A Reference Model for Firewall Technology

SPARTAN Symposium
University of Kansas, Lawrence
March 18-19, 1997

Christoph L. Schuba[1,2]
J. Bryan Lyles[1] and Eugene H. Spafford[2]

Computer Science Laboratory[1]
Xerox PARC
3333 Coyote Hill Road
Palo Alto, CA 94304-1314
{lyles,schuba}@parc.xerox.com

COAST Laboratory[2]
Purdue University
1398 Computer Science Building
West Lafayette, IN 47907-1398
{schuba,spaf}@cs.purdue.edu

Project funded by: Sprint Corporation, Xerox Corporation and other COAST sponsors

Motivation

Background

Problem

Reference Model

New Mechanisms

Conclusions and Contributions

Motivation

- Communication systems continue to be a fundamental infrastructure resource
- Risks for
  - Computation and communication resources
  - Data
  - Reputation
- Focus on
  - Firewall technology
    (one piece of a large security puzzle)

Background

Host-based security insufficient to address network security.

Mechanisms for Firewall Technology

- Packet-filtering routers
- Network address translators
- Circuit-level gateways
- Application-level gateways

...often a combination thereof.

Definition

We define firewall technology as a set of mechanisms that collectively enforce a network domain security policy on communication traffic entering or leaving a guarded network policy domain.

A firewall system, or short firewall is an instantiation of firewall technology.

Potential Advantages of Firewall Technology:

- Protection
- Controlled exposure of internal topology and external traffic
- Simplification of installation, configuration, and management of security functions
- Audit capability
- Focus of security decisions
- Transparency to user (not always...)
- Availability of technology

Shortcomings of Firewall Technology:

- No replacement for good host security
- Limited protection against

  malicious insiders
  tunneled connections
  data driven attacks
  novel attacks

- No protection against connections that circumvent firewall
- Operational difficulties

Problem

Problem Statement

Current firewall technology is not based on scientific principles, but rather ad hoc engineering solutions, and it does not offer sufficient mechanisms for new high performance networking technologies.

