QoSient LLC
Measuring, Assessing & Managing QoS

GIG EF
Global Information Grid
Evaluation Facilities

Securing Optical Network Data

IGrid 2005

Carter Bullard

September 26-29, 2005

Who Am I?

- Carter Bullard   carter@qosient.com
  - Currently developing monitoring technology for the DoD GIG Evaluation Facility to support Security, Performance and Operations Management.
- CMU/SEI CERT
  - Network Security Incident Coordinator
  - NAP Site Security Policy Development
- Law Enforcement Consulting
  - FBI/CALEA Data Wire-Tapping Working Group
- Standards Efforts
  - Editor of ATM Forum Security Signaling Standards
  - IETF Security Working Group (in the good ole days)
- Network Security Product Manager
- QoS Network Management Development

The Best of Times

Generalities are never true, but sometimes they can be more true than not.

- Attaching a device to an optical network isn’t dangerous to the device or the network
  - Most AONs are closed experimental
  - Most attaching devices are switches
- Optical network architecture is the best for network security
- Optical networks are not currently the focus of formal/coordinated attacks

The Worst of Times

You can never be wrong expecting the worst

- Will have to transition to commercial use
- Intrinsic security of the global network of networks is deteriorating
  - ITU Workshop on Creating Trust In Critical Network Infrastructures - May 2002
- Network components have been speculated to be the issue in recent security incidents
  - Stakkato, Titan Rain, Microsoft Code Theft
- Optical Networks are just networks

A real problem today

- NRL has a 10 Gbps Infiniband Wide Area Network transport capability.
- Demonstrated HDTV transmission Wash – Los Angeles as disk reads at 2-6 Gbps.
- Application is long haul Supercomputer Cluster Resource Sharing, and we can do this today.
- Deployment Barrier? Security

Today’s Solution

- Remote attachment breaks every security policy at most DoD sites, without some form of VPN.
- Short Answer
  - If optical network is bus extension.
    - No problem, well not really true.
    - If attached device is not dual homed, then No problem, well not really true.
    - Can we send a security officer to your site?
    - Do you have a firewall?
  - If optical network is a network?
    - Absolutely not!!!!!!!!

Real Solution

- Optical Networks must be able to “fit” into modern networks security infrastructures.
- Optical Networks must be able to contribute to modern network security policy enforcement.
- A lot of work needs to be done!!!

General Concepts in Network Security

What is Network Security?

There is no industry consensus on what ‘network’ security is.

- Network Security Policy Enforcement
  - Access Control
- Protecting Critical Network Infrastructure
  - Integrity
  - Reliability
  - Survivability
  - Recovery
- Providing security services to the user
  - End-point Assurance
  - Integrity
  - Privacy
- Network Security Incidence Response

Network Security Threats

These are the primary issues in each area, but are far from a complete set

- Threats are traditional crimes
  - Trophy/Nuisance/Extortion/Theft/Espionage
- Targets
  - Networks with Exploitable Assets
  - Specific Network Customers
  - Network Service Providers
- Psychological profiles are well understood
  - Individual
    - 15-20 year old male
      - Demonstration of control/power
    - 20-40 year old male
      - Traditional Criminal Activity
  - Group
    - Disjoint collection with single/multiple leader(s)
    - Coordinated
    - Highly Motivated
    - Can be well funded (corporate/gov’t espionage)

Network Attack Methods

These are the fundamental attack methods. They are generally combined to generate complex attack scenarios

- Traffic Analysis
- Eavesdropping
- Introducing Data Delay
- Service Denial
- QoS Degradation
- Spoofing
- Man-in-the-middle

Network Attack Strategies

This is a simple example taxonomy but includes many of known strategy classes

- Unsophisticated Attacks
  - Nuisance/Interruption/Denial of Service
- Theft/Extortion/Espionage
  - Target Discovery
    - Passive Eaves-dropping
    - Active Scanning
  - Initial Breach
    - Social Engineering
    - Vulnerability Exploitation
  - Establish a persistent “beach head”
    - Modify the infrastructure to facilitate future access
  - Collect Information
  - Extract Assest
  - Close up or Move on

Prevention, Detection & Response

This is THE Mantra of the Security Community and constitutes the mode of operation

