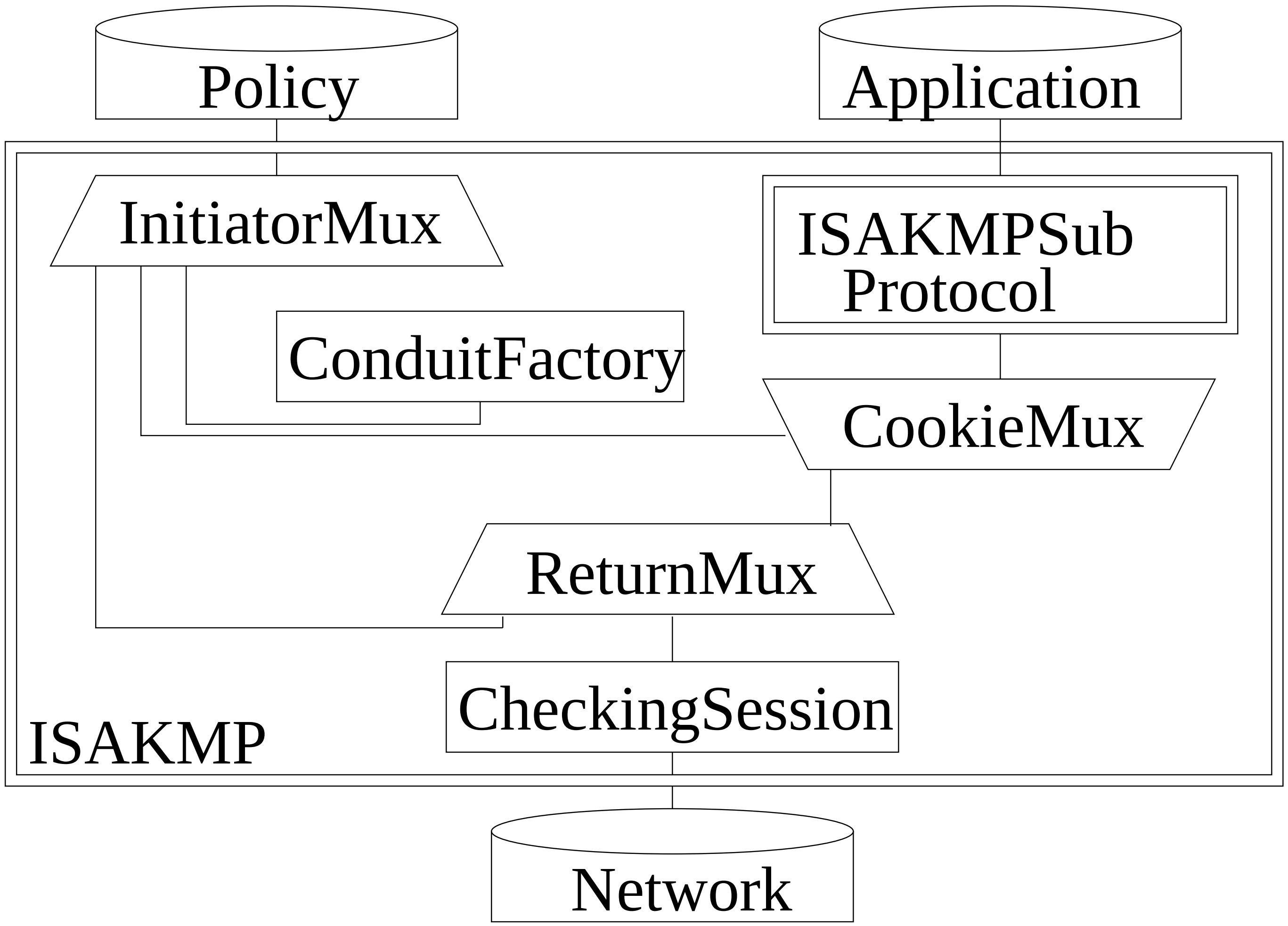
- Jacob is developed at HUT

- Jacob helps implementing cryptographic communication protocols

