



ATM Security - NOT! (at least NOT YET!)

Joyce Capell

Lockheed Martin Telecommunications

Phone: (408) 543-3185

email: Joyce.Capell@lmco.com

Outline



- Why ATM Networks
- The ATM Security Problem
- Some ATM Network Security Options
- The LM CalREN ATM Network Project
- ATM Encryption Testing
- Initial Test Results
- Conclusions from Testing
- What we learned about ATM Security
- Progress in ATM Security

Why LM is Moving to ATM Network Technology



- Supports high bandwidth applications
 - Multimedia collaboration
 - Virtual Reality
 - Simulations
 - Modeling
 - Interactive video, videoconferencing
- Provides bandwidth on demand
- Scalable performance
- Seamless access between local and wide area networks

The Security Problem



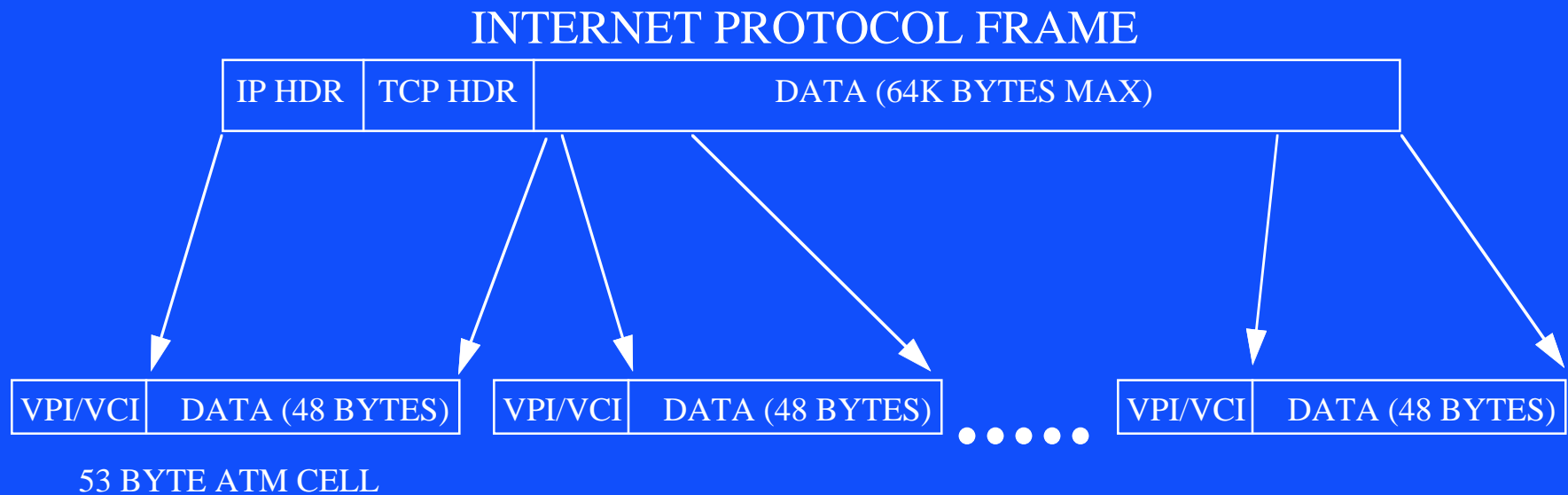
- **IP networks utilize a shared medium to broadcast packets**
 - IP networks provide a “single- point-of-entry” into the network
 - Firewalls are placed at the point of entry to the network
 - ◆ Can screen by address, application (SMTP, telnet, ftp)
- **ATM networks set up multiple switched connections based on signalling**
 - Multiple points of entry into the network
 - Permanent virtual circuits (PVCs) - more secure
 - Switched Virtual Circuits (SVCs) - less secure
 - ◆ Set up connections dynamically - similar to phone calls

Can IP Firewalls Protect ATM Networks?



