# NDSS’98

## March 12, 1998

# Introduction to Session #3

## All-Optical Network Security

Jeff Ingle

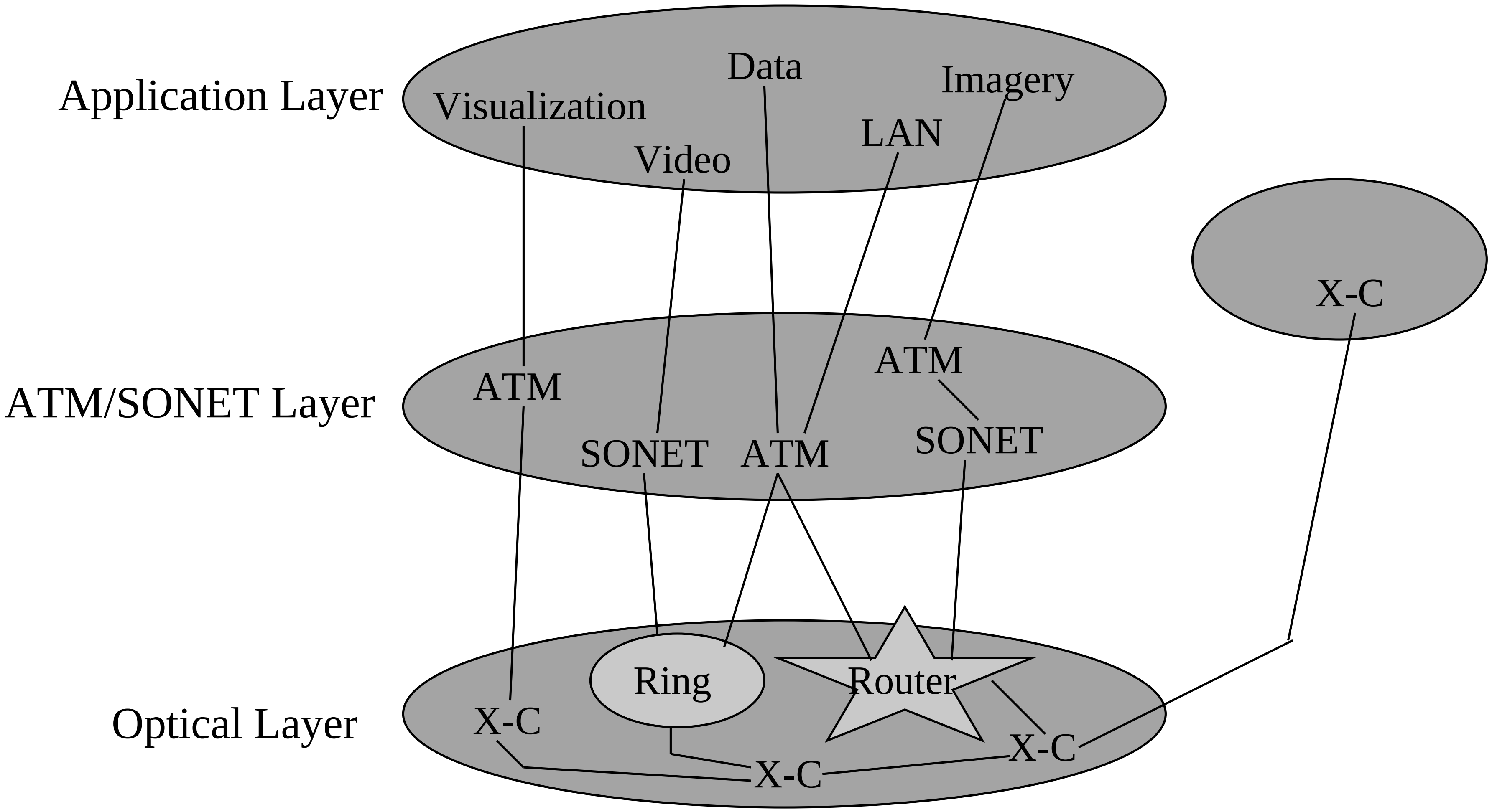
Advanced INFOSEC Technology
National Security Agency
9800 Savage Rd, Suite 6516
Ft. Meade, MD 20755-6516
jtingle@alpha.ncsc.mil
301-688-0291 phone
301-688-0289 fax

