

Workshop on “New Horizons for Security Standardization” Geneva, 3 - 4 October 2005

Address

by

Mr. Houlin ZHAO

Director, Telecommunication Standardization Bureau

Mr. Chairman,
Distinguished delegates,
Ladies and Gentlemen,

Good morning,

On behalf of ITU, please let me welcome you to this Workshop on “New Horizons for Security Standardization”.

With our increasing dependence on electronic communication networks, the importance of security cannot be overemphasized. The explosive growth in the use of this infrastructure has increased the reliance of organizations and individuals on the information stored and communicated using these systems. This has led to a heightened awareness of the need to protect data and resources.

The increased profile of ICT security may be attributed in part to widely reported incidents such as viruses, worms, hackers and threats to personal privacy. However, as computing and networking are now such an important part of daily life, the need for effective security measures to protect the computer and telecommunication systems of governments, industry, commerce, critical infrastructures and consumers is imperative.

In December 2003, the World Summit on Information Society (WSIS) unanimously adopted a Declaration of Principles and a Plan of Action. The WSIS Declaration of Principles highlights the importance of cybersecurity.

During PrepCom-3 of WSIS II, which was held in Geneva on 19-30 September 2005 these views were reconfirmed. In association with the WSIS process, ITU has organized several Cybersecurity Symposiums:

- the Cybersecurity Symposium was collocated with WTSA-04 in Florianópolis, Brazil in October 2004;
- Cybersecurity Symposium II, was held in Moscow, Russia in March this year;
- a Thematic Workshop on Cybersecurity was organized in Geneva in June 2005.

It should also be noted that the Plenipotentiary Conference of the ITU (PP-02), held in Marrakesh, Morocco, 2002, approved Resolution 130 regarding “strengthening the role of ITU in information and communication network security”.

The Standardization Sector of the International Telecommunication Union (ITU-T) has always put security high on its agenda. At WTSA-04, ITU-T approved new Resolution 50 on “Cybersecurity”. The last three World Telecommunication Standardization Assemblies (WTSA-1996, WTSA-2000 and WTSA-04) designated Study Group 17 as the Lead Study Group for Communication Systems Security. Over 70 ITU-T Recommendations were published in the field. ITU-T Recommendation X.509, developed in 1988, for electronic authentication over public networks, and ITU-T Recommendation X.805, which deals with security architecture for end-to-end communications are two examples. ITU-T, and particularly ITU-T SG 17, has organized several workshops on Security. A handbook “Security in Telecommunications and Information Technology – An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications” was prepared by TSB in coordination with ITU-T experts.

The overall objectives of this workshop are to help address information and communications security issues and promote increased cooperation between organizations engaged in security standardization work. Consideration will also be given to issues of adoption and implementation of security standards. In particular, the workshop will:

- seek to find out from stakeholders (e.g., network operators, system developers, users etc.) what are their primary security concerns/issues?
- determine where ITU-T and other standards development organizations (SDOs) can most effectively play a role in helping address the issues (i.e., which issues are amenable to a standards solution?);
- identify which SDOs are working on these issues or are best equipped to do so; and
- agree on next steps for security standardization.

A new initiative by ITU-T Study Group 17 is to develop a roadmap of security standardization of both ITU-T and other standards makers. We hope it will give a unique overview of security work going on across the standardization world and allow easy identification of any gaps in the work that need to be addressed. The discussions during this workshop will help SG 17’s endeavours.

Before concluding, I would like to extend my thanks to the members of the Steering Committee for their excellent work. I wish to thank Chairmen of sessions, Speakers and Moderators for having accepted our invitation to actively participate in this workshop. We also appreciate your presence.

I wish you a very successful workshop.

Thank you for your attention.