ITU-T Workshop

"New Horizons for Security Standardization"

Abstract

Geneva, 3 –4 October 2005

Speaker: **Mr. Eric Wiatrowski**

France Telecom – Enterprise Communication Services
Chief Security Officer

Session: **4**: Stakeholder Perspectives

Title of Presentation: **Security Standardization**

The Telco's Paradigm

Protocols and Security: Past, Present and Future

In the former times, protocols were designed with embedded security. For instance, the X.25 packet switching protocol defines many security features such as calling address check, closed user groups, network user identification… that help to protect against intrusions and denial of service.

Nowadays protocols are rapidly designed to be time to market. The result is that security is not part of the initial standard release. It is afterwards that security enhancements are made to supplement the initial specifications. The WiFi is a very good example of this behavior. To improve confidentiality and user identification, WAP and 802.1X mechanisms have been added to supplement the deficient WEP and MAC procedures.

It is a matter of fact we are facing more and more security issues in the telecommunication arena: Intrusions by hackers, Denial of Services, Data Privacy, Financial Regulations (SOX)… Consequently, we should pay again attention to security when designing protocols to support emerging services such as Voice, Conferencing, Groupware, and Unified Messaging… One of the many possibilities is to involve security experts in the groups in charge of designing protocols. Another way is to induce a methodology for designing protocols that includes a risk analysis approach. Threats to Confidentiality, Availability, and Integrity would be evaluated depending on the context: Wireless transmission, address spoofing, message flooding… and ad hoc mechanisms would be introduced in the initial definition of the protocol. ITU and other standardizations bodies could take initiatives in this domain.