A Brief Review of the IPsec Security Architecture

Steve Kent, BBN

39th IETF Meeting

Munich, Germany

August 15, 1997

Major Document Sections

- Introduction, Design Objectives, System Overv
- Security Associations (SPD, SAM, SAD, Selecto
- IPsec processing (outbound/inboound)
- PMTU
- Algorithms
- Usage Scenarios (illustrative examples)
- Use in Information Flow Security Environments
- Conformance
- Appendixes (Glossary, PMTU Analysis, Sequence Algorithm)

Security Association Selectors

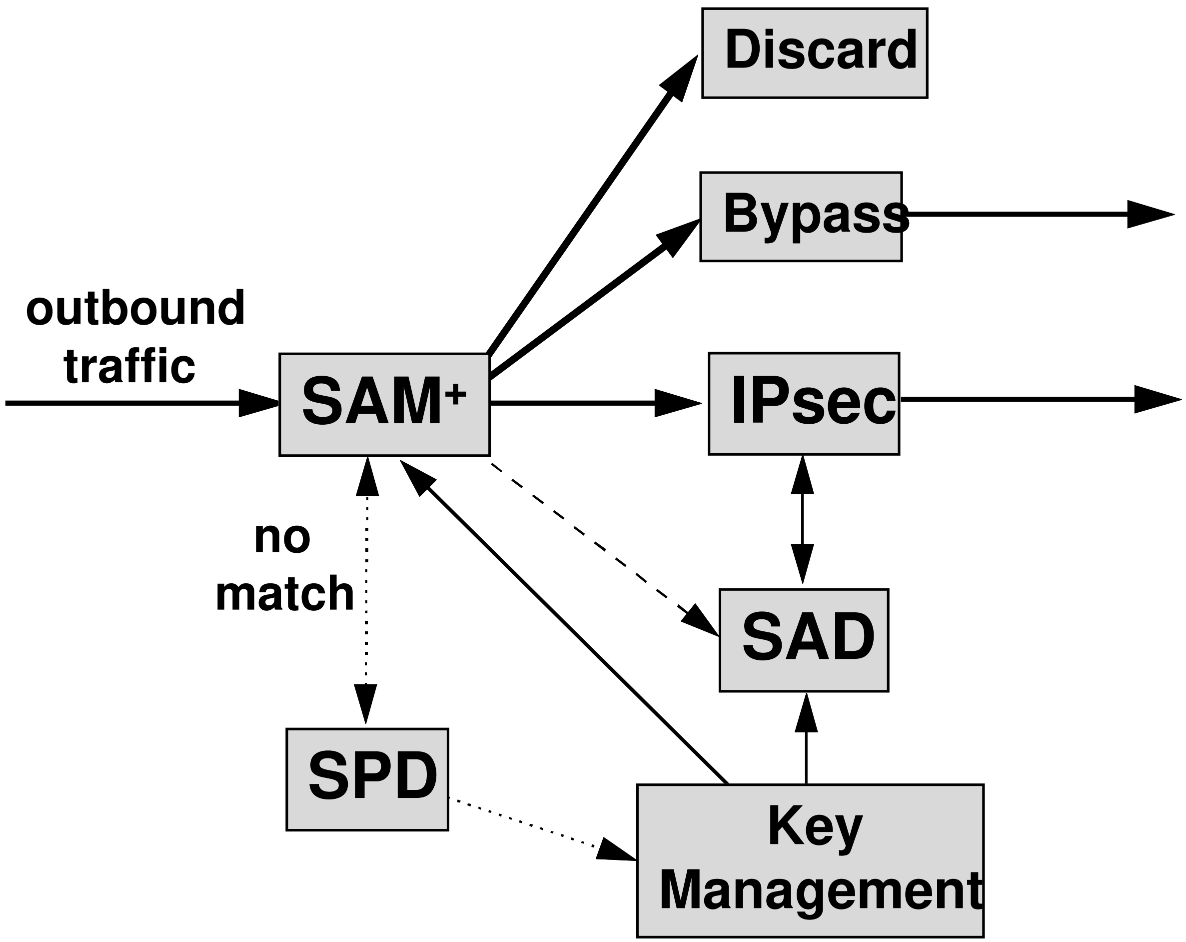
SELECTOR	H/GW	FORMAT
S/D IP address	R/R	explicit/mask
S/D Ports	R/O ?	explicit/mask
Transport Protocol	R/R	value(s)
User ID	R*/NO	OS-specific
Security Label	O/O	IPSO/CIPSO
Priority (IPv6 only)	R/R	values(s)
Flow label (IPv6 only)	R/R	values(s)

