



Air
Land
Sea
Space
Cyberspace

Innovation. In all domains.

First Net Information Assurance Guidance

Thomas Farley
Sr. Systems Engineer
April 23rd 2012

First Net Information Assurance Guidance and Interoperability

NCS Cyber Defense Solutions

Thomas Farley- Sr. Systems Engineer- CISSP

April 23rd 2012

Smart Device Technology

§ Speeds of 4G technology allow the wide spread use of data capable devices.

§ Data access will likely be the main cause of compromise.

- Over 40 virus families and more than 300+ mobile viruses since 2004
(www.fortinet.com)

- Only about 16% of users have adequate security on their smart phones
(www.symantec.com)

§ Access contact lists from both email and phone #'s

§ Dial premium rate numbers

§ Send SMS/MMS as spam

§ Spread via Bluetooth, WiFi, memory cards (sims)

§ No difference between Computers and Phones

LTE is built with all the new and existing features of IP protocols but also inherits the flaws and vulnerabilities.

Interoperability points

§ LTE Transport

- 4G Network, distributed IP Network, Non 3gpp gateways

§ LTE Access Device

- Wireless access points

§ End Point Devices

- Smart Phone devices, Over Air (push to talk) radios, laptops/tablets

§ Core Services

- SMS, location services

§ LTE Management

- VPN access, authentication mechanisms

LTE is built with all the new and existing features of IP protocols but also inherits the flaws and vulnerabilities.

LTE Transport

§ Vulnerability/Attack Vectors

- Ipsec, Session Key Generation, USIM, some security features are optional...transport versus tunnel

§ Response

- Compatible vendor matrix, Key length (security configuration guidance), Key Hierarchy, vulnerability assessments

§ Interoperability Considerations

- Certificate and Key management, Access domains, data domains, partner roaming

LTE is built with all the new and existing features of IP protocols but also inherits the flaws and vulnerabilities.

LTE Access Device

§ Vulnerability/Attack Vectors

- Hotspot firmware attacks, Device Software, session Hi-jacking, concurrent paths

§ Response

- trace back protocols, encryption (WPA2, PSK), timed credentials, firmware updates

§ Interoperability Considerations

- login process, EAP Encryption Types, Roaming partners (SSID's)

LTE is built with all the new and existing features of IP protocols but also inherits the flaws and vulnerabilities.

End Points (Mobile Phones, Over Air Radios, Laptops)

§ Vulnerability/Attack Vectors

- Worms, Trojans, packet sniffing, spoofing

§ Response

- Antivirus/malware detection, Encrypted Tunnels, patch management/firmware updates, digital rights management, vulnerability assessments

§ Interoperability Considerations

- VPN client compatibility, multifactor authentication schemes

LTE is built with all the new and existing features of IP protocols but also inherits the flaws and vulnerabilities.

Core Services

§ Vulnerability/Attack Vectors

- application attacks, SMS, location based services, IPTV

§ Response –

- digital signatures, subscriber services, data meta-tagging/filtering, vulnerability assessments

§ Interoperability Considerations

- Certificate management, credential schemas, policy mismatch

LTE is built with all the new and existing features of IP protocols but also inherits the flaws and vulnerabilities.

LTE Management services

§ Vulnerability/Attack Vectors

- Split tunneling, password attacks, keystroke logging

§ Response –

- digital signatures, dual factor authentication, concurrent interface control, vulnerability assessments

§ Interoperability Considerations

- Certificate management, authentication mechanisms

LTE is built with all the new and existing features of IP protocols but also inherits the flaws and vulnerabilities.

Interoperability and Security Measures

- § Documented Configuration guidance
- § Communicated processes and procedures
- § Vendor Selection Compatibility Matrix
- § Periodic Vulnerability assessments/Penetration Testing
- § User/Admin Security Awareness training

LTE is built with all the new and existing features of IP protocols but also inherits the flaws and vulnerabilities.