

# Security Solutions for ATM

Dan Stevenson  
919-248-1160  
[stevenson@secantnet.com](mailto:stevenson@secantnet.com)

# Public Perception

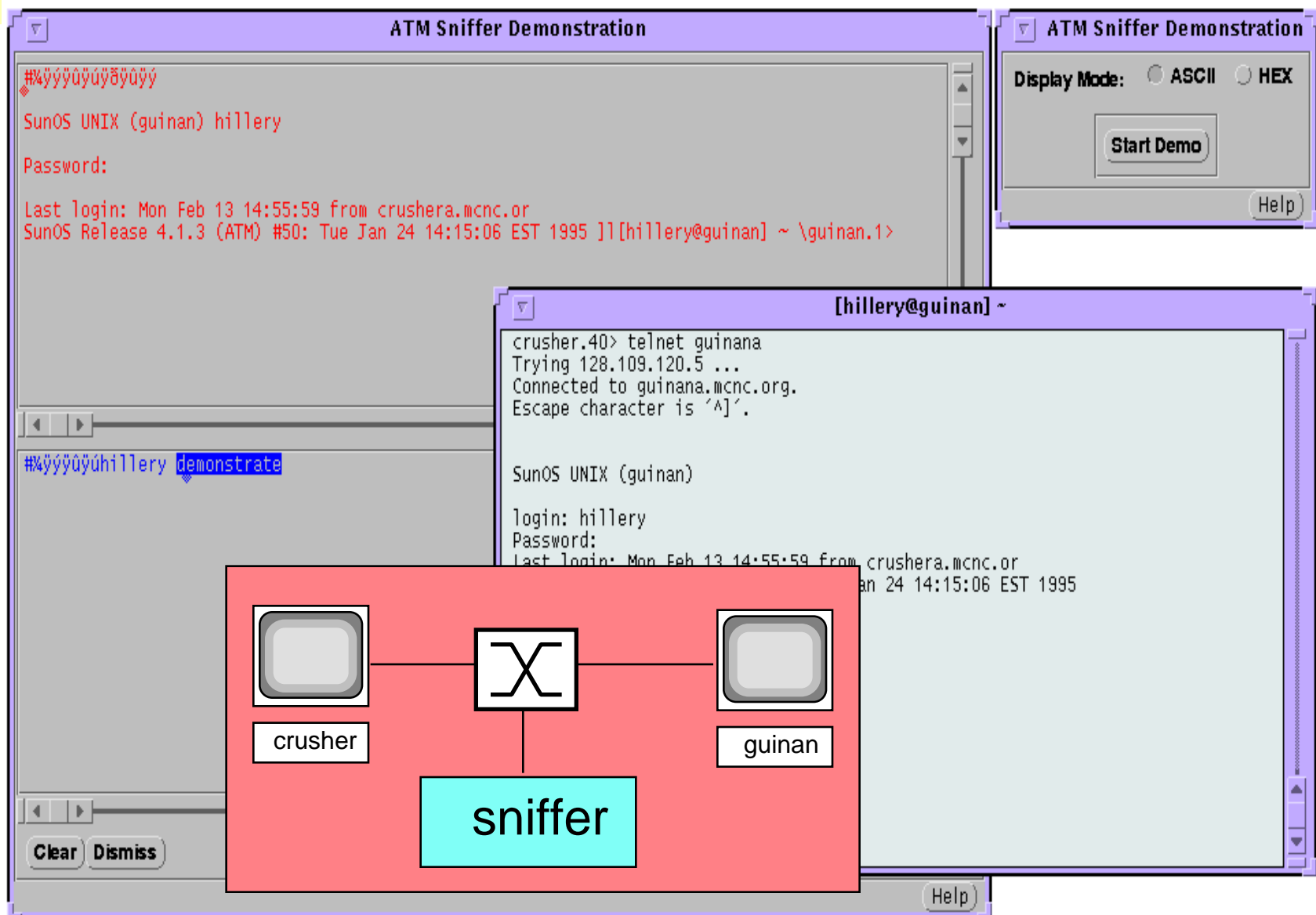
- I am naively writing in a report that it is very difficult to tap into a fiber ATM network. One has to correctly splice strands of fiber into the tap and inevitably signal and timing will be lost across the connection. In order to eavesdrop in ATM, one would have to place an analyzer somewhere into the backbone of the carrier's network. How can anyone learn something they shouldn't by attaching an analyzer at a customer's premise?