R= required, O= optional

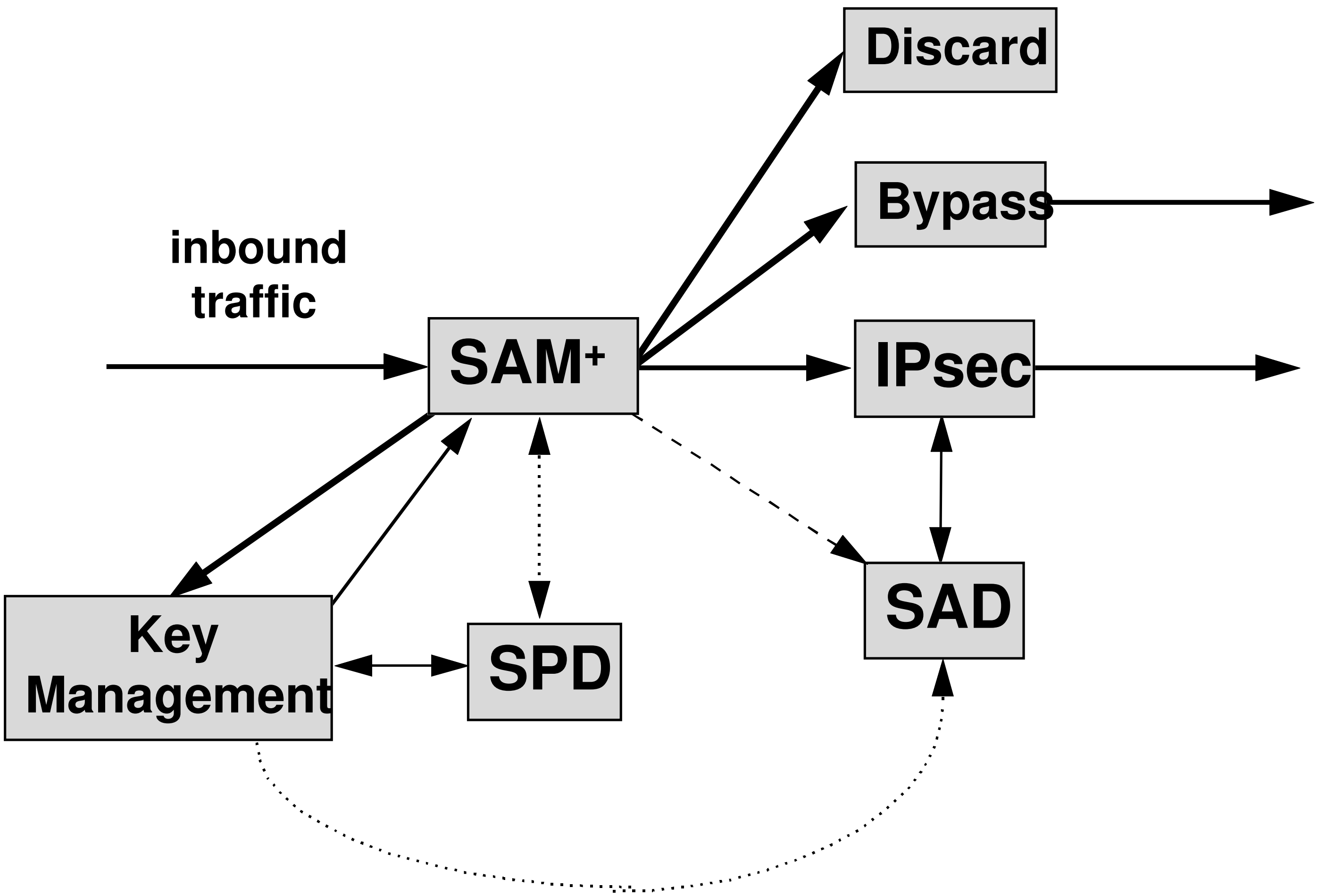
SPD, SAM, & SAD

- Security Policy Database: a database used to
IPsec services, if any, are applied to traffi
be applied, one or more SAs will be invoked,
Traffic flows are characterized by selectors,
selectors may overlap, this database must be
- Security Association Map: a database used to
traffic to an SA (or SA bundle). The mapping
This database is required for BITS, BITW, and
iplementations, but not for socket interface
- Security Association Database: a database con
parameters. Outbound traffic is mapped to th
from the SAM; inbound traffic is mapped by De
address, IPsec protocol, and SPI.