# Component Vulnerabilities

M. Medard, D. Marquis, R. A. Barry, S. G. Finn, "Security Issues in All-Optical Networks," IEEE Network, pp. 42-48, May/June 1997

- Vulnerabilities particular to all-optical networks arise from a combination of
  - crosstalk
    - linear / nonlinear
    - homowavelength / heterowavelength
    - directly detected / coherent (homodyne / heterodyne)
  - transparency
- Crosstalk in components
  - fibers (nonlinear)
  - optical amplifiers (nonlinear)
  - multiplexers / demultiplexers (linear)
  - switches (linear)
  - wavelength converters (nonlinear)

# Heirarchical Layering



Application Layer

Visualization

Data

Video

LAN

Imagery

ATM/SONET Layer

ATM

SONET

ATM

ATM

SONET

X-C

Optical Layer

X-C

Ring

Router

X-C

X-C

# Network Architecture Issues

From the workshop “The Role of Optical Systems and Devices for Security and Anticounterfeiting,” sponsored by DARPA, NSF, USAF, February 26-28, 1996.

- Architecture
  - topology, network node composition
  - service provisioning and signaling
  - security implications of “just-in-time” signaling for minimal latency
- Network Control and Management (NC&M)
  - fault detection and localization
  - configuration management
  - quality of service (QoS) management
  - resource allocation
  - security management

# Architecture Security Issues

- Authentication
  - end users
  - signaling
  - QoS negotiation
  - for access control, accounting and billing
- Security service negotiation capability
  - level of security
  - type of encryption and key exchange algorithms
  - authentication protocol
  - data integrity
  - etc. (possible model in IPv6)

# Research Areas in Optical Network Security

- Survivability
  - reduce vulnerability to jamming
  - reduce crosstalk
  - organize subsystems within component for best resistance
  - develop comprehensive set of design rules and methods to counter attacks, make robust devices
  - investigate effects of architecture, including consideration of component vulnerabilities, on overall security concerns
- Network Security Management
- Confidentiality and Key Management
  - symmetric encryption algorithms for high speed encryption
  - public key cryptography to distribute keys (may need to speed up)
  - extend SONET or ATM encryptor model to WDM environment
  - need for optical encryptors is niche market - DoD, DOE, NASA - supercomputer facilities

# Packet-Switched Optical Networks

- Network Architecture Study
  - Follow similar approach as for circuit-switched optical networks
    - authenticated signaling
    - flexible security negotiation mechanisms
    - security fields in signaling for crypto sync/resync - especially when no initial end-to-end connectivity
- Research to develop devices and components
  - Counter vulnerabilities in network components like switches and routers
  - Optical packet encryptor
    - word-based - one-dimensional string of bytes
    - page-based - two-dimensional array of bytes
    - packet identifier, key generator (KG), optical delay, optical XOR

# Longer-Term Technologies

- Soliton transmission
  - method to avoid problems with dispersion
  - near term implementation in intercontinental submarine links
  - could emerge as long term network technology
  - confidentiality - mux parallel encryptors or high-speed cryptographic algorithm in fiber loop or other logic
- Code Division Multiple Access (CDMA)
  - optical spread spectrum techniques
  - privacy system, limited in distance and networking
  - may be possible to use very fast cryptographic algorithm and technology to implement for high security
- Quantum Communications
  - may reduce threat of covert channels
  - high theoretical security, but not amenable to networks
  - possible for key distribution
- Wideband Coherent Communications
  - may reduce threat of covert channels
  - may not be feasible for network distribution

# Security Opportunities

- Concerns
  - Survivability (jamming, eavesdropping)
  - Network Control & Management security/survivability
  - Confidentiality - scalable encryption to Gb/s rates +, with care in synchronization, especially for “just-in-time” signaling
- Opportunities
  - New, fundamental telecommunications architecture means that security mechanisms can be developed with the architecture
    - include security features in signaling and network management
      - security negotiation capability
      - authentication
    - minimize security problems inherent to architecture
- Demonstrate in consortia testbeds
  - AON (All-Optical Network)
  - MONET (Multiwavelength Optical NETwork)
  - NTONC (National Transparent Optical Networks Consortium)