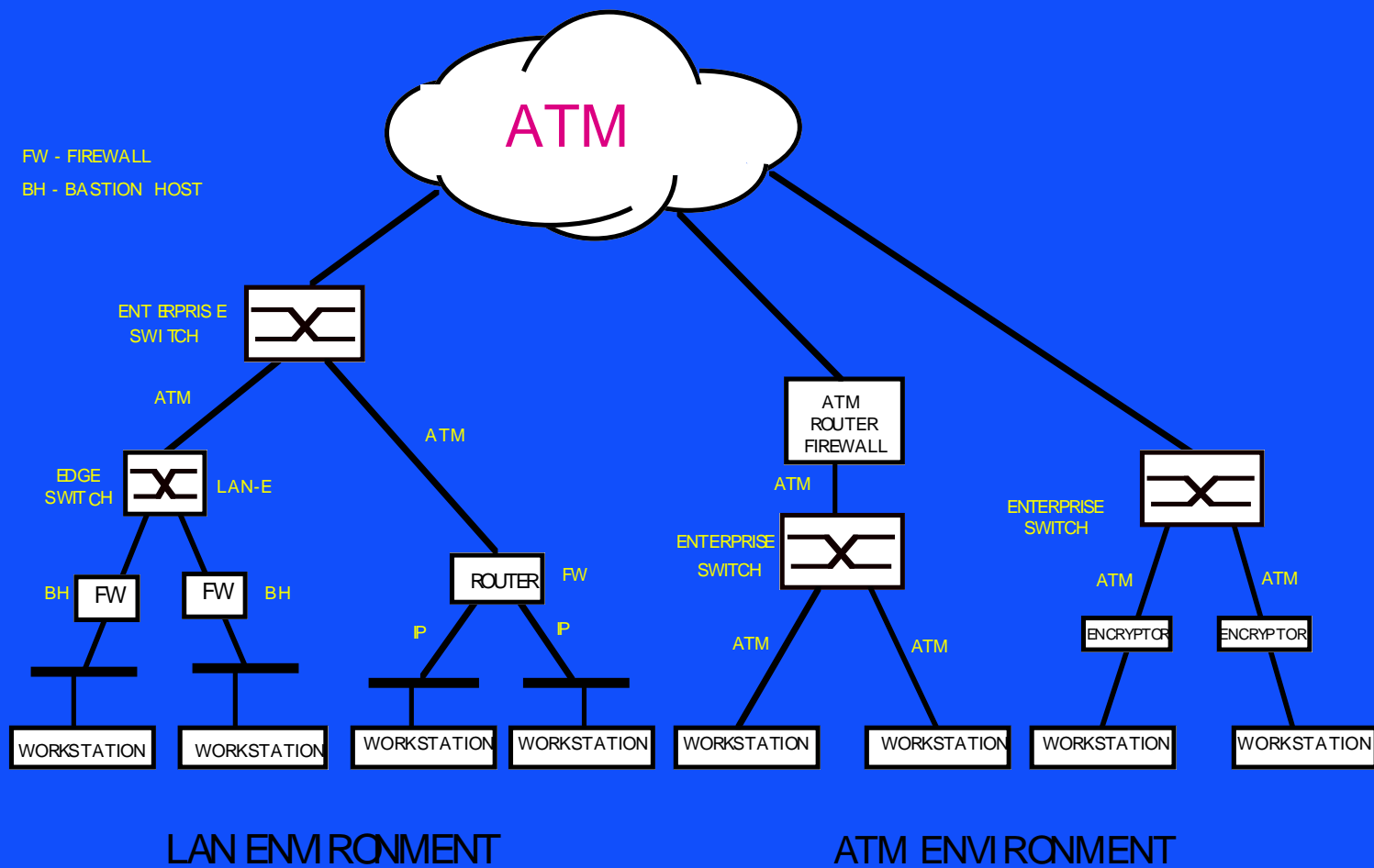
- **ATM networks don't readily support IP firewalls**
 - Firewalls filter based on IP header information
 - ATM breaks IP packets into multiple cells
 - Header information not carried in each cell
 - Cells must be reconstituted into packets before delivery
 - Native ATM applications don't use IP packets
- **Firewalls work in ATM only if IP header information is available**
 - Place firewall after packets are reconstituted
 - Read header information within ATM cells