Thanks,

Bill J. , XYZ Corp. (names changed)

Email of Feb 1995

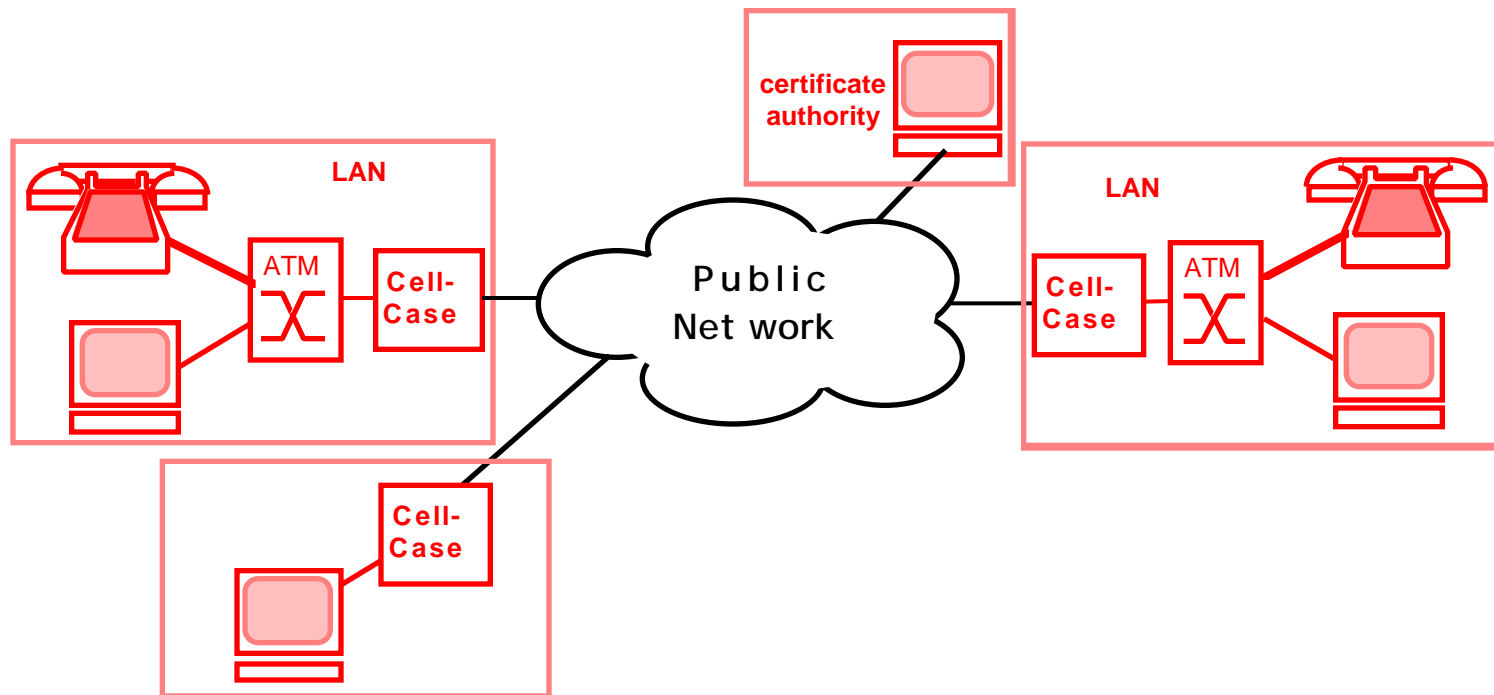
# ATM Sniffer



# ATM Vulnerabilities

- Privacy
  - Physical wiretapping
  - Rerouting SONET streams
  - Rerouting ATM LANs
- Denial of Service
  - Forced disconnects
  - Signaling message tampering
- Other
  - User impersonation
  - Covert Channels

