

### *Performance evaluation of IEC 61850 MMS messages under cybersecurity considerations*

This is the Published version of the following publication

Ustun, Taha Selim, Hussain, SM Suhail and Kalam, Akhtar (2021) Performance evaluation of IEC 61850 MMS messages under cybersecurity considerations. Energy Reports, 8 (1). pp. 1189-1199. ISSN 2352-4847

The publisher's official version can be found at https://www.sciencedirect.com/science/article/pii/S2352484721013329?via%3Dihub Note that access to this version may require subscription.

Downloaded from VU Research Repository https://vuir.vu.edu.au/45039/



Check for

Available online at www.sciencedirect.com



Energy Reports 8 (2022) 1189-1199



## 2021 8th International Conference on Power and Energy Systems Engineering (CPESE 2021), 10–12 September 2021, Fukuoka, Japan

# Performance evaluation of IEC 61850 MMS messages under cybersecurity considerations

Taha Selim Ustun<sup>a,\*</sup>, S.M. Suhail Hussain<sup>a</sup>, Akhtar Kalam<sup>b</sup>

<sup>a</sup> Fukushima Renewable Energy Institute, AIST (FREA), Koriyama, 963-0298, Japan <sup>b</sup> College of Engineering and Science, Victoria University, Australia

> Received 26 October 2021; accepted 8 November 2021 Available online 29 November 2021

#### Abstract

IEC 62351-4 standard is published to address cybersecurity vulnerabilities of IEC 61850 Manufacturing Message Specification (MMS) messages. This standard includes a set of cipher suites that are recommended for securing MMS messages. However, these are only a set of recommendations. There is no work in the literature that implements them on an IEC 61850 MMS message and reports the performances. In order to fill this importance knowledge gap, this short communication reports results of implementing cipher suites recommended by IEC 62351-4 on IEC 61850 messages. In addition to implementation details, real message exchanges are demonstrated with lab experiments. Finally, changing certificate and message sizes are reported. The results show that cipher suite selection is critical as some suites have 29.67 % smaller certificate size than others. The novelty of this short communication is showing details of IEC 62351 application and relevant changes on message sizes and structures of IEC 61850 MMS messages. There is no similar work or publication showing such procedures and results.

© 2021 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

Peer-review under responsibility of the scientific committee of the 8th International Conference on Power and Energy Systems Engineering (CPESE 2021).

Keywords: Power system communication; Smart grid; IEC 61850; MMS message; IEC 62351-4

#### 1. Introduction

Smart grid operation requires high volume of information exchanges [1]. IEC 61850 is utilized to achieve interoperability between different devices present in electrical networks [2–4]. Recent cyberattacks showed that power systems are vulnerable to data manipulation attacks [5,6] and IEC 61850 standard does not address cybersecurity issues [7]. IEC 62351 standard is published to mitigate cybersecurity vulnerabilities of IEC 61850 standard [8–10]. Part 6 of IEC 62351 deals with well-known Generic Object-Oriented Substation Event (GOOSE)

\* Corresponding author. *E-mail address:* selim.ustun@aist.go.jp (T.S. Ustun).

https://doi.org/10.1016/j.egyr.2021.11.187

<sup>2352-4847/© 2021</sup> The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons. org/licenses/by/4.0/).

Peer-review under responsibility of the scientific committee of the 8th International Conference on Power and Energy Systems Engineering (CPESE 2021).

and Sampled Value (SV) messages [11]. Also, recent literature is rich with works that investigate cybersecurity of GOOSE and SV messages [12–17].

On the other hand, security of IEC 61850 Manufacturing Message Specification (MMS) messages is not investigated in detail. Part 4 of IEC 62351 recommends use of certain cipher suites during Transport Layer Security (TLS) session [8]. There are limited number of studies where authentication mechanisms regarding MMS message security are discussed [18,19]. A recent work has investigated implementation of IEC 62351-4 on IEC 61850 MMS messages and studied its performance [20]. However, in this paper, only one cipher suite has been implemented. The other recommended suites have not been implemented and investigated.

This short communication fills in this knowledge gap. Being an applied research paper, it shows how IEC 62351-4 recommended ciphers are implemented on IEC 61850 MMS messages. Lab experiments are run to capture real message exchanges to show-case IEC 61850 MMS messages and related TLS session details. Furthermore, certificate and message sizes for all cipher suites are reported. This is the contribution of this work to the body of knowledge as it has not been done before. The rest of this short communication is organized as follows: Section 2 gives a very brief overview of IEC 61850 MMS messages and recommendations of IEC 62351-4 to secure them. Section 3 implementation details and test results for different cipher suites. Finally, Section 4 draws the conclusions.

#### 2. Overview of IEC 61850 and IEC 62351-4

IEC 62351-4 stipulates securing MMS messages at two profiles of protocol stack: application and transport. As shown in Fig. 1, the former consists of the top 3 layers of the stack while the latter is made up of bottom 4 layers.

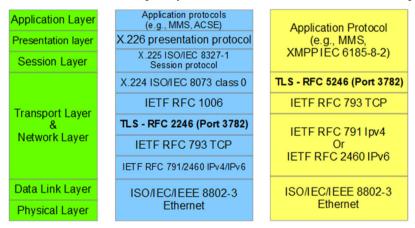


Fig. 1. Protocol stack for compatible and native T-security specifications for MMS messages [9].

For transport security (T-Security), use of TLS 1.2 is stipulated by RFC 5246. MMS messages are exchanged through port 3782 in two steps. Firstly, a handshake is performed to verify certificates of both parties and exchange a session key. With this key cipher suite that is going to be used for the actual data exchange is negotiated. Depicted in Fig. 2, this process is only performed once to establish the TLS session. Here, client and server exchange hello messages which is followed by exchange of individual certificates. This is performed to authenticate the parties, i.e. making sure they are who they claim to be. After this initial key is exchange which is, then, utilized to decide on the cipher suite that will be used for the rest of the session. Cipher suite means a set of cryptographic algorithms for all of (i) keys, (ii) digital signature, (iii) encryption and (iv) message authentication.

The list of recommended suites and their individual components are given in Table 1. For instance, initial key exchange process can be done with a selection of algorithms such as RSA, DH, DHE or ECDHE. On the other hand, digital signatures are only validated with RSA or ECDSA algorithms. Two versions of Secure Hash Algorithm (SHA 256-384) is utilized to generate a hash value which can be later used to authenticate the message contents. The message is encrypted with Advanced Encryption Standard's 128 or 256 (AES 128-256) version. In this fashion, TLS mechanism provides security for all four aspects mentioned above.

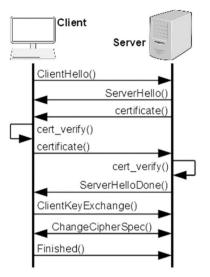


Fig. 2. Message exchanges for TLS establishment [20].

Table 1. IEC 62351-4 recommended cipher suites for MMS messages.

