ITU-T e-FLASH

Telecommunication Standardization Sector

Helping the world communicate

International Telecommunication Union

Issue No. 1

This news update is available electronically – if you would like to received a regular copy please send an e-mail to ITU-T_e-flash@itu.int and type "subscribe" in the subject field.

Work Continues to Enhance Broadband Cable Offering

Study Group 9's recent Hawaii meeting, saw a raft of new and revised Recommendations seeking to enhance broadband cable services. One significant new Recommendation - J.179 - gives service providers using the IPCablecom standard the ability to offer the whole range of digital multimedia services including video, interactive TV and games. IPCablecom is an end-to-end system for the delivery of time-critical communications to cable TV customers using Internet Protocol (IP). It builds on widely deployed digital cable modem architectures specified in ITU-T Recommendation J.112.

Workshop on Home Networks Announced

Also in Hawaii Study Group 9 agreed to hold a workshop - Home Networking and Home Services - June 17-18 in Tokyo (on June 16 there will be a tutorial session for Japanese speaking participants). There is industry demand for standardization in the area, as more consumers seek to link home appliances such as TVs, PCs and even refrigerators. The workshop will examine these possibilities as well as the means of connection - wireless, powerline, Ethernet etc. - and security implications.

Group to Tackle Firewall/NAT Traversal

Study Group 16 - the multimedia Study Group - has started work on a standard that will allow VoIP and other IP based protocols to be more easily implemented in a secure enterprise or service provider environment. VoIP and other IP-based protocols have long been plagued with problems when trying to work across network address translation (NAT) and firewall boundaries. Despite previous attempts to address the issue, no standardized way of dealing with the problem has emerged.

Currently many network managers and operators have found that the only way to allow inbound VoIP calls in a firewall-protected environment is to leave a permanent hole from the outside world to gateways or to the user's IP phone. Obviously, this violates even the most basic firewall security policies. Compounding the problems with VoIP and firewalls is the fact that VoIP doesn't really work well with NAT (changing the IP address and/or port used internally to be different from the IP address and/or port used externally). NAT is typically performed by the enterprise firewall.

The new work aims to create a robust and easy to implement solution that will allow any device communicating on an IP network to more easily communicate across the network boundary imposed by NAT or firewalls.

Security Flaw Affects VoIP

Recent press reports have highlighted vulnerabilities in some applications using ITU-T Recommendation H.323. Experts were quick to point out however, that the security issues are not related to H.323, but rather to poor implementation that can cause improper handling of messages in some vendors' products. Indeed not all products using H.323 are at risk. Correcting the problem is relatively straightforward and most vendors impacted have reportedly taken corrective action.

The problem stems from the fact that some products fail to perform proper checking of messages to ensure that they are correctly formed. As a result, malformed messages transmitted can result in system failures of various types. In the worst case, an attacker could have intentionally caused buffer overflow, giving the opportunity to execute malicious code on the target system. This is unlikely now that the problem has been addressed in most vendors' products.

H.323 is the most widely used VoIP communication protocol worldwide. In common with all protocols its implementation should be adhered to carefully, to avoid security vulnerabilities. It is unlikely, according to ITU's H.323 experts, that global long distance networks based on H.323 carrying billions of voice minutes each month will be impacted at all. Continued vigilance by security monitoring organizations and by manufacturers will mean that these small windows of opportunity for hackers will be quickly closed.

Group Works to Protect Networks from Nuclear Threat

At its latest meeting the ITU-T Study Group responsible for protection against electromagnetic environment effects, has proposed new work that will help protect networks against electromagnetic threats such as nuclear attack. Specifically the proposed work will examine how to protect against malicious man-made phenomena such as High-Altitude Electromagnetic Pulse (HEMP) and High-Power Microwave (HPM). The new study into electromagnetic security will also look at the potential for information leaks from networks by accidental radio emission from equipment.

Home Networking Safety Threat Addressed

Other new work proposed at the (Study Group 5) meeting was study into Electromagnetic Compatibility (EMC), resistibility (the ability of a device to survive power and lightning surge) and safety issues for home networks. Work on standards in this area is seen as increasingly important given the research and development dollars going into the networks that may one-day link all our domestic devices. Study Group Chairman Roberto Pomponi of Telecom Italia says that he expects that one field of study may relate to in-home Power Line Communications.

New Standard for EMC Testing

As well as identifying new areas for study, Study Group 5 agreed on a new Recommendation that outlines a methodology to check if equipment maintains its designed and tested EMC performances. Pomponi said that the Recommendation (K.63) was designed to address a network operator need to cheaply and efficiently check EMC performance of equipment during its acceptance procedures. The Recommendation also provides a way for manufacturers to perform rapid assessment of a production run.

ITU-T Manual Addresses Security Concerns

ITU-T has been active in security in telecommunication and information technology for many years. However, it may not always have been easy to find out what has been covered, and where it can be found. For this reason *'Security on Telecommunications and Information Technology. An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications'*, has been produced. The manual is a first attempt at aggregating all of the available information. It aims to act as a guide for technologists, middle level management and regulators to assist in the practical implementation of security functions.

An electronic version of the guide is available: itu.int/ITU-T/edh/files/security-manual.pdf

UPCOMING EVENTS

- **ITU-T Meetings:**
  - **SG 13** - Multi-protocol and IP-based networks and their internetworking
    (Geneva, 3-12 February 2004)
  - **SG 2** - Working Party 2 - Network service and assessment, and traffic engineering
    (Geneva, 1-3 March 2004)
  - **SG 11** - Signalling requirements and protocols
    (Geneva, 1-12 March 2004)
  - **SG 17** - Data Networks and Telecommunication Software
    (Geneva, 10-19 March 2004)
  - **SG 12** - End-to-end transmission performance of networks and terminals
    (Geneva, 24-31 March 2004)

- **Workshops and Seminars:**
  - **ITU Seminar on Standardization**
    Phnom Penh, Cambodia, 11-13 February 2004
  - **High-level workshop on International Standards for Medical Technologies**
    WHO (World Health Organization), Geneva, 26-27 February 2004
  - **Convergent regulation - Is it becoming technology-neutral?**
    ITU Headquarters, Geneva, 17 May 2003
  - **All Star Network Access Workshop**
    CICG building (International Conference Centre of Geneva), Geneva, 2-4 June 2004
  - **Home Networking and Home Services Workshop**
    Japan, 16-18 June 2004