Liaisons and Other Security Efforts

Chris Lonvick
Cisco Systems
clonvick@cisco.com

IETF Liaisons

IETF Liaisons are handled by the IAB

- http://www.iab.org/liaisons/index.html

-

- IAB Liaison Statements

  - IAB Liaison Statements are archived by the IAB in a Liaison Correspondance directory.

    - http://www.iab.org/documents/selected-iab-documents.html

  - All IETF Liaison statements are archived in the IETF's Liaison Statement directory.

    - https://datatracker.ietf.org/public/liaisons.cgi

IETF Liaisons

- http://www.ietf.org/internet-drafts/draft-baker-liaison-statements-01.txt

- Abstract:

  - This document describes the procedure for proper handling of incoming liaison statements from other standards development organization (SDOs), consortia, and industry fora, and for generating liaison statements to be transmitted from IETF/ISOC to other SDOs, consortia and industry fora. This procedure allows IETF to effectively collaborate with other organizations in the international standards community.

  - Liaison Statements are only exchanged within the context of established liaison relationships, which are managed by the IAB.

Liaisons at Other SDOs

- Liaisons at other SDOs are handled in a very well-known and formal manner.

- Liaison statements MUST be dealt with in the proper group (Working Party, Study Group, etc.), and a response sent before work can continue.

What Does This Mean for Us?

- We probably shouldn't ask for any Liaisons until after the WG has been formed.

- The WG will need to exchange Liaison Statements with other SDOs through IAB Members.

What Do We Need To Do Before We Ask for Liaison Statements With Other SDOs

- We need to identify specific efforts and decide if we want to communicate our own efforts with them. This may be used to ensure that there are no conflicts with Standards being produced by other SDOs.

- If we send a liaison statement, then we will be asking for the formal opinion of the other SDO and we must commit to receive and act upon their response.

Other Operational Security Efforts

Other Operational Security Works

- http://www.ietf.org/internet-drafts/draft-lonvick-sec-efforts-00.txt

- 3 Parts:
  - Glossaries
  - SDOs
  - SDO Efforts

- Will be contributed as a WG document when the WG is formed.

- Feedback is appreciated.

Other Operational Security Works

- The Intent of this ID: Awareness
- Multiple OpSec Standards may result in:
    - Vendors of networking equipment unsure of which standard to follow.
    - Purchasers of networking equipment unsure of which standard will best apply to the needs of their business or organization.
    - Network Administrators and Operators unsure of which standard to follow to attain the best security for their network.

