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

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

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*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62351-3, IEC TS 62351-4 and IEC TS 62351-5 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.2 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

CA	Certificate Authority
DPI	Deep Packet Inspection
GDOI	Group Domain of Interpretation
IED	Intelligent Electronic Device
LDAP	Lightweight Directory Access Protocol
TLS	Transport Layer Security
PDU	Protocol Data Unit
PFS	Perfect Forward Secrecy
RBAC	Role Based Access Control
SCADA	Supervisory Control and Data Acquisition
SNMP	Simple Network Management Protocol

4 Overview

DPI is a form of network communication analysis applied to every single bit of information exchanged by nodes over the network. It is used for protocol validation, live virus checking, and in general for intrusion detection or intrusion prevention purposes. DPI enables advanced network monitoring and management but at the same time can enable for malicious intentions as well (e.g. eavesdropping).

Plaintext communications between nodes can be easily examined with DPI tools over their route. Encrypted channels on the other hand require additional steps to enable DPI, for instance:

a) the sharing of the encryption key with the system performing DPI or

b) letting the communication flow into the DPI system be plaintext again.

Sharing some of the keying materials used for encryption with a DPI Probe will make the end to end encryption less secure, and thus when adopting one approach or another it is important to know advantages and disadvantages with respect to security impact, implementation costs and performance impact.

The driving factor behind this document is the need of a structured, standardized manner of enabling DPI with encrypted channels, to eliminate the chance that unofficial, less secure methods will be used.

5 Monitoring and auditing requirements

5.1 Use cases from utilities

Ensuring reliable 24/7 operation of power systems requires:

1) The visibility of communication details, to validate correct behavior and troubleshoot issues coming from software bugs, hardware malfunctions and/or network failures.
2) The need to continuously validate that the given security requirements are always applied and not bypassed, temporarily or permanently after the first acceptance tests of the system.

The need for deep monitoring of communication channels between IEDs and SCADA and/or between IEDs by an independent device is basically driven by the same factors behind the independent monitoring system required by IEC 62351-7. Leaving the system without an independent monitoring device would expose its state to issues caused and hidden by the system itself: these issues can be bugs, defects, software or hardware failures.

This trusted device, namely a DPI Probe, is needed to inspect the communication channels in a controlled and trusted manner.

IEC 62351-7 defines a framework for proper monitoring of IEDs by employing a specific set of status variables to be monitored through SNMP. Given the requirements detailed in this section it should be clear that the current aim of IEC 62351-7 is quite different, as it enables the provision of a synthesis of the status of IEDs and is not engineered to support the detailed analysis of network packets sent and received on IEC 62351 channels.

5.2 Use cases from vendors

Automation vendors implement and maintain the hardware and software equipment behind utilities' infrastructures. The need to monitor encrypted channels can be analyzed considering the different communications happening in the system:

1) Configuration communication between tool (client) and devices/IEDs (servers): when encrypted, a TLS communication is often used to perform these tasks. Monitoring this kind of communication can help to spot attacks trying to upload bad configuration data to the IED.
2) SV (Sample Values) going to or coming from external sources, integrity checked with IEC TS 62351-6. Monitoring this communication can spot if fake data is being injected into the network and used to alter the process.
3) User authentication at GUIs/Applications/Tools: LDAP communication protected with TLS (with Windows protocols or IEC TS 62351-8). It can be interesting to inspect these steps to detect specific attacks to the authentication system.
4) Applications/Tools Browser GUIs: HTTPS. Attacks targeting HTTP/HTTPS endpoints are worth analyzing to prevent several kinds of issues on the server side.
5) Patching: should be delivered via TLS. This is worth monitoring to help detect malicious updates being delivered to IEDs or other system components.

Even though advanced/proper application logging may be used by the vendor to detect and notify security breaches in all the communications happening above, there is still a blind spot left: improper or incomplete implementation of the system itself. Combining logging and monitoring by a trusted DPI Probe allows the improvement of detection capabilities.

5.3 A similar use case: Encrypted SIP Calls Recording

A similar use case is reported and analyzed in the report of the IETF – SIPPING Working Group 2008 [3][1]. In particular, in this scenario the communications of interest are VoIP calls using the SIP protocol.

Citing words in the IETF work, call recording is an important feature in enterprise telephony applications. Some industries such as financial traders have requirements to record all calls in which customers give trading orders. In others, calls are recorded, as the near ubiquitous announcement says, “for training and quality control purposes”. Yet in others, all calls are not recorded, and only statistical audits are done.

This scenario does not use TLS but instead a bespoke encrypted variation of the plain RTP protocol, named SRTP.

Moreover, the system uses a scheme with a master key and session keys, thus without mutual authentication.

Although the SIP use case has some technical differences with the use case analyzed in this document, it will be used throughout the document as a basis for technical solutions and known issues.

6 Overview of encrypted channels in IEC 62351

6.1 General

IEC 62351 defines encryption functionality in different parts of the standard. These are briefly depicted in this clause. Note that although IEC 62351-3 defines encryption functionality by defining specific cipher suites, it can only be used in conjunction with other parts such as 4, 5, and 6.

6.2 IEC 62351-3

IEC 62351-3 regulates the use of the TLS protocol. It narrows down the available options in TLS by predefining a certain feature set or functionality to be used. This relates to cipher suites, enabling encryption and also specific requirements to the TLS session management. It is the foundation of several specific secure protocols, such as IEC TS 62351-4, IEC TS 62351-6, and IEC 60870-5-7 and is thus the base for transport level security. Besides the narrowing of options, IEC 62351-3 also requires the referencing standard to define certain other features and setting of TLS.

6.3 IEC TS 62351-4

In IEC TS 62351-4, communication to IEDs can be secured with two main approaches:

1) T-Profile – transport level profile by means of TLS as described in IEC 62351-3. Note that IEC TS 62351-4 defines a set of cipher suites to be supported mandatorily as well as specific TLS session management settings. The negotiation of the encryption settings is part of the TLS handshake, which is done at the setup time of a TLS session or as part of the session management, when reconnecting or updating the session key. The negotiated session key is direction specific and applied on a per message base.
2) A-Profile – application profiles define different cryptographic protection on application level. Specifically, the A+-Profile and the AE+-Profile are defined. In the context of encryption, only the AE+-Profile provides the features for confidentiality protection. In the AE+-Profile the key management is included in the profile definition and is performed also

[1] Numbers in square brackets refer to the bibliography.