

IMPACT EVALUATION OF IEC 62351 CYBER SECURITY ON IEC 61850 COMMUNICATIONS PERFORMANCE

Mauro G. TODESCHINI
RSE S.p.A. – Italy

maurogiuseppe.todeschini@rse-web.it

Giovanna DONDOSSOLA
RSE S.p.A. – Italy

giovanna.dondossola@rse-web.it

Roberta TERRUGGIA
RSE S.p.A. - Italy

roberta.terruggia@rse-web.it

ABSTRACT

Power system is not exempt from the cyber security threats that threaten almost all digitalised society sectors and activities. Consequences of cyber-attacks to power control infrastructures can be extremely significant for operators' core business, but also for most of the essential services of developed society, even potentially affecting safety of people. Fortunately countermeasures exist as there are international standard that specify which countermeasures have to be applied to raise the security level and to allow interoperability between operators', vendors', and customers' devices. Cyber security countermeasures have an impact on performance that must be evaluated early enough to assess the adequacy of a solution, or to select the most appropriate configuration among multiple alternatives. This article describes a platform developed to measure the impact of cyber security measures indicated by the TLS profiles specified by IEC 62351 standard series. The experimental platform is described and the performances of different cypher suites supported by the standard are reported for communications using a IEC 61850 protocol stack.

INTRODUCTION

The issues related to cyber security are gaining more and more attention from professionals, stakeholders and the community in general; the consequences of cyber-attacks have increasingly significant effects from an economic (e.g. disservice, loss of communication, loss of internet, power blackout) and social (e.g. block of air transportation or medical services) point of view, and their severity can be extremely significant, both in peace and in war conflict times. The effects are not limited to utilities, their workforce and their equipment, but they can affect industries, hospital, transports and individual end users.

Fortunately the countermeasures to many of the cyber security threats exist: some have already been defined within international standards, others are about to be; in some cases there are ongoing updates of outdated standards to adapt them to the evolving threat scenarios. Implementing standards requirements while satisfying the performance constraints of the specific application requires time and specific skills. The standards leave a range of possibilities to the implementer who must be able to evaluate the most appropriate solution. This is especially the case when security measures have repercussions on system performance.

Impact evaluation of cyber security measures is therefore a fundamental step in the successful solution design or

upgrade of power control applications. Cyber security operations have to be supported by specific monitoring platforms based on performance indicators [1]; hereafter a custom developed platform is described which is used to evaluate the performance of IEC 62351 configurations in specific test scenarios. The following section reports the results of two different test sessions intended to measure different performance indicators. At the end the conclusions and the expected future developments are reported.

IEC 62351 STANDARD SERIES

The International Electrotechnical Commission (IEC) Technical Committee (TC) 57 Working Group (WG) 15 has developed the IEC 62351 set of standards to provide security for power system data communications protocols, such as IEC 60870-6, IEC 61850, IEC 60870-5, and IEEE 1815 (DNP3). The availability of IEC 62351 standards has provided the ability to implement secure versions of these communications protocols in Supervisory Control and Data Acquisition (SCADA) systems. Essentially the IEC 62351 standards provide well founded specifications of how to protect the ICT assets from possible ongoing threats at different layers.

Specifically, the recently updated part 4 of IEC 62351 [2] in conjunction with part 3 [3], in addition to indicating the use of the TLS protocol to secure end-to-end communications between two connection terminals, specifies the mandatory cypher suites which shall be implemented and the recommended ones.

The goal of this work is to evaluate the impact of the different cypher suites on the performance of IEC 61850 communications. Mainly cypher suites recently added to part 4 of IEC 62351 have been considered, since those concerning backward compatibility with legacy equipment have higher chance to be outdated or underperforming. To achieve the cyber security impact evaluation goal a custom software platform has been developed.

IEC 62351 Impact Measurement Platform

The IEC 62351 Impact Measurement Platform (62351IMP) has been developed as a couple of client/server peers that exchange data through IEC 61850 Manufacturing Message Specification (MMS) protocol stack over a TLS secured channel. Moreover a set of support tools have been developed to manage the measurement phase (62351IMPGR).

In order to leverage open source software (OSS) and consolidated solutions the client (61850CLI) and server (61850SER) peers have been developed using *libiec61850* version 1.2 [4] which is a client and server library implementing the IEC 61850 MMS stack [5];

libiec61850 v1.2 is the first release that optionally supports TLS through the OSS library *mbed TLS* version 2.6.0 [6]. In addition, OSS library *zlog* [7] has been used to log relevant events to syslog/console along with accurate timing information. Finally OSS library *libconfuse* [8] has been used to ease the reconfiguration and parameters setting of a peer, to allow the execution of the different testing scenarios.