Outbound Processing Example



Inbound Processing Example



Unresolved Issues

- Tunnel mode header processing
  - document contains strawman. RFC 1853 defines simple processing for IPv4, but does not address inbound pr
- PMTU: trusted vs.untrusted sources
  - document currently defines how to manage MTU based c ICMP from any source, trusted or not. potential deni problems
  - Richardson I-D is a start at dealing only with trust
- Conformance requirements
  - IPv6 compliance calls for AH and ESP, but what about
  - since AH and ESP both point to this document, can ar only implementation be compliant?
  - what AH & ESP combinations are required in hosts vs.

Required AH and ESP Combinat

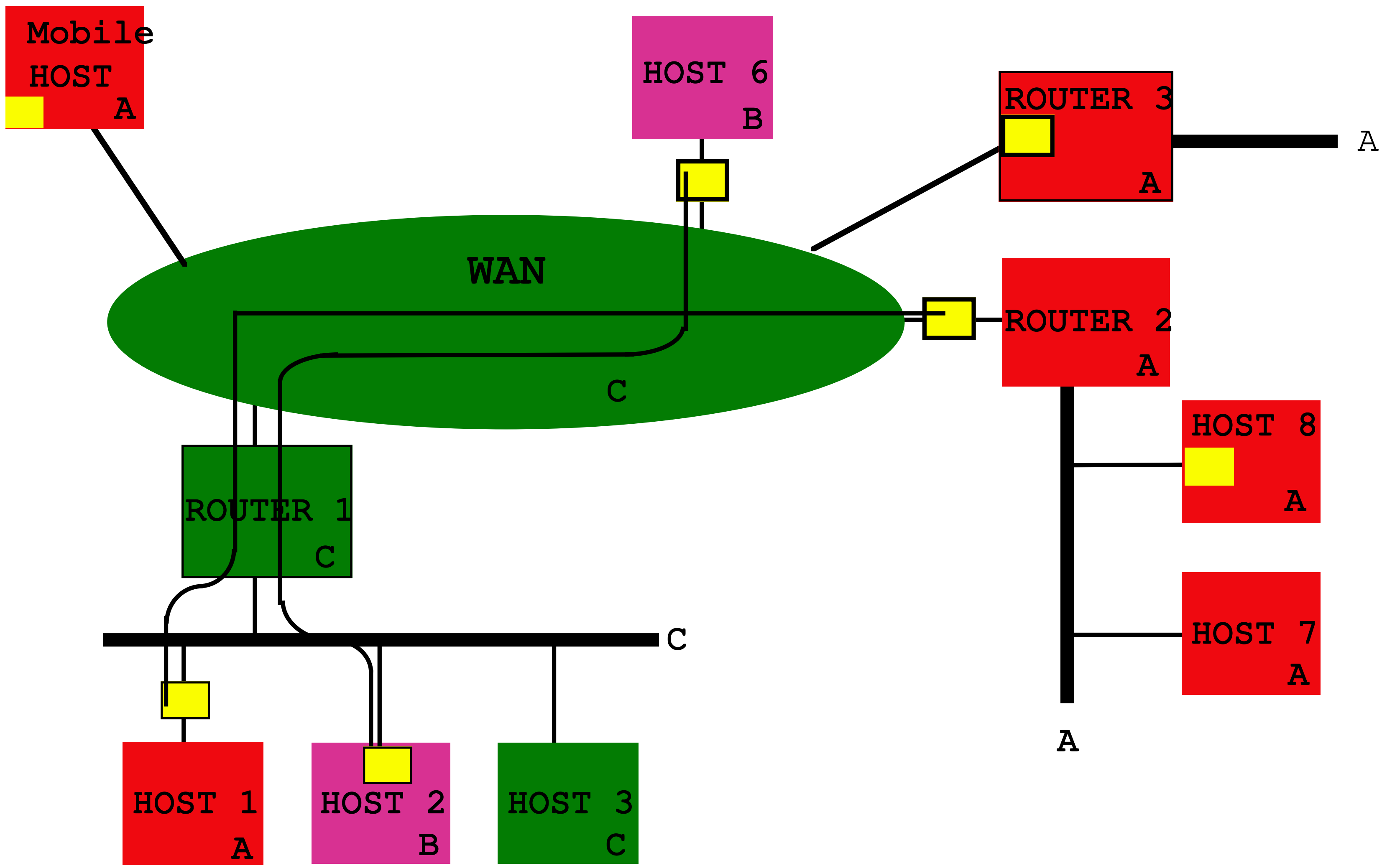
TRANSPORT MODE

	IP HDR	AH	TRANSPORT ...		
	IP HDR	ESP	TRANSPORT ...		
	IP HDR	AH	ESP	TRANSPORT ...	

