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 It also gives information on projects, replaced and withdrawn publications.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

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.

on application level. The negotiated key is used on a per message-level. The session key may be updated during the established session by either side. The negotiated session key is direction specific and applied on a per message base.

These two approaches can also be used jointly. Note that in IEC TS 62351-4:2008, the A-Profile did not provide encryption options.

6.4 IEC TS 62351-6

In IEC TS 62351-6 the IEC 61850 communication channels are secured with different approaches. GOOSE, GSE Management and Sampled Values channels use an authentication, integrity and confidentiality security extension with group keys distributed through GDOI. MMS communications are secured as specified in IEC TS 62351-4.

7 DPI for encrypted communication techniques evaluation framework

Existing or possibly new DPI techniques will be evaluated according to security, performance and costs criteria:

Security

- Preserves End to End confidentiality: this criterion will be Yes if the communication between devices is left “as-is”. It will be No if plaintext communication is restored at some point.
- IEC 62351 RBAC works: this criterion is a Yes/No result on whether the technique allows the RBAC functionalities to work in a transparent manner.
- Works without seeing handshake: this criterion is Yes if DPI can be performed without having captured the entire handshake of the communication. This criterion has been added because sometimes it’s interesting to start performing DPI even though the communication is already active, as re-initializing just for DPI purposes may impact the systems under observation in an undesired manner.
- Full third-party monitoring: this criterion is Yes if the technique allows to perform DPI with a completely independent Probe and does not require to modify the endpoints and require them to work properly.
- Cipher suite completeness: this criterion will be Yes if no limitation on cipher suite selection is introduced. Otherwise if only some cipher suites can be used, it will be No.
- Difficulty to inject packets: can be Same/Easier where Same means same difficulty of the case when no DPI has to be performed (e.g. the TLS using ephemeral ciphersuites, periodic renewal of session keys, etc).
- Difficulty to steal data: scale as previous point.

Performance impact

- Real time or delayed: this criterion will say if DPI is performed in real time traffic or on historical/delayed data.
- Adds constant delays to each frame: is a Yes/No criterion specifying if this technique requires some computation on the endpoints for each application frame to be sent or received.
- Requires more bandwidth: if Yes, it means that some additional packets have to be transmitted from/to the endpoints, and thus additional bandwidth will be required.
- Requires more CPU power: if Yes, it means that the endpoints will need additional CPU power to accomplish DPI-related tasks.

Cost

- Requires novel systems: Yes/No depending on whether or not all systems / protocols already exist.
- Implementation: Low/Mid/High. Low means that the design and implementation of the technique requires a reasonably low amount of time, High means that a completely new (maybe complex) system must be designed and implemented, Mid is in-between.
- Operational: Low/Mid/High – depending on the effort required to operate and maintain the system up and running.

8 State of the art of ready techniques

8.1 General

In this clause, commonly used techniques for DPI of encrypted channels are analyzed. We will also review how these techniques cope with the aforementioned criteria.

8.2 Unencrypted TLS

A very simple solution to the whole issue discussed here is to completely avoid encrypted channels using a non-encrypting TLS cipher, as shown in Figure 1.

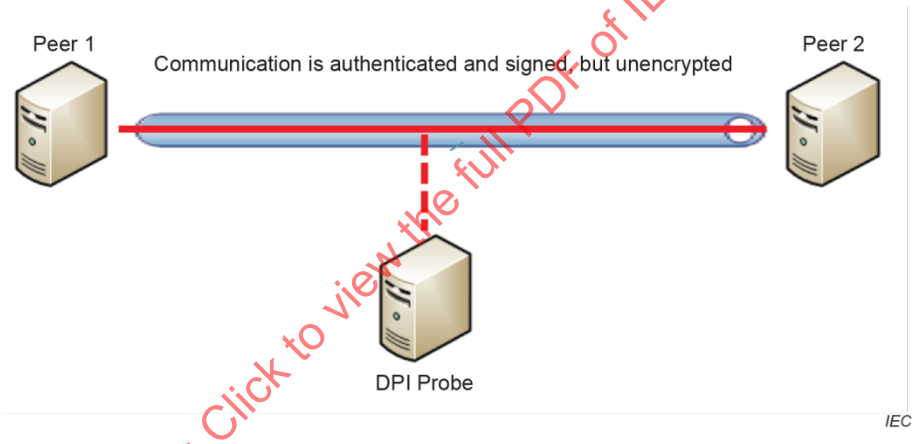

Figure 1 – Unencrypted TLS sample architecture

Adopting this approach would naturally remove end-to-end channel encryption from the system. A proper setup of IPsec (or similar protocol/technology) equipment should be added to the architecture to introduce again encryption at least on the WAN segment, even if not in an end to end manner. If IPsec is used, the DPI Probe should be located between the IPsec front-end and the peer, thus on an unencrypted communication.

