NSA's Secure Mobility Program

Margaret Salter

NATIONAL SECURITY AGENCY

INFORMATION ASSURANCE DIRECTORATE

Session ID: PNG 202

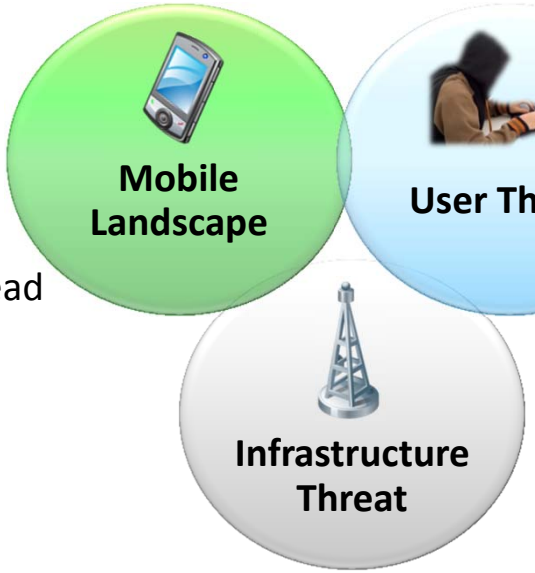
Session Classification: Intermediate

Secure Anywhere, Anytime Access to Enterprise Infrastructure

Current Mobility Environment

Mobile Landscape

- Ease of use is valued over security
- Vulnerabilities are widespread
- Attacks are cheap and easy



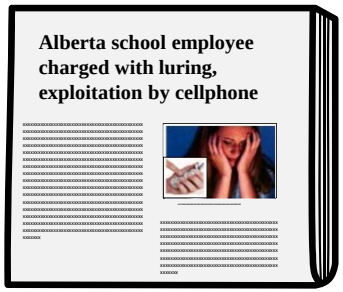
User Threat

Users are vulnerable to:

- Social engineering
- Ignorance of threats
- Bypassing inconvenient security
- Insider threat

"The average computer user is going to pick dancing pigs over security any day."

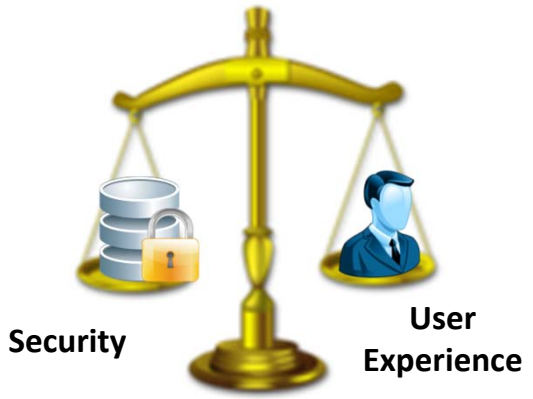
- Just do an Internet search
- Numerous commercially available applications
- Low cost and in some cases "free"
- Minimal user technical experience required