IP over ATM



**IP packets are broken into multiple ATM cells.
IP header information typically appears in the first cell.**

Some ATM Security Options



PacBell CalREN Project



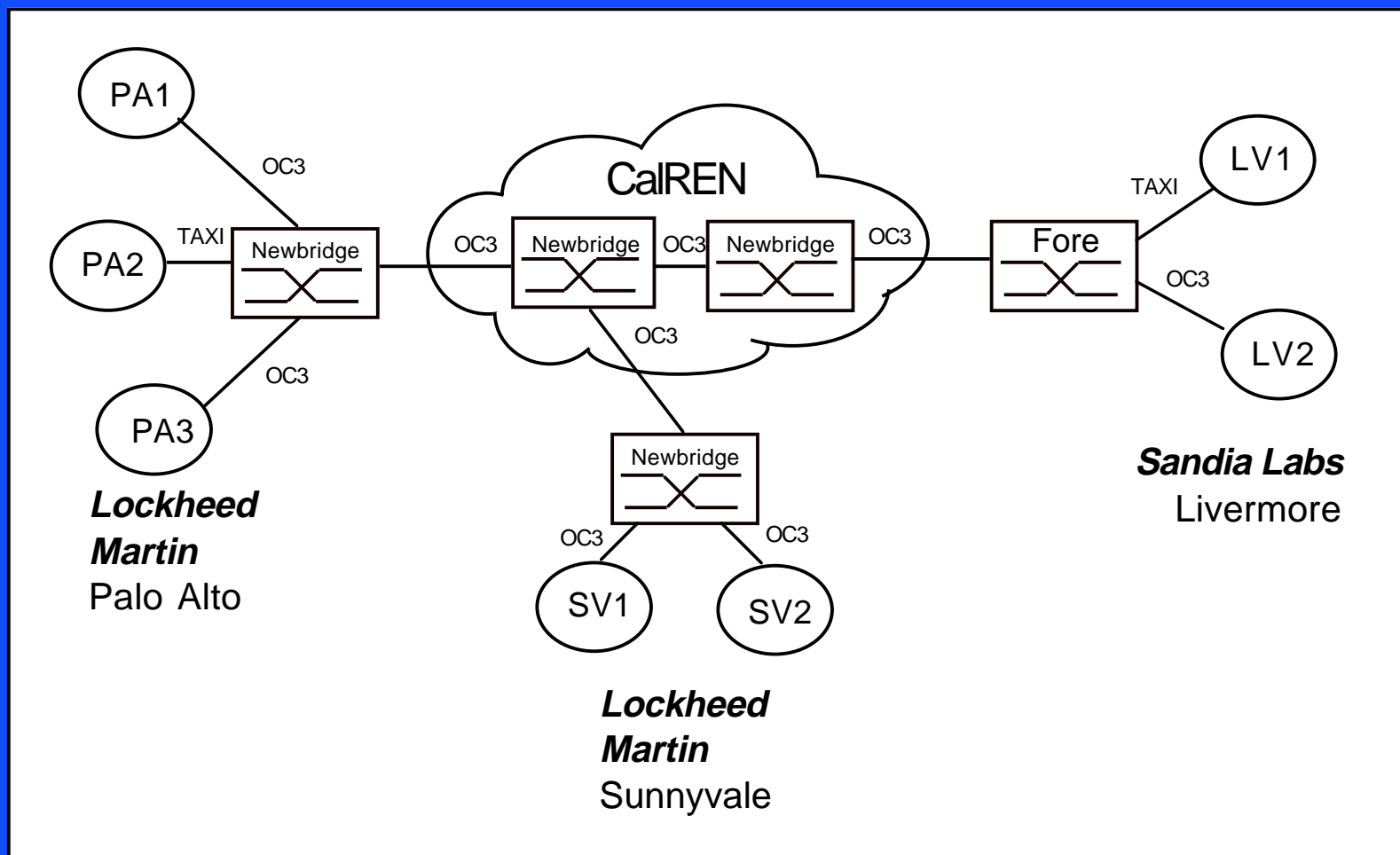
- **PacBell Goal: sell ATM service**
 - Problem: can't sell it if people don't know how to use it
 - Must use it to know why they need to buy it
 - Solution: provide free service to users who will demonstrate how to effectively use ATM
- **Two LM applications were funded**
 - Concurrent Collaborative Design
 - Distributed Interactive Simulation
- **Additional LM Objective: ATM Security**
 - Tested two prototype ATM encryption devices