61850CLI application

61850CLI peer has been developed as a native Linux x64 application. Its main execution steps are:

- 1) Read configuration from file.
- 2) Connect to 61850SER through MMS protocol over TLS. Take a timestamp just before attempting connection (timestamp name: HT_START_TS), and another just after receiving a confirmation of successful connection (timestamp name: HT_END_TS).
- 3) Wait for MMS report and process it. Take timestamp just after receiving confirmation of receiving a new timestamp and before processing it (timestamp name: RT_END_TS).
- 4) Loop to 3)

The configuration file provides the following settings:

- a) X.509 certificates and private keys:
 - Certification Authority root certificate, for peer authentication.
 - 61850CLI private key.
 - 61850CLI certificate, to present to 61850SER.
 - 61850SER certificate, to check and allow only communications with that specific server.
- b) TLS protocol version to propose to 61850SER.
- c) Cypher suite to propose to 61850SER.

61850CLI is a console application which can be started from the shell and terminated by using operating system commands.

61850SER application

Analogously to 61850CLI, 61850SER also has been developed as a native Linux x64 application. Its main execution steps are:

- 1) Read configuration from file.
- 2) Wait for 61850CLI connections request through MMS protocol over TLS.
- 3) Update values to send in MMS report.
- 4) Send MMS report to 61850CLI through connection established at 2). Take a timestamp just before transmission start (timestamp name: RT_START_TS).
- 5) Wait 500 milliseconds (*ms*).
- 6) Loop to 3).

The configuration file provides the following settings:

- a) X.509 certificates and private keys:
 - Certification Authority root certificate, for peer authentication.
 - 61850SER private key.
 - 61850SER certificate, to present to 61850CLI.
 - 61850CLI certificate, to check and allow only communications with that

specific client.

- b) Acceptable TLS protocol version.
- c) Acceptable cypher suite.

61850SER is a console application which can be started from the shell and terminated by using Linux commands.

62351IMPGR application

IEC62351 Impact Measurement Platform ManaGeR is a shell script that manages the tests execution. Its main execution steps are:

- 1) Prepare 61850CLI configuration file.
- 2) Prepare 61850SER configuration file.
- 3) Launch 61850SER.
- 4) Wait a predefined amount of time (*200 ms*) to allow 61850SER to reach its step 2) and allow 61850CLI connections.
- 5) Launch 61850CLI.
- 6) Wait a configurable amount of time to allow enough MMS reports flow from 61850SER to 61850CLI.
- 7) Loop to 3) for a configurable number of times.
- 8) Loop to 1) until all test scenarios have been accomplished.

In particular the configurable amount of time defined at point 6) determines the number of MMS reports sent from 61850SER to 61850CLI so that transmission latency can be measured. The number of times specified at point 7) determines the number of connections established so that connection phase latency can be measured. A test scenario, as considered at point 8) is a combination of configuration parameters whose performance is intended to be measured; configuration parameters include cypher suite, TLS protocol version, keys and certificates.

Tests and performance indicators

Two test session have been conducted each intended to measure a specific performance indicator; the two performance indicators are:

- Handshake Time (HT): is the time interval (latency) that 61850CLI experiences since when it starts attempting a connection to 61850SER and when 61850CLI receives confirmation of a successful completion of the connection procedure.
- Report transmission Time (RT): is the latency between the readiness of a MMS report of 125 bytes size on 61850SER and its availability for processing on 61850CLI after transmission.

HT is therefore the time interval between HT_START_TS and HT_END_TS; it includes substeps such as TCP/IP three-way handshake and TLS handshake with TLS version negotiation, cypher suite negotiation, certificates exchange and session key generation. In order to carry out HT measurement session 62351IMPGR has been configured to establish a total of 1090 subsequent connections for each test scenario.

RT instead is the time interval between RT_START_TS and RT_END_TS. RT includes a MMS report encryption substep at the server side, a TCP/IP transmission substep, and a MMS report decryption substep at the client side.

RT measurement session has been accomplished by configuring 62351IMPGR to wait for the completion of a total of 4000 MMS report transmission for each test

scenario.

The test scenarios that have been considered are centered around a set of cypher suites that has been selected on the base of requirements and recommendations in [2]. The name of the cipher suite is constructed by sequencing the name of the key exchange algorithm, encryption algorithm and Message Authentication Code (MAC) algorithm so that the relevant components can be easily identified.

