ITU-T / ATIS Workshop
"Next Generation Network Technology and Standardization"
Las Vegas, 19-20 March 2006

The ITU-T NGN Security Standards—Status and Challenges

Igor Faynberg, Ph.D.

Technical Manager, Lucent Technologies

ITU-T SG 13 Security (Q.15) Rapporteur

ITU-T

Outline

- Why NGN security?
- The ITU-T work on NGN Security
- Relationship to other SDOs
- Output of the NGN Focus Group
- Recent developments—starting the SG 13 Security work
- Top NGN security issues that need resolution

Security is among the key *differentiators* of the NGN. It is also among its biggest *challenges*!..

Why Security? (Threat examples)

- Subscriber's perspective
  - Eavesdropping, theft of PIN codes
  - Tele-spam
  - Identity theft
  - Infection by viruses, worms, and spyware
  - Loss of privacy (call patterns, location, etc.)
  - Flooding attacks on the end point

- Provider's perspective
  - Theft of service
  - Denial of service
  - Disclosure of network topology
  - Non-audited configuration changes
  - Additional related risks to the PSTN...

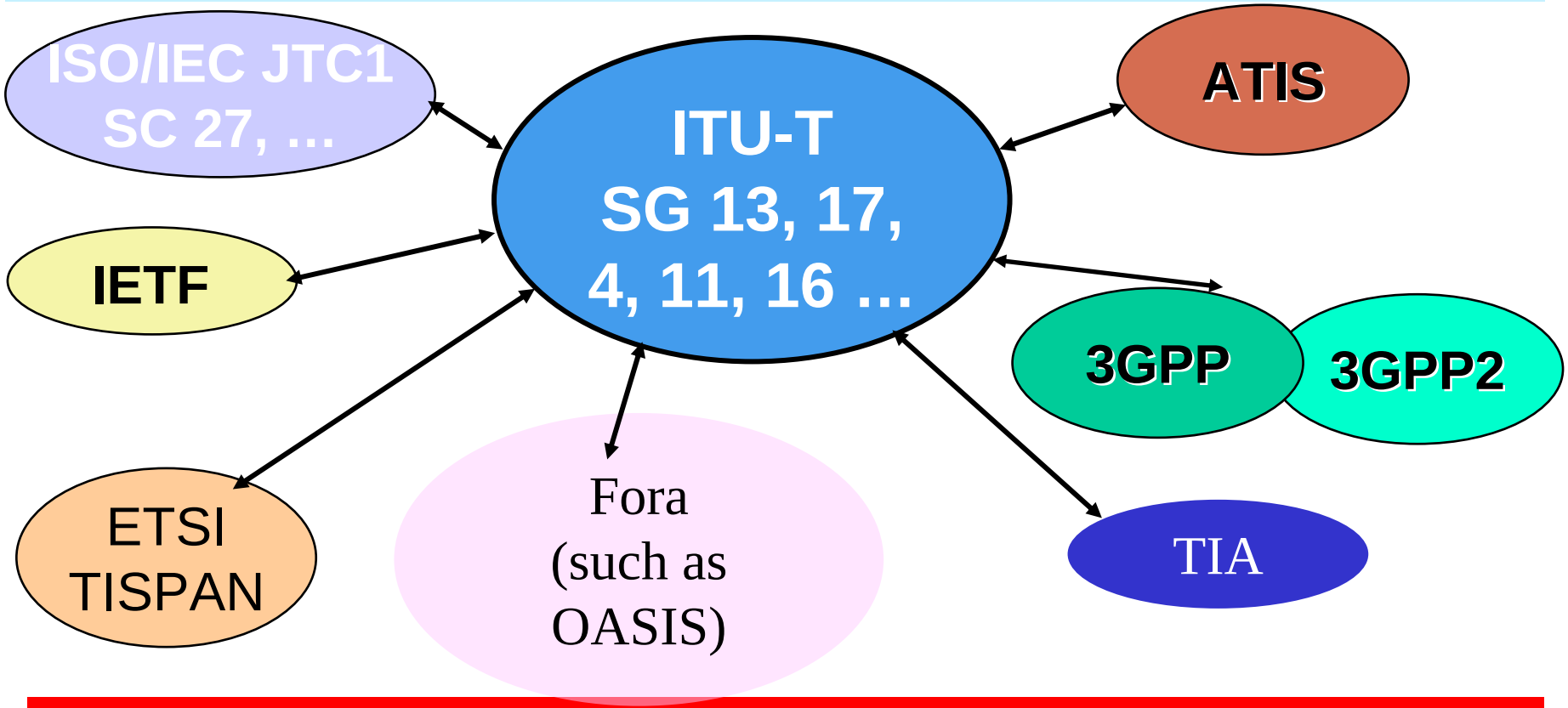
In NGN, known IP security vulnerabilities can make PSTN vulnerable, too!