CaIREN ATM Project



- Pacific Bell sponsored (2 year) ATM network trial
- Lockheed Martin CaIREN team: LM Missiles & Space (LMMS) Co. , Sandia Labs CA & NM, ARPA/DISA JPO, NSA
- OC3 connectivity between 3 sites:
 - LMMS - Sunnyvale
 - LM Research Labs - PaloAlto
 - Sandia Labs- Livermore
- Objective: demonstrate bandwidth demanding applications over an ATM network
 - Demonstrate prototype ATM security devices

LM CalREN Network Testbed



LM CalREN ATM Network Trial



- Applications to be tested:
 - Distributed Interactive Simulation (DIS) - Wargaming
 - Concurrent Collaborative Design - Simulation Based Design for shipbuilding
 - (VR - Immersive environment)
- Encryption testing: two prototype “key agile” ATM encryptors
 - Sandia Labs (NM) “proof-of-concept” encryptor for proprietary data protection
 - NSA “MILKBUSH” “proof-of-concept” encryptor for classified data protection

Prototype Encryptors



- **NSA “MILKBUSH” prototype - box level device**
 - Uses “Vince” ATM drivers: limits performance
 - “Dummy” algorithm
- **Sandia prototype - board level device**
 - Hard wired addresses
 - “Dummy” algorithm

Why ATM Encryptors?



- Only prototype ATM security products available at the time (1993)
- Encryption provides “secure tunnel” through ATM network
 - Secure virtual circuit end-to-end
- Transparent to network and users
 - Not user managed

Original Encryption Test Plan

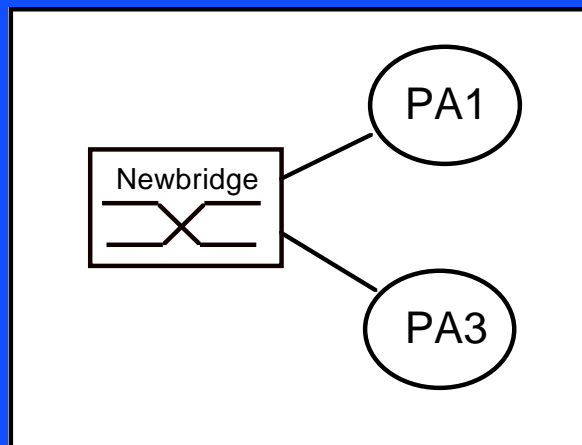


- **Goal:** analyze performance and functionality characteristics of each prototype ATM encryptor
- **Procedure:**
 - Install a pair of encryptors at one site to benchmark performance
 - Move one encryptor to second site and perform same tests
 - Install a third encryptor to test multi-point capabilities
- **Testing:**
 - Measure performance using file transfer
 - Measure performance using applications