Evaluation with respect to criteria of Clause 7:

Security

- Preserves End to End confidentiality: No, as it disables encryption.
- IEC 62351 RBAC works: Yes, as it is just a ciphersuite change of TLS.
- Works without seeing handshake: Yes, as it is just a matter of getting the application payload on top of TLS.
- Full third-party monitoring: Yes, as it is just a ciphersuite change of TLS.
- Cipher suite completeness: No, as it is restricted to those ciphersuites that disable encryption.

- Difficulty to inject packets: Same, as it is the same of TLS (it's not easier than other TLS ciphersuites).
- Difficulty to steal data: Easier, as frames are being exchanged in plaintext.

Performance impact

- Real time or delayed: Real time, as communications do not get changed.
- Adds constant delays to each frame: No, as nothing changes with respect to TLS.
- Requires more bandwidth: No, as nothing changes with respect to TLS.
- Requires more CPU power: No, it may even require less since no encryption is performed.

Cost

- Requires novel systems: No, as nothing changes with respect to TLS.
- Implementation: No, as nothing changes with respect to TLS.
- Operational: No, as nothing changes with respect to TLS.

8.3 Private key sharing

In this scenario, the peers' private key and the corresponding certificate is shared with an authorized third-party Probe. With the original private keys at hand, the authorized third-party Probe can intercept the handshake phase and obtain the session keys, as shown in Figure 2.

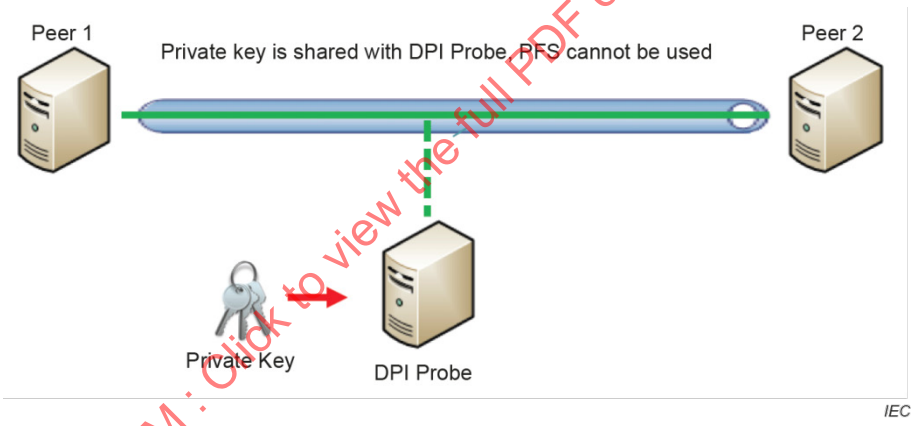

Figure 2 – Private Key sharing sample architecture

The downside of this solution is that the overall attack surface is broadened. An unauthorized access to the third-party Probe can give an attacker the complete set of private keys. Consequently, appropriate security measures should be taken when designing and deploying the third-party Probe – these devices must be protected at least up to the same level as the devices that are part of the encrypted communications.

Another issue with TLS and DPI enabled with private key sharing is that ephemeral cipher suites (e.g. the ones with Diffie-Hellman ephemeral key exchange) supporting Perfect Forward Secrecy (PFS) are not supported. The latest draft of TLS 1.3 (Rescorla 2018 [6]) will make PFS mandatory, making Private Key Sharing applicable only in those situations where TLS 1.3 is not required / applicable.

Evaluation with respect to criteria of Clause 7:

Security

- Preserves End to End confidentiality: Yes, encryption is still enabled between the two peers.