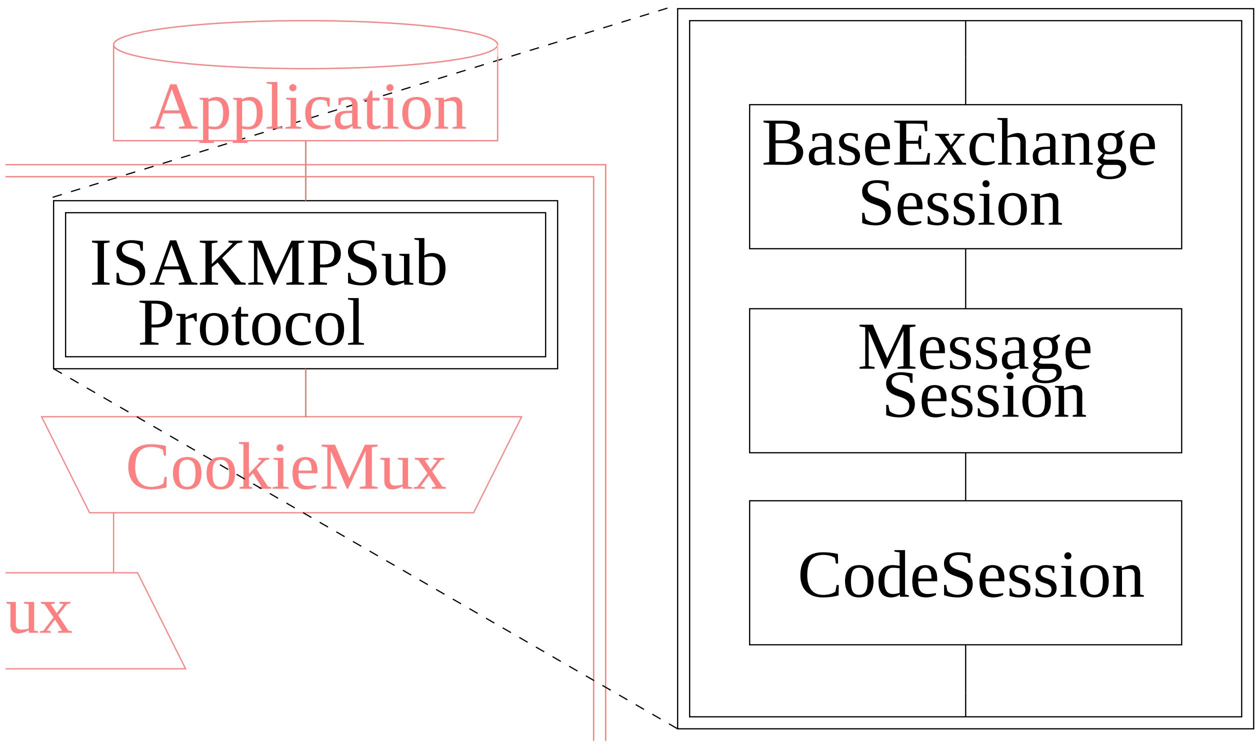
Conduits in Jacob



Conduits+ graph of ISAKMP

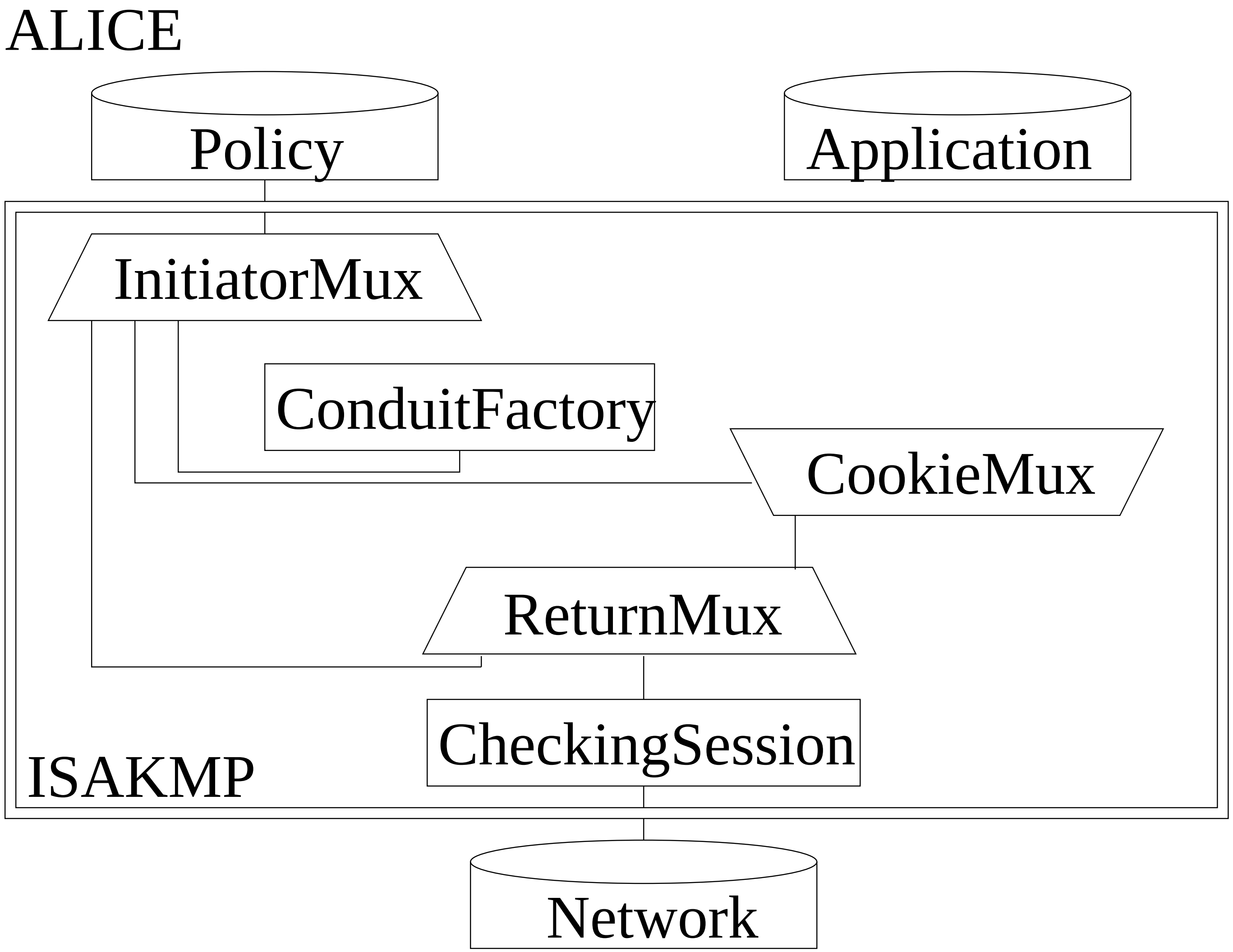

Policy
Application
InitiatorMux
ISAKMPSub Protocol
ConduitFactory
CookieMux
ReturnMux
CheckingSession
ISAKMP
Network

