

# ATM Security

1997 RSA Data Security Conference

January 31, 1997

G.M. Haskins

bruman@wpi.edu

C. Paar

christof@wpi.edu

---

Worcester Polytechnic Institute ECE Dept  
Research Partially Funded by Lockheed Martin Corp.

# ATM Security

- ATM Overview
- ATM Security Issues
  - Potential Threats
  - Security Services
  - Design Considerations
  - Security Topology

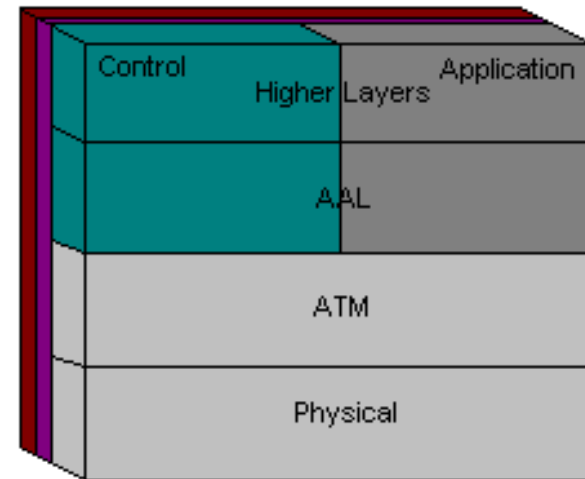
# ATM Overview

## ■ ISDN and B-ISDN

- ISDN=> 64-128 Kbps
- B-ISDN=> 45-622(++ ) Mbps

## ■ ATM

- Scalable, fast, flexible
- Simple model
- Fixed length cell



# ATM Security Issues:

## Threats

- Potential threats against data transfer and network nodes
  - disclosure
  - denial of service
  - modification/insertion/removal
  - illegal access
  - fraud

# ATM Security Issues:

## Security Services

- Solutions using cryptography and security models
  - Privacy
  - Authentication
  - Integrity
  - Access Control
  - Replay Prevention
  - Non-Repudiation

# ATM Security Issues:

## Design Considerations

- Algorithms and Protocols
- Mode of Operation
- Synchronization
- System Agility
- Memory Requirements

# Design Considerations:

## Symmetric Algorithm Requirements

- The block size should divide evenly into 384 bits (The size of the 48 byte ATM cell payload)
- Should be larger than 64 bits for security reasons

Therefore: Block sizes should be one of 64, 128, 196, or 384

- Should be at least the strength of DES
- Should be easy to implement in hardware

# Design Considerations: Algorithms and Protocols

## ■ Encryption

- DES
- FEAL-32

## ■ Key Exchange

- RSA
- Diffie Hellman

## ■ Integrity and Digital Signatures

- RSA
- DSS
- Elliptic Curves

( SHA is used to provide integrity with most algorithms)

# Design Considerations:

## Mode of Operation - Block Ciphers

### ■ ECB

- Very fast
- Simple to implement (No synchronization)
- Weaker security due to one-to-one mapping

### ■ Feedback Modes

- Slower
- More complex
- Requires lock-step between parties
- Higher security
- Can be used to provide integrity checks

# Design Considerations:

## Mode of Operation - Stream Ciphers

- Very fast
- Weak integrity detection

# Design Considerations:

## Synchronization

- Feedback modes must recover from cell loss/corruption
- Designer must decide how to maintain sync between parties.
  - Intelligent AAL marker identification
  - OAM Cells
  - Combination (Required for some classes such as AAL 5)

# Design Considerations: System Agility

- Two main types of agility
  - Key
  - Algorithm
- Key Agility requires loading keys on a per cell basis
  - design constraint with memory designs
  - low access speeds increase cell latency in ATM stream
- Algorithm Agility requires changing algorithms, potentially on a per cell basis
  - More difficult to achieve than key agility because of ATM's dependency on HW encryptors