Search for

1. Reference Model
2. New Mechanisms

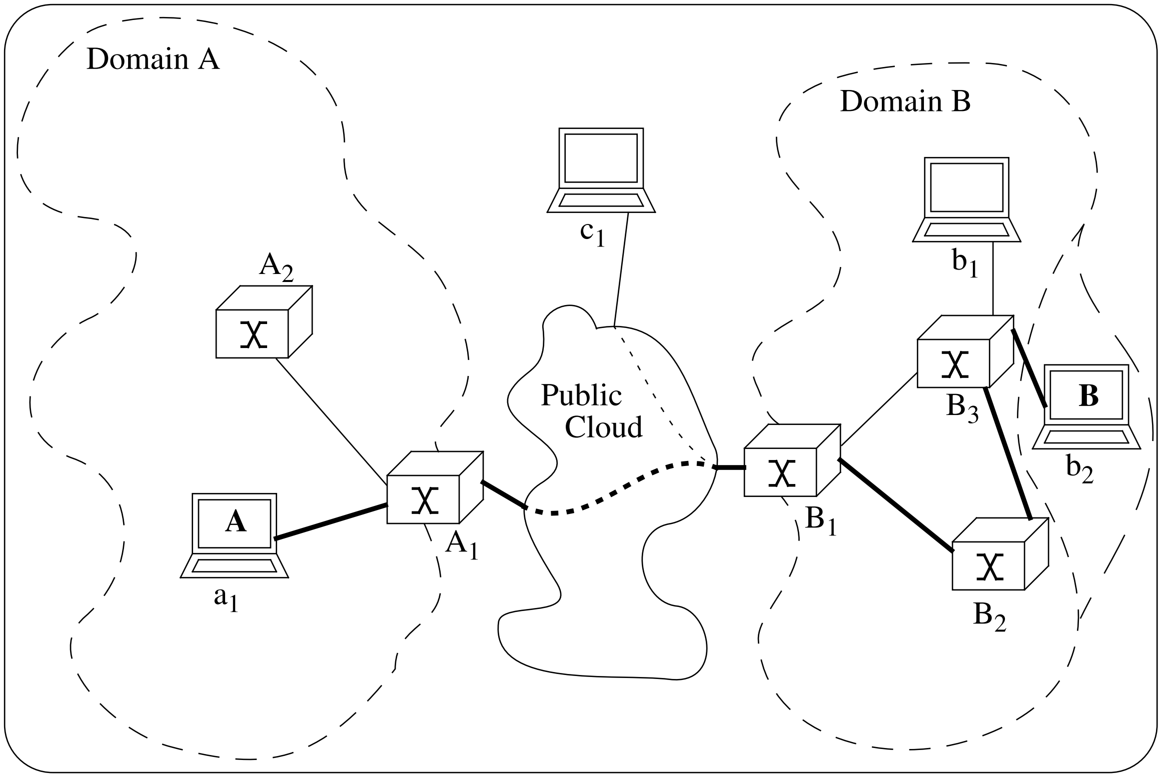
Reference Model

Security Services

- Authentication
- Access Control
- Audit
- Integrity - (protection against unauthorized modification)
- Confidentiality - (protection against disclosure)
- Accountability - (non-repudiation)

...of what?

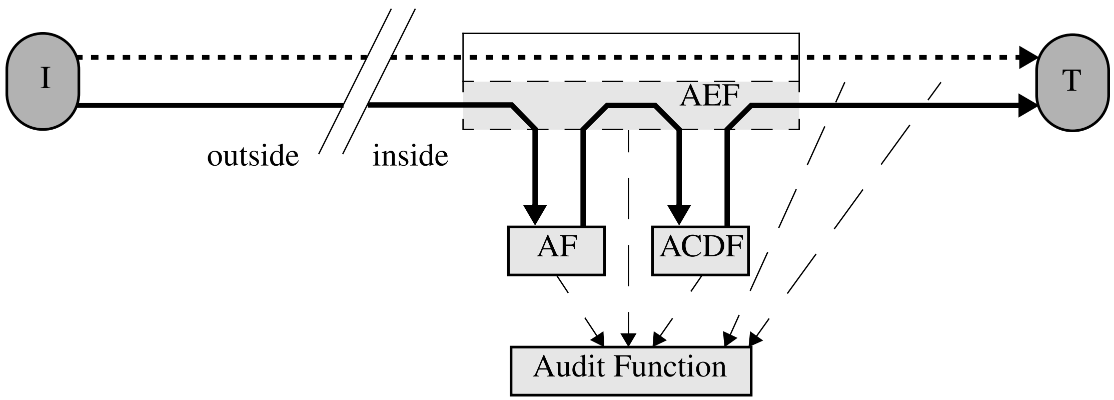
Example



Assumptions

- Secure public key infrastructure, name service
- Secure binding between principals and keys
- Integrity of trusted computing base
- Strength of cryptographic algorithms
- Policy can be captured

Reference Model



I	Initiator		Data traffic
T	Target		Control traffic
AEF	Access Enforcement Function		Audit data flow (AUDIT)
AF	Authentication Function (AUTH)		
ACDF	Admission Control Decision Function (ACTL)		

Essential Components

- AUTH - authentication function
- ACTL - access/admission control decision function
- AUDIT - audit function

Some Important Issues

- Unilateral/mutual authentication
- Unicast/multicast communication
- Centralization and delegation of security policy
- Distribution of its enforcement
- Statement of policy

Importance of *Connections* for Network Security

- Security context/association
- Separation of control information and data
- Quality of service -> availability
- Natural mapping to higher level entities desired

  Example: authenticated `nv` streams

New Mechanisms

- High Performance Packet Filtering
- High Performance Key-agile Encryption and Crypto Synchronization
- Signaling Support for Authentication
- Signaling Support for Other Security Services

Challenge

Mismatch between:

- functionality provided by available mechanisms
- functionality required for secure firewall architecture