Key exchange	nge Hash function		Encryption algorithm	TLS version	
Algorithm	Signature				
TLS RSA	_	SHA256	WITH AES 128 CBC	TLS 1.2	
TLS DH	RSA	SHA256	WITH AES 128 CBC	TLS 1.2	
TLS DH	RSA	SHA256	WITH AES 128 GCM	TLS 1.2	
TLS DHE	RSA	SHA256	WITH AES 128 GCM	TLS 1.2	
TLS DH	RSA	SHA384	WITH AES 256 GCM	TLS 1.2	
TLS ECDHE	RSA	SHA256	WITH AES 128 GCM	TLS 1.2	
TLS ECDHE	RSA	SHA384	WITH AES 256 GCM	TLS 1.2	
TLS ECDHE	ECDSA	SHA256	WITH AES 128 GCM	TLS 1.2	
TLS ECDHE	ECDSA	SHA384	WITH AES 256 GCM	TLS 1.2	

#### 3. Implementation details and test results

In order to run lab tests, the procedure explained in [20] is followed. Two terminals emulating IEC 61850 client and server nodes are connected over TLS 1.2 protocol. The IEC 61850 client and server are emulated with the help of IEC 61850 emulation software. The corresponding system configuration description (SCD) file describing the capabilities of IEC 61850 client and server is generated and loaded to the IEC 61850 emulation software on two terminals to emulate IEC 61850 client and server.

The first step to exchange secure MMS messages is to establish a TLS connection between IEC 61850 client and server. To implement TLS in emulated IEC 61850 client and server, security module is configured with the security profile. The first step for configuring security profile is to setup certificates for client and server. Upon receiving the certificate request in X.509 format from the IEC 61850 client or server, CA signs the request using any of the public key algorithms such as RSA or ECDSA. In this implementation, three signed certificates 'ENT-PC.pem', 'dhcert.pem' and 'ecdhcert.pem' for IEC 61850 server and 'beast-X99-s01.pem' for IEC 61850 client are generated by trusted certificate authority (CA). 'ENT-PC.pem' is utilized when using the TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 cipher suite. For the other cipher suites TLS\_DH\_XXX\_XXX and TLS\_ECDHE\_XXX\_XXX the certificates 'dhcert.pem' and 'ecdhcert.pem' certificates are utilized, respectively. Fig. 3(a) depicts the encoded signed certificate 'ENT-PC.pem' and Fig. 3(b) shows details of 'ENT-PC.pem' generated by CA. It can be noticed that the certificate follows X.509 format and the algorithm used for generating signature is SHA256 with RSA.

BEGIN CERTIFICATE	
MIIDgzCCAmugAwIBAgIJAK1cN6AYqYgcMA0GCSqGSIb3DQEBCwUAMEUxCzAJBgNV	
BAYTALVTMQ4wDAYDVQQKDAVYZWxhczEVMBMGA1UECwwMWGVsYXNfRW51cmd5MQ8w	
DQYDVQQDDAZFT1RBQzEwHhcNMjAwNjIyMDUxMjMxWhcNMjMwNjIyMDUxMjMxWjBF	
MQswCQYDVQQGEwJVUzEOMAwGA1UECgwFWGVsYXMxFTATBgNVBAsMDFh1bGFzX0Vu	
ZXJneTEPMA0GA1UEAwwGRU5UQUMxMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB	
CgKCAQEAyP3YDAbV1b4ycdUeHBHPxeqBFnBzfJwdbSr94zLWvNmClanwtQnqs5I9	
EhJoDqcOt5FGBQoukxZH2NhisX5ujMrLvvi4PyUTLI0hyMaQgsXxoiJxb/m9wmpP	
zBKkdB517tk78A1TQPJNWLy1aO1bY058gYU6nP5Vtrmh5e13h8+3o3p2wD319Ufk	
05vVKMgR8NXm7Fa88PRwOXKHxtTsL0nPIkACYXMNZ+37MXS1+BTYPrf4Vzy9JTmX	
Hdp39c64fek0QjR14ZwcQgficTDKI51uVSHXxhStSVt3KTq1X1YDVIjodoBuKT43	
5Yrqnen6UVKzP2v7HV1Z9YUAtQC48wIDAQABo3YwdDARBglghkgBhvhCAQEEBAMC	
BkAwDwYDVR0TBAgwBgEB/wIBADALBgNVHQ8EBAMCAgQwEwYDVR01BAwwCgYIKwYB	
BQUHAwEwLAYJYIZIAYb4QgENBB8WHXhlbGFzIHNlbGYtc2lnbmVkIGNlcnRpZmlj	
YXR1MA0GCSqGSIb3DQEBCwUAA4IBAQCR7yBIC3+jn6dryHocz/hehIoNwa8aCewB	
9SSsdSmxVswwjg/hWLCv/BlSR5VrRDieIn1uMRQKwRAoJEeXH6v+D9varu12z2Zg	
Ra/DohEeKLBHj4//bpwmXc3dCLitrclcpTxFl0KWsYq4hr3sJTfde1zPuWSWX7YC	
z2P9e4aYnkB6cD8BGAED8+pIt4VHn7sT73j/IeGZkwwH3jb9zBmAunszq6Bn446D	
iJYZ4s37r6QTd55WF8/+u6M43s8Q5BSHmo5siafNKNiIxvvOFedkR445ti+SAp83	
3XledtMtMJeFvyImohsIH2kN5mXCIDooPyIoBSa3Y4M77m7ZNXjI	
END CERTIFICATE	

```
Certificate
  Data:
     Version: 3 (0x2)
     Serial Number
        d9 12 7d 13 c4 cd 16 87
  Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, 0=Xelas, OU=Xelas_Energy, CN=ENT-PC
     Validity
     Validity
Not Before: Aug 7 01:49:26 2019 GMT
Not After : Aug 6 01:49:26 2022 GMT
Subject: C=US, O=Xelas, OU=Xelas_Energy, CN=ENT-PC
     Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
           Public-Key: (2048 bit)
           Modulus
              00:b0:8e:5a:f5:39:d5:b5:27:1d:f5:ca:61:f9:c9:
              50:eb:46:4f:c9:83:b4:29:ab:78:34:33:da:c9:9b:
5e:6a:4c:98:d0:4c:b7:a6:f6:28:f1:12:c3:61:66:
              bc:82:85:8f7e:29:a2:b8:2e:66:df 12:a7:8b:e7
              52:09:10:6c:ca:bd:91:fc:29:79:30:68:7f:33:2c
              ca:aa:3b:0b:2b:46:86:10:68:0c:12:12:25:35:73:
             fe:10:fc:bc:99:55:72:81:f7:55:02:30:b7:e9:f5
             ab:2e:7a:ea:f9:ae:aa:10:98:e1:01:51:60:9c:cc
f5:25:3a:64:af:0a:69:96:c8:52:95:57:8b:bd:7f:
              d614.dd 68.1e.c5.45.87.38.ce.18.b6.b4.42.b3
              39:be:45:bd:4b:00:92:da:14:03:46:f5:18:79:5d
              ad:ed:38:fe:e9:27:ca:6a:a3:da:3c:b3:68:85:8d
              e77d:da:4c:e4:ab78:a9:44.0b;da:f6:25:e7:1a:
a6:a3:3d:06:5c:2f:80:ce:35:22:bc:c0:a1:13:fe:
e7:b5:0f:1b:2c:97:ed:6c:af:b7:8b:5f:9c:b3:8b;
              46:b1:61:0c:73:d7:f0:60:00:47:d9:55:1c:d4:db
              30:5a:4b:d6:d3:f7:2e:2b:48:e8:e0:41:89:2d:c3
              3fc1
     Exponent: 65537 (0x10001)
X509v3 extensions:
        Netscape Cert Type
           SSL Serve
        X509v3 Basic Constraints
     CA:TRUE, pathlen:0
X509v3 Key Usage:
        Certificate Sign
     X509v3 Extended Key Usage
         TLS Web Server Authentication
     Netscape Comment
xelas self-signed certificate
Signature Algorithm: sha256WithRSAEncryption
    76:97:ab:14:d8:fb:08:70:e4:ba:4b:65:84:28:84:d3:c1:eb
   07:10:09:20:8a95:10:11:56:11:671:32:04:81:36:11:68
bb:5a:37:7b:01:80:b1:58:72:16:71:39:d3:6d:42:c7:16:08
    49:38:86:f3:d3:30:67:80:69:d0:a5:e0:3f:68:b5:fb:6c:48:
    ae:0d:bd:56:c7:6a:1a:ef:26:e8:05:3e:65:fd:68:ee:dc:e2
1c:54:f5:f0:cd:93:44:24:97:08:08:e9:d4:31:7d:92:28:5f.
    24:b9:6b:9e:55:d9:65:3e:dc:bb:d5:a0:ac:5b:47:5c:62:4c
    74:47:91:46:65:5a:cd:27:08:88:87:59:12:a8:30:e8:8b:67
    9b;ff:9d;79;a6;1d;6c;3a;47;f8;a3;af;45;4f;0f;2a;9e;f0
    22:15:1f.c3:e3:55:02:5c:da:cb:cc:52:cf.76:95:e5:06:cc
e3:54:83:55:89:64:e5:be:41:a5:af.2a.fc:75:1f.ba:c4:c0
   f3:fe:ec:c2:7e:87:83:3d:b3:6b:32:0f:a6:b5:34:7a:15:3d
                                      (b)
```