- Prevention
  - Effective countermeasures to real threats
  - Vulnerability exploitation reduction
  - Today, this is primary security focus
    - Cryptography
    - Firewalls
    - Software Updates
  - No prevention scheme is 100% reliable
- Detection
  - Intrusion Detection
  - Situational Awareness Systems
  - General solutions are somewhat difficult
- Response
  - The most critical part of any security architecture

Security Incident Response

Sample Emphasis Text

- Initial response is traditional fault management
  - Identification, Isolation, Analysis, Plan/Correction
  - Recovery
  - Tracking
- Security Specific Response
  - CERT
  - Forensics Analysis/ Evidence Development
    - Attack Classification
    - Authenticity of Evidence
      - Original Data/Handling Practices/Interpretation
  - Customer Involvement
  - Law Enforcement
  - Prosecution
  - Risk Mitigation

Who is Defining Network Security?

US is used here only as an example. Many governments have formal IT security specification efforts.

- Federal Governments
  - – US Department of Defense
  - – US Department of Homeland Security
    - Information Analysis and Infrastructure Protection
      - – National Security Telecommunications Advisory Committee (NSTAC)
      - – National Communications System (NCS)
  - – Committee on National Security Systems
    - Subcommittee on Telecommunications Security
  - – National Institute of Standards
- Telecommunications Industry

US DoD IT Assurance Policy

Sample Emphasis Text

- DoD Directive 8500.1 Information Assurance
  - Applies to all information systems that receive, process, store, display or transmit DoD information.
  - Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems.
- DoD Instruction 8500.2 IA Implementation
  - 5.6.3 Generate Protection Profiles for IA and IA-enabled IT products used in DoD information systems based on Common Criteria (International Common Criteria for Information Technology Security Evaluation (CC))
- October 2002

Common Criteria

Defines what and how to test. Does not tell you what to do to get a good security strategy.

- ISO/IEC 15408:1999 Common Criteria for Information Technology Security Evaluation (CCITSE)
  - Replaced US DoD Trusted Computer Security Evaluation Criteria, “Rainbow Series”
  - Specified TCSEC Trust Levels as Protection Profiles
  - Three Sections
    - Introduction and General Model
    - Security functional components
    - Security assurance components
- Version 3 released for public consultation July, 2005
- If you want to be ‘certified’ this is what you have to do.