The cypher suites considered are:

- i. TLS_RSA_WITH_AES_128_CBC_SHA256
- ii. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- iii. TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- iv. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- v. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Some cypher suites specified in the standard have not been considered in test scenarios:

- TLS_DH_RSA * cypher suites are not implemented in *mbed TLS* version 2.6.0 and therefore couldn't be tested.
- To ease comparison of measurements only keys of type RSA have been generated, because of their widespread use. Cypher suites requiring other key types have not been considered for tests.

Two orthogonal factors have been considered in addition:

- Key-length: cypher suite v.) (the Roman numeral refers to the position in the previous list of cipher suites) has been tested with keys of different lengths (1024, 2048, 4096, 8192 bits) to highlight impact on performance. The choice of cypher suite v.) lies in its supposed robustness and heaviness.
- TLS version: cypher suite iii.) has been tested using different version of TLS protocol (v1.0, v1.1, v1.2) to evaluate the impact for backward compatibility applications.

The test execution environment consisted of a Linux virtual machine (VM) running on top of a Windows host inside Power Control Systems Resilience Testing lab of RSE. The VM was running both 61850CLI and 61850SER which were communicating over TCP/IP on the loopback interface.

Benefits of this environment are:

- Running both peers in the same machine limits the effects of physical data transmission across network interfaces and infrastructure. Impact of cypher suites on performances are therefore highlighted.
- Timestamps are consistent since they are measured against the same time source; there is no need for clock synchronization solutions.
- VM capabilities can be re-configured easily to the desired scenario.
- VM snapshots ease reproduction of a specific situation and configuration, and allows results repeatability.

The VM specifications were:

- Processor: Intel i7-6700 (4 cores) at 3.40Ghz.
- RAM: 8Gb.
- OS: Linux Ubuntu 64-bit (version 18.04).
- Disk: virtual disk on SSD.

HT test results

The results of the HT test are shown in Table 1. The table

shows the mean value and the standard deviation of HT measurements. The last column shows the increment (VAR.) of the mean latency compared to cypher suite iii.); TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA has been selected as a reference because it is the only belonging to compatibility mode and being supported by TLS v1.0, v1.1 and v1.2. Each cypher suite has been tested with TLS v1.2 and a key-length of 2048 bits:

- TLS v1.2 has been selected since it is the recommended version in part 3 of IEC62351 standard (IEC 62351-3:2014/AMD1:2018) which is referred by part 4 for specifications on TLS parameters. TLS v1.0 and v1.1 are allowed for backward compatibility.
- Key-length of 2048 bit is the minimum recommended in IEC 62351-3:2014/AMD1:2018, with 1024 bits keys being allowed for interoperability with legacy devices.

CYPHER S.	MEAN (ms)	ST. DEV. (ms)	VAR. (%)
i.)	21.599	3.022	-59.94%
ii.)	53.465	6.592	-0.83%
iii.)	53.913	7.746	0.00%
iv.)	305.777	14.718	467.17%
v.)	308.171	16.709	471.61%

Table 1: HT test measurements.

The measurements show that cypher suite selection has considerable impact on HT: the gap between the fastest cypher suite i.) and the slowest cypher suite v.) is about 285.877 ms which is an increase of 1326.80% . As one might expect it seems to be the key exchange algorithm that plays the fundamental role in this test with respect to encryption and Message Authentication Code (MAC) algorithms; the similar performance of cypher suite ii.) and iii.) which share the same key exchange algorithm but different encryption and MAC algorithms further support this statement.

TLS version impact on HT

Evaluation of the impact of TLS version (v1.0, v1.1, v1.2) has been carried out on cypher suite iii.) which compatible with all the three versions. Key-length used during test was 2048 bits for consistency with previous results.

The results of Table 2 show no evidence of a significant impact on performance of TLS version.

CYPHER S.	MEAN (ms)	ST. DEV. (ms)	VAR. (%)
iii.) (TLS v1.0)	54.490	6.529	1.07%
iii.) (TLS v1.1)	53.375	6.996	-1.00%
iii.) (TLS v1.2)	53.913	7.746	0.00%

Table 2: Impact of TLS version on HT; percentage increments are calculated with respect to TLS v1.2.

Key-length impact on HT

Cypher suite v.) has been tested with keys of different length to measure the impact of this parameter on performance. Cypher suite v.) has been selected for this test because of its higher system requirements and its

robustness. The tests have been performed using TLS v1.2.

The results show that key-length impact can be significant at 8192 bits, noticeable at 4096 bits, while there is virtually no difference in performance if using 2048 bits keys instead of 1024 bits.