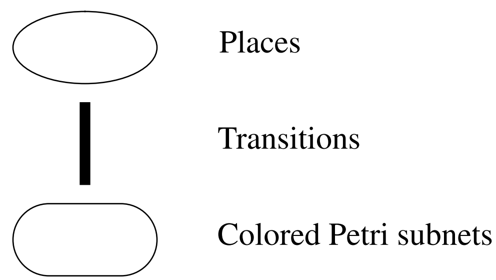
Addressing the Challenge

- Reference model for validation of systems
- Formalism for

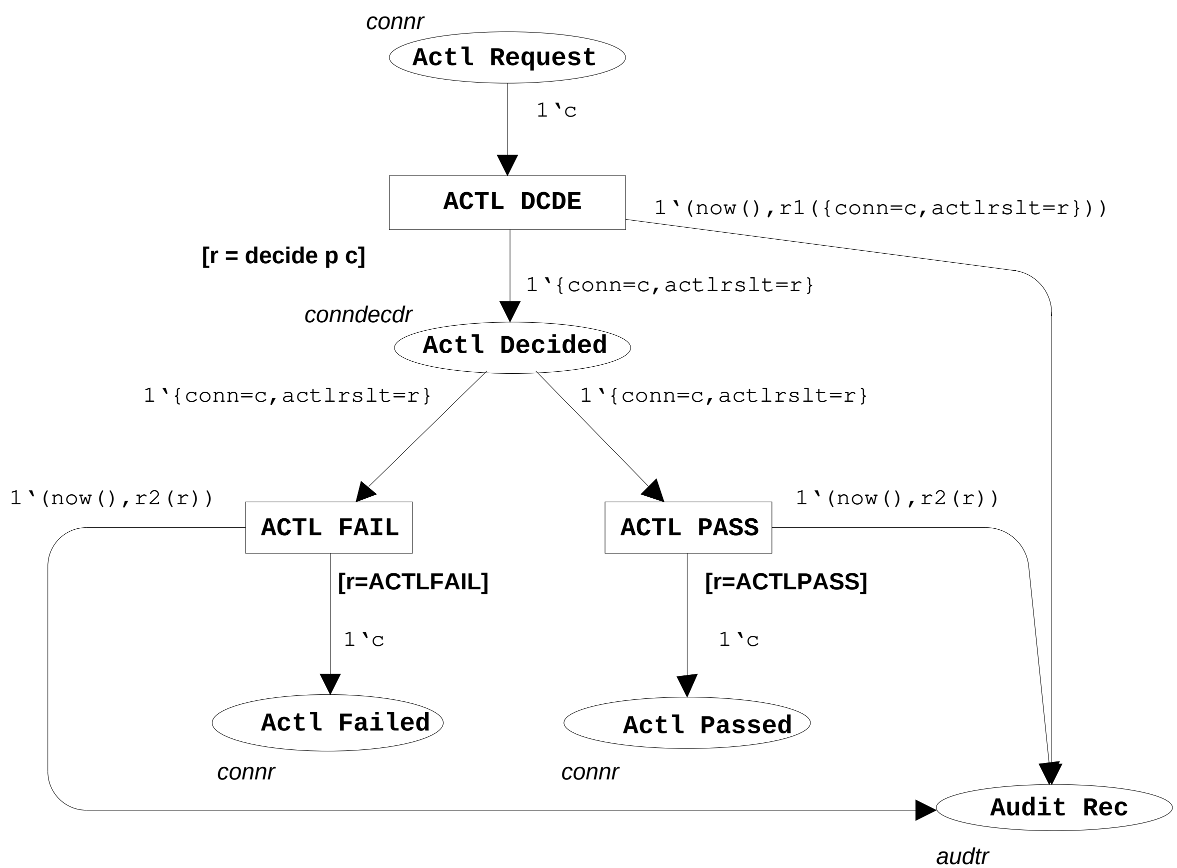
  specification,
  combination,
  simulation, and
  analysis of mechanisms

Formalism

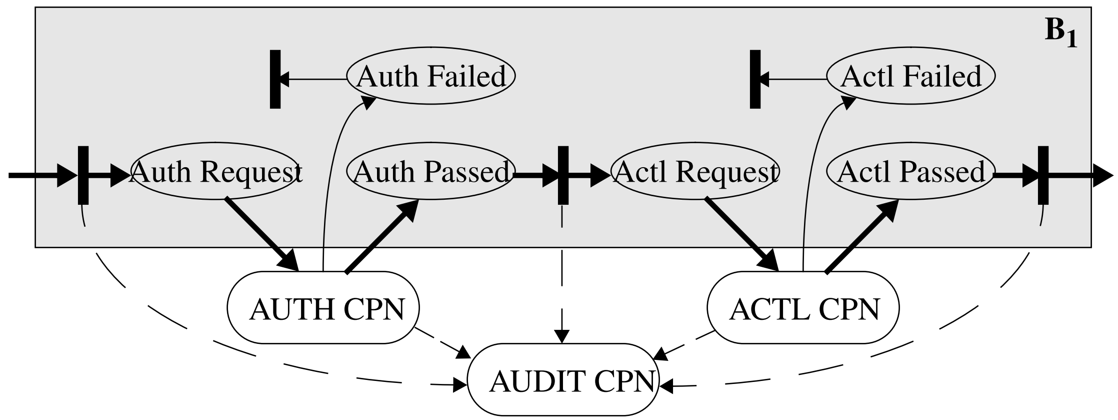
- Colored Petri Nets (CPN)