# Design Considerations:

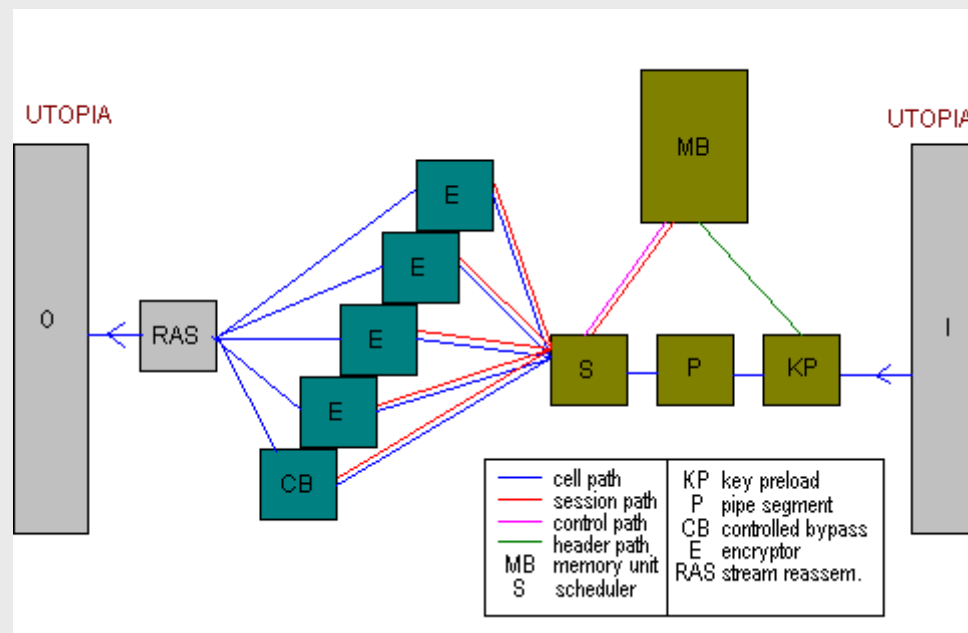
## Memory Requirements

- Keys must be stored on local machines
- Asymmetric keys (Call Establishment)
  - Can be stored off device if HW is not integrated with ATM device
  - Can be stored off device if call establishment encryption is done in software
  - Can be stored in higher latency RAM off local silicon if HW is build into ATM device.
- Symmetric keys (Privacy Service)
  - Must be stored locally.
  - Can consume large amounts of real estate
  - Care must be taken with design to allow fast access

# Design Considerations:

## Scaleable encryptor design

Parallelism can be exploited in several ways to achieve a completely scaleable encryptor design capable of any link rate



# Design Considerations:

## Scaleable encryptor design

- Parallelism on a per cell basis
  - Maintains link rate effectively
  - very low stream latency (equal to  $1/(\text{cell arrival rate})$ )
- Parallelism on a stream basis
  - Also maintains link rate
  - low memory requirements next to cell-parallel designs

# ATM Security Issues:

## Security Topology

- Signaling and Management
- Key Management and Distribution
- Service Location
- Network Placement

# Security Topology:

## Signaling and Management

- Four proposed methods for signaling
  - Q.2931 signaling protocol manages security
  - OAM cells carry signaling inf. OOB
  - Use of call completion delays
  - Auxiliary channel negotiates security inf.

# Signaling and Management:

Q.2931 signaling protocol manages security

Information Elements are added to the existing Q.2931 set to include certificate entries, session keys, labels, etc.

## ■ Advantages

- Very clean
- Easy to understand

## ■ Disadvantages

- May take time to pass in the standards bodies

# Signaling and Management:

OAM cells carry signaling inf. OOB

OAM cells could be transmitted to the remote host to exchange security information, Out-of-Band (OOB) from the original call

## ■ Advantages

- Doesn't need to modify the existing Q.2931 protocol

## ■ Disadvantages

- Would require a multicell OAM transmission, which means changing the AAL specification