- IEC 62351 RBAC works: Yes, as it just requires particular static key exchange ciphersuites at TLS level.
- Works without seeing handshake: No, as the keying materials of the session to be decrypted with the Private Key are seen during the TLS handshake. If this phase is lost, no decryption is possible.
- Full third-party monitoring: Yes, as it is just a ciphersuite change of TLS.
- Cipher suite completeness: No, as it is restricted to those ciphersuites that exchange keys in a static way.
- Difficulty to inject packets: Easier. Since the key is shared with a Probe, there are more places where this information is stored, and getting updated. Likely, there can be more opportunities to have the private key and inject packets.
- Difficulty to steal data: Easier. Same consideration as above. Since the Private key is shared and accessible in another place, and likely being updated, once the Private key is accessed decryption will be possible.

Performance impact

- Real time or delayed: Real time, as communications do not get changed.
- Adds constant delays to each frame: No, as nothing changes with respect to TLS.
- Requires more bandwidth: No, as nothing changes with respect to TLS.
- Requires more CPU power: No, as nothing changes with respect to TLS.

Cost

- Requires novel systems: No, as nothing changes with respect to TLS.
- Implementation: Mid, as it may require putting in place some procedure/tools to have Private keys timely updated on DPI Probes when they are changed on IEDs. It can boil down to a procedure or some form of automation
- Operational: High, as requires executing the procedure or making sure that the tools defined in the implementation phase work. Also, it is wise to ensure that improper access to the DPI probe holding the Private keys is logged and periodic auditing of security breaches is necessary.

9 State of the art of techniques that need adaptation

9.1 General

In this clause, known techniques for DPI of encrypted channels that require some modification to be applied to IEC 62351 communications are analyzed.

9.2 Proxy

In this scenario the communication between peers is broken by an authorized “man in the middle”, the Proxy, as shown in Figure 3.

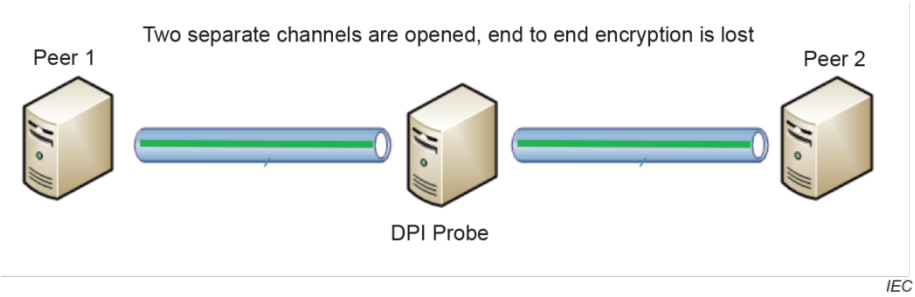

Figure 3 – Proxy scenario sample architecture

Web Proxies have proven to be valuable in the enterprise field as they allow to enforce usage policies and to block harmful content. As a result, TLS DPI is quite common in the web field.

Normally, the two peers interacting in the web are a user's browser (the client) and a web site (the server) and only the server is provided with a proper certificate that can be recognized by a CA known to the client.

In this case, during the TLS setup the client generates a part of the secret and encrypts it using the public key from the server. In this way, the secret is only shared between the client and the server that can decrypt it with its private key. This shared secret is used to generate a symmetric key, the session key, which is then used to encrypt packets inside a TLS session.

To perform DPI a Proxy must insert between the client and the server without harming the client or the server in the process. To do this, two steps must be performed:

1) the proxy establishes a point-to-point session with the client (i.e., the client starts itself the connection to the proxy) and another point-to-point session with the server. This will ensure that the TLS handshake process can be broken and the session key intercepted and stored for DPI purposes.
2) to guarantee a "safe browsing" experience, the user must be cheated in some way. Browsers are designed to prompt the user for confirmation when the server's certificate is not trusted or does not match the server address. To do this, the Proxy must contain a CA authority (trusted only inside the organization employing the Proxy). When the client attempts to connect to the target server, the Proxy will:
   a) intercept the connection attempt
   b) establish a TLS connection to the target server
   c) generate through its CA a certificate mimicking the original server's certificate
   d) present to the client the generated certificate and thus establish a TLS connection with the client

   The client will receive no alerts from its browser, because the CA of the Proxy is trusted, and the generated certificate will report the same name of the original one. The only way for the client to discover this "man in the middle" is to inspect the server's certificate, and find that the issuer is an internal CA.

However, this established technique simply does not work when mutual authentication is required because in this case the client would also sign the secret with its private key. In the Federal Public Key Infrastructure Policy Authority, 2009 [2], a good overview of SSL/TLS Proxy inspection issues with mutual authentication is given.