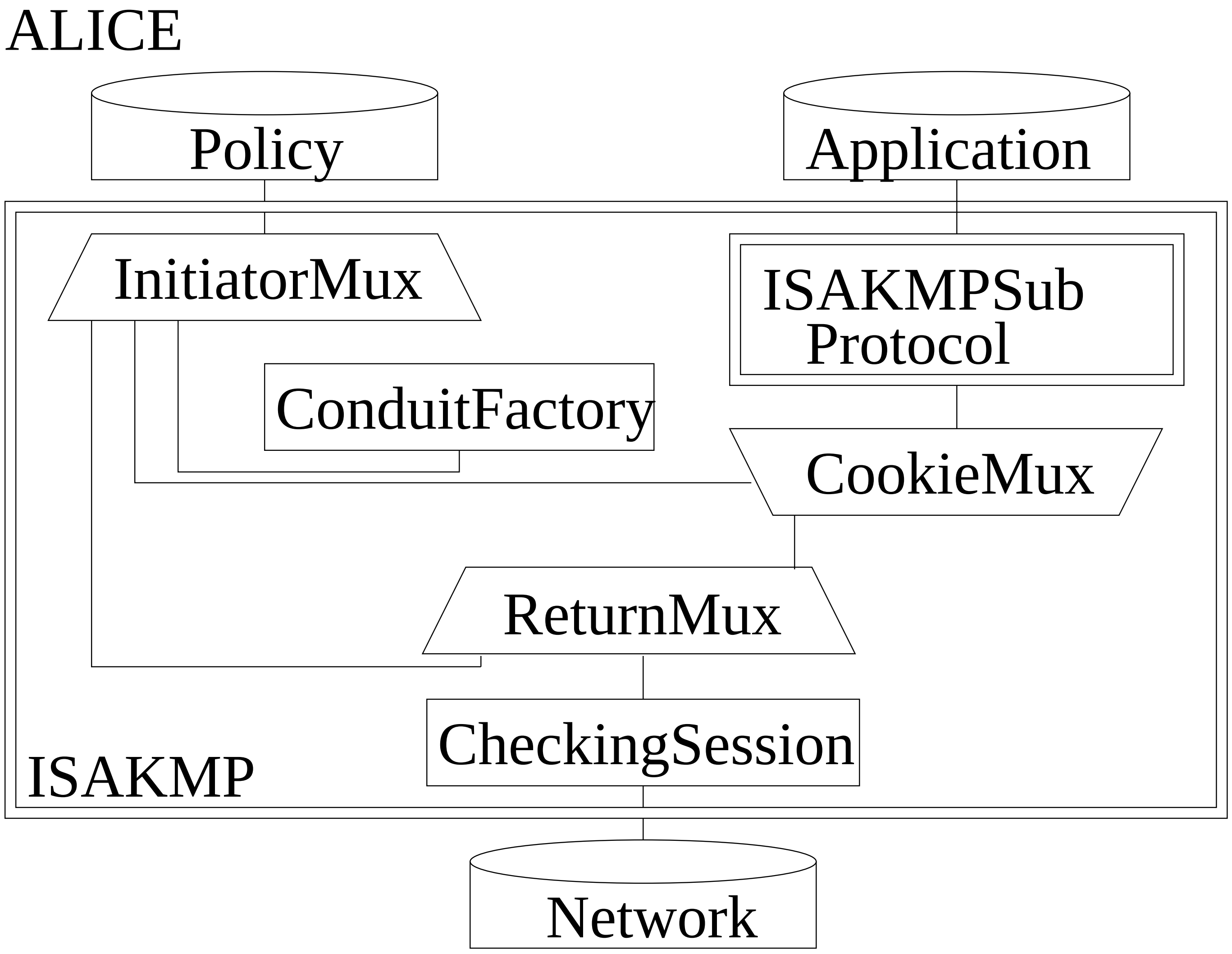
ISAKMPBaseExchangeSubProtocol

