

IMPORTANCE OF CYBERSECURITY STANDARDS

INTERNATIONAL EFFORTS

- ITU-T
- 3GPP
- OTHER SDOs

X.1154

- Recently, many application services, especially financial services, require more reliable or combined authentication methods such as multifactor authentication due to the increase in identity (ID) theft. For example, one-time password authentication and other new authentication methods are used instead of traditional password-based authentication.

The combinations of authentication methods provide multiple identity service providers (IdSPs) the ability to enhance the assurance of authentication. Recommendation ITU-T X.1154 provides the general framework of combined authentication in multiple IdSP environments for a service provider. In this Recommendation, three types of combined authentication methods are considered: multifactor authentication, multi-method authentication and multiple authentications.

X.1208

- Recommendation ITU-T X.1208 describes a methodology for organizations to use cybersecurity indicators when computing a risk measure and it provides a list of potential cybersecurity indicators.
- Recommendation ITU-T X.1208 is intended to help organizations that implement or operate a portion of the global infrastructure of information and communication technologies to evaluate their own cybersecurity capability and risk. These guidelines are intended to facilitate the decision-making process within organizations on how to lower their risks and how to identify where they could/should invest resources to improve their cybersecurity capabilities.

X.1210

- **Overview of source-based security troubleshooting mechanisms for Internet protocol-based networks**
- Source-based troubleshooting security issues in Internet protocol-based networks involve techniques used to discover technical information concerning the ingress points, paths, partial paths or sources of a packet or packets causing a problematic network event, generally for the purposes of applying mitigation measures.
- Recommendation ITU-T X.1210 provides source-based security troubleshooting mechanisms for security issues, as well as selection criteria and basic security guidelines of troubleshooting mechanisms.

X.1544

- Recommendation ITU-T X.1544 is an XML/XSD-based specification for the identification, description, and enumeration of attack patterns. Attack patterns are a powerful mechanism to capture and communicate the attacker's perspective. They are descriptions of common methods for exploiting software. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples. The objective of the common attack pattern enumeration and classification (CAPEC) is to provide a publicly available catalogue of attack patterns along with a comprehensive schema and classification taxonomy.

X.1546

- Recommendation ITU-T X.1546 on the use of malware attribute enumeration and characteristics (MAEC) is an international, information security, community standard to promote open and publicly available security content about malware and malware behaviors. This Recommendation also aims to standardize the transfer of this information across the entire spectrum of security tools and services that can be used to monitor and manage defences against malware. MAEC is a language used to encode malware relevant details.
- MAEC, through its uniform encoding of malware attributes, provides a standardized format for the incorporation of actionable information regarding malware in these processes.

X.1582

- **Summary**
- Recommendation ITU-T X.1582 provides an overview of transport protocols that have been adopted and adapted for use within the Cybersecurity Information Exchange (CYBEX). The Recommendation outlines applications of transport, transport protocol characteristics, as well as security considerations.
-

X.1601

- Recommendation ITU-T X.1601 describes the security framework for cloud computing. The Recommendation analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for cloud computing. Appendix I provides a mapping table on how a particular security threat or challenge is addressed by one or more corresponding security capabilities.

Y1271

- **Summary**
- Many challenges and considerations need to be addressed in defining and establishing the functional capabilities to support emergency telecommunications in evolving circuit- and packet-switched telecommunications networks. This Recommendation presents an overview of the basic requirements, features, and concepts for emergency telecommunications that evolving networks are capable of providing.

Y.2705

- Emergency telecommunications service (ETS) is a national service, providing priority communications services to ETS authorized users in times of disaster and emergencies. Recommendation ITU-T Y.2705 provides minimum security requirements for the inter-network interconnection of ETS. This will allow ETS to be supported with the necessary security protection between different national networks with bilateral and/or multilateral agreements in times of disaster and emergencies.

Y.2771

The scope of this Recommendation includes:

- basic architectural principles that will be encountered in combining DPI in various network architectures;
- protocol architectural aspects from the perspective of DPI;
- example functional models and their application to DPI use case scenarios; and
- performance frameworks in order to assist in DPI performance discussions like the identification of key performance indicators related to DPI.

ITU WORKSHOP

- **ITU Workshop on ICT Security
Standardization Challenges for Developing
Countries - Geneva, Switzerland, 15 – 16
September 2014**

3GPP : Security Assurance Methodology (SECAM)

- 3GPP Security Assurance Methodology (SECAM) aims at providing common and testable baseline security properties for the different network product classes.
- Benefits of this work are twofold:
 - Better assurance regarding 3GPP nodes security level and robustness thanks to clear and testable requirements, whose detailed results are provided to the operators;
 - Providing for the easier management of operators security needs, with a common reference model being agreed.

3GPP contd

- [TR 33.805](#) studies the suitability of different industry methodologies that achieve these goals, with the chosen methodology integrating Common Criteria concepts where efficient – and providing the necessary adaptation to 3GPP context where necessary - allowing for accredited self-evaluation with a single assurance level and security baseline per network class.

3GPP contd

Major areas covered by TR 33.805 are:

- Agreement on the relevant threat model and needed assurance level
- Definition of the process to build the SeCurity Assurance Specifications (SCAS), which is the document containing the security requirements for a network product class and the associated test cases
- Description of the roles and process needed for security assurance/evaluation/accreditation

References

- ITU-T website
- 3GPP website