Red Book Security

NCSC-TG-005

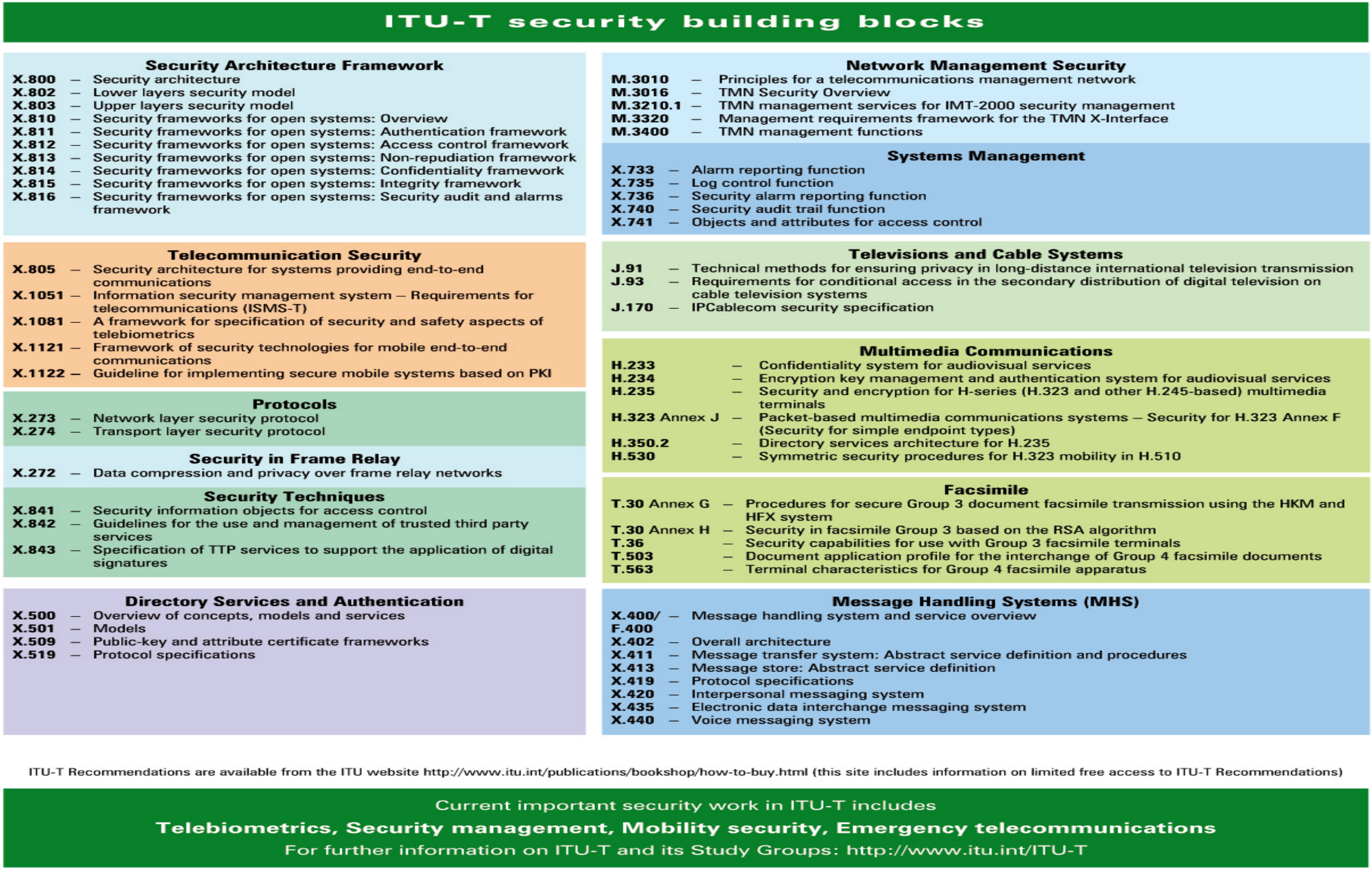
- Trusted Network Interpretation of the TCSEC (TNI)
  - DoD Trusted Computer System Evaluation Criteria (TCSEC) July 31, 1987
    - Provided a standard to manufacturers as to what security features and assurance levels to build into their new and planned, commercial network products.
  - Interpreted how DoD security requirements specified for host systems would be resolved in networks.
  - Structured around a ‘Single Trusted System View’
  - Based on a connection-oriented security service model
    - Driven by formal methods
  - Specified four types of security policies
    - Mandatory/Discretionary Access Control (1,2)
    - Supportive policies (Authentication and Audit) 3
    - Application Policies (ie DBMS Access Authorization) 4

Theoretical Information Security Threats and Countermeasures

Countermeasures		Threat				
		Unauthorized			Denial of Service	Repudiation
		Use	Modification	Disclosure		
Authentication	Cryptographic	🟥 X				🟨 x
Integrity			🟥 X			
Confidentiality				🟥 X		
Access Control		🟥 X	🟨 x	🟨 x	🟥 X	
Audit		🟨 x			🟨 x	🟥 X

🟥	Primary Security Countermeasure
🟨	Secondary Security Countermeasure

ITU Security Efforts



ITU-T security building blocks

Security Architecture Framework

X.800	Security architecture
X.802	Lower layers security model
X.803	Upper layers security model
X.810	Security frameworks for open systems: Overview
X.811	Security frameworks for open systems: Authentication framework
X.812	Security frameworks for open systems: Access control framework
X.813	Security frameworks for open systems: Non-repudiation framework
X.814	Security frameworks for open systems: Confidentiality framework
X.815	Security frameworks for open systems: Integrity framework
X.816	Security frameworks for open systems: Security audit and alarms framework

Telecommunication Security

X.805	Security architecture for systems providing end-to-end communications
X.1051	Information security management system – Requirements for telecommunications (ISMS-T)
X.1081	A framework for specification of security and safety aspects of telebiometrics
X.1121	Framework of security technologies for mobile end-to-end communications
X.1122	Guideline for implementing secure mobile systems based on PKI

Protocols

X.273	Network layer security protocol
X.274	Transport layer security protocol

Security in Frame Relay

X.272	Data compression and privacy over frame relay networks

Security Techniques

X.841	Security information objects for access control
X.842	Guidelines for the use and management of trusted third party services
X.843	Specification of TTP services to support the application of digital signatures

Directory Services and Authentication

X.500	Overview of concepts, models and services
X.501	Models
X.509	Public-key and attribute certificate frameworks
X.519	Protocol specifications

