

Supplement

ITU-T G Suppl. 81 (07/2024)

SERIES G: Transmission systems and media, digital systems and networks

Supplements to ITU-T G-series Recommendations

Practical aspects of PON security

ITU-T G-SERIES RECOMMENDATIONS
Transmission systems and media, digital systems and networks

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100-G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200-G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300-G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400-G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450-G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600-G.699
DIGITAL TERMINAL EQUIPMENTS	G.700-G.799
DIGITAL NETWORKS	G.800-G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900-G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000-G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000-G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000-G.7999
PACKET OVER TRANSPORT ASPECTS	G.8000-G.8999
ACCESS NETWORKS	G.9000-G.9999

For further details, please refer to the list of ITU-T Recommendations.

Supplement 81 to ITU-T G-series Recommendation

Practical aspects of PON security

Summary

Supplement 81 to the ITU-T G-series Recommendations gives an overview of passive optical network (PON) security, collects the use cases on PON security with associated expectations, and reviews security aspects and methods applicable to PON systems, including a general PON threat model, unicast data encryption key exchange, duplicate-ONU-SN, security enhancement Recommendations in OMCI-based authentication, which may be considered in future PON Recommendations to support security enhancement features.

History*

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T G Suppl. 81	2024-07-12	15	11.1002/1000/16157

Keywords

Authentication, eavesdropping, encryption, impersonation, intrusion, PON, security.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the standards development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2024

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
4 Abbreviations and acronyms	1
5 Introduction: PON security in perspective	2
6 Use cases and expectations.....	3
6.1 Use case 1: Transmission security in industrial PON	3
7 Review of security technologies for PON technologies.....	5
7.1 General PON threat model	5
7.2 Unicast data encryption key exchange	8
7.3 Duplicate-ONU-SN	14
7.4 Security enhancement Recommendations in OMCI-based authentication	17

Supplement 81 to ITU-T G-series Recommendation

Practical aspects of PON security

1 Scope

This supplement addresses the system invariant aspects of the threat model in passive optical networks (PONs), the operator expectations about the security of the PON-based optical access networks, the method of how to utilize the techniques and features within the scope of the existing system specifications to achieve the best possible security performance, and feasible innovative technical extensions/mechanisms which may be considered in future PON recommendations to support security enhancement features.

2 References

- [ITU-T G.987.3] Recommendation ITU-T G.987.3 (2014), *10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) layer specification*.
- [ITU-T G.989.3] Recommendation ITU-T G.989.3 (2021), *40-Gigabit-capable passive optical networks (NG PON2): Transmission convergence (TC) layer specification*.
- [ITU-T G.9804.2] Recommendation ITU-T G.9804.2 (2021), *Higher speed passive optical networks: Common transmission convergence layer specification*.
- [ITU-T G.9804.3] Recommendation ITU-T G.9804.3 (2021), *50-Gigabit-capable passive optical networks (50G-PON): Physical media dependent (PMD) layer specification*.
- [ITU-T G.9807.1] Recommendation ITU-T G.9807.1 (2023), *10-Gigabit-capable symmetric passive optical network (XGS-PON)*.
- [IEEE 802.1X] IEEE 802.1X (2020), *IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control*.

3 Definitions

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
CT	Channel Termination
EK	Encryption Key
KEK	Key Encryption Key
MSK	Master Session Key
ODN	Optical Distribution Network
OLT	Optical Line Terminal
OMCI	ONU Management and Control Interface
ONU	Optical Network Unit
PFS	Perfect Forward Secrecy

PLOAM	Physical Layer Operations, Administration and Maintenance
PON	Passive Optical Network
PSK	Pre-shared Secret Key
PtMP	Point-to-Multipoint
SK	Session Key
SMA	Secure Mutual Association
SN	Serial Number

5 Introduction: PON security in perspective

In the last quarter of a century, the three-letter acronym PON has become a ubiquitous synonym of high-capacity, simple-to-operate and easy-to-maintain optical-based access network. The world's operating companies value PON systems for their *cost-efficiency*; that is, the highly favourable ratio of the overall service capacity to the capital and operational expenses. It is prudent to assume that such a ubiquitous technology would become a focus of attention for malicious players presenting a threat to the communication systems. The potential threats include:

- eavesdropping
- theft of service
- denial of service
- theft of data
- impersonation
- intrusion into operations systems
- disruption of operations.

For the expert community involved in the development of the PON system standards it is natural to focus their efforts on the PON-specific security threats and mitigation means. However, these efforts should not be restricted to the scope of a single link, which a PON system effectively represents, but must be considered within the context of end-to-end communications.

An important example of a threat which cannot be mitigated by the PON-specific means only and must be addressed in the end-to-end context is eavesdropping, or unauthorized intercept of the content of communications. While encryption provides a common and effective mitigation tool against eavesdropping, its application as a link-level method specific to a PON system should be a subject to realistic evaluation. Most mathematical results concerning the strengths of (and plausibility of attacks against) the cryptographic suites have been obtained in the context of end-to-end communications between well-behaved and cooperating parties. An all-too-popular approach extending those results to the PON-specific link-level encryption is inherently flawed. The mathematics behind the modern cryptographic suites is much stronger than the link end points or the other links in the end-to-end communication path. The weakest, most vulnerable and easiest to attack element in the end-to-end communication path is the human being at its end. In fact, regardless of how strong the link-level encryption strength is, no end-to-end data security property can be derived from it. Even the most advanced and complex PON-specific cryptographic methods cannot compensate for the security faults in the other nodes and links or for the delinquency of an end user who does not take proper care of the end-to-end data security.

The PON systems indeed exhibit highly specific properties that are potentially exploitable by adversaries and must be accounted for in a PON-specific security discussion.