ATM Firewall Technology: Lessons for Intrusion Detection

Workshop on Computer Misuse and Anomaly Detection (CMAD) IV
Monterey, CA

November 12-14, 1996

Christoph L. Schuba

Purdue University
COAST Laboratory
1398 Department of Computer Sciences
West Lafayette, IN 47907- 1398

schuba@cs.purdue.edu

Overview

Problems

ATM Firewall Technology

Lessons

Problems

Quality of Audit Data in Large Systems

- Level of detail vs. amount of data:

  >compression, reduction/aggregation, deduction

- Context of data:

  >users, connections, actions,. ..

- Value of data:

  > authenticity, integrity

E.g., IP, ATM addresses (low level access, e.g., /dev/ip)

Integration of Intrusion Detection and System Design

- Design of large scale distributed systems is *hard*
- Getting designers to include security is *harder*
- Adding intrusion detection support mechanisms is ______

ATM Firewall Technology

Goal

Develop Model for ATM Firewall Technology

Instantiation of Model (Implementation):

- Proof of concept
- Gaining practical experiences

Background and Definitions

Definition Firewall Technology:

Mechanism to help enforce access policies about communication traffic entering or leaving networks.

ATM Technology

- Developed for use in B-ISDN
- Switching of small fixed-length packets (cells)
- Pt-to-pt, pt-to-mpt communication
- Connection-oriented

- permanent connections: administrative mechanisms
- switched connections: connection establishment protocol

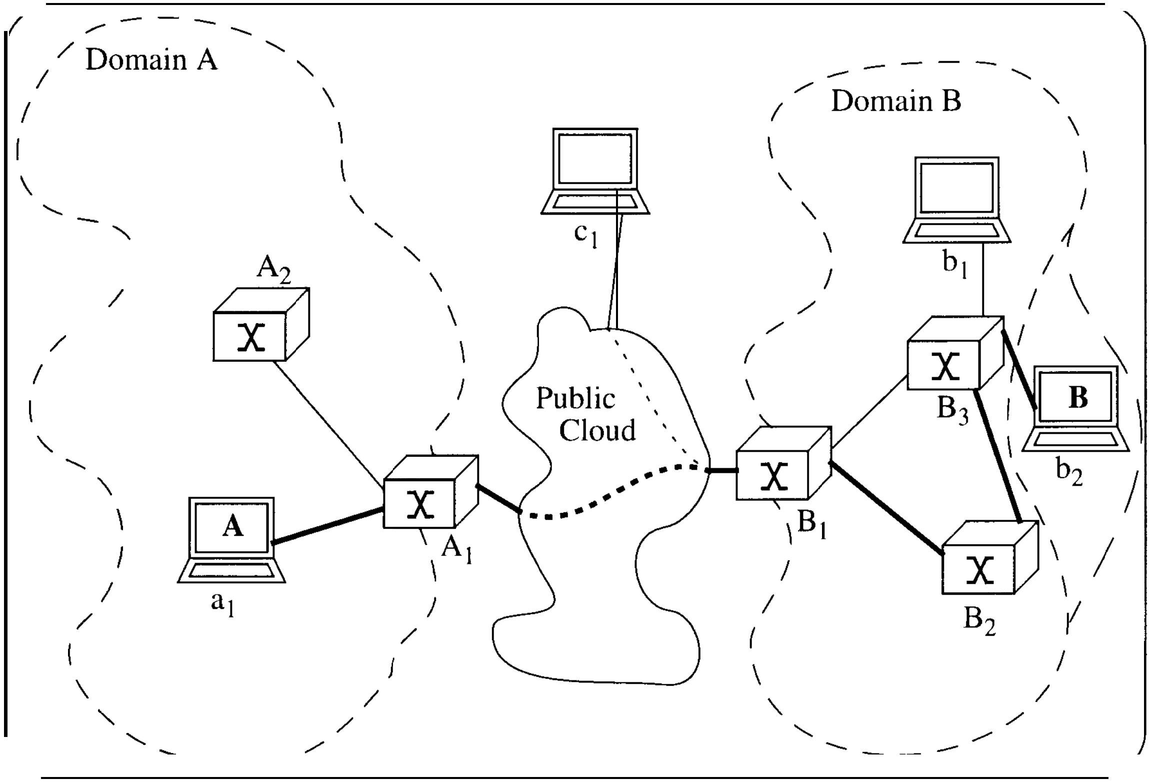
- Quality of service guarantees

IP over ATM

Interesting case for the purpose of this workshop session:

- ATM: spans local-wide area networks systems
- ATM: still room for standard improvement
- IP: legacy system baggage

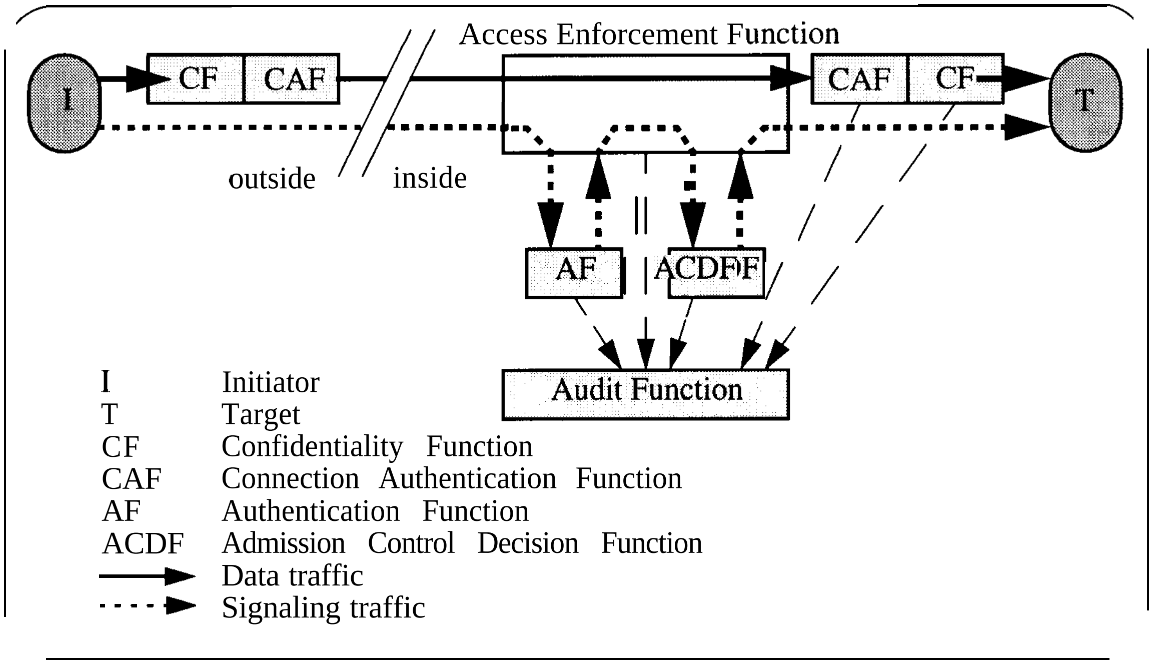
Example



Assumptions

- Connection oriented character of communication
- Secure public key infrastructure, name service
- Secure binding between principals and keys
- Integrity of trusted computing base
- Strength of cryptographic algorithms

Reference Model



I	Initiator
T	Target
CF	Confidentiality Function
CAF	Connection Authentication Function
AF	Authentication Function
ACDF	Admission Control Decision Function
——►	Data traffic
- - - -►	Signaling traffic

Essential Elements

- Endpoint authentication
- Domain based call admission control
- Connection authentication (authenticity and integrity)
- Audit
- Centralized policy with distributed service and enforcement

Contributions

- Concept of firewall technology is viable in connection-oriented highspeed networks
- Five elements are essential for a reference model of firewall technology
- Few additions to signaling protocol and system are necessary and sufficient for implementation

Lessons

(Quality of Audit Data)

1.) Authenticity

- Lack of authenticity - see ATM firewall architecture
- Context establishment problem - security context
- Level of detail - e.g., information elements

(Integration of ID and System Design)

2.) Functional Dependencies

Between *authentication* and *access control*

Between *audit* and *all other security services!*

Now, who *acts* accordingly?

3.) Prevention vs. Detection/Recovery

There should be no tension between *prevention* and *detection*

There should be an *integrated approach*, where

- Preventive mechanisms operate under the assumption that they will fail in certain circumstances
- Preventive mechanisms should provide as much help for detection mechanisms as possible

4.) **Intrusion Detection List of Mechanisms**

What basic *mechanisms* are necessary (e.g., audit; secure, reliable communication)?

Make certain this list becomes second nature for system designers.

5.) Motivation for Businesses

Leverage off advantages for other industries

- Telecommunication carriers want nonpudiable billing information
- Identical mechanisms required for billing and ID

Pay close attention to justifying our case not for the sake of ID alone, but also different business needs that can be fulfilled.