Fig. 3. Certificate of IEC 61850 server in X.509 format (a) encoded and (b) decoded.

These generated certificates are configured in emulated IEC 61850 client and server using the security module. Fig. 4(a) and (b) shows the configuration process of certificates in emulated IEC 61850 client and server respectively. Once the certificates are configured in emulated IEC 61850 client and server, a TLS connection can be established. Initially, client hello and server hello messages along with certificates are exchanged. Both the client and server verify the respective certificates. If the certificates verification process fails, the TLS connection is aborted.

However, this time, instead of a single cipher suite, all IEC 62351-4 recommended suites are implemented and validated. Same MMS message is relayed from server to the client and the messages are captured as shown in Figs. 5–14.

As shown, Fig. 5 shows a plain MMS message without any security features. For this reason, the network analyzer detects protocol as "MMS", parses the message and shows its contents as "initiate request". Also, from Fig. 5 it is noticed that the destination port for MMS message is the default '102'. For all the other captures. Figs. 6–14, protocol is shown as TLS1.2 proving that client and server are connected via secure transport layer as stipulated by IEC 62351-4. Furthermore, from Figs. 6–14 it can be noticed that the destination port for all the secure MMS messages is 3782 as specified by the IEC 62351-4 standards. Also, additional TLS establishment messages discussed in Fig. 2 are shown: Client Hello, Server Hello-Certificate, Client Key Exchange and Change Cipher Specs. The message captures are selected to show which cipher suites are utilized during TLS establishment, e.g. in Fig. 9 below cipher suite is used: TLS\_DH\_RSA\_WITH\_AES\_128\_CBC\_SHA256.

20	Certificates	🗏 Local Server	📃 Desti	nations 🛛 🖳 G	DOSE/SV	Deployment	Configuration	🔋 🗏 Help	
Name	e:				Bigvaio				
Sour	ce Port:				3783				
Clien	t Certificate:								-
Dest	ination IP:				192.168.0.4	4			
Dest	ination Port:				3782				
Serve	er Certificate	:			ENT-PC.pem				
	Id	Name Lo	cal TCP Port	Client Certificate	Remote	IP Remote TLS P	ort Server Certific	Active	
1	Bi	gvaio 378	3		192.168.0.4	4 3782	ENT-PC.pem	true	

**(a)** 

0 🖳	ertificate	es 🛛 😐 Local	Server 🛛 🖳 D	estinations	GOOSE/SV	🖳 Deployme	nt 🛛 🗏 Config	uration			
Name:					TestServer						
Source	Port:				3783						
Client (	Certificat	ie:						•			
Destina	ation IP:				192.168.0.7						
Destina	ation Por	t:			3782						
Server	Certifica	ate:			beast-X99-S01.pem						
	ld	Name	Local TCP Port	Client Certific	Remote IP	Remote TLS	Server Certific	Active			
1		TestServerWin	3784		192.168.0.5	3782	LAPTOP-RS7	true			
2		TestServer	3783		192.168.0.7	3782	beast-X99-S0	true			
					• •						

#### **(b)**

Fig. 4. Certificate configuration in emulated IEC 61850 client and server [20].

No.		Time	Source	Destination	Protocol	Length Info	
	12	14,276452	192.168.0.14	192,168,0,15	MMS	245 initiate-RequestPDU	
		14.401857	192.168.0.15	192.168.0.14	MMS	212 initiate-ResponsePDU	
		14,410380	192.168.0.14	192.168.0.15	MMS	90 00 confirmed-Request	
		14.586913	192.168.0.15	192.168.0.14	MMS	168 00 confirmed-Response	
		14.592632	192.168.0.14	192.168.0.15	MMS	103 01 confirmed-Request	
		16.900689	192.168.0.15	192.168.0.14	MMS	572 01 confirmed-Response	
		16.904984	192.168.0.14	192.168.0.15	MMS	131 02 confirmed-RequestP	
> F	came	12: 245 byte	s on wire (1960 bi	ts), 245 bytes canture	ed (1960 bits	s) on interface \Device\NPF	{77
			•	30:80:10:da:8b), Dst:	•		
				2.168.0.14, Dst: 192.1		,	
				ort: 50118, Dst Port:		3. Ack: 23. Len: 191	
		Version: 3,		·····			
				ted Transport Protocol			
			sion Protocol				
			ntation Protocol				
			ociation Control S	ervice			
V M			octaction concroit 1	ci vice			
		tiate-Reques	+ PDU				
			alling: 65280				
			ervOutstandingCall	ing: 1			
			ervOutstandingCall				
			StructureNestingLe				
		mmsInitReque:		Vel: 10			
	*						
			ersionNumber: 1				
		Padding: 5					
			arameterCBB: f100				
		Padding: 3					
		> servicesSu	upportedCalling: e	e1c00000402000001ed18			
		30 80 11 59			·Y··0 ·····		
		e7 50 94 40			••@•••• (•••••		
		0f c3 c6 00			···f·G ·····R		
0030		00 d6 b5 00					
		13 01 00 16 00 01 c1 a0					
		04 00 00 00					
0070		01 01 06 04			··· R···· 0····0		
0080		02 01 03 06			(. "		
0090		61 62 30 60			0 [. Å		
00a0	0 28	ca 22 02 03	a2 07 06 05 29 0	1 87 67 01 a3 03 (·"	····· ·)···g·		
00b0	0 02	01 0c a6 06	06 04 29 01 87 6	7 a7 03 02 01 0c ···	····) ··g···		
00c6		33 28 31 06	02 51 01 02 01 0 01 01 82 01 01 8	3 a0 28 a8 26 80 ·3(	1. Q (·		

Fig. 5. Plain MMS message (No Security).

The very first message after this block is the actual MMS message that is sent by the server to the client. Since it is encrypted by AES128 or AES 256, network analyzer cannot parse the message or show its contents. It is only shown as applicated data, as a chunk of data.