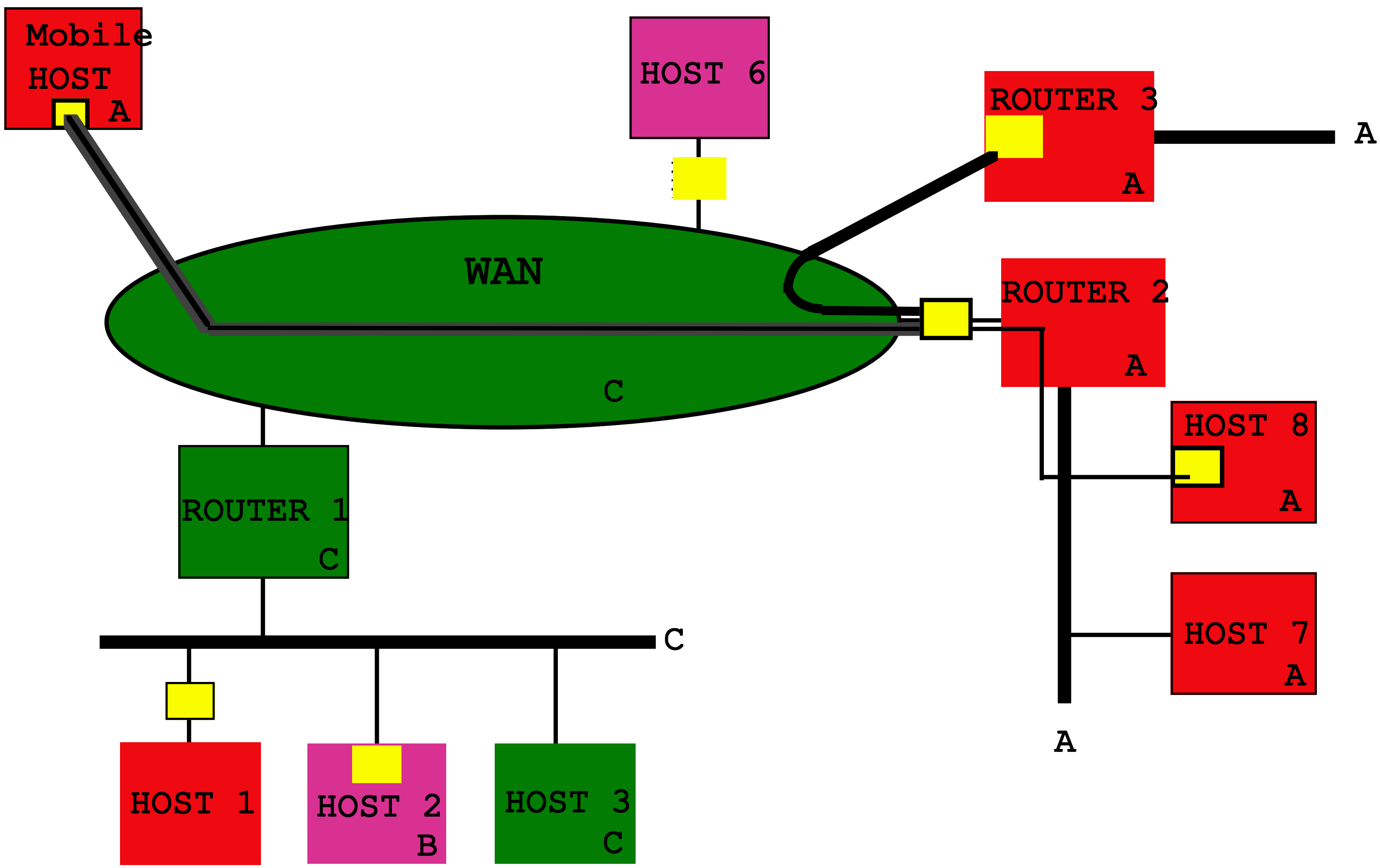
TUNNEL MODE

?	IP HDR	AH	IP HDR	TRANSPORT ...	
	IP HDR	ESP	IP HDR	TRANSPORT ...	
?	IP HDR	AH	IP HDR	ESP	TRANSPORT ...
	IP HDR	ESP	IP HDR	AH	TRANSPORT ...
	IP HDR	ESP	IP HDR	ESP	TRANSPORT ...

IPSEC Path Options



More IPSEC Path Options



Completing the Document

- **More feedback needed from WG members!**
- More detail needed on inbound and outbound pr
  - critical, just a matter of timing, implementor feede
- Usage scenarios (helps explain conformance re
  - critical, just a matter of timing, input would be he
- Automated gateway discovery
  - will be critical, but can defer to separate document
- Information flow security environment requirer
  - not critical for most users, defer to separate docum
- Multicast scenarios and multicast key manageme
  - not yet critical, defer to separate document(s)