As a result, using a Proxy successfully within T-profile protected communication channel (by applying IEC 62351-3) would require a complete loss of mutual authentication and RBAC information between peers (as the RBAC role information is stored a certificate extension).

Another issue with the Proxy is given by its architecture:

- it is an inline device, and would become a new source of potential failures
- it would require an on-the-fly, inline decryption and encryption process that will introduce additional latency

Evaluation with respect to criteria of Clause 7:

Security

- Preserves End to End confidentiality: No. The channel is broken in two channels and is plaintext just inside the DPI Probe. So, we can say “No” with an asterisk, meaning that it is something in between.
- IEC 62351 RBAC works: No, as stated above the RBAC information stored on the certificate, does not allow making the RBAC-dependent functionalities working.
- Works without seeing handshake: No. The Proxy approach requires the DPI Probe to be in the middle of the communication and manage the handshake in a different way, to make sure the two channels are setup correctly.
- Full third-party monitoring: Yes.
- Cipher suite completeness: Yes. No special restrictions.
- Difficulty to inject packets: Easier. As one attacker may be able to get into the DPI Probe acting as proxy and eventually change/inject packets between the two channels.
- Difficulty to steal data: Easier. Since the previous statement implies read access to packets.

Performance impact

- Real time or delayed: Real time.
- Adds constant delays to each frame: Yes. As this approach requires frames to be decrypted/encrypted inside the DPI Probe.
- Requires more bandwidth: No. Frames are as big as they are without the Proxy in-line.
- Requires more CPU power: No. It does require more CPU power on the DPI Probe, but definitely not on the communicating peers.

Cost

- Requires novel systems: No. Proxies are quite available on the market – even though they would need changes to make them work with channels secured with IEC 62351.
- Implementation: High. Implementing Proxies can have an infrastructure impact as it requires the Proxy’s internal CA to be trusted by all peers, and since the Proxy is an online device special attention should be devoted to making sure that High Availability / Redundancy is considered.
- Operational: Mid. Is not Low because the infrastructure will need some maintenance and attention being an in-line device.

9.3 Advanced Middlebox (mcTLS)

Within the Proxy / Middlebox approach, as shown in Figure 4, there is an interesting proposal in literature called Multi-Context TLS (Naylor 2015 [5]).

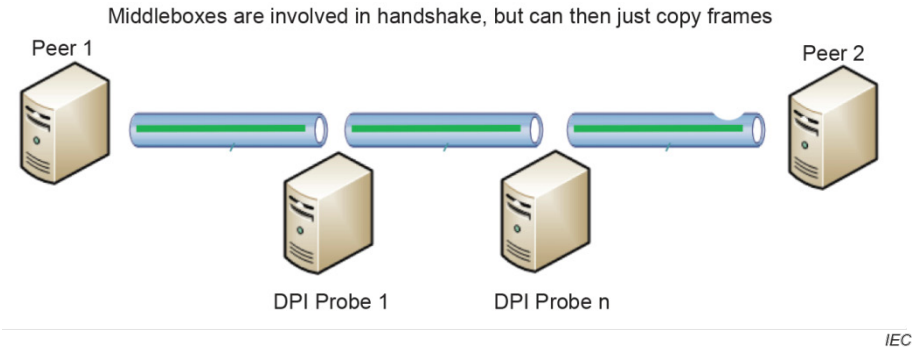

Figure 4 – Advanced Middlebox sample architecture

Multi-Context TLS (mcTLS) is a middlebox approach with the goal of a) creating different contexts inside the TLS channel, that can be encrypted/decrypted/changed by different roles/actors and b) allowing different actors to have read or read/write access to the payloads.

The foundation idea of mcTLS is to let all the middleboxes know the session encryption key, and to allow only some in write mode, by having them add an HMAC. Only the middleboxes knowing the "write" key will be able to calculate the HMAC correctly, and both the endpoints will know if an authorized write has occurred in the payload just by checking the HMACs.

An interesting achievement of mcTLS with respect to classic Proxy approaches is that after the handshake is performed, it does not require a full channel to be open from the client to the middlebox and from the middlebox to the server, but due to its design it allows a cheap frame copying approach inside the middlebox itself.

Another foundational aspect of mcTLS is that it is designed to play well in scenarios where several middleboxes can be involved in a single communication, minimizing the impact/latency of each one.