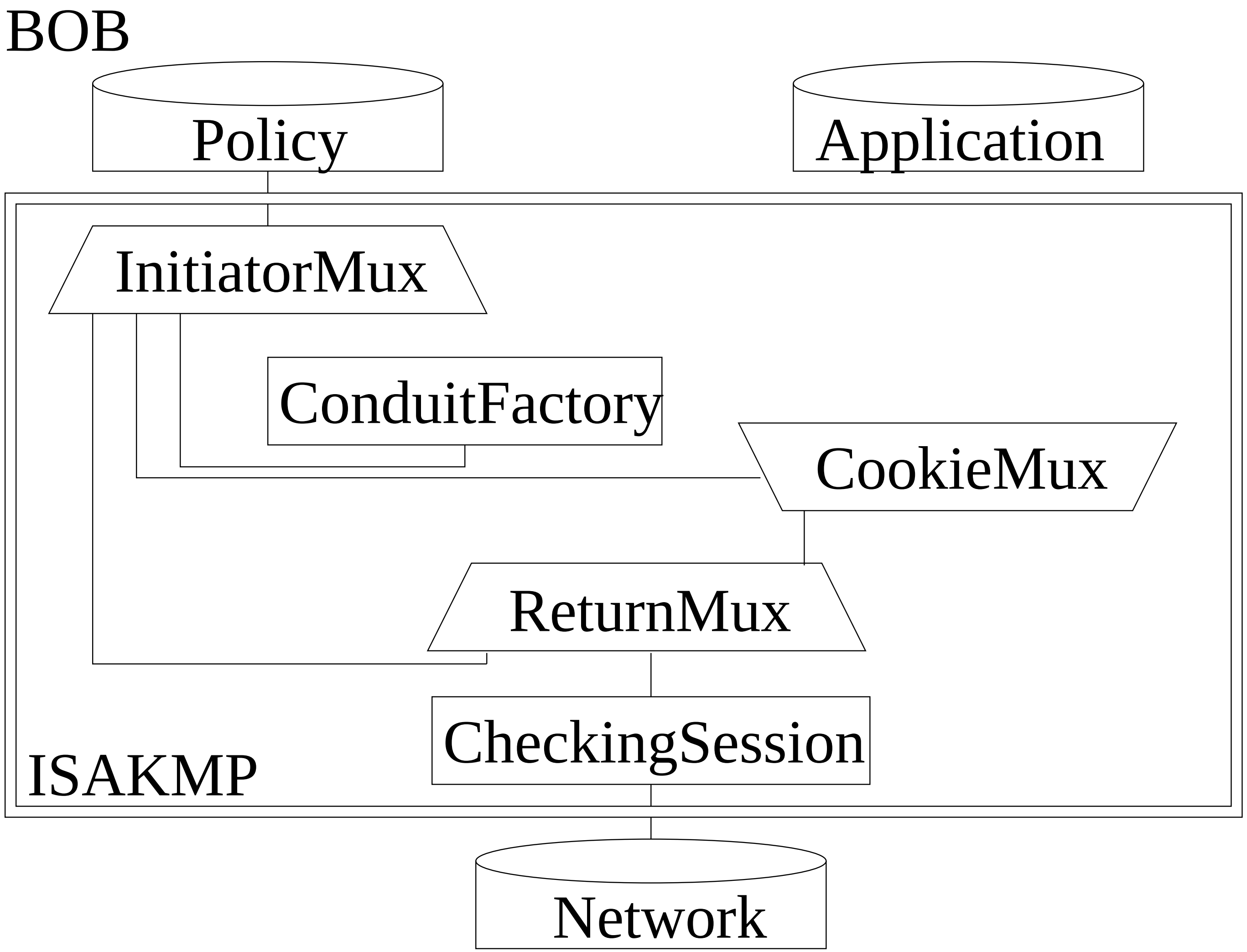