The important finding of this work is to report changes in sizes of certificate and application data exchanges (ADE). As shown in Figs. 5–14 and summarized in Table 2, MMS messages that use different cipher suites as well

No.	Time	Source	Destination	Protocol Length Info
	15 1,938073	192,168,0,15	192,168,0,14	TLSv1.2 174 Client Hello
	16 1.940746	192.168.0.14	192.168.0.15	TLSv1.2 1076 Server Hello, Certif
	17 1.941698	192.168.0.15	192.168.0.14	TLSv1.2 412 Client Key Exchange,
	18 1.950191	192.168.0.14	192.168.0.15	TLSv1 2 145 Change Ciphon Spec
	19 1.950916	192.168.0.15	192.168.0.14	TLSv1.2 139 Application Data
	20 1.969054	192.168.0.14	192,168,0,15	TLS /1.2 139 Application Data
		1 /1000 111		
				ed (1392 bits) on interface \Device\NPF
				VAIO_10:da:8b (cc:30:80:10:da:8b)
			2.168.0.15, Dst: 192.1	
			ort: 52298, Ust Port:	3782, Seq: 1, Ack: 1, Len: 120
	Transport Layer Se			
			otocol: Client Hello	
		: Handshake (22) 1.0 (0x0301)		
	Length: 115	1.0 (0x0501)		
		otocol: Client Hell		
		Type: Client Hello	-	
	Length: 1		(1)	
		TLS 1.2 (0x0303)		
			85a07ee7c77638f1hahc4	3d4cf6194f7ce9aa593afae
		D Length: 0	0500/00/00/100004	54401019417009489558180
		ites Length: 4		
		ites (2 suites)		
			H AES 128 CBC SHA256	(0x003c)
			ENEGOTIATION INFO SCS	
		on Methods Length:		()
		on Methods (1 metho		
		s Length: 66	,	
		: server name (len=	17)	
		: session ticket (1		
	> Extension	: signature algorit	hms (len=32)	
	0 cc 30 80 10 da	8b cc 30 80 11 59		0YE- @
	0 00 50 77 2d 40		a8 00 0f c0 a8 •••	-W
001	0 00 a0 77 2d 40		15 97 89 59 18	1(IP.
001 002	0 00 0e cc 4a 0e	c6 28 4c 09 ab 5b		J. (L[P.
001 002 003	0 00 0e cc 4a 0e 0 02 01 82 00 00	c6 28 4c 09 ab 5b	01 00 00 6f 03 ····	
001 002 003	0 00 0e cc 4a 0e 0 02 01 82 00 00 0 03 05 0e f8 d0	c6 28 4c 09 ab 5b 00 16 03 01 00 73	01 00 00 6f 03 ··· 85 a0 7e e7 c7 ···	····· ··· ··· ··· ··· ··· ··· ··· ···
001 002 003 004 005 005	<ul> <li>00 0e cc 4a 0e</li> <li>02 01 82 00 00</li> <li>03 05 0e f8 d0</li> <li>76 38 f1 ba bc</li> <li>ae 00 00 04 00</li> </ul>	c6         28         4c         09         ab         5b           00         16         03         01         00         73           71         8e         08         03         a8         4a           43         d4         cf         61         94         f7           3c         00         ff         01         00         00	01 00 00 6f 03 85 a0 7e e7 c7 ce 9a a5 93 af v8 42 00 00 00 11	······································
001 002 003 004 005 006 006	00         0e         cc         4a         0e           02         01         82         00         00           03         05         0e         f8         d0           07         38         f1         ba         bc           08         00         0f         00         0e         oc	c6         28         4c         09         ab         5b           00         16         03         01         00         73           71         8e         08         03         a8         4a           43         d4         cf         61         94         f7           3c         00         ff         01         00         00           31         39         32         2e         31         36	01 00 00 6f 03 85 a0 7e e7 c7 ce 9a a5 93 af v8 42 00 00 00 11 38 2e 30 2e 31	······································
001 002 003 004 005 006 006 007	00         0e         cc         4a         0e           02         01         82         00         00           03         05         0e         f8         d0           76         38         f1         ba         bc           ae         00         00         0e         0e         d0         0e           00         00         0f         00         0e         d0         d0         d0         d0         d2         d0         d2         d0         d0         d2         d2         d0         d0         d2         d0         d2         d2	c6         28         4c         09         ab         5b           00         16         03         01         00         73           71         8e         08         03         a8         4a           43         d4         cf         61         94         f7           3c         00         ff         01         00         02         13           31         39         32         2e         31         36         00         1e	01         00         06         03           85         a0         7e         e7         cr           ce         9a         a5         93         af         v8           42         00         00         01         1         38         2e         30         2e         31           06         01         06         02         06         4/t         #         #	······································
001 002 003 004 005 006 006 007 008 009	0         00         0e         cc         4a         0e           0         02         01         82         00         00           0         03         05         0e         f8         d0           0         76         38         f1         ba         bc           ae         00         00         06         00         0c           0         00         0f         00         0c         0c           34         00         23         00         00         00         00         00         00         00         0c         00         0c	c6         28         4c         09         ab         5b           00         16         03         01         00         73           71         8e         08         03         a8         4a           43         d4         cf         61         94         f7           3c         00         ff         01         00         00           31         39         32         2e         31         36	01         00         00         6f         03           85         a0         7e         e7         c7           ce         9a         a5         93         af         v8           42         00         00         01         1            38         2e         30         2e         31            06         01         66         20         66         4 #           04         03         03         01         03	······································

Fig. 6. TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA25.

No.	Time	Source	Destination	Protocol Length Info	
	9 5.874885	192.168.0.14	192.168.0.15	TLSv1.2 174 Client Hell	0
	10 5.876818	192.168.0.15	192.168.0.14	TLSv1.2 1008 Server Hell	o. Certif
	11 5.884207	192.168.0.14	192.168.0.15	TLSv1.2 284 Client Key	-
	12 5.888730	192.168.0.15	192.168.0.14	TLSv1.2 145 Change Ciph	
	13 5.889080	192.168.0.14	192.168.0.15	TL v1.2 139 Application	
	14 5.913131	192.168.0.15	192.168.0.14	TL v1.2 139 Application	
> Fran	ne 9: 174 byte	s on wire (1392 bits	;), 174 bytes capture	d (1392 bits) on interface \De	vice\NPF_
> Ethe	ernet II, Src:	VAIO_10:da:8b (cc:3	0:80:10:da:8b), Dst:	VAI0_11:59:fd (cc:30:80:11:59	:fd)
> Inte	ernet Protocol	Version 4, Src: 192	2.168.0.14, Dst: 192.	168.0.15	
> Trar	ismission Cont	rol Protocol, Src Po	ort: 60675, Dst Port:	3782, Seq: 1, Ack: 1, Len: 120	9
Y Tran	sport Layer Se	ecurity			
× 1	LSv1.2 Record	Layer: Handshake Pr	otocol: Client Hello		
	Content Type	: Handshake (22)			
	Version: TLS	5 1.0 (0x0301)			
	Length: 115				
,	✓ Handshake Pr	otocol: Client Hell	0		
	Handshake	Type: Client Hello	(1)		
	Length: 1		(-)		
		TLS 1.2 (0x0303)			
			6af1344e920b7e0833a62	ac523dad1f2a8e9286cb0a0	
		D Length: 0			
		ites Length: 4			
		ites (2 suites)			
			WITH AES 128 CBC SHA2	56 (0x003f)	
			ENEGOTIATION INFO SCS		
		on Methods Length:		(0,0011)	
		on Methods (1 metho			
		is Length: 66	u)		
		: server name (len=	17)		
		: session ticket (1			
		: signature algorit			
	/ Excension	. signature_aigorit	niis (ien=sz)		
0000	cc 30 80 11 59	fd cc 30 80 10 da	8b 08 00 45 00 ·0	·Y··0 ·····E·	
0010	00 a0 76 c9 40	00 80 06 02 21 ce	a8 00 0e c0 a8 ···	··@···· ·!·····	
		c6 d0 2c 01 1b b7		····, ···D··P·	
		00 16 03 01 00 73		····· ·· ·· ·· ·· ·· ·· ·· ·· ·· ·· ··	
		7 3a 80 12 04 f3 3a		Y.:	
		5 2a c5 23 da d1 f2		3.*.#(1.	
		3f 00 ff 01 00 00 31 39 32 2e 31 36		···?·· B···· ··192 .168.0.1	
		31 39 32 2e 31 36 00 0d 00 20 00 1e			
	03 05 01 05 02		04 03 03 01 03		
		02 02 02 03 00 0f			
0000					