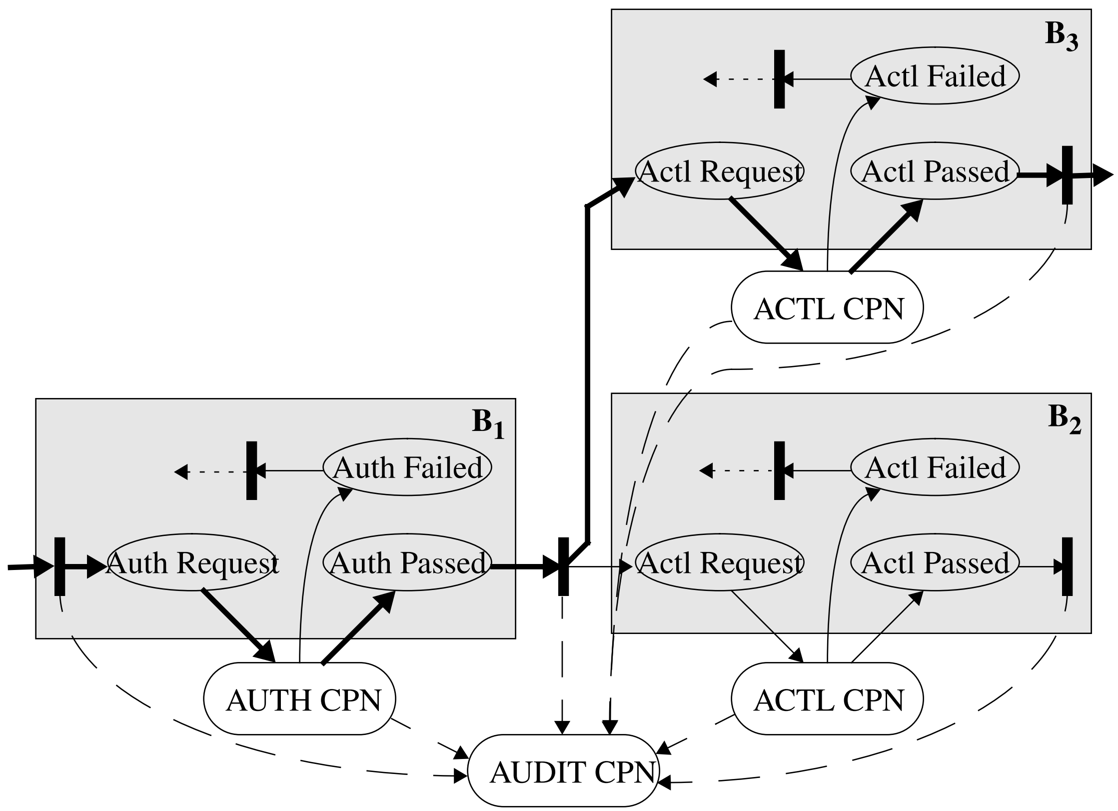
Example


connr
Actl Request
1`c
ACTL DCDE
1`(now(),r1({conn=c,actlrslt=r}))
[r = decide p c]
1`{conn=c,actlrslt=r}
conndecdr
Actl Decided
1`{conn=c,actlrslt=r}
1`{conn=c,actlrslt=r}
1`(now(),r2(r))
ACTL FAIL
ACTL PASS
1`(now(),r2(r))
[r=ACTLFAIL]
[r=ACTLPASS]
1`c
1`c
Actl Failed
Actl Passed
connr
connr
Audit Rec
audtr

Example: Centralized case



Example: Distributed case



Conclusions

- Concept of firewall technology is viable in connection-oriented high speed networks

Contributions

- Definition of firewall technology
- Introduction of a reference model
- Investigation of new mechanisms
- Development of a formalism for mechanisms
- Design and Implementation of new mechanism for ATM