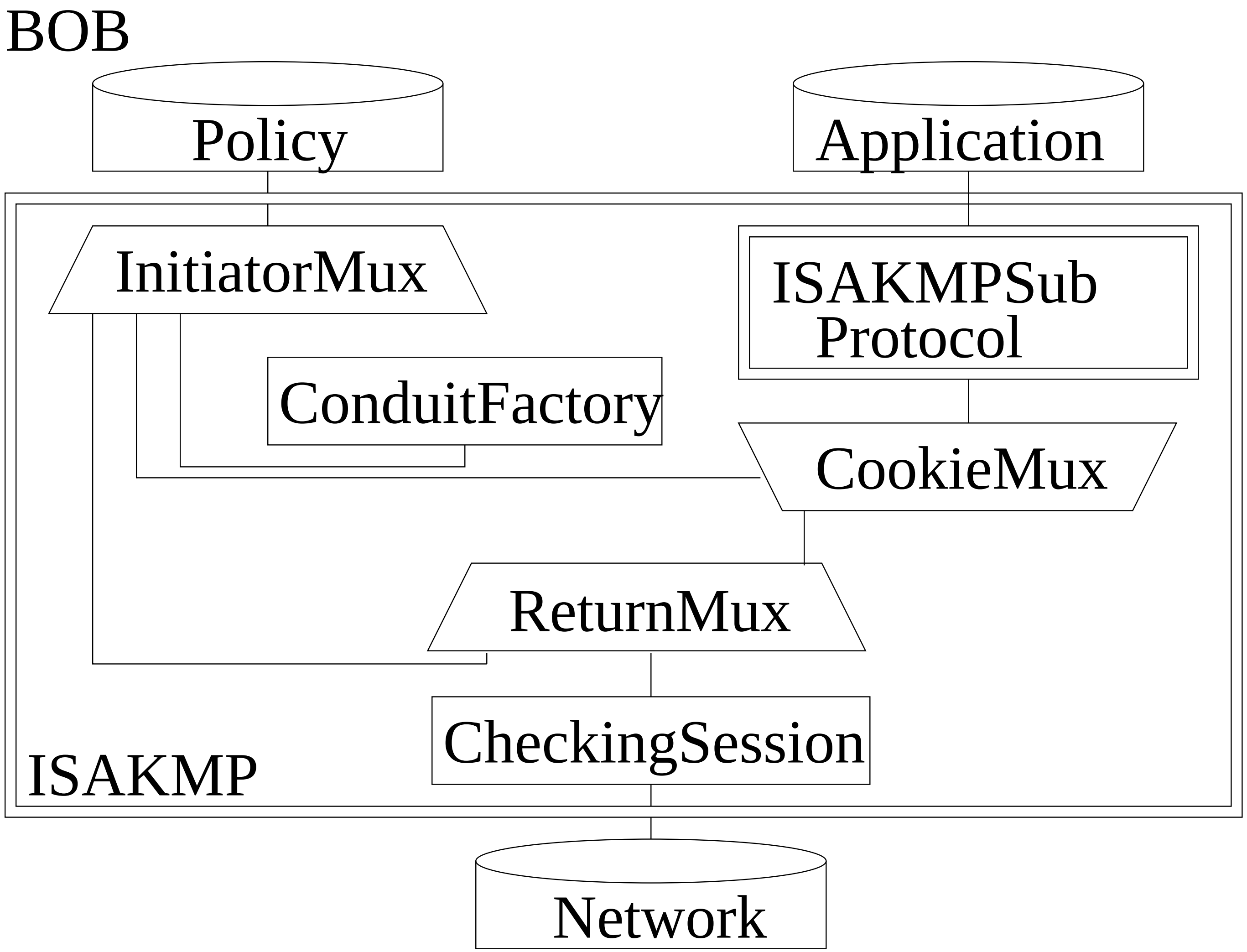
Alice Wants a Secure Connection with Bob