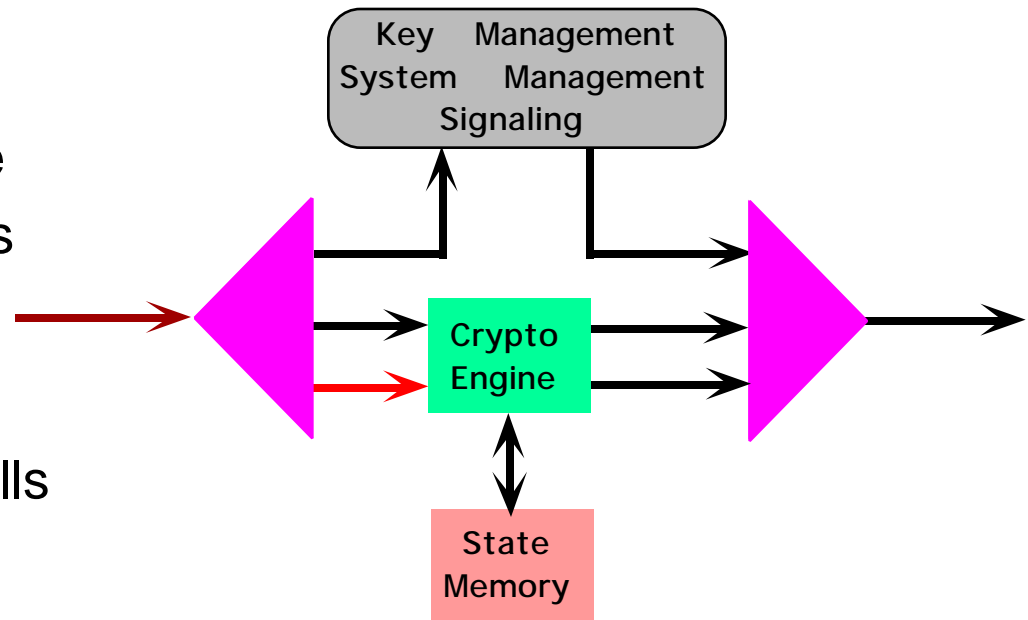
# Virtual Trusted Networks



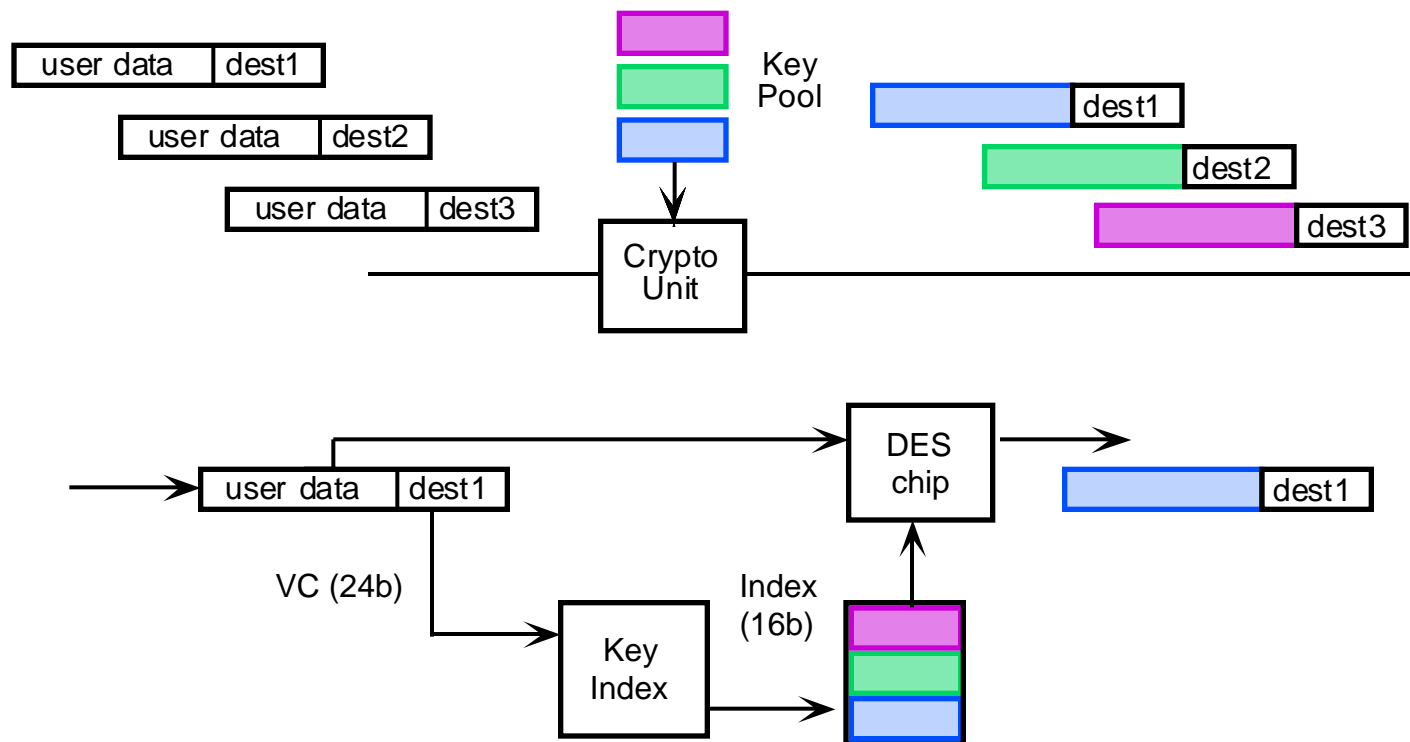
- ATM LAN extension replaces private lines
- Security solution is necessary to extend trust