The main pain point of mcTLS is the requirement to introduce minor, but necessary changes to the frame format and to the SSL code itself, which may not be possible or cost-effective in most scenarios. A secondary limitation is given by the supported ciphersuites.

Other key limitations are the same as the Proxy approach:

- it is an inline device, and would become a new source of potential failures
- it would require an on-the-fly, inline decryption and encryption process that will introduce additional latency (this point may be close to zero since after the initial handshake frames may be just copied on the two channels).

Evaluation with respect to criteria of Clause 7:

Security

- Preserves End to End confidentiality: Yes. The channels remain encrypted from end to end.
- IEC 62351 RBAC works: Yes, as the two peers will see/know each other (and the middleboxes too).
- Works without seeing handshake: No, as the approach require the middleboxes to be involved into the handshake process.
- Full third-party monitoring: No. As it requires the peers to be involved into the middlebox operation.
- Cipher suite completeness: Yes.

- Difficulty to inject packets: Easier. Since we have one more piece of the system (the DPI Probe) that is in the channel and can change packets, an attacker has a wider attack surface to consider.
- Difficulty to steal data: Easier. Same considerations as above.

Performance impact

- Real time or delayed: Real time.
- Adds constant delays to each frame: Yes, but after handshake is performed overhead can be very little as frames can be copied in and out without being decrypted/encrypted.
- Requires more bandwidth: Yes, in the sense that additional HMACs are appended to the frames.
- Requires more CPU power: No.

Cost

- Requires novel systems: Yes. Middlebox systems and protocols still need to be developed / tested / standardized. And of course, IEC 62351 communication channels will require some modification to properly work.
- Implementation: High. Implementation costs once the solution will be available are aligned to the Proxy case.
- Operational: Mid. Operational costs once the solution will be available are aligned to the Proxy case.

9.4 Secure session-key sharing

The sharing of session-keys, as illustrated in Figure 5, has also been discussed in other application domains. One example is from the Voice-over-IP domain the option to perform call recording by sharing the session key with trusted (authorized) third parties. For this scenario solutions have been discussed (IETF – SIPPING Working Group 2008), which may be leveraged also for the power systems domain.

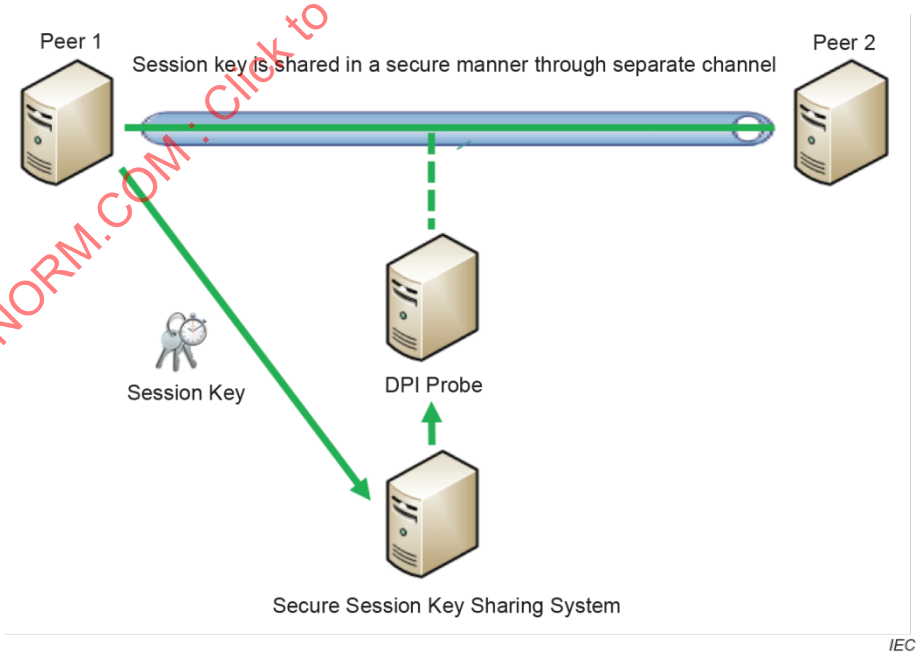

Figure 5 – Secure session-key sharing sample architecture

In that proposal, an application-specific protocol (IETF Network Working Group 2004 [4]) is employed to allow a DPI system to recover the plaintext of application payloads.