Uncontrolled Infrastructure Threat

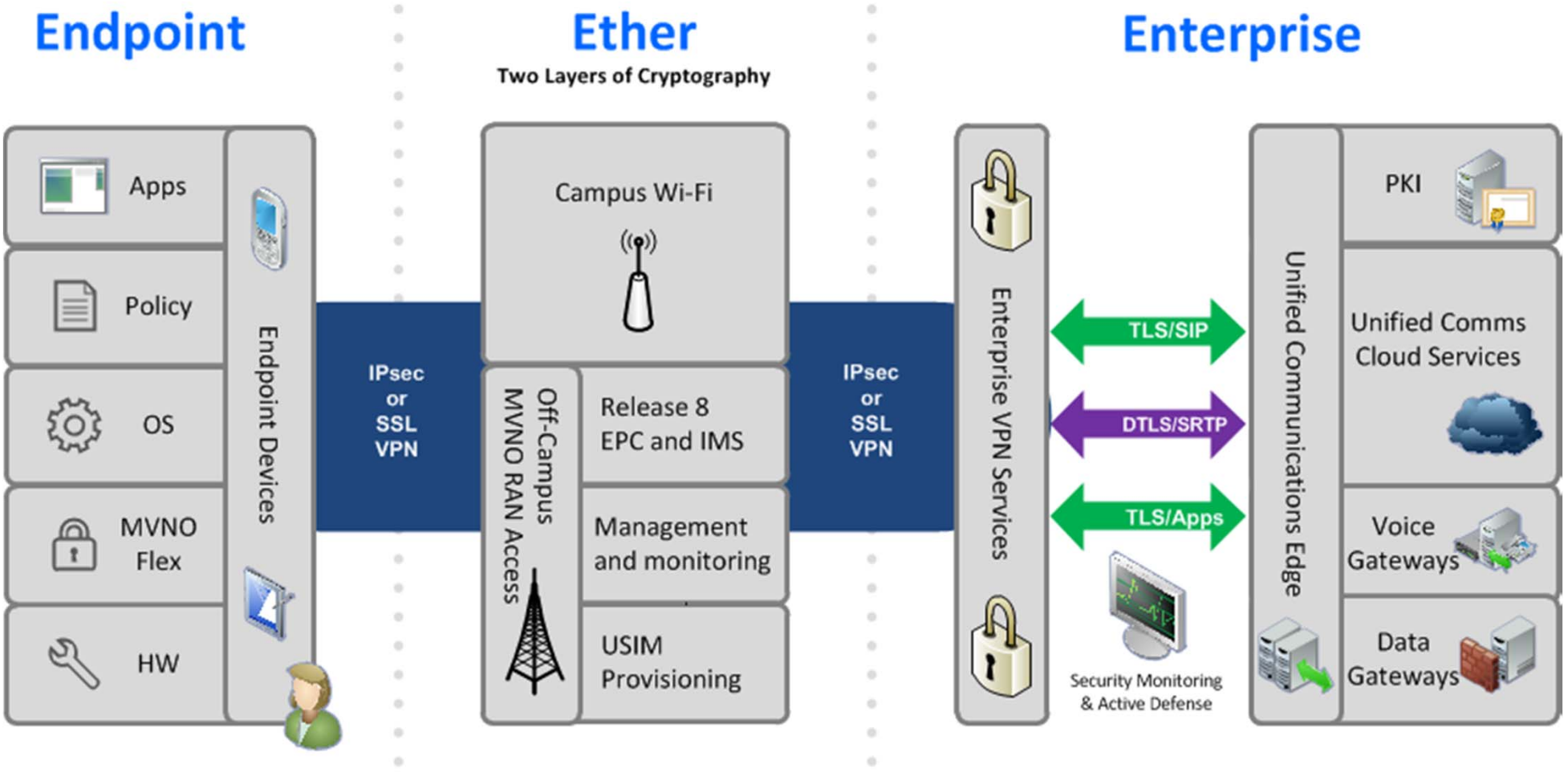
- Towers
- Communication centers
- Communication lines
- Main data centers
- Carrier updates
- Rogue base stations