Network Management Security

M.3010	Principles for a telecommunications management network
M.3016	TMN Security Overview
M.3210.1	TMN management services for IMT-2000 security management
M.3320	Management requirements framework for the TMN X-Interface
M.3400	TMN management functions

Systems Management

X.733	Alarm reporting function
X.735	Log control function
X.736	Security alarm reporting function
X.740	Security audit trail function
X.741	Objects and attributes for access control

Televisions and Cable Systems

J.91	Technical methods for ensuring privacy in long-distance international television transmission
J.93	Requirements for conditional access in the secondary distribution of digital television on cable television systems
J.170	IPCablecom security specification

Multimedia Communications

H.233	Confidentiality system for audiovisual services
H.234	Encryption key management and authentication system for audiovisual services
H.235	Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals
H.323 Annex J	Packet-based multimedia communications systems – Security for H.323 Annex F (Security for simple endpoint types)
H.350.2	Directory services architecture for H.235
H.530	Symmetric security procedures for H.323 mobility in H.510

Facsimile

T.30 Annex G	Procedures for secure Group 3 document facsimile transmission using the HKM and HFX system
T.30 Annex H	Security in facsimile Group 3 based on the RSA algorithm
T.36	Security capabilities for use with Group 3 facsimile terminals
T.503	Document application profile for the interchange of Group 4 facsimile documents
T.563	Terminal characteristics for Group 4 facsimile apparatus

Message Handling Systems (MHS)

X.400/F.400	Message handling system and service overview
X.402	Overall architecture
X.411	Message transfer system: Abstract service definition and procedures
X.413	Message store: Abstract service definition
X.419	Protocol specifications
X.420	Interpersonal messaging system
X.435	Electronic data interchange messaging system
X.440	Voice messaging system

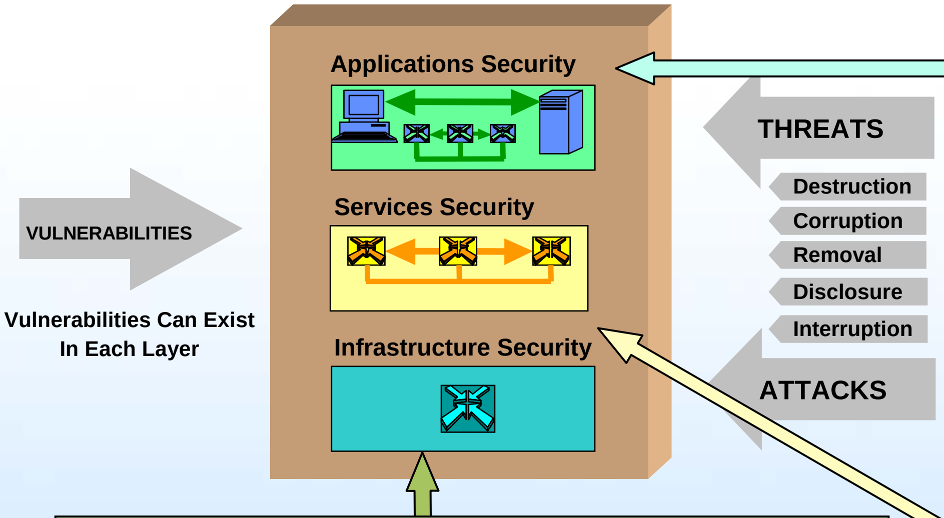
ITU-T Recommendations are available from the ITU website http://www.itu.int/publications/bookshop/how-to-buy.html (this site includes information on limited free access to ITU-T Recommendations)

Current important security work in ITU-T includes

Telebiometrics, Security management, Mobility security, Emergency telecommunications

For further information on ITU-T and its Study Groups: http://www.itu.int/ITU-T

X-805 Architecture



3 - Applications Security Layer:

- Network-based applications accessed by end-users
- Examples:
  - Web browsing
  - Directory assistance
  - Email
  - E-commerce

1 - Infrastructure Security Layer:

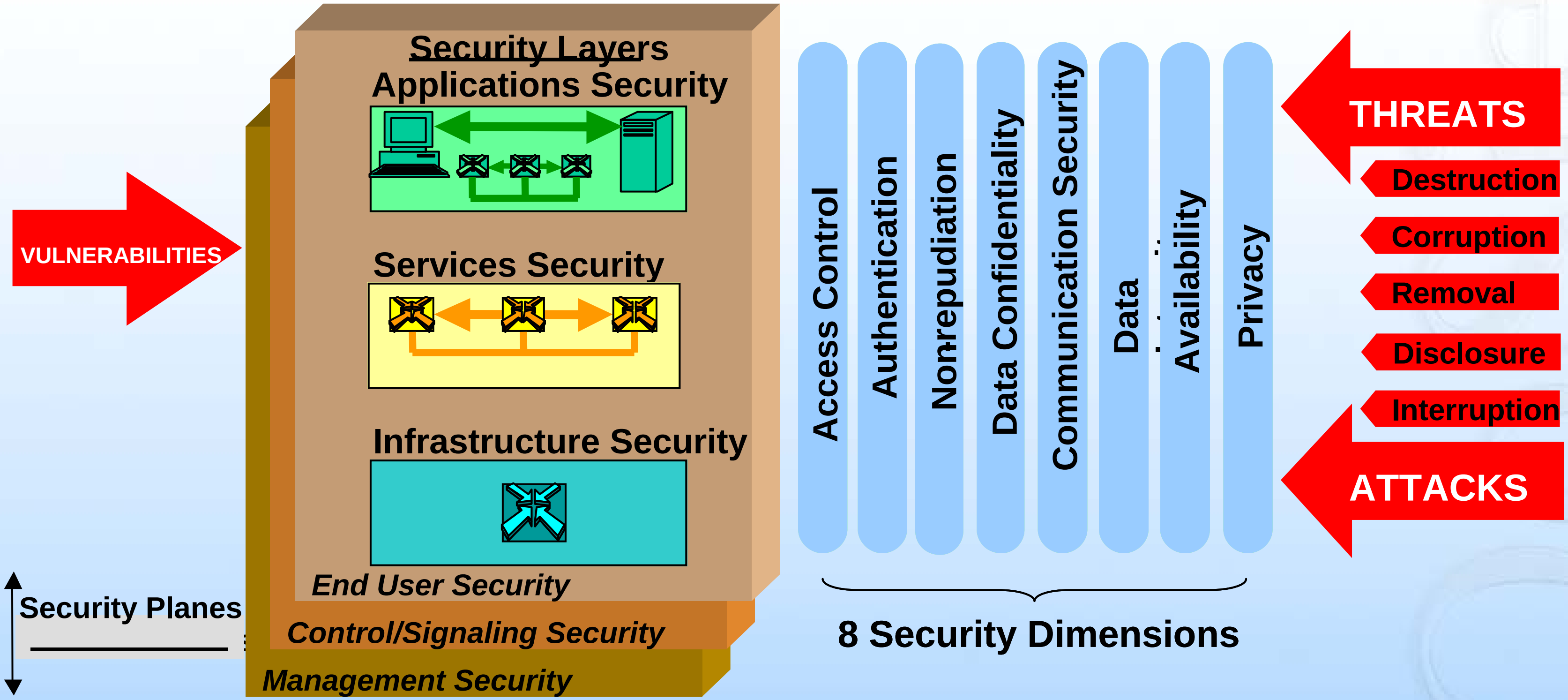
- Fundamental building blocks of networks services and applications
- Examples:
  - Individual routers, switches, servers
  - Point-to-point WAN links
  - Ethernet links

2 - Services Security Layer:

- Services Provided to End-Users
- Examples:
  - Frame Relay, ATM, IP
  - Cellular, Wi-Fi,
  - VoIP, QoS, IM, Location services
  - Toll free call services

- **Each Security Layer has unique vulnerabilities, threats**
- **Infrastructure security enables services security enables applications security**

ITU X-805 End-to-End Security Architecture



Security Layers

Applications Security

Services Security

Infrastructure Security

End User Security

Control/Signaling Security

Management Security

VULNERABILITIES

Security Planes

Access Control

Authentication

Nonrepudiation

Data Confidentiality

Communication Security

Data

Availability

Privacy

8 Security Dimensions

THREATS

Destruction

Corruption

Removal

Disclosure

Interruption

ATTACKS

Optical Network Security

Optical Network Security

- Infrastructure Security Layer
  - Must support security dimensions applied to the control plane and management planes
  - Physical Layer Security
- Services Security layer
  - Oriented to network interfaces
    - Signaling Security Support
      - GMPLS/RSVP-TE/OSPF-TE
- Application layer?
  - If there is an application interface
    - It will need security!!!!!