# Cell Layer Security Issues

- Speed
  - Searching VC space
  - Key context changes
- Traffic filtering
  - Protected user cells
  - Unprotected user cells
  - Management
  - Signaling
- Synchronization
  - Recovery from lost cells
- Covert channels
  - Cross traffic information leaks

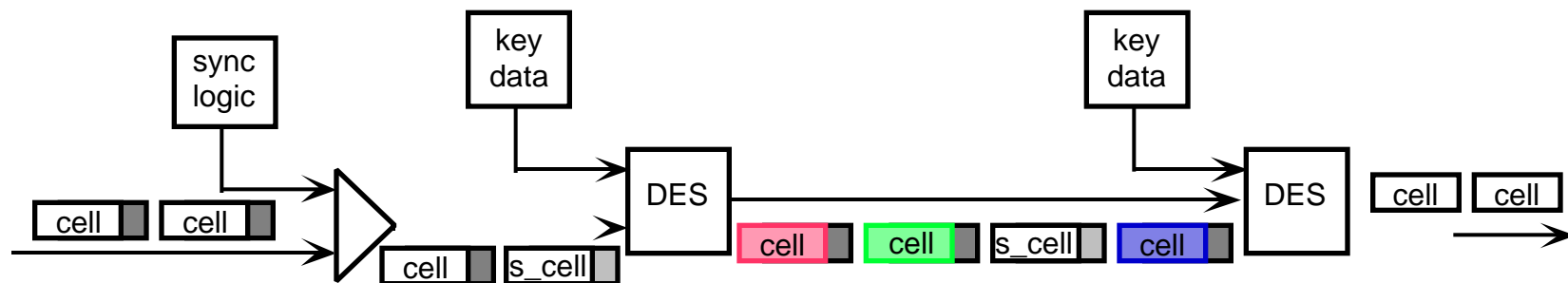


# Key Agility



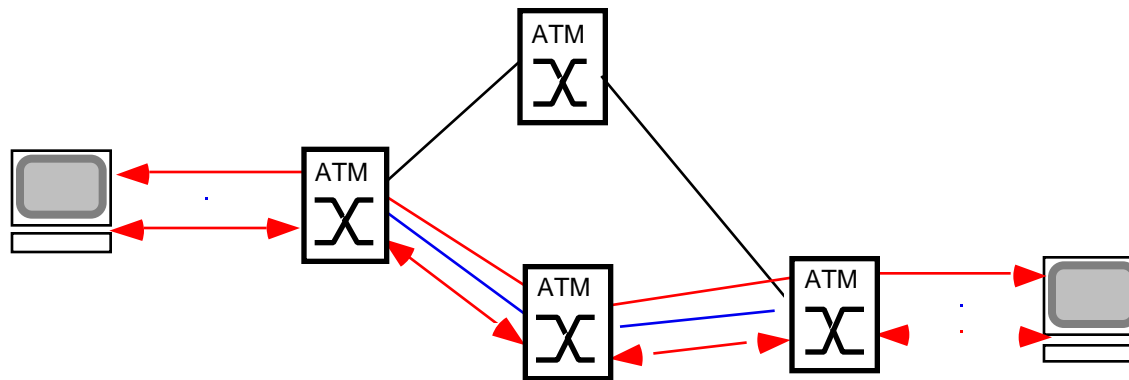
- Unique key for each active session
- Dynamic switching between session keys

# Synchronization



- ATM loss cell rate implies:
- Loss of receiving crypto sync
  - Counting mode
  - AAL3/4 AAL5 auto resync
  - Others need OAM sync cell
- Ideally block size = PDU size