CYPHER S.	MEAN (ms)	ST. DEV. (ms)	VAR. (%)
v.) (1024b keys)	307.476	17.287	-0.23%
v.) (2048b keys)	308.171	16.709	0.00%
v.) (4096b keys)	339.863	15.732	10.28%
v.) (8192b keys)	617.582	23.338	100.40%

Table 3: Impact of key-length on HT; percentage increments are calculated with respect to 2048 bits keys.

RT test results

The results of RT tests are shown in Table 4, Table 5 and Table 6; the three tables have great similarities with Table 1, Table 2, Table 3 respectively. The same approach has been followed in conducting and displaying measurements in terms of reference cypher suite, TLS protocol versions and key-lengths.

The measurements show little impact of cypher suites, TLS versions and key-length on RT; some explanation of this behavior could be:

- in RT measurements there should be no impact of key exchange algorithm and higher impact of encryption and MAC algorithms if compared to HT results. Encryption algorithms benefit of modern hardware acceleration which can speed up calculations significantly eventually equalizing latencies of different algorithms to some extent;
- hardware acceleration may speed up calculations so much that impact of encryption/decryption substeps latencies might be limited if compared to TCP/IP transmission substep latency of RT measurement.

CYPHER S.	MEAN (ms)	ST. DEV. (ms)	VAR. (%)
i.)	1.279	0.721	-3.47%
ii.)	1.321	0.762	-0.35%
iii.)	1.325	0.758	0.00%
iv.)	1.304	0.738	-1.57%
v.)	1.294	0.730	-2.37%

Table 4: RT test measurements.

CYPHER S.	MEAN (ms)	ST. DEV. (ms)	VAR. (%)
iii.) (TLS v1.0)	1.371	0.746	3.48%
iii.) (TLS v1.1)	1.309	0.713	-1.21%
iii.) (TLS v1.2)	1.325	0.758	0.00%

Table 5: Impact of TLS version on RT; percentage increments are calculated with respect to TLS v1.2.

CYPHER S.	MEAN (ms)	ST. DEV. (ms)	VAR. (%)
v.) (1024b keys)	1.353	0.810	4.54%
v.) (2048b keys)	1.294	0.730	0.00%
v.) (4096b keys)	1.324	0.767	2.34%
v.) (8192b keys)	1.329	0.772	2.74%

Table 6: Impact of key-length on RT; percentage increments are calculated with respect to 2048 bits keys.

CONCLUSIONS AND FUTURE WORKS

The impact of cypher suites and related parameters may be significant on the performance of IEC 61850 communications. IEC62351IMP has highlighted high impact on HT, both of key-exchange algorithms and key-lengths; the graphs in Figure 1 and Figure 2 show the distribution of the measures for the cypher suites at the extremes of the performance range. The impact on RT of encryption and MAC algorithms resulted quite limited in the test environment; Figure 3 shows the distribution of values for reference cypher suite iii.), which is analogous to the others.

From the results an implementer of a IEC 62351-compliant application could decide to:

- select a faster cypher suite, or set of cypher suite if the performance of the slower ones do not meet the requirements of the specific application;
- select a cypher suite that is slower in HT but more robust from the point of view of cyber security threats, if the application allows to establish a session in advance and keep the session active for multiple report transmission. This way the overhead of HT, which is relevant at session establishment, is mitigated by the early session establishment strategy and longer renegotiation time of the security session ;
- select the best performing processing/communication hardware if performances of some alternative is inadequate for the targeted application.

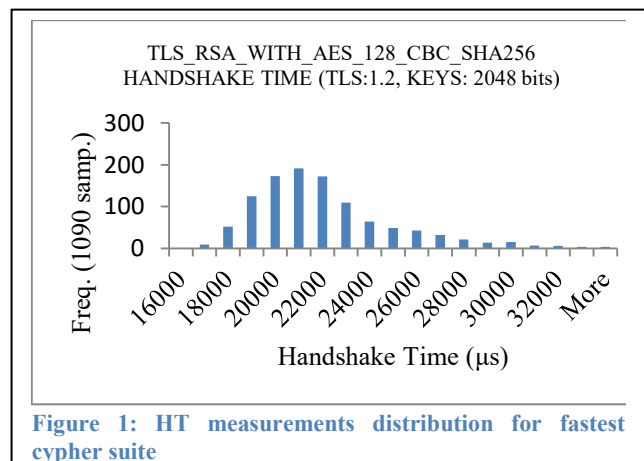
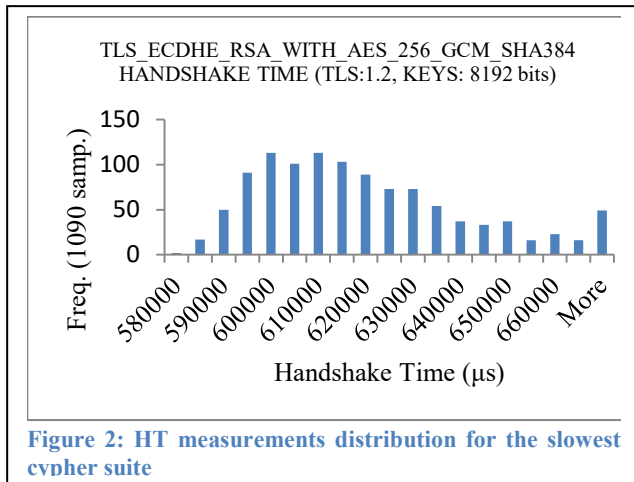