Establishing a Balance

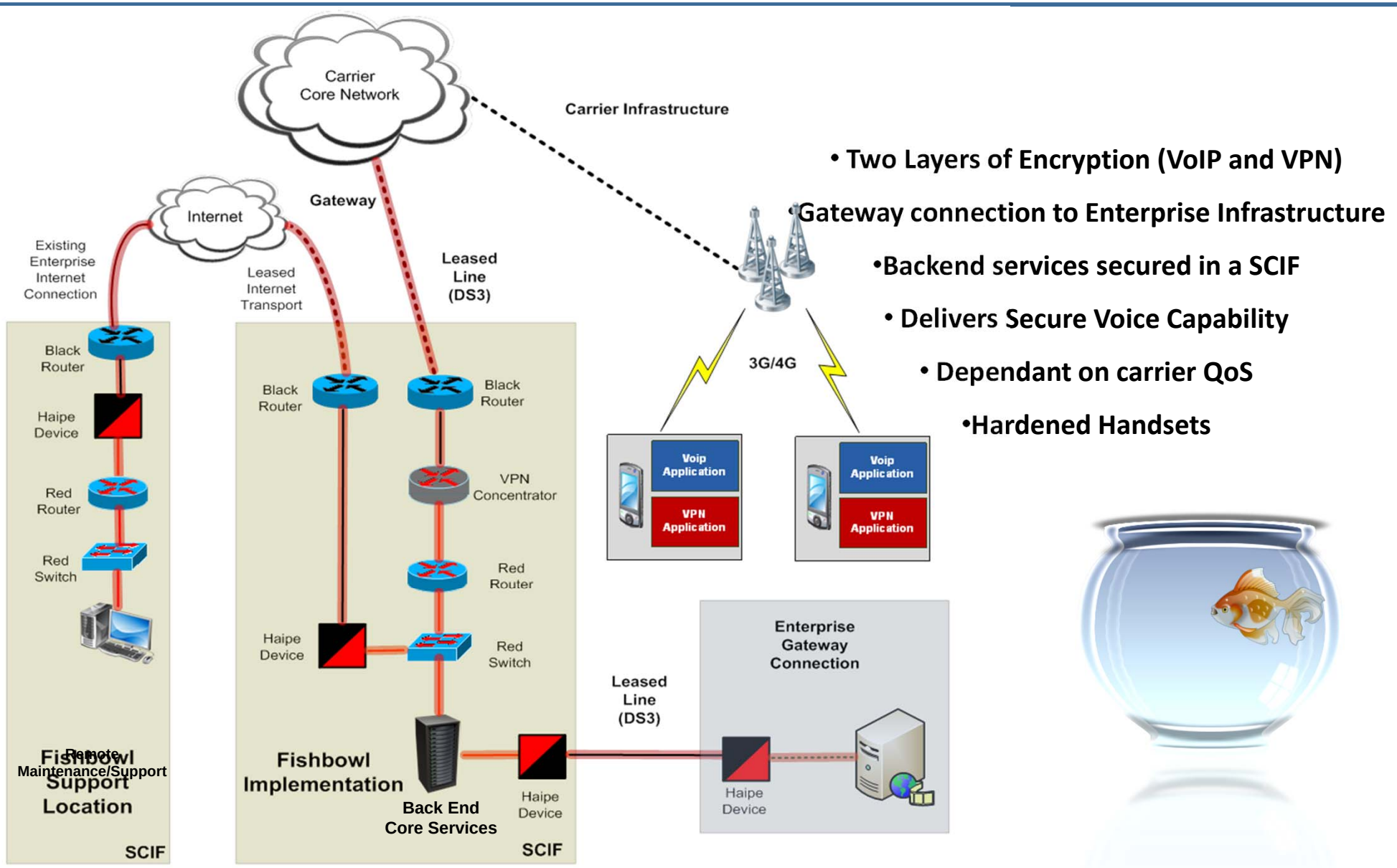


- Security must be integrated into components.
- User interfaces must be intuitive and familiar.
- Solutions should support commercial functionality.
- Solutions should be cost effective.
- Solutions should align with commercial product lifecycles and standards.

