IEC TR 62351-90-2

Edition 1.0 2018-09

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security –
Part 90-2: Deep packet inspection of encrypted communications

IEC TR 62351-90-2:2018-09(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC TR 62351-90-2

Edition 1.0 2018-09

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security –
Part 90-2: Deep packet inspection of encrypted communications

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.200

ISBN 978-2-8322-6038-8

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 7
2 Normative references 7
3 Terms, definitions and abbreviated terms 8
3.1 Terms and definitions 8
3.2 Abbreviated terms 8
4 Overview 8
5 Monitoring and auditing requirements 9
5.1 Use cases from utilities 9
5.2 Use cases from vendors 9
5.3 A similar use case: Encrypted SIP Calls Recording 10
6 Overview of encrypted channels in IEC 62351 10
6.1 General 10
6.2 IEC 62351-3 10
6.3 IEC TS 62351-4 10
6.4 IEC TS 62351-6 11
7 DPI for encrypted communication techniques evaluation framework 11
8 State of the art of ready techniques 12
8.1 General 12
8.2 Unencrypted TLS 12
8.3 Private key sharing 13
9 State of the art of techniques that need adaptation 14
9.1 General 14
9.2 Proxy 14
9.3 Advanced Middlebox (mcTLS) 16
9.4 Secure session-key sharing 18
9.5 Delayed secure session-key sharing 20
9.6 Application-level mirroring 21
10 Additional proposals 23
10.1 Secure private-key sharing 23
11 State of the art summary 24
12 Practical considerations for ready techniques 26
12.1 General 26
12.2 Unencrypted TLS 26
12.3 Private-key sharing 26
12.4 Recommendations to mitigate risks 26
13 Future challenges 27
Bibliography 28

Figure 1 – Unencrypted TLS sample architecture 12
Figure 2 – Private Key sharing sample architecture 13
Figure 3 – Proxy scenario sample architecture 15
Figure 4 – Advanced Middlebox sample architecture 17

Figure 5 – Secure session-key sharing sample architecture 18
Figure 6 – Delayed secure session-sharing sample architecture 20
Figure 7 – Application-level mirroring sample architecture 22

Table 1 – State of the art summary 25

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 90-2: Deep packet inspection of encrypted communications

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 62351-90-2, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this Technical Report is based on the following documents:

Enquiry draft	Report on voting
57/1939/DTR	57/2002/RVDTR

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This part of IEC 62351, which is a technical report, analyses the impact of encrypted communication channels in power systems introduced with the IEC 62351 series. As defined in IEC 62351 an encrypted channel can be employed when communicating with IEDs and encryption can be adopted at message level as well. For example, the use of encrypting TLS setups according to IEC 62351-3 introduces some difficulties when Deep Packet Inspection (DPI) is needed to inspect the communication channel for monitoring, auditing and validation needs.

In this document different techniques are analyzed that can be employed to circumvent these issues when DPI of communications is required.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 90-2: Deep packet inspection of encrypted communications

1 Scope

This part of IEC 62351, which is a technical report, addresses the need to perform Deep Packet Inspection (DPI) on communication channels secured by IEC 62351. The main focus is the illustration of the state-of-the art of DPI techniques that can be applied to the various kinds of channels, highlighting the possible security risks and implementation costs. Additional, beyond state-of-the-art proposals are also described in order to circumvent the main limits of existing solutions.

It is to be noted that some communications secured by IEC 62351 are not encrypted, but only add integrity and non-repudiation of the message – however they are mentioned here for the sake of completeness around IEC 62351 and DPI.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62351-3, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*

IEC TS 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS*

IEC TS 62351-5, *Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives*

IEC TS 62351-6, *Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850*

IEC 62351-7, *Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models*

IEC TS 62351-8, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*