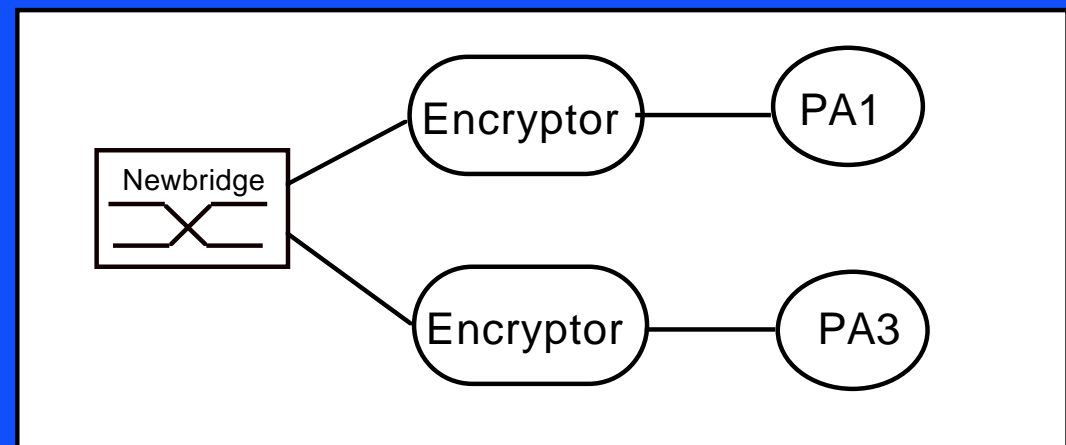
ATM Test Configuration



Benchmark Test Configuration

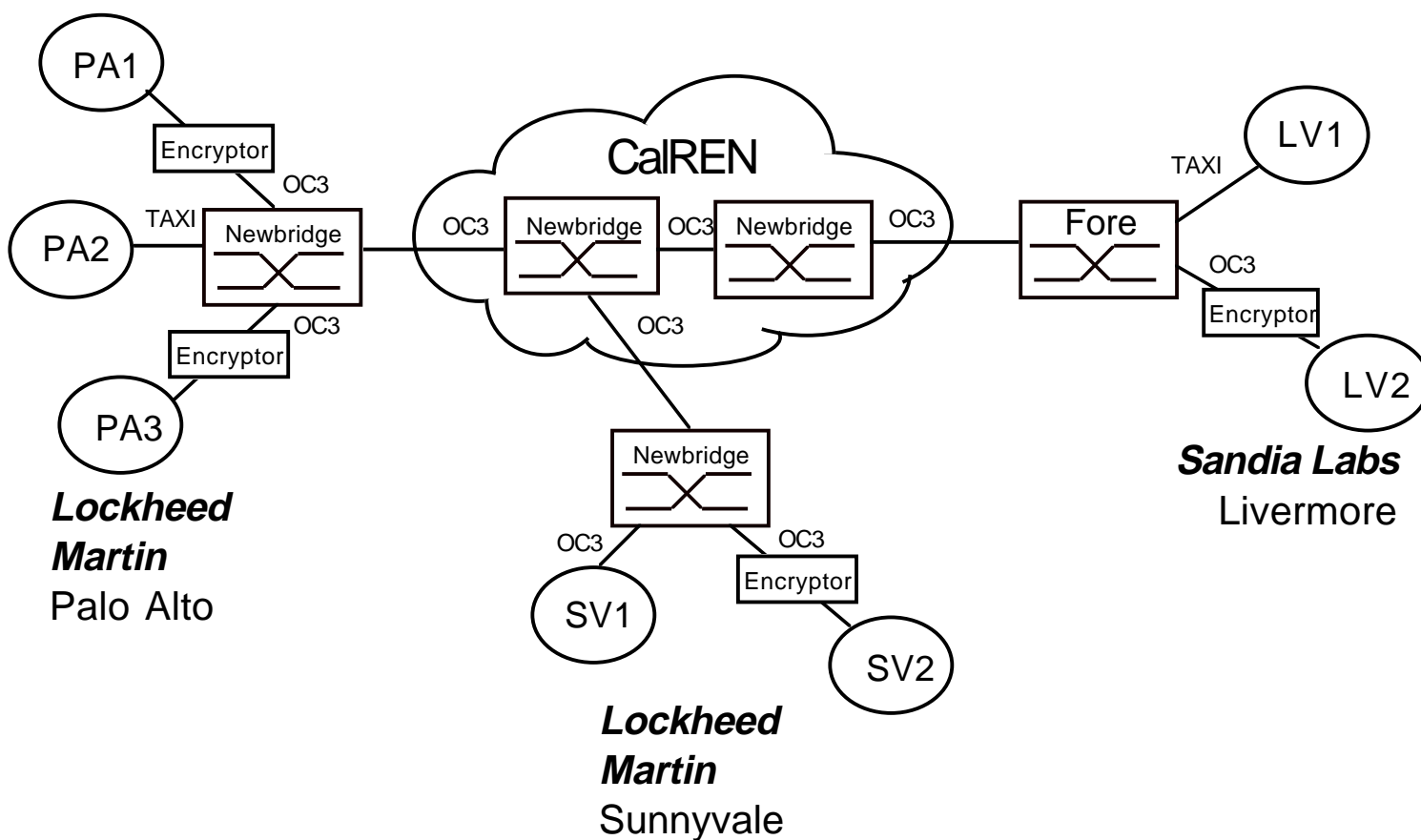


Without Encrptor



With Encryptor

PVC Test Configuration



Initial Test Plan

- **Step 1: In Palo Alto test two Sparc10 W/Ss with encryptors connected to separate OC3 ports on same switch**
 - Verify performance
 - Compare thruput with and without encryptors
- **Step 2: Move one encryptor to Sunnyvale and repeat test**
 - Compare performance over wide area ATM network
 - Compare results: single switch vs. dual switch
- **Step 3: Place an encryptor at Sandia Labs in Livermore**
 - Repeat testing and compare results
- **Step 4: Reconfigure all sites to test SVCs**
 - Compare performance over SVCs using Fore switches
 - Test key agility

Initial Sandia Encryptor Testing



- Tests between two Sun Sparc 10's in Palo Alto
 - OC3 interface cards (SBA200)
- Expected results: no loss of thruput as result of encryption
- Actual results: experienced an increase in thruput (but statisitcally insignificant)
 - Immeasurable increase in delay using “ping”
 - 1-2 miliseconds with or without encryption
- Conclusion: Sandia proof of concept devices indicate that encryption “transparency” is achievable

NSA “MILKBUSH” Encryptor Testing



- Repeated Sandia encryptor configuration
- Ran same tests as before
- Results:
 - File transfers were completed with and without encryption
 - Vince drivers reduced performance to under 5MB
- Conclusion: MILKBUSH prototype could not be measured for performance due to Vince implementation

Sandia Encryptor Long Haul Testing



- Left one encryptor behind switch in Palo Alto