AON Security Concerns

- Technology obsoletes prevention technology
  - Data rates exceed encryption capabilities
  - No all-optical policy enforcement schemes
- Latency puts more data “in flight’
  - Increases the instantaneous value of a fiber.
- Transparency enables new attack strategies.
- Single fiber support multiple services
  - Divergent Security and QoS Requirements
- New security fault discrimination techniques
- Control Network
  - Physical Isolation generate false sense of security

Who is Defining Optical Network Security?

- NCS TIB 00-7 August, 2000
  - Examines AON issues associated with their applications and discusses their applicability into National Security and Emergency Preparedness (NS/EP)
- Security Focus
  - Physical Security
  - Architectural Concerns

AON Component Threats

These are theoretical threats. No known use of these threats has been documented

- Physical Component Specific Vulnerabilities
  - Gain Competition Attacks (Jamming)
    - In-band jamming (hot source signal)
      - Can affect combiners/multiplexors/amplifiers
      - Difficult to detect actual source
    - Out-of-band jamming (hot source signal)
      - Mediated through amplifier cross-gain modulation
      - Steals gain from real network signals.
  - Traffic analysis and eavesdropping
    - Mediated through optical cross-talk

Optical Attack Prevention

For specific optical vulnerabilities these are the minimum

- Vulnerability exploitation reduction
  - Optical limiting amplifiers
  - Bandwidth limiting filters
  - Crosstalk minimizing components
- Adoption of transmission techniques that are effective against certain attacks
  - acclimated modulations
  - coding (anti-jamming mechanisms)
  - signal constraint (bandwidth/frequency/strength)
  - diversity mechanisms (frequency hopping, etc).
- Secure architecture and protocol adoption
  - judicious wavelength and path assignments
    - to separate trusted from non-trusted users

Optical Attack Detection

Sample Emphasis Text

- Passive Statistical Analysis of Data
  - Wideband Power Anomaly Detection
    - Needed to detect in-band jamming attack attempts
  - Optical Spectral Analysis (OSA) Methods
    - Used to detect Gain Competition Attack attempts
- Active Signals Devoted to Diagnostic Purposes
  - Pilot Tone Methods
    - Sub-carrier Multiplexed signals used to detect tapping (signal loss)
  - Optical TDR Methods
    - Used to detect fiber tampering
    - Man-in-the-Middle insertion
    - Can support in-band jamming detection
    - Can be used to detect in-line eavesdropping.

Optical Network Security

Sample Emphasis Text

- Back to our problem
- Optical path as a single link
  - Does use of the optical path modify the risk assessment?
    - Yes
  - Are there prevention strategies?
    - Yes/No
  - Are there adequate detection methods?
    - Yes

Cryptography in Optical Networks

Optical specific cryptography is not designed to protect user data, just protect key exchange

Means that most prevention strategies are not available for optical networks.

- Quantum Cryptography
  - Used to generate and transmit conventional encryption key material
  - Very sensitive eavesdropping detection
  - Very low bandwidth
- Conventional Cryptographic Methods
  - Expected for user data cryptography
  - Performance Limited
    - Fastest encryptors rated at 10Gbps
    - Packet based encryptors doing 1Gbps
  - Required for control network security

Control Network Security

If you want to view an optical network as a network, from a security perspective, you have to get a security grip on the control network

- Control Network is an Internet
  - Couldn’t be a worst security model
  - Lots of well seasoned attackers
- #1 Job Keep the Control Network Isolated
  - Reduces Security to a Host Security Problem
    - Software Diversity Issues
    - Back to basics
      - Password management is critical
      - Software configuration management is HUGE
  - Shifts paradigm to an insider threat model
    - Poor prevention technology
    - Adopt Authentication/Authorization Infrastructure
- Once breached, recovery is very complex
  - Complete “reload/reboot” scenarios

Control Security Prevention

Encryption is not the only technology available for Internet technology, but it does dominate the landscape.

May need something else.

- Today, the security focus is on hosts
  - Top 25 security problems are host based
    - Sans Institute/CERT-US/etc……
  - A lot of people working in this area
- Traditional Internet mechanisms may not be appropriate.
  - Internet security technology is not really ready for insider threat, yet.
  - Encryption as the principal countermeasure is inappropriate
    - Don’t need confidentiality protection
    - Introduces complexity that impacts reliability and recoverability

Control Security Detection

These schemes are useful, but they do have limited utility in Optical Control Network Security because of deployment contraints or just usefulness.

