Internet Security Association and Key Management Protocol

(ISAKMP)

draft-ietf-ipsec-isakmp-03.txt, .ps

Mark J. Schertler
Office of INFOSEC Research and Technology
National Security Agency

phone: (301) 688-0850
email: mjs@tycho.ncsc.mil

FUNDAMENTALS

- Security Protocol Independence
  - IP ESP / AH
  - Session Layer Security Protocols (SSL, PCT Record Protocol)
  - Routing Protocols (RIP-II Authentication, OSPF Authentication)
  - Others: IEEE 802.10 Secure Data Exchange (SDE), Transport Layer Security

  BENEFIT: Avoid Proliferation of Handshake, Authentication, and Key Exchange Protocols on Internet

- Security Policy Independence
  Internal / External / Allies

  BENEFIT: This Is The Current Government And Corporate Environment

- Security Mechanism / Algorithm Independence
  Define Base Security Attributes for NOW

  BENEFIT: Allows Migration Path for FUTURE

UPDATES FROM ISAKMP V2

- User Negotiation Protected by Server Established SA
- Situation
- Authentication Only Exchange
- Version Number

PROTOCOL COMPARISIONS

- SKIP - Solution For Connectionless Protocols

  Discovery Protocol Actually Connection Oriented

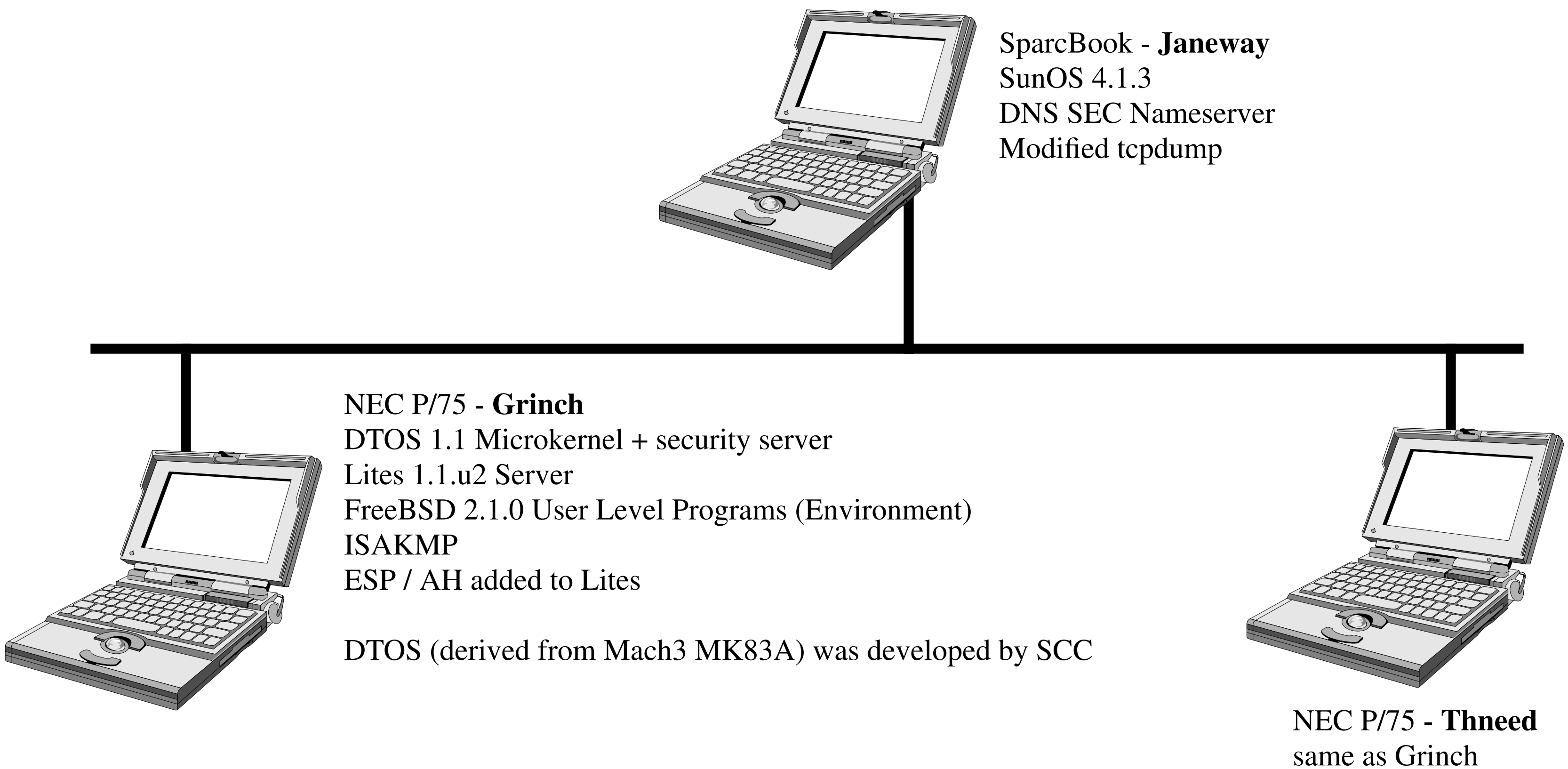
- Photuris - Solution For ESP and AH

  Single Key Exchange Algorithm and Key Derivation
  - Eliminates Use Of Security Tokens in Future

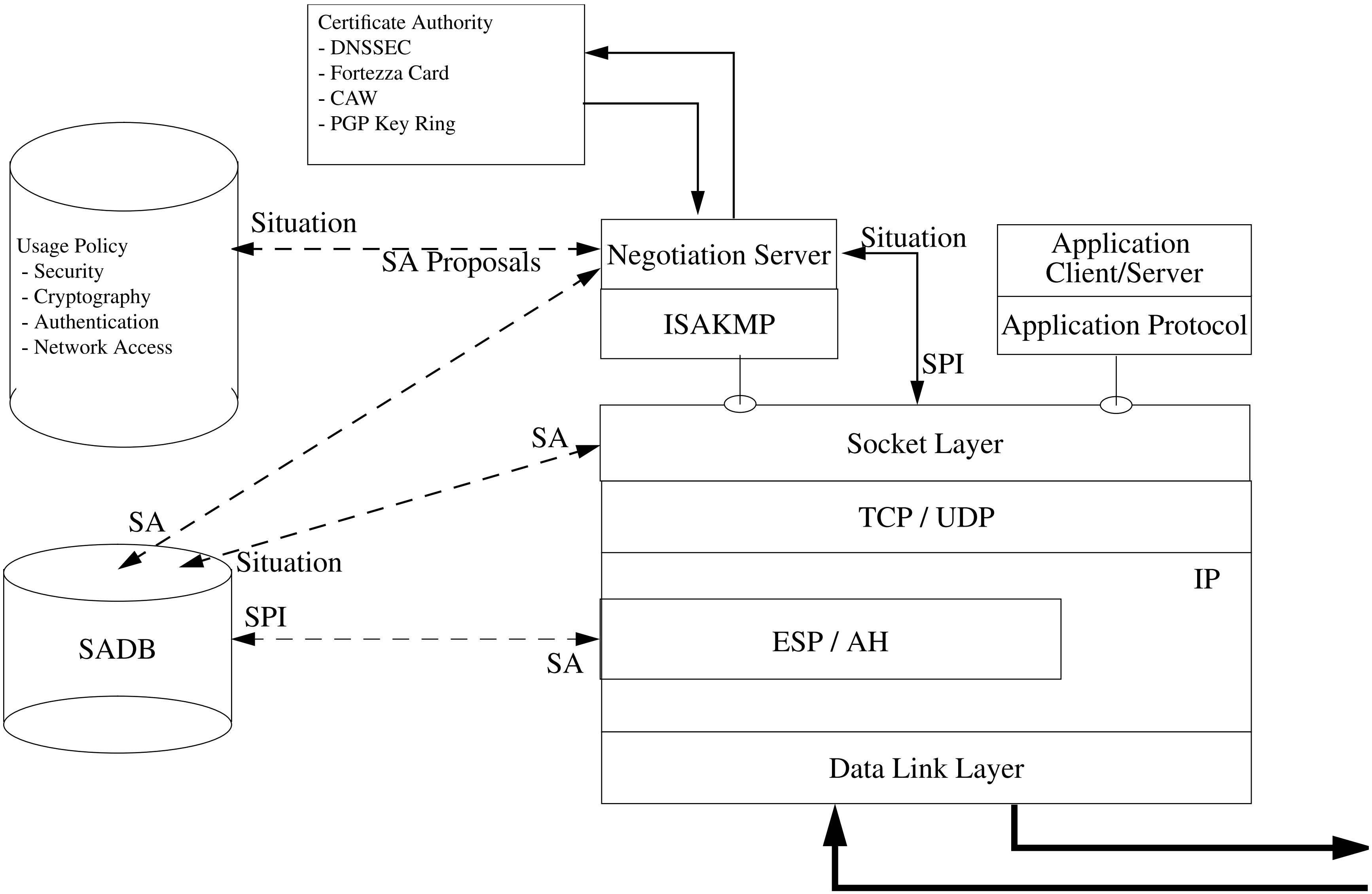
- ISAKMP - Solution for Security Protocols on Today's Internet