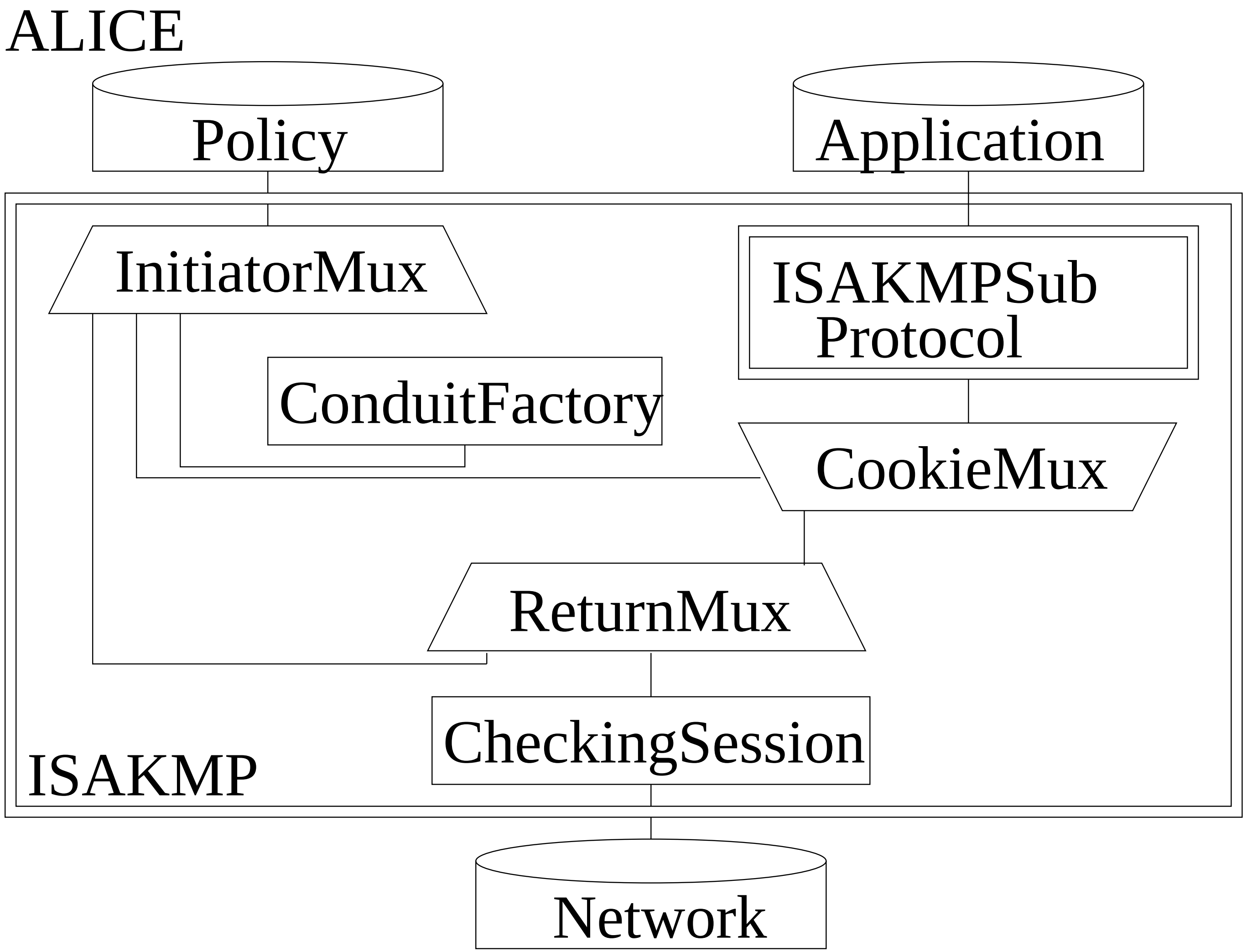
- Next slides shows how a new connection is established using Base Exchange


ALICE
Policy
Application
InitiatorMux
ConduitFactory
CookieMux
ReturnMux
CheckingSession
ISAKMP
Network


ALICE
Policy
Application
InitiatorMux
ISAKMPSub
Protocol
ConduitFactory
CookieMux
ReturnMux
CheckingSession
ISAKMP
Network


BOB
Policy
Application
InitiatorMux
ConduitFactory
CookieMux
ReturnMux
CheckingSession
ISAKMP
Network


BOB
Policy
Application
InitiatorMux
ISAKMPSub
Protocol
ConduitFactory
CookieMux
ReturnMux
CheckingSession
ISAKMP
Network


ALICE
Policy
Application
InitiatorMux
ISAKMPSub
Protocol
ConduitFactory
CookieMux
ReturnMux
CheckingSession
ISAKMP
Network

Experiences

- The idea of a framework is good
- Understanding the framework takes time
- ISAKMP's RFC supports functional programming, not OO-programming
- Adding new exchanges to ISAKMP is easy

More information

- <URL:http://www.tcm.hut.fi/Research/TeSSA/>