- Installed another encryptor behind a switch in Sunnyvale
- Attempted to repeat same tests as performed in Palo Alto
- Results: inconclusive
 - Were able to perform file transfers without encryption
 - Could not repeat tests with encryption
- CalREN testbed connectivity ended in October 1996

What Was Learned



- **ATM technology presents a security challenge!**
 - Lockheed Martin is concerned
 - ATM is strategic to LM programs
 - Security solutions must be found
- **The LM CalREN ATM testbed provided the opportunity to explore security issues**
 - A lot was learned about security requirements for ATM networks
- **ATM Forum “Security Working Group” has now defined security services for ATM**

ATM Forum Security Specification Highlights



- **User Plane Security:**
 - Endpoint-to-endpoint
 - Authentication--Digital Signatures
 - Confidentiality--Encryption
 - Data Integrity--Digital Signature
 - Access control--Sensitivity Labels
- **Control Plane**
 - End-to-end and hop-by-hop
 - Authentication--Digital Signatures

- **Support Services:**
 - Certification Definition
 - Key Exchange
 - Basic negotiation of security requirements and capabilities
- **Future security specification:**
 - Management plane security services

Conclusions



- The LM CalREN ATM testbed provided the opportunity to learn a lot about ATM networks
- Security continues to be a concern for the successful use of ATM technology
 - Protection of proprietary data
 - Protection of government classified data
- There has been progress in addressing ATM security issues
 - Some emerging ATM security products
 - ATM Forum Security Specifications