May need something else.

- Internet Strategies
  - Active Vulnerability Testing
    - Nessus, ISS, Nprobe, Nmap
  - Firewalling
    - Access Control coupled with logging
  - Intrusion Detection Systems
    - Snort
    - Military NIDS
  - Anomaly Detection Strategies
    - Not predominate in marketplace

Control Security Detection

Sample Emphasis Text

- GIG-EF approach
  - Complete packet capture of all control plane and management plane traffic
    - Protocol Assurance Analysis
    - Functional Assurance Analysis
    - Comprehensive Situational Awareness
  - Exhaustive analysis of all other traffic in the optical control network.
    - FTP sessions?
    - Telnet?
    - Web Traffic?
    - SSH?
- Leverage this effort to support operations and performance management tasks in the complete control network.

Conclusions

A lot of work needs to be done, but optical networks will ultimately work.

- Optical Networks Can Support Sound Network Security
  - User/Control Network Separation
  - Tolerable Threat Model
  - Limited prevention good detection schemes
  - May not provide user security services
- #1 Job is Secure the Control Network
  - Signaling security is an Achilles heel
- Optical Network will modify security protection strategies to rely on detection.
- Audit and Monitor Everything

Thanks!!!!!!

Any Questions?????

Supporting Slides

ITU X.805 Security Dimensions

Sample Emphasis Text

- Set of security measures designed to address a particular aspect of network security.
  - Access Control
  - Authentication
  - Non-repudiation
  - Data Confidentiality
  - Communication Security
  - Data Integrity
  - Availability
  - Privacy
- Designed to implement security policy enforcement

Access Control

No access control standards exist for data networks

User oriented access control gets a lot of attention, virtually no standards work progressing

- Mandatory
  - – Security Domain Policy Requirement
- Discretionary
  - – Users can allow others to use/access data
- Generally implemented using labels
  - – DoD Specified Label Systems
    - IETF IP Security Options
    - IEEE 802.10
  - – PSTN
    - Calling Party ID (caller ID).
- Firewalls designed to fill in the gaps
  - – More gaps than not in today networks.

Authentication

- Identification of entities
  - Group/Person/Machine/Software
  - Biometrics are the buzz, for people
- Usually coupled with Authorization
- Cryptographically Implemented
  - Plain text
  - Shared key
  - Public/Private Key strategies
  - Public Key Infrastructures
  - Token Schemes

Lots of standards here, maybe too many, making adoption somewhat problematic.

For a new protocol, do you use plaintext passwords, shared secret, public/private key, Kerberos, RADIUS, MD5 HMAC, Kerberos, IKE, etc…….?

Non-Repudiation

Absolutely no standards here!!!!!

- Preventing Deniability
- Requires Accountability
  - Data Origin
  - Proof of Ownership
  - Proof of Resource Use
- Provide Source of Evidence
- Principal Deterrent

Data Confidentiality

Wayyyyy to many standards here

- Protects from disclosure
- Requires cryptography
- Many strategies employed:
  - – Bulk Link Encryption
  - – Hop-to-Hop Encryption
  - – End-to-End Encryption
  - – VPN Tunnels
- Many many many standards.

Communication Security

PSTN concept with little attention given by data communications industry

- End point assurance
- Path Assurance
- Man-in-the-middle protection
- Eaves-dropping protection
- Generally non-cryptographic

Data Integrity

Many standards available

- Ensure Data Correctness
  - Protects against data modification
- Simple schemes prevail
  - Bit error detection and correction
  - All vulnerable to padding attacks.
- Cryptographically Based Schemes
  - “chksum with an added secret”
  - Additional support data authentication
- Some algorithms “cracked”
  - SHA-1

Availability Security

Absolutely no standards here!!!!!

- Category to address DOS security
- Protects Access To:
  - Network Elements
  - Stored Information
  - Information Flows
  - Services and Applications
- Addresses Disaster Recovery
  - Involves Role Identification
  - Planning
  - Contingency

Privacy Security

Absolutely no standards here!!!!!

- Protection for information
  - – Traffic Analysis Protection
- Expanded to include:
  - – Content protection
  - – Geographic Location protection
  - – Identifier protection
    - Caller ID Block