  Can Perform Functions of SKIP Discovery Protocol
  Can Perform Photuris Functionality and Key Exchange

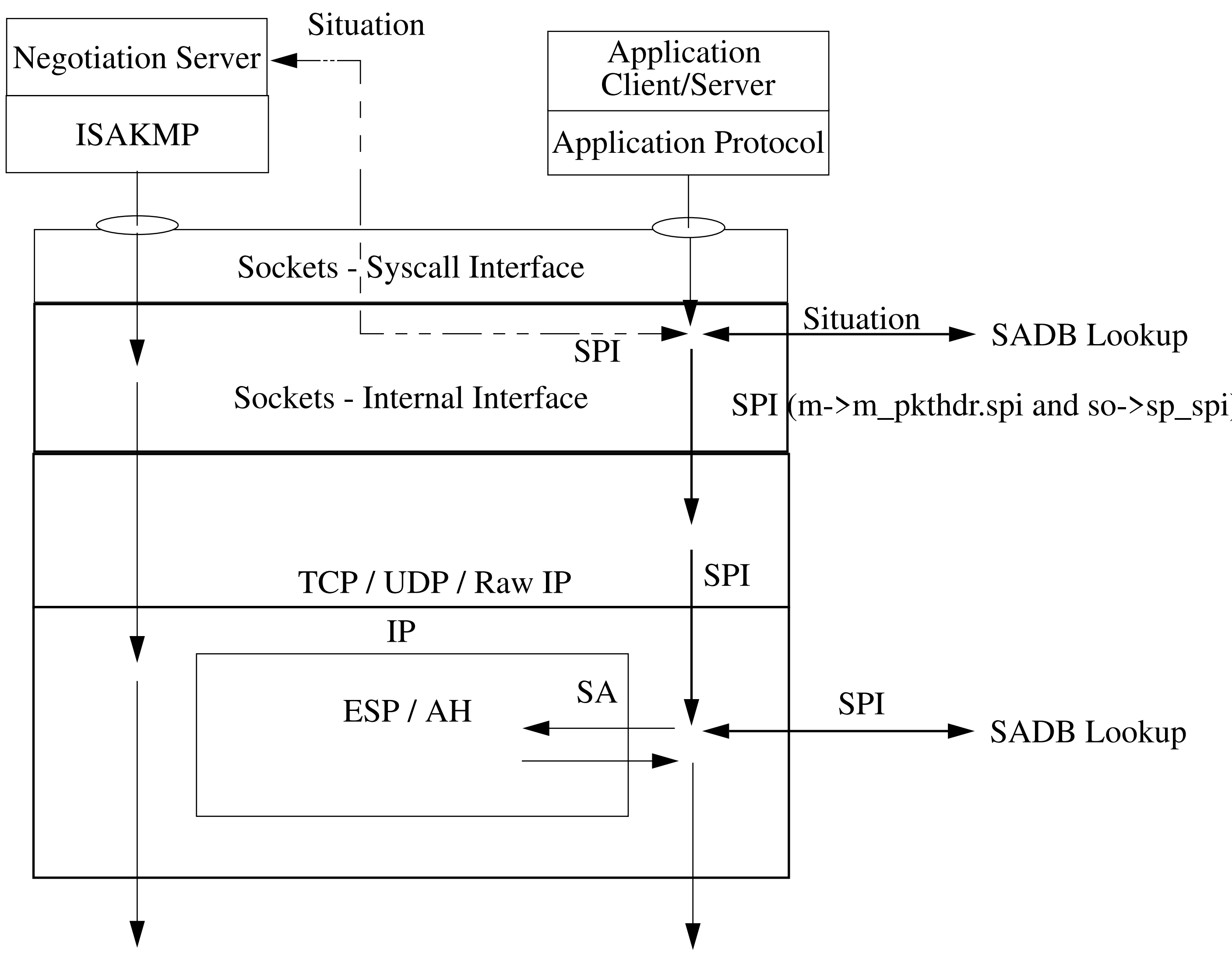
DEMO HARDWARE / SOFTWARE CONFIGURATION



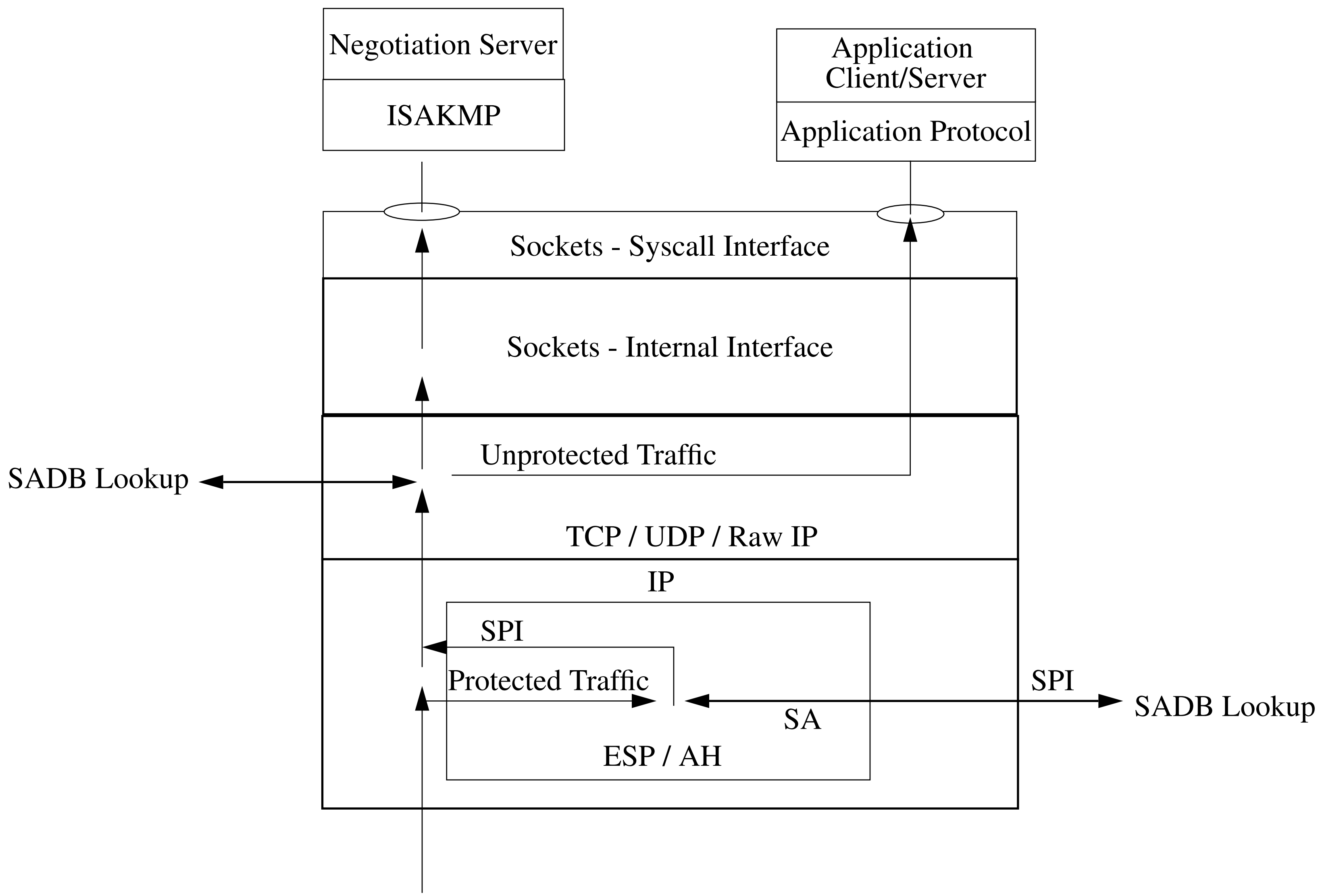