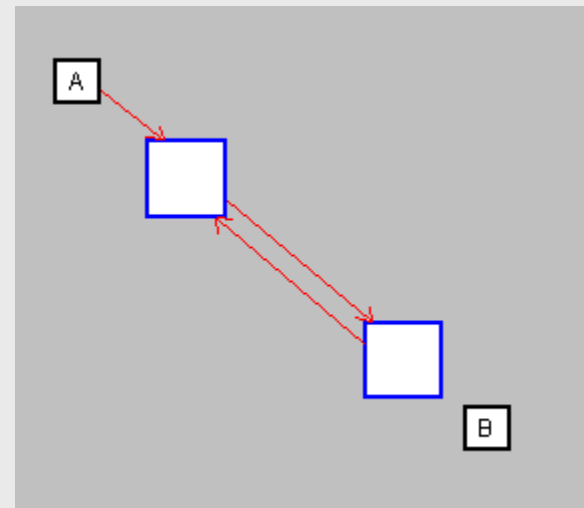
# Signaling and Management:

## Use of call completion delays

Standard call procedures would take place between hosts, but the security devices at each end would hold off making the final connection to the higher layers until negotiations have completed.

### ■ Disadvantages

- Restricted by users QOS



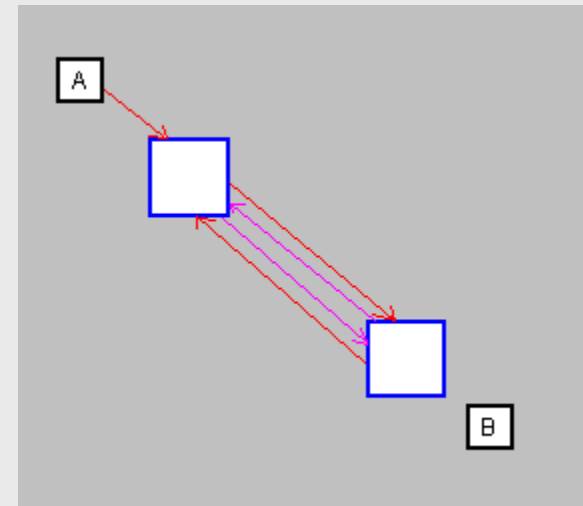
# Signaling and Management:

Auxiliary channel negotiates security inf.

Before connecting the actual call, and auxiliary channel would be opened between the two hosts to negotiate security information.

## ■ Advantages

- Not restricted by QOS



# Security Topology:

## Key Management and Distribution

### ■ Distribution Algorithms

- RSA
- Diffie-Hellman

### ■ Topographical Location for Keys

- Centralized, variable address models
- Centralized, fixed “Certificate” channel allocation

# Security Topology:

## Service Location

- Privacy
- Authentication
- Integrity
- Access Control
- Replay Prevention
- Non Repudiation

Service	UPLANE	CPLANE	MPLANE
Privacy	M		
Authentication	M	M	M
Integrity	R,O	M	M
Access Control	M		
Replay	H,O	M	M
Non Repudiation	H		