The main issue with this solution is that a malicious third party able to attack the session-sharing system and to obtain a valid session-key can be in the situation to have all data needed to forge fake packets between peers.

During the analysis of existing solutions with this approach the patent (David G. Kuehr-McLaren 2007 [1]) that specifies novel method for secure sharing of session-keys has been found. The work proposes a novel scheme for sharing session keys but assumes that other proposals already exist and thus covers a specific variation of session-keys.

This approach can be applied in a straightforward manner for IEC TS 62351-6 channels. In that case the DPI Probe can be joined as a part of the GDOI group as defined in IEC 62351-9 and thus easily handle decryption and verification of PDUs.

With IEC 62351-3 and IEC TS 62351-4 channels, the GDOI may also be adapted in the future to act as a key sharing solution for DPI Probes (in principle allowing it to "reverse" its behavior), however some modification to the standard will be required to make it work properly.

The session-key can be ideally shared by either the client or the server, that both know it. Depending on the architecture, it may be better to have it shared by either the client or the server. For instance, if the client resides in a control center, it may be wiser to have it shared on the client side.

Evaluation with respect to criteria of Clause 7:

Security

- Preserves End to End confidentiality: Yes. The channel remains encrypted end to end.
- IEC 62351 RBAC works: Yes. The peers do not need to change the handshake phase exposed with each other (one of them will need to share the session key with the DPI Probe or system devoted to keep active Session keys).
- Works without seeing handshake: Yes. If the session key is stored and shared with a Secure Session Key sharing system, the DPI Probe can then recover it later on and decrypt the traffic after the handshake phase is performed.
- Full third-party monitoring: No. The two peers need to be modified in order to share the session key with the Secure Session Key sharing system.
- Cipher suite completeness: Yes.
- Difficulty to inject packets: Easier. Because there is one more place where the session key is stored/available (or better, at least two: The Secure Session Key sharing system and the DPI Probe).
- Difficulty to steal data: Easier. See above.

Performance impact

- Real time or delayed: Real time.
- Adds constant delays to each frame: No. Nothing outside the handshake is modified with this approach.
- Requires more bandwidth: No. It does need some additional external calls during handshake, but not during application-level communication of peers.
- Requires more CPU power: No.

Cost

- Requires novel systems: Yes. It does needs development of the Secure Session Key sharing system and related protocols.

- Implementation: High. It will need to deploy one more system (the Secure Session Key sharing system) and to make sure that all peers can communicate with it.
- Operational: Mid. It will require the operation of the infrastructure above and making sure nothing breaks.

9.5 Delayed secure session-key sharing

Given the monitoring needs described in Clause 5, DPI operations can be said to be purely read-only as it is not necessary (or desirable) to modify packets. Consequently, DPI processing can be performed with some delay, as shown in Figure 6.

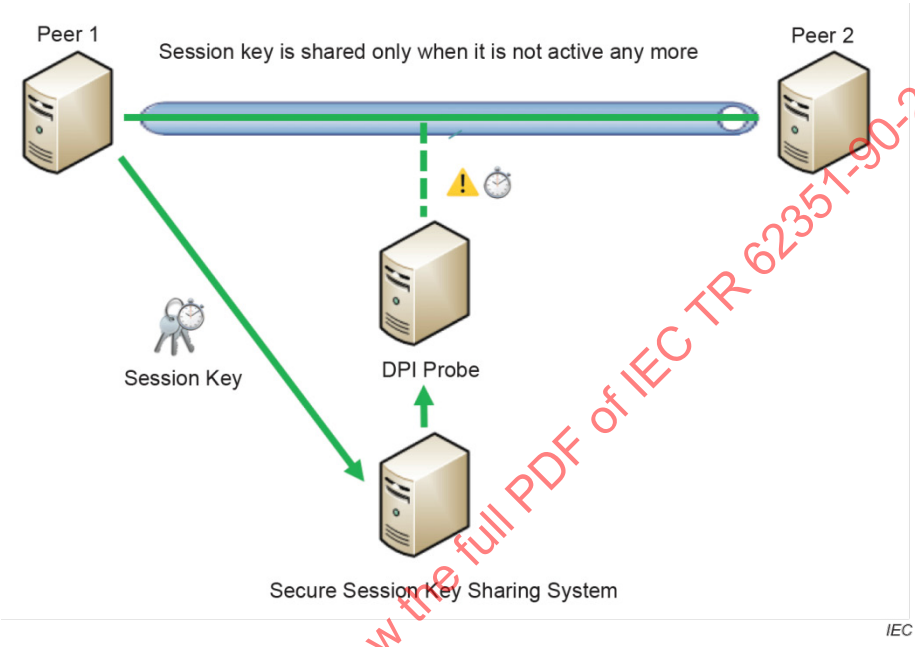

Figure 6 – Delayed secure session-sharing sample architecture

This assumption allows us to introduce a security improvement over Subclause 9.4. The basic idea is that sharing an old session-key would enable:

a) Elimination of the possibility for a malicious third party to inject valid packets in the network

b) Preservation of DPI functionalities on previously seen traffic

This approach thus would require:

1) Having a secure manner to share time-stamped session-keys by the peers to the trusted third-party Probe

2) Having the trusted DPI Probe record all the traffic, waiting for the proper session-key to be invalidated and shared

This approach has been researched and implemented and is now known as TLS-RaR (Wilson 2017 [7]). The interesting part of TLS-RaR is that it does not require changes in TLS frames.

The session-key can be ideally shared by either the client or the server, that both know it. Depending on the architecture, it may be better to have it shared by either the client or the server. For instance, if the client resides in a control center, it may be wiser to have it shared on the client side.

An Attacker gaining access to all required keying materials would however still be able to decrypt the traffic and acquire information about the system. This level of security can be

seen an intermediate between Private Key sharing and what is accomplished with Perfect Forward Secrecy (PFS).

Security

- Preserves End to End confidentiality: Yes. The channel remains encrypted end to end.
- IEC 62351 RBAC works: Yes. The peers do not need to change the handshake phase exposed with each other (one of them will need to share the session key with the DPI Probe or system devoted to keep active Session keys).
- Works without seeing handshake: Yes. If the session key is stored and shared with a Delayed Secure Session Key sharing system, the DPI Probe can then recover it later on and decrypt the traffic after the handshake phase is performed.
- Full third-party monitoring: No. The two peers need to be modified in order to share the session key with the Delayed Secure Session Key sharing system once it gets invalidated.
- Cipher suite completeness: Yes.
- Difficulty to inject packets: Same. Since Session Key is shared only when not valid, the attacker does not have more information available to perform data injection.
- Difficulty to steal data: Easier. With the Session Key available somewhere, it would not be possible to use to inject (since it is invalidated), but it would be possible to decrypt some traffic and therefore get some information.

Performance impact

- Real time or delayed: Delayed. This technique requires by design to process frames only after the related Session Key becomes invalid.
- Adds constant delays to each frame: No. Nothing outside the handshake is modified with this approach.
- Requires more bandwidth: No. It does need some additional external calls during handshake, but not during application-level communication of peers.
- Requires more CPU power: No.

Cost

- Requires novel systems: Yes. It does needs development of the Delayed Secure Session Key sharing system and related protocols.
- Implementation: High. It will need to deploy one more system (the Delayed Secure Session Key sharing system) and to make sure that all peers can communicate with it.
- Operational: Mid. It will require the operation of the infrastructure above and making sure nothing breaks.

9.6 Application-level mirroring

Another possible solution could be to introduce some form of application-level mirroring of decrypted frames through a dedicated, secure channel to be used by trusted Probes, as shown in Figure 7.

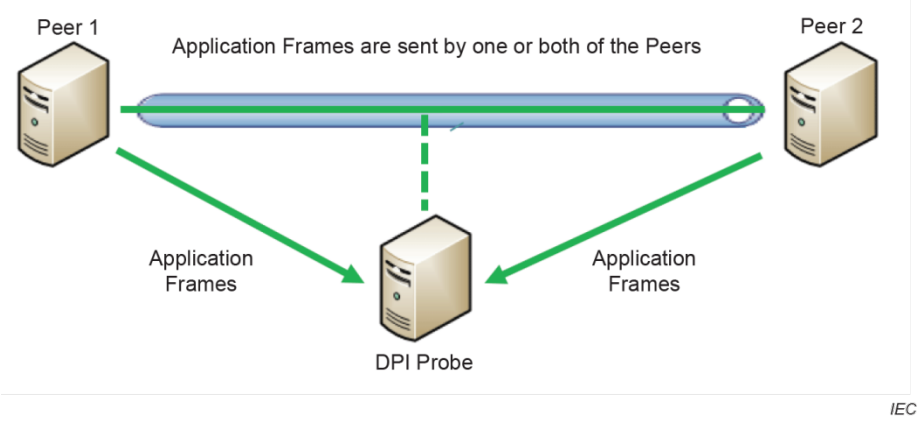

Figure 7 – Application-level mirroring sample architecture

The idea is to introduce a dedicated, secure interface inside the endpoints that are the only entities allowed to have the plaintext version of application frames.