Fig. 7. TLS\_DH\_RSA\_WITH\_AES\_128\_CBC\_SHA256.

No.	Time	Source	Destination	Protocol Length	Info
	5 2.735469	192.168.0.14	192.168.0.15	TLSv1.2 174	Client Hello
	6 2.737341	192.168.0.15	192.168.0.14	TLSv1.2 1008 :	Server Hello, Certif:
	7 2,744054	192,168,0,14	192.168.0.15	TLSv1.2 244	Client Key Exchange,
	8 2.750225	192.168.0.15	192,168,0,14	TLC 0.0 000	
	9 2.750619	192.168.0.14	192.168.0.15	LSv1.2 113	Application Data
	10 2.775421	192,168,0,15	192,168,0,14		Application Data
-					
			s), 174 bytes capture		
			30:80:10:da:8b), Dst:		30:80:11:59:fd)
			2.168.0.14, Dst: 192.		
			ort: 60600, Dst Port:	3782, Seq: 1, Ack:	1, Len: 120
	ransport Layer Se				
`			rotocol: Client Hello		
		: Handshake (22)			
		1.0 (0x0301)			
	Length: 115				
	✓ Handshake Pr	otocol: Client Hell	.0		
	Handshake	Type: Client Hello	(1)		
	Length: 1	11			
	Version:	TLS 1.2 (0x0303)			
	> Random: 3	addec43ffd158ea4693	74b6d72b3711e32727a42	6f83775471ca5d2afea	6934
	Session I	D Length: 0			
	Cipher Su	ites Length: 4			
		ites (2 suites)			
	Cipher	Suite: TLS_DH_RSA_	WITH_AES_128_GCM_SHA2	56 (0x00a0)	
	Cipher	Suite: TLS_EMPTY_R	ENEGOTIATION_INFO_SCS	V (0x00ff)	
	omnressi	on Methods Length:	1		
	> Compressi	on Methods (1 metho	d)		
		s Length: 66			
	> Extension	: server_name (len=	17)		
	> Extension	: session_ticket (1	en=0)		
	> Extension	: signature_algorit	hms (len=32)		
000	cc 30 80 11 59	fd 20 - 00 10 d-	8b 08 00 45 00 ·0	··Y··0 ·····E·	
	0 00 a0 76 82 40			/@··· .h····	
		c6 5b 74 7c 6a c5		[t  j"P.	
		00 16 03 01 00 73		\	
		ff d1 58 ea 46 93		·C··X ·F·t··+7	
		26 f8 37 75 47 10		'-&-7 uGi	
		a0 00 ff 01 00 00		····B····	
		31 39 32 2e 31 36			
008		00 0d 00 20 00 1e			
009		05 03 04 01 04 02 02 02 02 03 00 0f			
00a					



No.		Time		Source			Destin	ation		Protocol	Length	Info	
	8	9.6108	99	192.1	58.0.15		192.	168.0.	L4	TLSv1.2	174	Client	Hello
	10	9.6562	58	192.1	58.0.14		192.	168.0.	15	TLSv1.2	1514	Server	Hello, Cert:
	11	9.6562	59	192.1	58.0.14		192.	168.0.	15	TLSv1.2	404	Server	Key Exchange
	13	9.7148	59	192.1	58.0.15		192.	168.0.	4	TLSv1.2	372	Client	Key Exchange
	14	9.7420	16	192.1	58.0.14		192.	168.0.	15	16391.2	105	change	cipiler sper
	15	9.7425	13	192.1	58.0.15		192.	168.0.	4	TLSv1.2	113	Applic	ation Data
													e (Device (NPF
									Dst: VAIO		sb (cc:	30:80:1	L0:da:8b)
									192.168.0				
					col, Sr	c Port:	51907	, Dst	Port: 3782	2, Seq: 1	l, Ack	1, Ler	1: 120
		ort Lay											
				-	andshak		col: C	lient	Hello				
					ake (22)	)							
				1.0 (0x	0301)								
		Length:											
	~				Client H								
		Hand	shake '	Type: C	lient He	ello (1)							
		Leng	th: 11	1									
		Vers	ion: T	LS 1.2	(0x0303)								
		> Rand	om: b8	bbbbab8	60870670	de8a106	6ce19	7f48f8	55463ad396	3321e783	90f193	36658	
		Sess	ion ID	Length	: 0								
		Ciph	er Sui	tes Len	gth: 4								
		Ƴ (iph	er Sui	tes (2	suites)								
		C	ipher S	Suite:	TLS_DHE_	RSA_WIT	H_AES	_128_G	CM_SHA256	(0x009e)			
		C	ipher S	Suite:	TLS_EMPT	Y_RENEG	OTIAT	ION_IN	FO_SCSV (0	x00ff)	- 1		
		(lomp	ression	n Motho	de Longt	by 1							
		> Comp	ressio	n Metho	ds (1 me	thod)							
		Exte	nsions	Length	: 66								
		> Exte	nsion:	server	_name (]	en=17)							
		> Exte	nsion:	sessio	n_ticket	: (len=0	))						
		> Exte	nsion:	signat	ure_algo	orithms	(len=	32)					
000	0 00	30 80	10 da	8b cc 3	0 80 11	1 59 fd	08 00	45 00	.0	0 ···Y····	E-		
001					6 00 00								
000	0 00	Øe ca	c3 0e	c6 d4 6	b ed 85	5 2e f2	4e d1	50 18		k · · . · N·	P -		
	0 02	01 82	00 00	00 16 0	3 01 00	73 01	00 00	6f 03		· · · s · · ·	o ·		
003	0 03				0 67 00					p g1			
003 004			54 63	ad 39 6	3 32 16					c 2·x9··			
003 004 005	0 <b>f</b> 4					00 42	00 00	00 11	X · · · · ·	· · · · B · ·			
003 004 005 006	0 f4	00 00		9e 00 f									
003 004 005 006 007	i0 f4 i0 58 i0 00	00 00 0f 00	00 0c	31 39 3	2 2e 31	L 36 38				2 .168.0	.1		
003 004 005 006 007 008	i0 f4 i0 58 i0 00 i0 34	00 00 0f 00 00 23	00 0c 00 00	31 39 3 00 0d 0	2 2e 31 0 20 00	L 36 38 9 1e 06	01 06	02 06	4.#		.1		
003 004 005 006 007	i0 f4 i0 58 i0 00 i0 34 i0 03	00 00 0f 00 00 23 05 01	00 0c 00 00 05 02	31 39 3 00 0d 0 05 03 0	2 2e 31	L 36 38 9 1e 06 4 02 04	01 06 03 03	02 06 01 03	4.#		.1		

Fig. 9. TLS\_DHE\_RSA\_ WITH\_AES\_128\_GCM\_SHA256.