NETWORK ARCHITECTURE



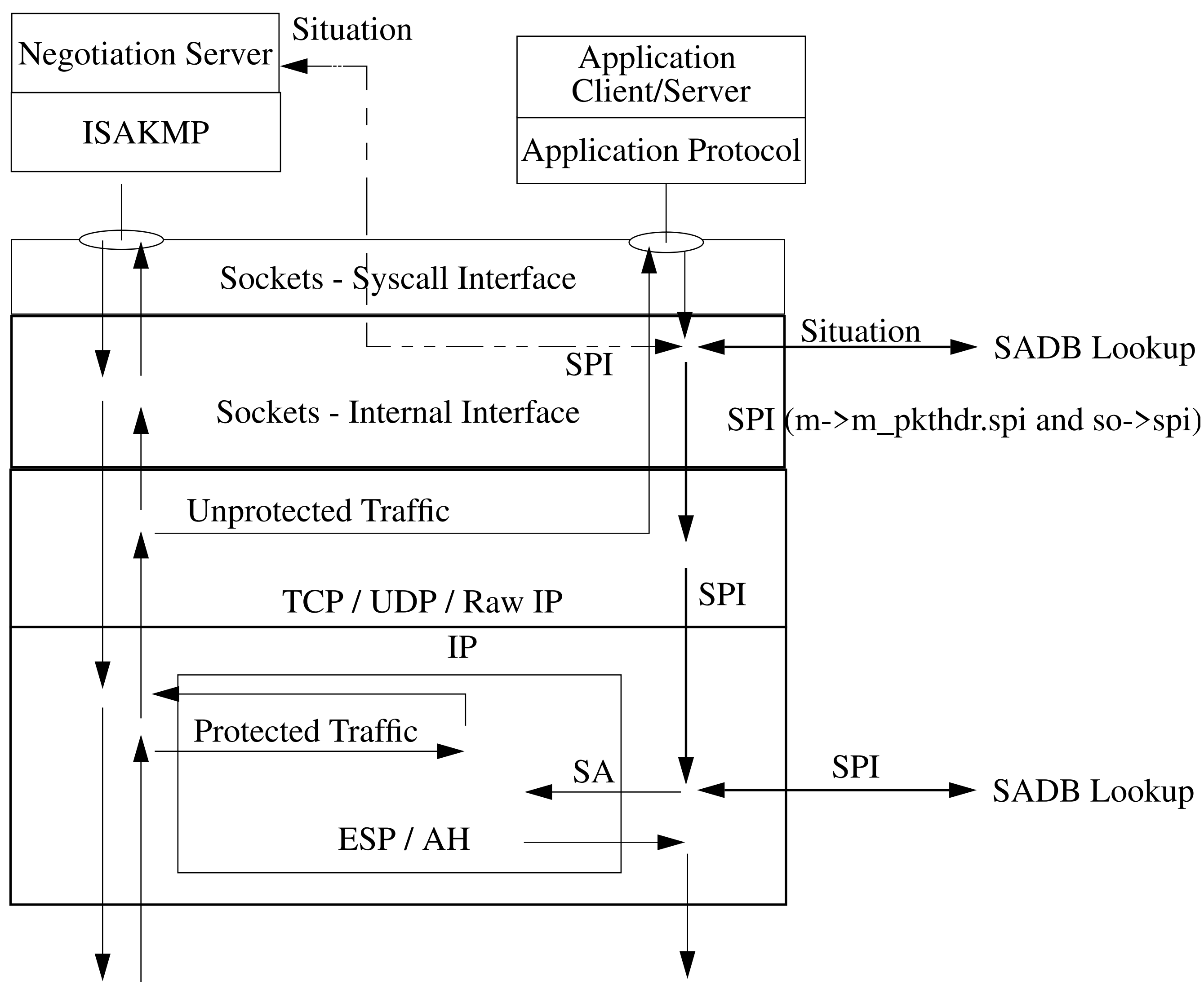
NETWORK STACK MODIFICATIONS - OUTGOING THREAD