# Available Bit Rate

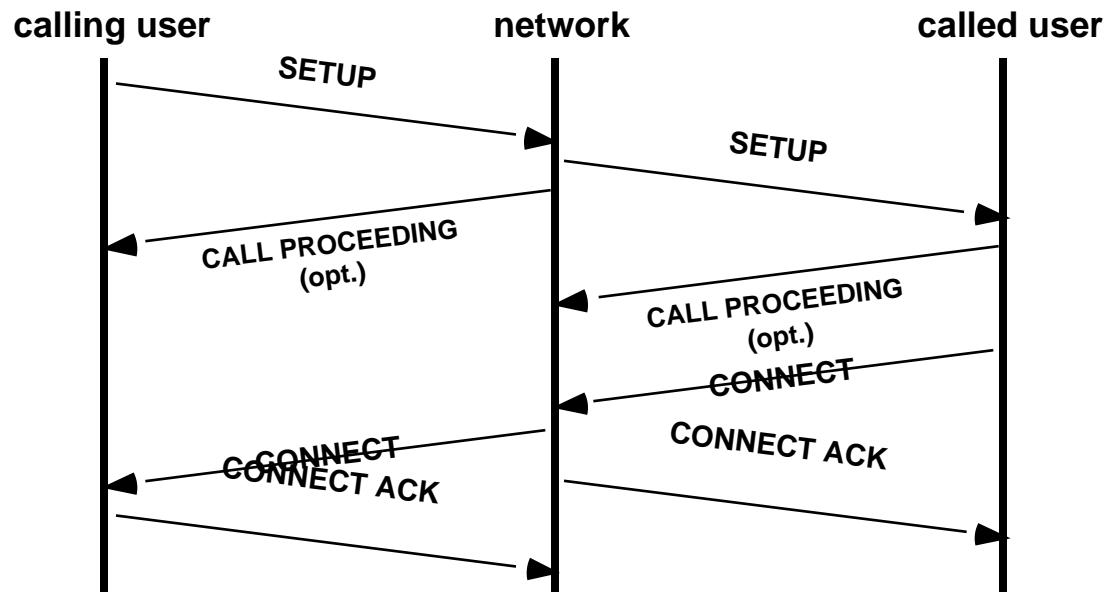


- New traffic class
  - Provides end-to-end feedback loops
  - Uses Resource Management (RM) cells
- RM cell info
  - As often as every 32 data cells
  - Carries bandwidth requirement/availability data
  - Modified by switches in path

# ABR Security Issues

- Service disruption
  - Insertion of bogus RM cells
- RM cells are in clear
  - Covert Channel risk
  - Breaks VC link level encryption

# Standard ATM Call Management



- Performance requirements
  - Average of 80 ms per switch
  - Complete in 4 seconds or
  - Extend to 14 seconds with **Call\_Proceeding** msg
    - Must specify VPI/VCI value