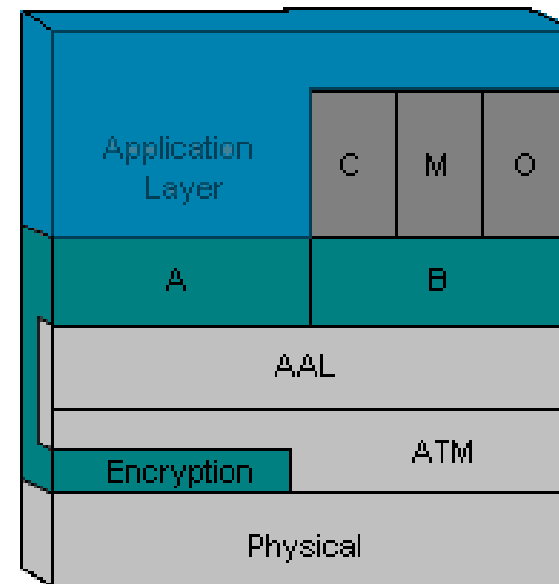
M = Mandatory R = Recommended

O = Optional H = Higher Layers

# Security Topology:

## Service Location - 3D service model

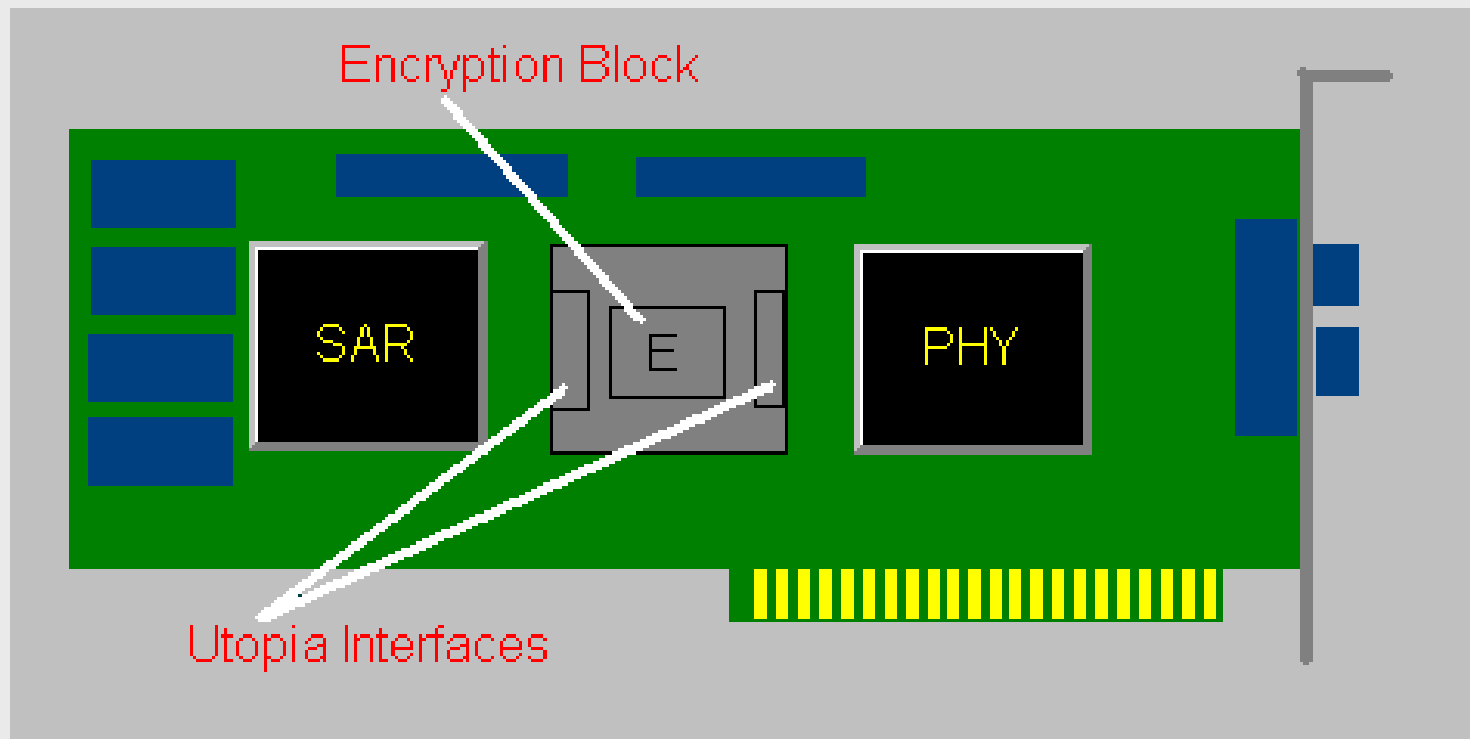
- A Layer
  - Integrity Padding
- B Layer
  - Authentication
  - Access Control
  - Replay Prevention



Note: A and B can be done in software

# Security Topology:

## Service Location - Physical Layout



# Security Topology: Network Placement

- End-to-End
- Edge-to-Edge
- End-to-Edge