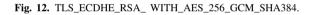
	Time	Sourc	e	Destination		Protocol	Length	Info	
	18 6,63002	192.	168.0.14	192,168,0		TLSv1.2	-	Client	Hello
	19 6.63370	4 192.	168.0.15	192.168.0	.14	TLSv1.2	1008	Server	Hello, Cert
	20 6.64035	8 192.	168.0.14	192.168.0	.15	TLSv1.2	244	Client	Key Exchang
	21 6,64499	0 192.	168.0.15	192,168,0	.14	TI Sv1 2			Cinher Sner
	22 6,64556		168.0.14	192.168.0		LSv1.2	113	Applica	ation Data
	23 6.67786		168.0.15	192.168.0		LSv1.2			ation Data
-							_		
				bits), 206 bytes					
				c:30:80:10:da:8b			d (cc:	30:80:1	1:59:fd)
				192.168.0.14, Ds					
			tocol, Src	Port: 60510, Ds	t Port: 3782,	Seq: 1	, Ack:	1, Len	152
	ransport Lay								
`	✓ TLSv1.2 Re	cord Layer:	Handshake	Protocol: Client	t Hello				
	Content	Type: Hands	shake (22)						
	Version	: TLS 1.0 (0	0x0301)						
	Length:	147							
	✓ Handsha	ke Protocol:	Client He	ello					
	Hand	shake Type:	Client Hel	lo (1)					
	Leng	th: 143							
	Vers	ion: TLS 1.2	(0x0303)						
	> Rande	om: 2f3dc86e	d85b010542	6ac53fe2ec5c0aec	2dc0579782d9	830e94a	01a810	c4485	
	Sess	ion ID Lengt	:h: 32						
				95102c9001ec1e37	Scaac60163dd	b077969	de4b28	4c0ead2	68
				95102c9001ec1e37	'5caac60163dd	b077969	de4b28	4c0ead20	68
	Sess		fe516555ad	95102c9001ec1e37	'5caac60163dd	b077969	de4b28	4c0ead20	68
	Sess: V Liph	ion ID: c62e cuites (2	fe516555ad stb: 4 suites)	95102c9001ec1e37			de4b28	4c0ead20	68
	Sess Ciph Ciph Ci	ion ID: c62e er Suites (2 ipher Suite:	fe516555ad gth: 1 suites) TLS_DH_RS		CM_SHA384 (0	x00a1)	de4b28	4c0ead20	68
	Sess Viph C: C:	ion ID: c62e er Suites (2 ipher Suite:	fe516555ad suites) TLS_DH_RS TLS_EMPTY	A_WITH_AES_256_G _RENEGOTIATION_I	CM_SHA384 (0	x00a1)	de4b28	4c0ead20	68
	Sess: Ciphe Ci Ci Ciphe Ci	ion ID: c62e er Suites (2 ipher Suite: ipher Suite:	fe516555ad suites) TLS_DH_RS TLS_EMPTY	A_WITH_AES_256_G _RENEGOTIATION_I	CM_SHA384 (0	x00a1)	de4b28	4c0ead20	68
	Sess iph C: C: C: C: C: C: C: C: C: C:	ion ID: c62e er Suites (2 ipher Suite: ipher Suite: ession met	efe516555ad soth: 4 suites) TLS_DH_RS TLS_EMPTY cods Length cods (1 met	A_WITH_AES_256_G _RENEGOTIATION_I	CM_SHA384 (0	x00a1)	de4b28	4c0ead20	68
	Sess iph C: comp C: C: C: C: C: C: C: C: C: C:	ion ID: c62e er Suites (2 ipher Suite: ipher Suite: ession met ression Meth	fe516555ad suites) TLS_DH_RS TLS_EMPTY rods Length rods (1 met th: 66	A_WITH_AES_256_6 '_RENEGOTIATION_I . 1 :hod)	CM_SHA384 (0	x00a1)	de4b28	4c0ead2(	68
	Sess iph C: C: C: C: C: C: C: C: C: C:	ion ID: c62e Pr Suites (2 ipher Suite: ipher Suite: ression met ression Meth nsions Lengt	suites) TLS_DH_RS TLS_EMPTY TLS_EMPTY TLS_EMPTY tods (1 met th: 66 er_name (1e	A_WITH_AES_256_G RENEGOTIATION_I i hod) m=17)	CM_SHA384 (0	x00a1)	de4b28	4c0ead2(	68
	Sess Ciph Ci Comp Exter > Exter > Exter	ion ID: c62e cuites (2 lpher Suite: lpher Suite: ession metr ression Metr nsion: Lengt nsion: serve nsion: sessi	fe516555ad t suites) TLS_DH_RS TLS_EMPTY rods tength rods (1 met th: 66 r_name (1e con_ticket	A_WITH_AES_256_6 _RENEGOTIATION_I  hod) :n=17) (len=0)	CM_SHA384 (0 NFO_SCSV (0x	x00a1) 00ff)		4c0ead20	68
	Sess Sess	ion ID: c62e c Suites (2 ipher Suite: ipher Suite: ression Meth ression Meth nsion: Serve nsion: serve nsion: sessi 11 59 fd cc	fe516555ad suttes) TLS_DH_RS TLS_EMPTY Hods Length Hods (1 met th: 66 rr_name (1e con_ticket 30 80 10	A_WITH_AES_256_0 _RENEGOTIATION_I         	CM_SHA384 (0 NFO_SCSV (0x 90 00.Y.0	x00a1) 00ff)	E+	4c0ead20	68
001	Sess: 	ion ID: c62e er Suites (2 ipher Suite: ession Meth ression Meth nsion: serve nsion: serve nsion: sessi 11 59 fd cc a3 40 00 80	efe516555ad reth: 4 resultes) TLS_DH_RS TLS_EMPTY rods_Length rods (1 met th: 66 er_name (le ton_ticket 30 80 10 06 03 27	A_WITH_AES_256_0 _RENEGOTIATION_I       (len=0) da 8b 08 00 45 0 c0 a8 00 0e c0 a	CM_SHA384 (0 NFO_SCSV (0x 10 - 0 - · Y - · 0 18 - · u · 0 - · · 1	x00a1) 00ff)	E+ 	4c0ead20	68
001	Sess: Sess: Siph Comp Ster Stes	ion ID: c62e er Suites (2 ipher Suite: ression Meth- ression Meth- nsion: serve nsion: sessi 11 59 fd cc a3 40 00 80 56 0e c6 7c	fe516555ad rgth: 1 : suites) TLS_DH_RS TLS_DH_RS TLS_EMPTY Rods Lengch rods (1 met h: 66 :r_name (1e con_ticket 30 & 80 10 06 & 03 27 b6 72 c3	A_WITH_AES_256_0 _RENEGOTIATION_I         	CM_SHA384 (0 NFO_SCSV (0x 00 00.4Y.0 18	x00a1) 00ff)  r.jBR#	E -	4c0ead20	68
001 002 003	Sess: Comp Comp Comp Comp Exter Exter Comp Exter Our of Fc Our of Fc Our of Fc	ion ID: c62e er Suites (2 ipher Suite: ipher Suite: ession Meth ression Meth ression Meth ression Serve nsion: serve nsion	efe516555ad roth: 4 2 suites) TLS_DH_RSS TLS_EMPTY rods tength rods (1 met th: 66 rr_name (le con_ticket 30 80 10 06 03 27 b6 72 c3 03 01 00	A_WITH_AES_256_6 _RENEGOTIATION_I :n=17) (len=0) da 8b 08 00 45 0 c0 a8 00 00 45 0 c0 a8 00 00 c0 a 6 a42 52 23 50 1	CM_SHA384 (0 NFO_SCSV (0x 00 0 · Y · 0 18 ·	x00a1) 00ff)  r.jBR#	E -	4c0ead20	68
001 002 003	Sess + iph - iph - comp - comp - xte - Exte - Exte - Exte - Exte - 00 of ec 0 00 of 95 - 00 of 97 - 0	ion ID: c62e er Suites (2 lpher Suite: ipher Suite: tession Hett ression Mett nsions Lengt rsion: serve nsion: serve nsion	fe516555ad mgth: 4 : suites) TLS_DH_RS TLS_EMPTY mods tength mods (1 met th: 66 :r.name (le con_ticket 30 80 10 06 03 27 b6 72 c3 03 01 00 01 05 42	A WITH AES 256 6 _RENEGOTIATION_I 	CM_SHA384 (0 NFO_SCSV (0x) 00 -0Y0 18	x00a1) 00ff)  r.jBR#  Bj.?.	E	4c0ead20	68
001 002 003 004 005 006	Sess + 1ph Comp > Comp Exter > Exter > Exter 0 Cc 30 80 0 0 of ec 01 00 74 0 3 2f 3d 0 85 20 c6	ion ID: c62e er Suites (2 ipher Suite: ession meth ression Meth nsions Lengt rsion: serve sion: serve sion: serve sion: serve sion 8 ession sion 8 ession si	fe516555ad suite suites) TLS_DH_RST TLS_EMPTY the formation of the formation of the formation the formation of the form	A MITH AES 256 6 RENEGOTIATION 1 - 4 in-17) (1en=0) da 8b 08 09 45 6 a8 20 60 45 6 a8 25 2 23 50 9 3 01 00 60 8 f0 6 a6 3 37 62 ec 1 9 4 a0 1 a 81 0c 2 9 4 a0 1 a 81 0c 2 9 4 a0 1 a 81 0c 2 9 4 a0 9 1 ec 1	CM_SHA384 (0 NFO_SCSV (0x 0 0	x00a1) 00ff)  r·jBR#	E	4c0ead20	68
001 002 003 004 005 006 007	<ul> <li>Sess:</li> <li>Iph</li> <li>Comp</li> <li>Comp</li> <li>Exter</li> <li>Exter</li> <li>Exter</li> <li>Cc 30 80</li> <li>00 c0 75</li> <li>00 0f ec</li> <li>01 00 74</li> <li>03 2f 3d</li> <li>0a ed 2d</li> <li>83 20 c6</li> <li>37 5c aa</li> </ul>	ion ID: c62 er Suites (2 ipher Suite: ression ret ression Net histons Lengt 11 59 fd cc a3 40 00 80 56 00 c6 7c 35 00 00 16 68 6e d8 5b c0 57 97 82 20 fe 51 65 c6 01 63 dd	fe516555ad ochi i t suites) TLS_DEL85 TLS_EMPTY doub c regen doub	A_WITH_AES_256_C 	CM_SHA384 (0 NFO_SCSV (0x 88	x00a1) 00ff) r·jBR# .Bj·?. ,	E	4c0ead20	68
001 002 003 004 005 006 007 008	Sess: Comp Comp Comp Exte: Exte: 0 Cc 30 80 0 C	ion ID: c62 provide state of the state of t	fe516555ad octive I suites) TLS_DH_RS TLS_ENPTY the feature TLS_ENPTY the feature TLS_ENPTY the feature TLS_ENPTY the feature the feature feature the feature feature the featur	A_WITH_AES_256_6 	CM_SHA384 (0 NFO_SCSV (0x 8	x00a1) 00ff) , r.jBR# , , w	E	4c0ead20	68
001 002 003 004 005 006 007	Sess Comp Comp Exte Exte Exte Exte Exte Exte Comp Exte Exte Exte Exte Exte Comp Exte	ion ID: co2 r Suites (2) ipher Suite: ression Meth sions Lengt sion: server sion: server sion	fe516555ad rothin I s suites) TLS_DH_RS TLS_DH_RS TLS_EMPTY boos clength constitutet th: 66 fr_name (leconstitutet 30 80 10 06 03 27 06 03 21 06 03 21 06 03 20 10 542 49 83 06 55 ad 95 55 ad 95 55 ad 95 55 ad 95 50 47 96 ff 01 00 32 22 81 22 28	A_WITH_AES_256_C 	CM_SHA384 (0 NFO_SCSV (0x) 00 0 Y 0 880 180 180 190 190 1000 10000 100000 100000 10000 100000 10 .	x00a1) 00ff) r·jBR# , w	E	4c0ead2i	68



