Benefits of IPsec

Rodney Thayer

<rodney@internetdevices.com>

internet DEVICES

Solution Topics

- Network Architecture
- Network Security Topology
- Security Considerations
- Capabilities for Threat Prevention

Network Architecture

- Implemented at Network Layer -- all (appropriate) IP packets are protected
- Limits impact on existing network -- applications do not have to change, platform independance
- Various privacy and authentication options -- encryption and authentication or authentication-only
- Implemented within the protocol stack of intermediate systems or end systems

Network Security Topology

- Network layer processing allowsdeployment in Gateways ("Tunnel Mode")
- Capable of supporting End Systems as well ("Transport Mode")
- Controllable by Network Manager, as it's an infrastructure attribute
- Stackable -- since it properly uses the IP packet format, you can have tunnels within tunnels.
- Use of proper IP packets means conventional routing and other packet processing can be applied.

Security Considerations

- Developed in an open standards body (IETF) by a working group from various backgrounds.
- Publically reviewed use of Cryptography
- Capability to add or subtract cryptographic algorithms in case of new discoveries
- Architecture provides for implementations that apply control and filtering to network traffic
- Uses current state of the art technologies -- PKI, 3DES, SHA-1, key exchange, Perfect Forward Secrecy

Capabilities for Threat Prevention

- Implementation at the Network Layer provides capability to protect against Network Layer attacks
- Authentication protects against unauthorized packet traffic such as spoofing or IP header manipulation
- Privacy of Network Information can be used to protect user data as well as (control information), which protects agains both data theft and infrastructure attack
- Control Internal Network Access -- use of AH or Intranet IPsec can manage access to the Internet from within a site
- Allows Network-wide security parameters to be reconfigured - use of Gateways can provide scaled management of security