SECURITY MANAGEMENT SYSTEM
FUNCTIONAL ARCHITECTURE
FOR ENTERPRISE NETWORK

Shervin Erfani
Electrical and Computer Engineering
University of Windsor
Windsor, Ontario
BASIC PROBLEMS WITH SECURITY MANAGEMENT

- Remote attacks are easy
- Anonymity is easy
- Bad Software
- Bad configurations
- Stand-alone system implementing single security service
- Reliance on rigid conventional encryption techniques

“SECURITY MANAGEMENT SHOULD BE AN EVOLVING INTEGRATED PROCESS.”
FUNCTIONAL ARCHITECTURE

1. Security Policy and Business Requirements
2. Security Management
3. Security Service
4. Security Mechanism
5. Security Primitive Modules

FUNCTIONAL LAYERS OF SECURITY MANAGEMENT

10/15/03  S. Erfani, ECE Dept., University of Windsor
Layer 5 - Security Policy and business requirements

- The uppermost layer dictating the enterprise security policy and business requirements function
- Sets the overall user/corporation security vision
- Expert Systems or Rule-based techniques can be used for violation detection and prevention module
FUNCTIONAL LAYERS OF SECURITY MANAGEMENT

Layer 4 - Security Management Function

- Provision of security services and control
- Event logging, both for normal and abnormal situation
- Administration and management of various modules in lower layers
- User interface management
- Security monitoring for various security services
- Key and Security (state) recovery in case of violation
- Interaction establishment between different security management systems through use of appropriate security management protocol(s)
FUNCTIONAL LAYERS OF SECURITY MANAGEMENT

Layer 3 - Security Service Function

- Confidentiality Service
- Integrity
- Access Control Service
- Non-repudiation and Accountability
- Authentication Service
- Non-denial of Service
FUNCTIONAL LAYERS OF SECURITY MANAGEMENT

Layer 2 - Security Mechanism Function

- **Public-Key Encryption**: RSA, ECC, Rabin, ElGamal algorithms
- **Symmetric One-Key Encryption**: DES, Triple DES, FEAL, IDEA, RC2, RC4, SKIPJACK techniques
- **Message Authentication Code**: CBC-MAC, MAA, RIPE-MAC
- **Password techniques**, Biometrics mechanisms
- **Digital Signature**: DSA mechanism
- **Access Control**: access control matrix (ACM), access control list (ACL), conditional access mechanism
FUNCTIONAL LAYERS OF SECURITY MANAGEMENT

Layer 1 - Security Primitive (Mathematical) Function

- One-Way Hash (OWH): MD5, SHA-1, MDC2, MDC4, RIPE-MD methods
- Public Key Fundamental Modules: Fast Exponential, Pseudorandom Number Generator, Test for Primality
- Math Library Modules: Chinese Reminder Theorem, Multiplicative Inverse, Modular Multiplication, and other operations with large numbers
- Encryption Fundamental Modules: DES, Triple DES, IDEA, AES, RC2/RC4/RC5, FEAL
A repository for normal functioning of SMS

The conceptual segments of an SMIB are IDs for network secured resources, user profiles and privileges, secure associations, access control list, and security logs

SMIB must work in a manager/agent relationship to support other MIBs in use
Message Interaction
Protocol
Interface
PGP Realization: An Example
ROBUSTNESS ACHIEVED

- Many security services
- Many security mechanisms with different efficiencies and different levels of security
- Wide-range of management functions
- Full integration with Network Management System (NMS)
- Security policies accessible from NMS
- Efficient use of different security mechanisms by different security services
- Transparent to users and applications
- Easily applicable to any type of operational environment
- Designed and structured modularly to be used by larger customer base
- Flexible, expandable, and adaptive to network changes, enhancements, and new policies
- Adaptive to new mechanisms and new security services