# Signaling Security Issues

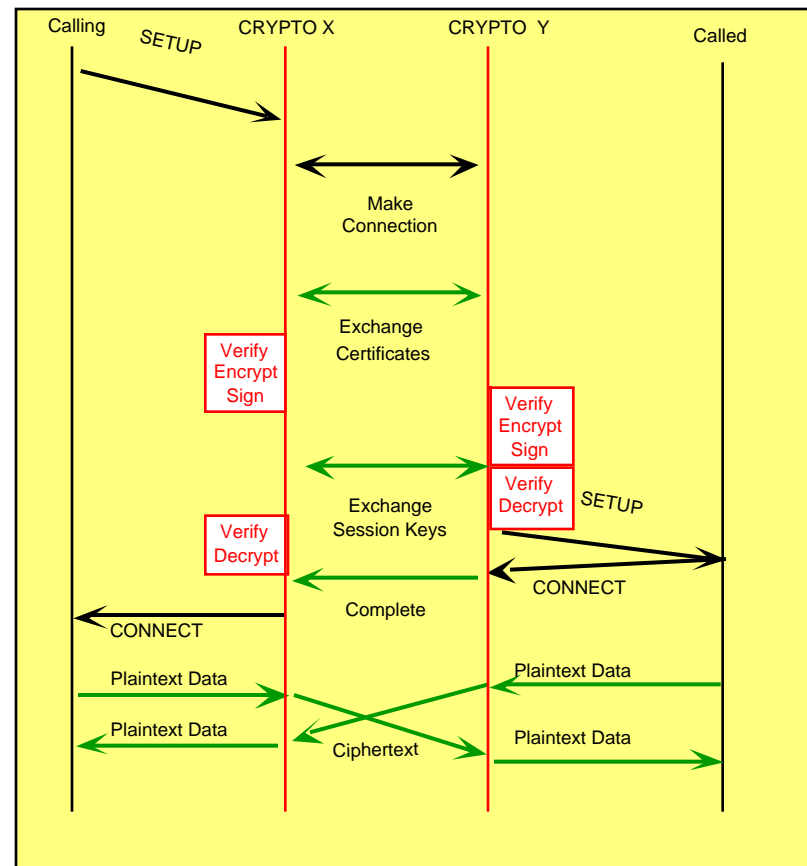
- Transparency
  - Point-to-point & Point-to-multipoint
  - Overwrite and replace call management data
- Denial of service
  - Restart message
  - Corruption of signaling data
  - Selective cell dropping
- Clear channels
  - User defined data in status messages
  - Valid at any time during call

# Key Management Approach

- Signaling message interception
  - Triggers key management functions
  - Crypto terminates and interprets management data
- Key Exchange Protections
  - Authenticity checks
  - Challenge response protocol
  - Sequence numbers
- Public key use
  - Directories distributed to crypto units
  - Public Keys provided by called crypto
  - Used only for initial crypto communication
- Session key chosen by transmitter
  - Simplifies key exchange protocol

# Key Management Basics

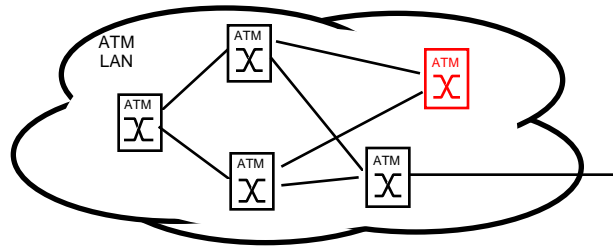
- Connection variations
  - Point to point
  - Point to multipoint
- Familiarity variations
  - Current KK
  - No KK
- Bandwidth variations
  - Adequate bandwidth
  - Zero back channel
  - Inadequate forward channel



# Secure Call Setup Performance

- Number of calls in progress
  - More complex software
  - More hardware filters
- Computationally intensive functions
  - Multi-processor systems
  - Hardware acceleration
- Call distribution statistics
  - Few frequently called cryptos vs.
  - Many infrequently called cryptos