EEE Components

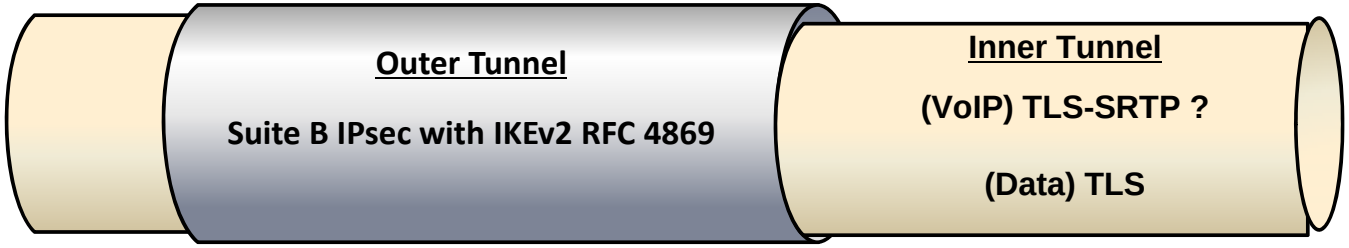


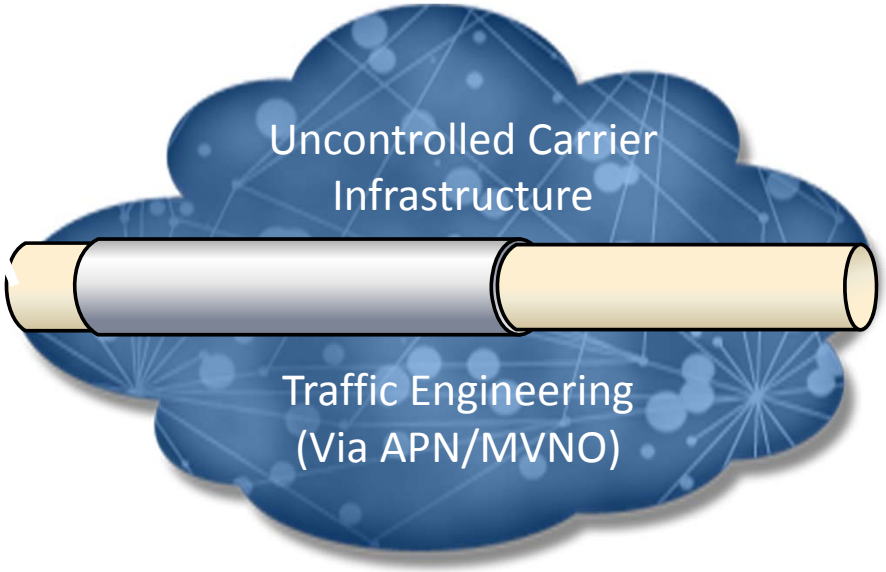
Fishbowl Architecture



- Two Layers of Encryption (VoIP and VPN)
- Gateway connection to Enterprise Infrastructure
- Backend services secured in a SCIF
- Delivers Secure Voice Capability
- Dependant on carrier QoS
- Hardened Handsets

Long-term Preferences





APN Gateway

Enterprise Infrastructure

Preferred Devices

- Supports Enterprise Management
- Supports Separation
- Secure Application Delivery
- Supports Thin Client Architecture
- Incorporates Certificate Stores
- Standards based design

Preferred Carrier Transport

- Provides Quality of Service
- Limits traffic exposure through engineering
- Supports global coverage
- Controls access to end user device and cellular metadata

Preferred Unified Communications Infrastructure

- Provides Unified Communications Services
- Supports Thin Client / Cloud computing Architecture
- Standards based design

Why is this so hard (OS...OEM)?

- IKEv2
  - AES 128 CBC
  - AES 256 CBC
  - ECDSA (P-256, P-384)
  - ECDH (P-256, P-384)
  - SHA2 (256 and 384)
- IPsec
  - AES 256 GCM
  - AES 128 GCM

8

Why is this so hard (Voice App)?

- SDES
  - TLS Version?
  - Client Auth
  - Suite B
  - Interoperability
- DTLS
  - Version?
  - Suite B
  - SBCs
  - UC servers

9

Why is this so hard?

- SIP Trunking
  - TLS
  - Interoperability
- 3G QoS

Requirements

- OS
- Apps
- Infrastructure

- www.iad.gov

Apply

Securing mobility requires a new way of thinking:

- Commercial standards, platforms, and applications must be leveraged.
- Solutions and services must be composable to achieve desired security.
- Commercial infrastructure may be integrated and hardened through the use of an MVNO.
- Strong partnerships between government and industry must be established to achieve preferred capabilities.
- Solutions must evolve to keep pace with emerging technologies.

Questions?