No.	Time	Source	Destination	Protocol Length Info	
	5 2.812629	192.168.0.15	192.168.0.14	TLSv1.2 214 Client He	110
	6 2.822713	192.168.0.14	192.168.0.15	TLSv1.2 1422 Server He	llo, Certi
	7 2.825623	192.168.0.15	192.168.0.14	TLSv1.2 180 Client Ke	y Exchange
	8 2.828317	192.168.0.14	192.168.0.15	TI SHI 2 105 Change Ci	hee Creek
	9 2.828822	192.168.0.15	192.168.0.14	LSv1.2 113 Applicatio	on Data
	10 2.859414	192.168.0.14	192.168.0.15	LSv1.2 106 Applicatio	on Data
) E.e.	me Er 014 hute		-) 214 huter conture	d (1712 bits) on interface \[	
				VAIO 10:da:8b (cc:30:80:10:c	
					14:00)
			2.168.0.15, Dst: 192.	3782, Seq: 1, Ack: 1, Len: 1	60
			ort: 51/01, DSt Port:	5/62, Seq: 1, ACK: 1, Len: 1	100
	ansport Layer S				
*			rotocol: Client Hello		
		: Handshake (22)			
		1.0 (0x0301)			
	Length: 155				
		otocol: Client Hel			
		Type: Client Hello	o (1)		
	Length: 1				
		TLS 1.2 (0x0303)			
			28d2eddba10ba53bdf27cb	cf5e45db6e8d6cebfb29bea	
		D Length: 0			
	-	ites Length: 4			
		ites (2 suites)			
			ISA_WITH_AES_128_GCM_S		
			RENEGOTIATION_INFO_SCS	V (0x00ff)	
		on Methods Length:			
		on Methods (1 metho	od)		
		s Length: 106			
		: server_name (len:			
		: ec_point_formats	. ,		
	> Extension	: supported_groups	(len=28)		
0000	cc 30 80 10 da	8b cc 30 80 11 5	9 fd 08 00 45 00 ·0	····0 ··Y···E·	
		00 80 06 00 00 c		r.@	
0020	00 0e c9 f5 0e	c6 bf f8 3f fb 5	3 e5 80 43 50 18 ····	····· ?·S··CP·	
		00 16 03 01 00 9		( · · · · · · · · · · · · · · · · · · ·	
		a0 e9 aa c2 d5 5		····· R· ···	
		bc f5 e4 5d b6 e		·I ]	
		2f 00 ff 01 00 0		··/·· ···j····	
0070		31 39 32 2e 31 3 03 00 01 02 00 0		192 .168.0.1	
0000		00 1b 00 18 00 1			
		00 09 00 0a 00 2		·····	
5040					

Fig. 11. TLS\_ECDHE\_RSA\_ WITH\_AES\_128\_GCM\_SHA256.