The T1M1.5 SEC Effort

T1M1.5SEC   http://www.t1.org

3M150074 → ANSI   http://www.ansi.org/
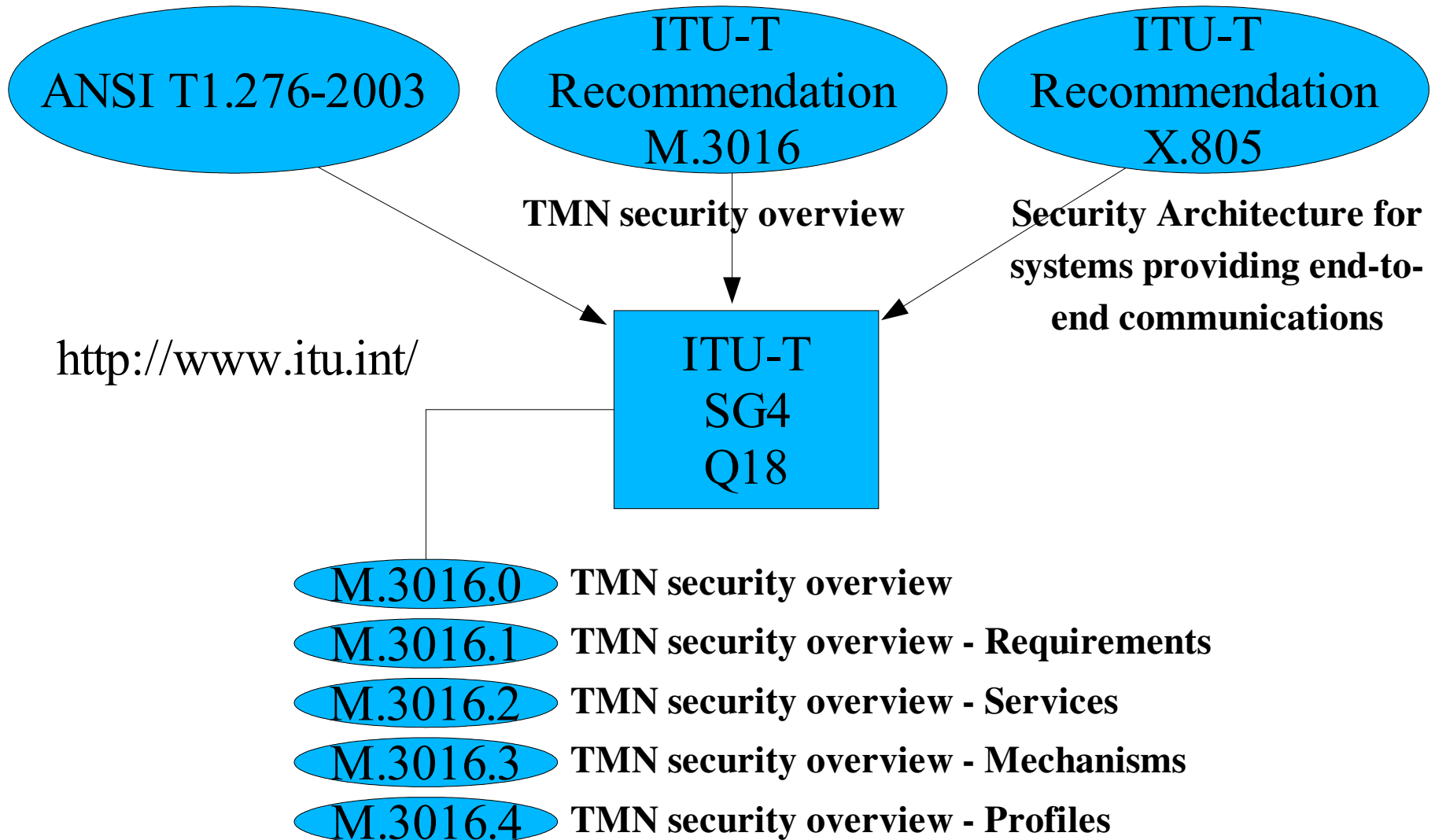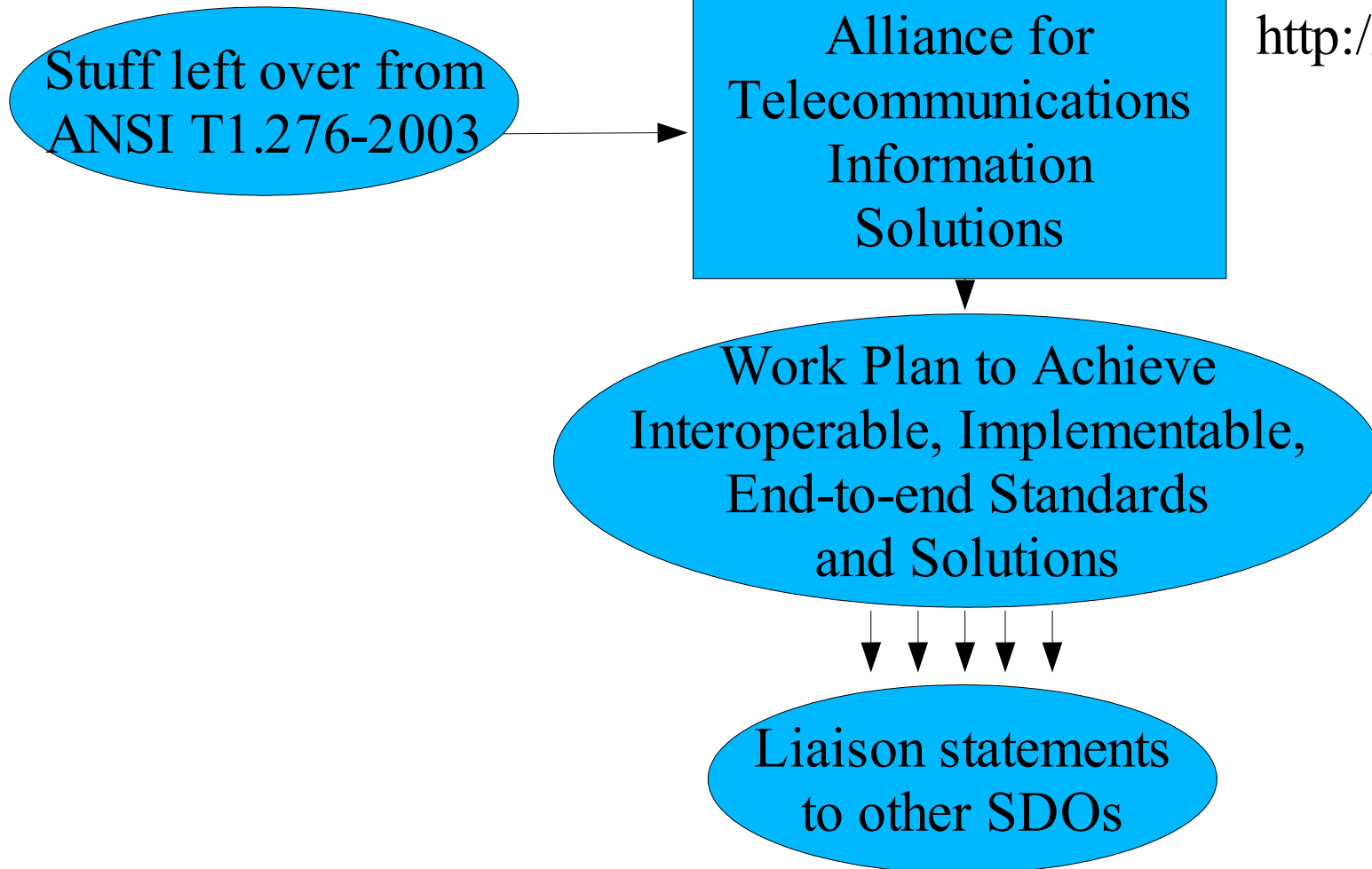
Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane

ANSI T1.276-2003

..going into ITU-T

ANSI T1.276-2003

ITU-T Recommendation M.3016

ITU-T Recommendation X.805

TMN security overview

Security Architecture for systems providing end-to-end communications

http://www.itu.int/

ITU-T SG4 Q18

M.3016.0 TMN security overview

M.3016.1 TMN security overview - Requirements

M.3016.2 TMN security overview - Services

M.3016.3 TMN security overview - Mechanisms

M.3016.4 TMN security overview - Profiles

..going back into ATIS

Stuff left over from ANSI T1.276-2003

→ Alliance for Telecommunications Information Solutions

http://www.atis.org/

↓

Work Plan to Achieve Interoperable, Implementable, End-to-end Standards and Solutions

↓ ↓ ↓ ↓ ↓

Liaison statements to other SDOs

T1M1.5 (Security)

- Work Items from ATIS Security Work Plan
- ftp://ftp.t1.org/T1M1/NEW-T1M1.0/3M101950.xls

Security Management System

- ftp://ftp.t1.org/T1M1/NEW-T1M1.5/3M151120.zip

- Stu Jacobs of Verizon - editor

  - **Part of TOPS Security Work Plan, Section 3:** Overall Security Management System includes:

    - Security Event Management and Attack Determination and Mitigation;

    - Configuration Management (including user accounts and passwords);

    - Credentials Management

    - Security Verification and Validation;

    - EMS Interface

Packet Filtering
to Prevent Unwanted Traffic

- Also a new Work Item in T1M1.5 – no submission yet.

- Kam Lam of Lucent

- **Part of TOPS Security Work Plan, Section 1.1.1.4:**

- A mechanism monitoring the end-userplane traffic to permit or discard packets based upon easily identifiable or commonly expected attributes of each packet.

Wrap Up

- Chris sent out an email to the group about these other efforts and how to participate. The documents in those other efforts have some restrictions and may not be available to this Working Group or to all Individuals. Chris will check and make them available if possible.

- This WG should be aware of the other efforts and they should be aware of our effort.