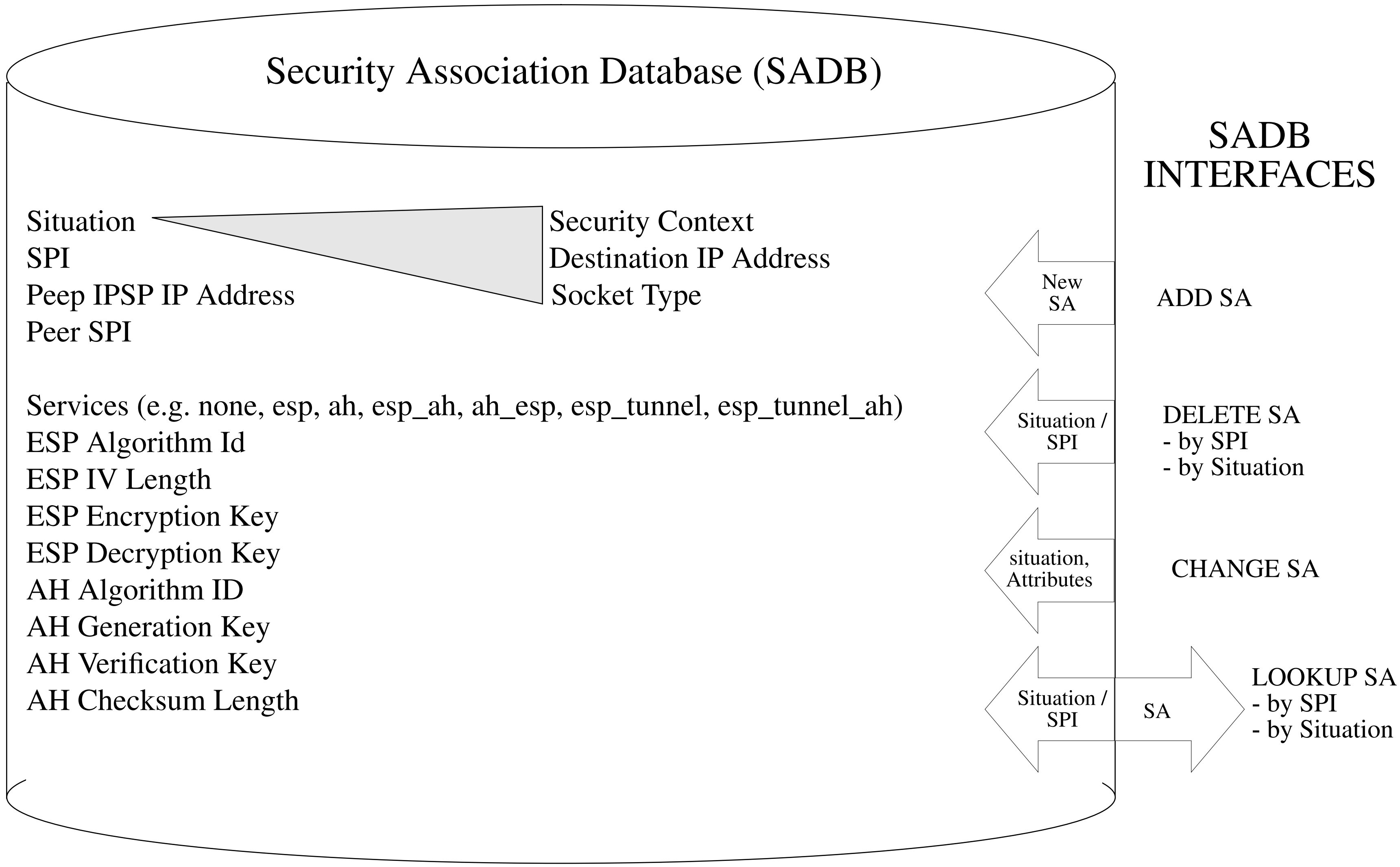
NETWORK STACK MODIFICATIONS - INCOMING THREAD



NETWORK STACK MODIFICATIONS - Complete THREAD



SECURITY ASSOCIATION DATABASE



CONCLUSIONS

- Security Protocol Independence

  - Security Attribute Grouping
  - Protocol Identifier for SA groupings

- Security Policy Independence

  - Situation Identifier
  - Security Attribute Grouping

- Security Mechanism / Algorithm Independence

  - Security Attribute (e.g. Key Exchange, Authentication) Identifiers