The ITU-T work on NGN Security

- SG 13: Lead Study Group on the NGN standardization. (Question 15/13 is responsible for X.805-based NGN security)
- SG 17: Lead Study Group on Telecommunication Security—the fundamental X.800 series, PKI, etc.
- SG 4: Lead Study Group on Telecommunication Management—Management Plane security
- SG 11: Lead Study Group on signaling and protocols—security of the Control and Signaling planes
- SG 16: Lead Study Group on multimedia terminals, systems and applications—Multimedia security

FGNGN has concluded; its work has moved to SG 13

Collaboration of ITU-T with other SDOs and fora on NGN security Recommendations



SG 13 is the Lead Study Group for NGN
SG 17 is the Lead Study Group for Security

Question 15 SG 13, NGN security

- Question 15 (NGN security) of SG 13 – ITU-T lead study group for NGN and satellite matters - will continue standards work started by FGNGN WG 5.
- Q.15/13 major tasks are:
  - *Lead* the NGN-specific security project-level issues within SG 13 and with other Study Groups. Recognizing SG 17's overall role as the Lead Study Group for Telecommunication Security, *advise* and *assist* SG 17 on NGN security coordination issues.
  - *Apply* the X.805 Security architecture for systems providing end-to-end communication within the context of an NGN environment
  - *Ensure* that
    - the developed NGN architecture is consistent with accepted security principles
    - Ensure that AAA principles are integrated as required throughout the NGN

FGNGN output: *Security Requirements for NGN Release 1* (highlights)

- Security requirements for the *Service Stratum*
  - IMS securty
  - Transport domain to NGN core network interface
  - Open service platforms and applications security
  - VoIP
  - Emergency Telecommunication Services and Telecommunications for Disaster Relief

- Security requirements for the *Transport Stratum*
  - NGN customer network domain
  - Customer network to IP-Connectivity Access Network (IP-CAN) interface
  - Core network functions
  - NGN customer network to NGN customer network interface

FGNGN output: *Guidelines for NGN Security Release 1* (highlights)

- General
  - General principles and guidelines for building secure Next Generation Networks
  - Detailed examination of IMS access security and NAT and firewall traversal
  - NGN Security Models
  - Security Associations model for NGN

- Security of the NGN subsystems
  - IP-Connectivity Access Network
  - IMS Network domain and IMS-to-non-IMS network security
  - IMS access
  - Framework for open platform for services and applications in NGN
  - Emergency Telecommunications Service (ETS) and Telecommunications for Disaster Relief (TDR) Security
  - Overview of the existing standard solutions related to NAT and firewall traversal

Focus of the current work of Question 15 SG 13, NGN security

- Security Requirements for NGN Release 1
- Authentication requirements for NGN Release 1
- AAA Service for Network Access to NGN
- Guidelines for NGN Security Release 1
- Security considerations for *Pseudowire* (PWE) technology

At the heart of securing network protocols, the biggest challenge is **authentication.**