This is similar to what is called “active recording” in (IETF – SIPPING Working Group 2008), but in this case the actor requesting and handling the mirroring/recording phase is the Probe and not the endpoint itself.

The main issue with this solution is that the capability to receive frames from the endpoint is strictly related to the endpoint itself. That is, this solution is not completely based on a trusted third party: a faulty software or hardware in the endpoint would lead to the loss of visibility on communications with that endpoint. This is a strong limitation with respect to the use cases listed in Clause 5.

Another aspect to keep in mind is that with this approach the DPI Probe should correlate in some way a) the Layer 2-3-4 network mirroring received from ordinary network mirror ports b) the Layer 7 mirroring received by endpoints. This technical issue may lead to incorrect correlations and inspections.

Evaluation with respect to criteria of Clause 7:

Security

- Preserves End to End confidentiality: Yes. The channel is kept encrypted end to end.
- IEC 62351 RBAC works: Yes. The encrypted channel is left almost unmodified and hence, no impact on this functionality.
- Works without seeing handshake: Yes. The peers are always capable of decrypting the payloads and give back to the DPI Probe.
- Full third-party monitoring: No. This approach requires an invasive change on the peers and their protocols since every frame needs to be sent back to the DPI Probe.
- Cipher suite completeness: Yes.
- Difficulty to inject packets: Same. Since the encrypted channels are unchanged, the difficulty remains unchanged.
- Difficulty to steal data: Same. Since the encrypted channels are unchanged, the difficulty remains unchanged.

Performance impact

- Real time or delayed: Real time.
- Adds constant delays to each frame: TBD.

- Requires more bandwidth: Yes. It will require a dedicated, continuous communication channel with the DPI Probe to send back the decrypted traffic.
- Requires more CPU power: Yes. Because the peers will have to do extra work for every frame (forwarding to the DPI Probe).

Cost

- Requires novel systems: Yes. It requires the development of protocols and systems to allow the decrypted payloads to be sent back to the DPI Probe.
- Implementation: High.
- Operational: Low.

10 Additional proposals

10.1 Secure private-key sharing

As described in 8.3, sharing private-keys exposes the system to a wide range of attacks where the private-keys of peers can be used to impersonate peers, inject traffic, etc.

To prevent this, a possible novel approach can be to share private-keys with a dedicated Hardware Security Module (HSM). An HSM is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing services. These modules traditionally come in the form of a plug-in card or an external device that attaches directly to a computer or network server and expose their services through an API. HSM clients can be configured to have their own security profile, allowing granular security access to digital keys, e.g. to allow encryption, decryption, sign, etc.

The HSM can then be configured to allow a trusted third-party Probe to use a given private-key just in decryption mode (to inspect the traffic), eliminating the possibility of traffic injection thanks to the HSM's functionalities.

The drawback of requiring third party access to the HSM requires the endpoints to be involved in the process (by passing through the HSM), making the inspection not completely independent / third party.

Evaluation with respect to criteria of Clause 7:

Security

- Preserves End to End confidentiality: Yes. The channel is left untouched.
- IEC 62351 RBAC works: Yes. The channel is left untouched.
- Works without seeing handshake: No. This approach still needs to have the DPI Probe to see the handshake to get the Session Key.
- Full third-party monitoring: No. It does require modification of whoever needs access to the Private Key to pass through the HSM.
- Cipher suite completeness: No. It does require ciphersuites with static key exchange and forbids, for instance, ephemeral key exchange approaches.
- Difficulty to inject packets: Same. Since the HSM allows that the Private Key is not accessed for other purposes other than decrypt, there is no more risk of packet injection.
- Difficulty to steal data: Easier. Since there is one more actor (the DPI Probe) who can decrypt payloads, we have a widened attack surface to allow more actors to read data.

Performance impact

- Real time or delayed: Real time.