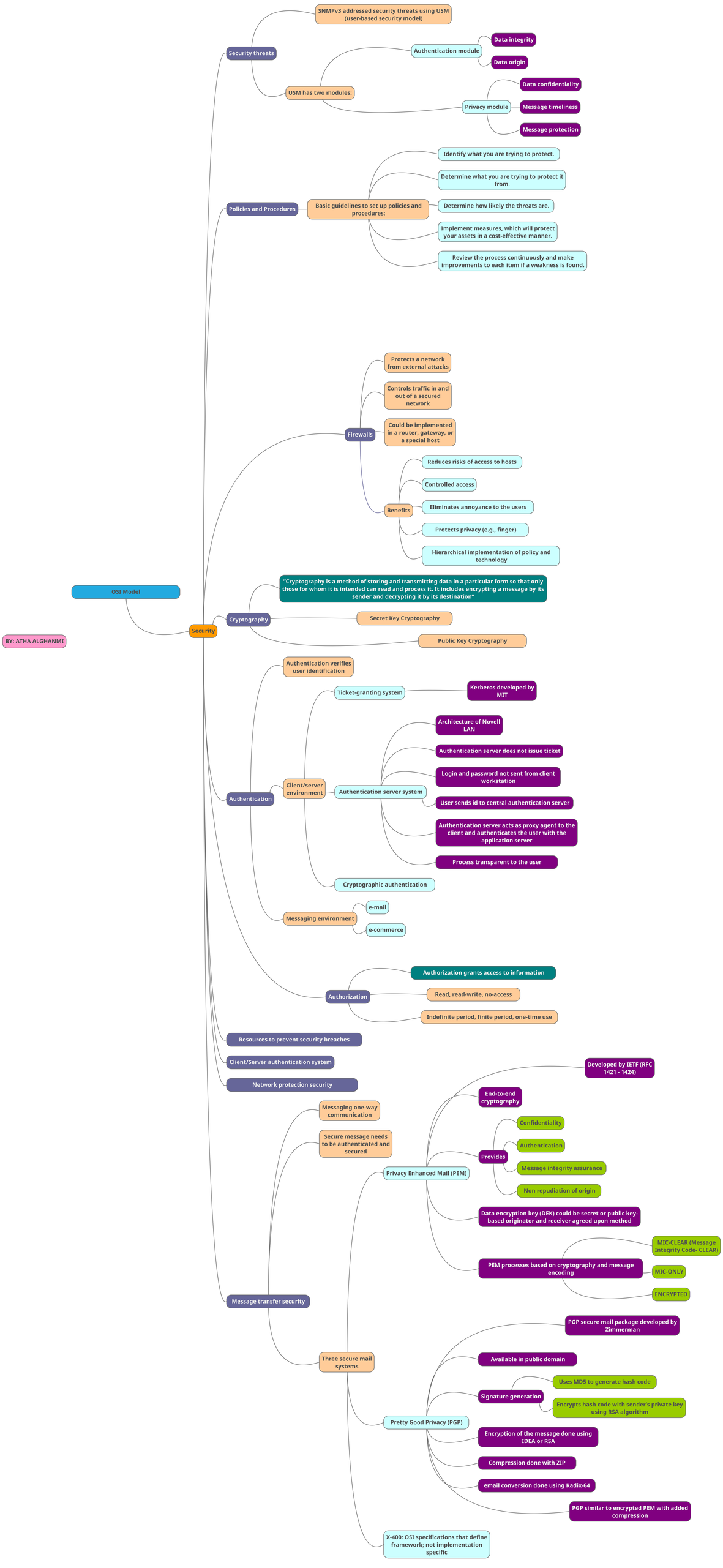
OSI Model
BY: ATHA ALGHANMI
Security
Security threats
SNMPv3 addressed security threats using USM (user-based security model)
USM has two modules:
Authentication module
Data integrity
Data origin
Privacy module
Data confidentiality
Message timeliness
Message protection
Policies and Procedures
Basic guidelines to set up policies and procedures:
Identify what you are trying to protect.
Determine what you are trying to protect it from.
Determine how likely the threats are.
Implement measures, which will protect your assets in a cost-effective manner.
Review the process continuously and make improvements to each item if a weakness is found.
Firewalls
Protects a network from external attacks
Controls traffic in and out of a secured network
Could be implemented in a router, gateway, or a special host
Benefits
Reduces risks of access to hosts
Controlled access
Eliminates annoyance to the users
Protects privacy (e.g., finger)
Hierarchical implementation of policy and technology
Cryptography
"Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It includes encrypting a message by its sender and decrypting it by its destination"
Secret Key Cryptography
Public Key Cryptography
Authentication
Authentication verifies user identification
Client/server environment
Ticket-granting system
Kerberos developed by MIT
Authentication server system
Architecture of Novell LAN
Authentication server does not issue ticket
Login and password not sent from client workstation
User sends id to central authentication server
Authentication server acts as proxy agent to the client and authenticates the user with the application server
Process transparent to the user
Cryptographic authentication
Messaging environment
e-mail
e-commerce
Authorization
Authorization grants access to information
Read, read-write, no-access
Indefinite period, finite period, one-time use
Resources to prevent security breaches
Client/Server authentication system
Network protection security
Message transfer security
Messaging one-way communication
Secure message needs to be authenticated and secured
Three secure mail systems
Privacy Enhanced Mail (PEM)
Developed by IETF (RFC 1421 - 1424)
End-to-end cryptography
Provides
Confidentiality
Authentication
Message integrity assurance
Non repudiation of origin
Data encryption key (DEK) could be secret or public key-based originator and receiver agreed upon method
PEM processes based on cryptography and message encoding
MIC-CLEAR (Message Integrity Code- CLEAR)
MIC-ONLY
ENCRYPTED
Pretty Good Privacy (PGP)
PGP secure mail package developed by Zimmerman
Available in public domain
Signature generation
Uses MD5 to generate hash code
Encrypts hash code with sender's private key using RSA algorithm
Encryption of the message done using IDEA or RSA
Compression done with ZIP
email conversion done using Radix-64
PGP similar to encrypted PEM with added compression
X-400: OSI specifications that define framework; not implementation specific