Major Issues for NGN Security Standardization

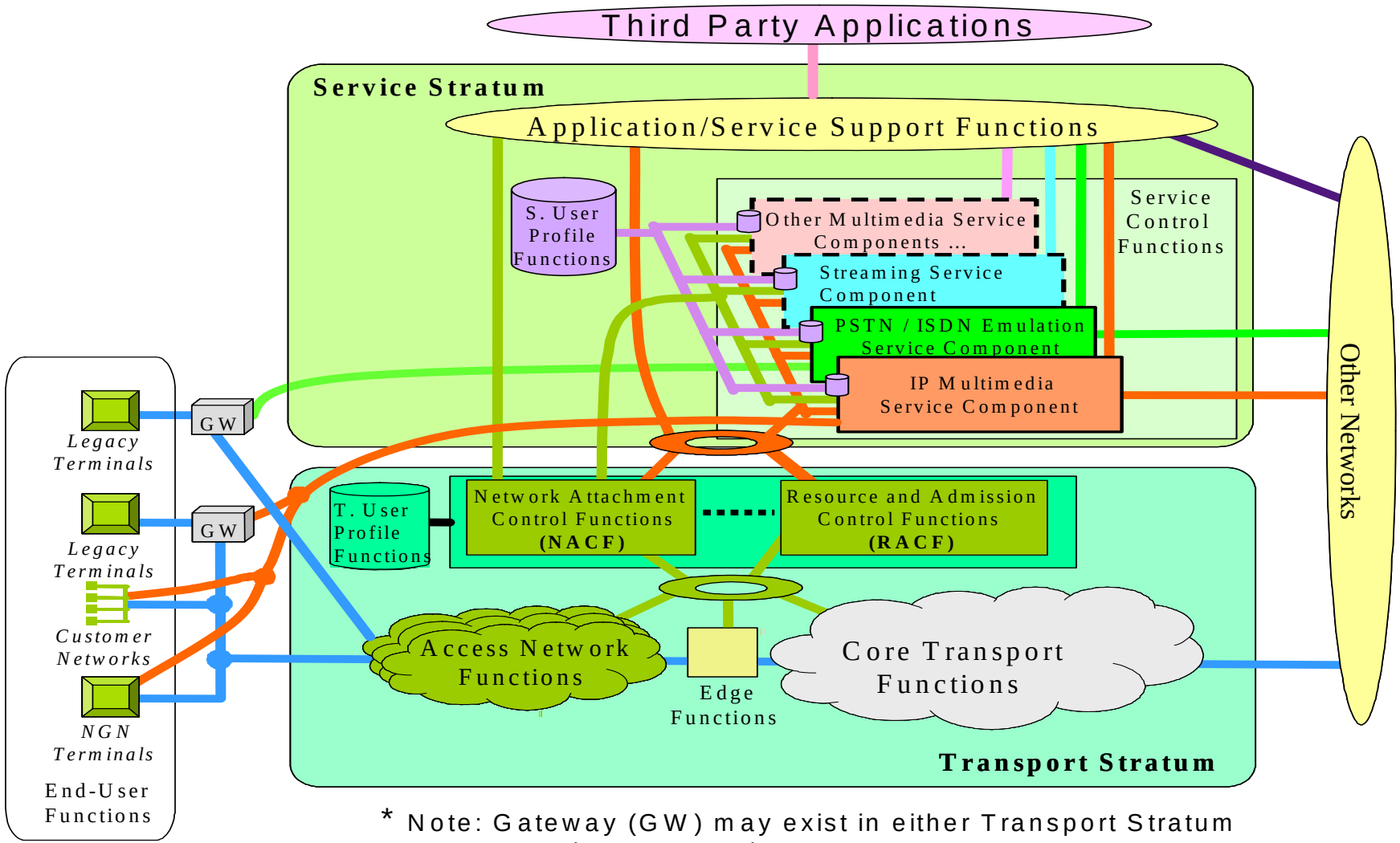
- Key distribution (for end-users and network elements) and Public Key Infrastructure
- "Network privacy"—topology hiding and NAT/Firewall traversal for real-time applications
- Convergence with IT security
- Management of security functions (e.g., policy)
- Guidelines on the implementation of the IETF protocols (e.g., IPsec options)
- Security for supporting access: DSL, WLAN, and cable access scenarios
- Guidelines for handling 3GPP vs. 3GPP2 differences in IMS Security

Both—network *assets* and network *traffic*—must be protected.

Proper *management* procedures will help prevent attacks from within.

Backup

Standard NGN Architecture



* Note: Gateway (GW) may exist in either Transport Stratum or End-User Functions.

Acronyms

- 3GPP — 3rd Generation Partnership Project
- 3GPP2 — 3rd Generation Partnership Project 2
- AAA — Authentication, Authorization, Accounting
- DSL — Digital Subscriber Line
- IETF — Internet Engineering Task Force
- IP CAN — IP Connectivity Access Network
- ETSI — European Telecommunications Standards Institute
- IMS — IP Multimedia Subsystem
- ISO — International Organization for Standardization
- IT — Information Technology
- NAT — Network Address Translation
- NGN — Next Generation Networks
- PWE — PseudoWire Emulation
- RACF — Resource and Admission Control Function
- SIP — Session Initiation Protocol
- WLAN — Wireless LAN