Figure 1: HT measurements distribution for fastest cypher suite

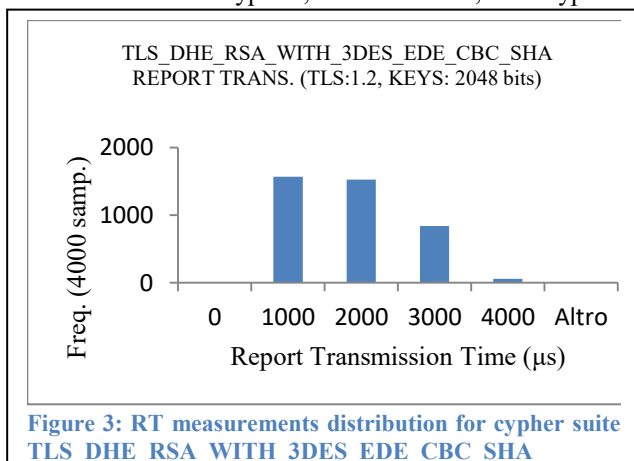


This work is not aimed at identifying the best solution for every situation (e.g. cypher suite/key-length combination) but to highlight that significant differences exist and that differences may occur in specific circumstances (e.g. session establishment) rather than others (e.g. operational data transmission). Therefore, a preliminary assessment of possible alternatives is appropriate when designing a new solution or updating an existing one, to reduce the possibility of underperforming or inadequate behavior and the consequent need of onerous corrective actions.

In the near future 62351IMP will be applied to evaluate the impact of different transmission technologies on communication performance, similarly to what has been done in [9] for 3G and 4G mobile networks.

At the moment 62351IMP has been executed on a powerful host; being able to run it on off-the-shelves operational technology solutions would give a finer evaluation tuned to the performance of field equipment. It is expected that achieved results will be still valid but absolute performance and relative percentage would likely be different due to different processor architectures (e.g. hardware acceleration, optimization) and communication interfaces.

The platform could also be extended to further detail substeps influence in a multistep communication (e.g. influence of encryption, transmission, decryption



substeps in RT measurements).

Configurable communication payload (e.g. payload length) and interaction patterns (e.g. request/reply sequences) between client and server could also be implemented to measure performance in real/complex scenarios.

ACKNOWLEDGMENT

This work has been financed by the Research Fund for the Italian Electrical System in compliance with the Decree of the Ministry of Economic Development, April 16, 2018.

REFERENCES

- [1] G. Dondossola and R. Terruggia, "A monitoring architecture for smart grid cyber security," *Cigré Science and Engineering Journal*, no. 10, 2018.
- [2] IEC IS 62351-4:2018, "POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY – Part 4: Profiles including MMS and derivatives", 2018.
- [3] IEC IS 62351-3:2018/AMD1, "POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY – Part 3: Communication network and system security – Profiles Including TCP/IP", 2018.
- [4] M. Zillgith, "libIEC61850 / lib60870-5 - open source libraries for IEC 61850 and IEC 60870-5-104," [Online]. Available: <https://libiec61850.com/libiec61850/>. [Accessed 14 01 2019].
- [5] IEC IS 61850-8-1:2011, "Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802", 2011.
- [6] ARM Limited, "mbed TLS," [Online]. Available: <https://tls.mbed.org/>. [Accessed 14 01 2019].
- [7] H. Simpson, "zlog," [Online]. Available: <https://hardysimpson.github.io/zlog/>. [Accessed 14 01 2019].
- [8] M. Hedenfalk and J. Nilsson, "libConfuse," [Online]. Available: <https://github.com/martinh/libconfuse>. [Accessed 14 01 2019].
- [9] G. Dondossola and R. Terruggia, "Mobile Secure Communications in Smart Grid Control," in *Smart Grid Inspired Future Technologies 2017, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 203*. Springer, Cham.