# Private Network-Network Interface

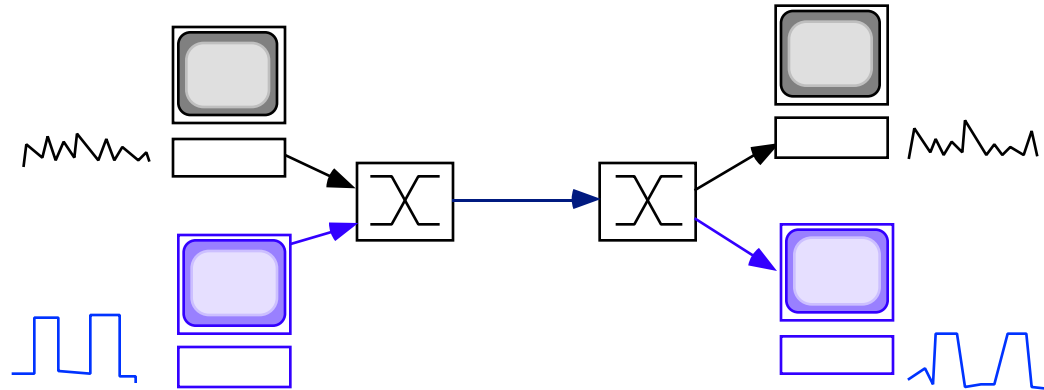


- Hello protocol
  - Private network routing discovery
  - Topology and QoS (bandwidth, delay)
  - Hierarchical approach for scaling
- Selection of Peer Group Leader
  - Communicates routing data to WAN

# PNNI Security Issues

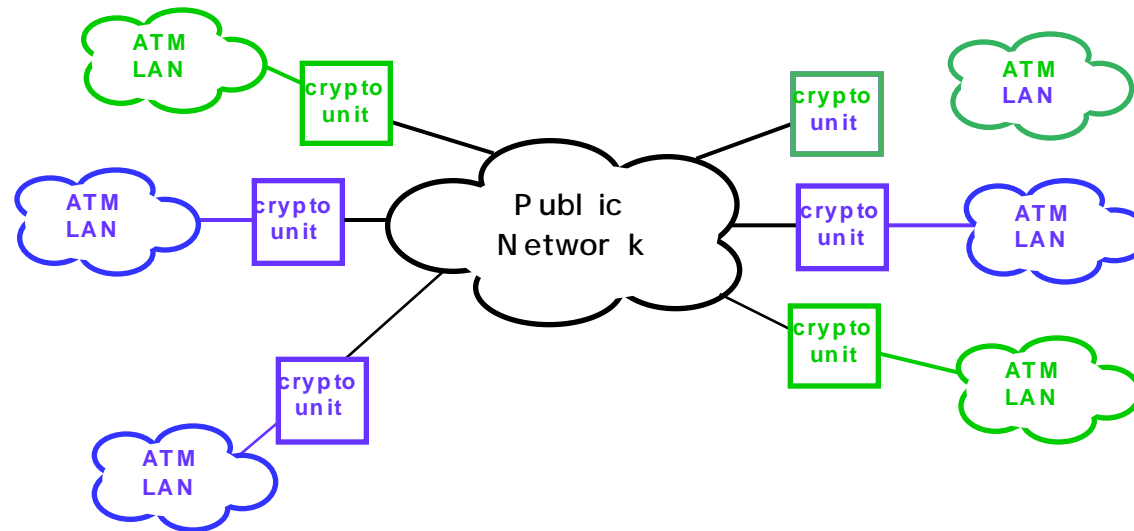
- No data authentication
  - All switches are trusted
  - Vulnerable to spoofing (W/O auth. element)
- Clear channels
  - Hello packets crossing PNNI boundary

# Covert Channels



- Cross traffic Interference
  - Multiple security partitions share resources
  - Load pattern of one group measurably affects other traffic
- Measurements made at PSU

# Access Control



- Closed user groups
  - Defined by policy
  - Implemented by crypto unit
- Two levels of screening
  - Cryptographic unit ID
  - NSAP

# Proof of Concept System

- DARPA funded effort
- MCNC research team
- Demoed July 1995
  - key agile encryption
  - transparent key management
  - 622 Mbps encryption