No.	Time	Source	Destination	Protocol Length Info		
	10 7.210771	192.168.0.15	192.168.0.14	TLSv1.2 246 Client Hello		
	11 7.213327	192.168.0.14	192.168.0.15	TLSv1.2 204 Server Hello, Chang		
	12 7.213656	192.168.0.15	192.168.0.14	TLSv1.2 105 Change Cipher Spec,		
	13 7.217740	192.168.0.15	192.168.0.14	TLSv1 2 113 Application Data		
	15 7.234439	192.168.0.14	192.168.0.15	TLSv1.2 106 Application Data		
	16 7.236035	192.168.0.15	192.168.0.14	TLSv1.2 301 Application Data		
				d (1968 bits) on interface \Device\NP VAIO_10:da:8b (cc:30:80:10:da:8b)		
> Ir	nternet Protocol	Version 4, Src: 19	2.168.0.15, Dst: 192.1	68.0.14		
> Tr	ransmission Cont	rol Protocol, Src P	ort: 51611, Dst Port:	3782, Seq: 1, Ack: 1, Len: 192		
× т₁	ransport Layer S	ecurity				
~	TLSv1.2 Record	Layer: Handshake P	rotocol: Client Hello			
	Content Typ	e: Handshake (22)				
	Version: TL	S 1.0 (0x0301)				
	Length: 187					
	✓ Handshake P	rotocol: Client Hel	10			
	Handshak	e Type: Client Helle	0 (1)			
	Length:					
		TLS 1.2 (0x0303)				
> Random: 5289ea55eaf17bfd2d41ff1c5cedf0dd25972168fcb7b7e681d5f96c6d759079						
	> Random:	5289ea55eaf17bfd2d4	1ff1c5cedf0dd25972168fc	b7b7e681d5f96c6d759079		
			1ff1c5cedf0dd25972168f0	:b7b7e681d5f96c6d759079		
	Session	ID Length: 32				
	Session Session	ID Length: 32 ID: 7710abcca9216434		:b7b7e681d5f96c6d759079 5bd6dddb3fc5076290f44a9df6f		
	Session Session Cipher S	ID Length: 32 ID: 7710abcca9216434 wites Length: 4				
	Session : Session : Cipher S V Cipher S	ID Length: 32 ID: 7710abcca9216434 uites Length: 4 uites (2 suites)	413a24e7382e70094f5a2a6	5bd6dddb3fc5076290f44a9df6f		
	Session : Session : Cipher S Cipher S Cipher	ID Length: 32 ID: 7710abcca9216434 uites Length: 4 uites (2 suites) r Suite: TLS_ECDHE_F	413a24e7382e70094f5a2a6 RSA_WITH_AES_256_GCM_SF	5bd6dddb3fc5076290f44æ9df6f		
	Session Session Cipher S Cipher S Cipher Cipher Cipher	ID Length: 32 ID: 7710abcca9216434 uites Length: 4 uites (2 suites) r Suite: TLS_ECDHE_F r Suite: TLS_EMPTY_F	413a24e7382e70094f5a2a6 RSA_WITH_AES_256_GCM_SH RENEGOTIATION_INFO_SCSV	5bd6dddb3fc5076290f44æ9df6f		
	Session Session Cipher S Cipher S Cipher Cipher Cipher	ID Length: 32 ID: 7710abcca9216434 uites Length: 4 uites (2 suites) r Suite: TLS_ECOHE_F suite: TLS_ECOHE_F suite: TLS_EMPTY_F	413a24e7382e70094f5a2a6 RSA_WITH_AES_256_GCM_SF RENEGOTIATION_INFO_SCSV 1	5bd6dddb3fc5076290f44æ9df6f		
	Session : Session : Cipher S Cipher S Cipher Cipher Cipher Compress	ID Length: 32 ID: 7710abcca921643- uites Length: 4 uites (2 suites) r Suite: TLS_ECDHE_F r Suite: TLS_EMPTY_F ion Methods Length.	413a24e7382e70094f5a2a6 RSA_WITH_AES_256_GCM_SF RENEGOTIATION_INFO_SCSV 1	5bd6dddb3fc5076290f44æ9df6f		
	Session Session Cipher Si Cipher Cipher Cipher Compress Extension	ID Length: 32 ID: 7710abcca921643 uites Length: 4 uites (2 suites) r Suite: TLS_ECDHE_F r Suite: TLS_ECDHE_F r Suite: TLS_ECDHE_F ion Methods Length: ion Methods (1 methods ns Length: 106	413a24e7382e70094f5a2ad RSA_WITH_AES_256_GCM_SH RENEGOTIATION_INFO_SCS\ 1 od)	5bd6dddb3fc5076290f44æ9df6f		
	Session : Session : Cipher S: Cipher Cipher Compress Extension Extension	ID Length: 32 ID: 7710abcca921643- uites Length: 4 uites (2 suites) r Suite: TLS_ECDHE_F r Suite: TLS_EMPTY_F ion Methods Length.	413a24e7382e70094f5a2ad RSA_WITH_AES_256_GCM_SF RENEGOTIATION_INFO_SCSV 1 od) =17)	5bd6dddb3fc5076290f44æ9df6f IA384 (0xc030)		
	Session Session Cipher S Cipher S Cipher Cipher Compress Extensio Extensio Cc 30 80 10 d	ID Length: 32 ID: 7710abccs921643 uites Length: 4 uites (2 suites) r Suite: ILS_EMPTY_I Son Methods Length- ion Methods (1 methons Length: 106 n: server_name (1en : ec_point_formats a 8b cc 30 80 11 5	413a24e7382e70094f5a2ad RSA_WITH_AES_256_GCM_SK RENEGOTIATION_INFO_SCSV od) =17) (1en=4) 9 fd 08 00 45 00 00	5bd6dddb3fc5076290f44a9df6f 14384 (0xc030) ( (0x00ff)		
0010	Session Session Cipher S Cipher Cipher Compress Compress Extensio Extensio Extensio Cc 30 80 10 d 00 e8 76 f9 4	ID Length: 32 ID: 7710abcca921643. uites length: 4 uites (2 suites) - Suite: TLS_ECOME_1 - Suite: TLS_ECOME_1 - Mathade: Length: ion Mathade: Length: ion Mathade: Length: ion Server_name (len: n: server) (len: n: server) (len:	413a24e7382e70094f5a2ad RSA_NITH_AES_256_GCM_SF RENEGOTIATION_INFO_SCS\ 	bbd6dddb3fc5076290f44a9df6f IA384 (0xc030) / (0x00ff)		
0010 0020	Session : Session : Cipher S: Cipher S: Cipher S: Cipher S: Cipher S: Cipher S: Extension Extension Compress: Extension Compress: Extension Compress: Extension Compress:	ID Length: 32 ID: 7710abccs921643. UITS: Length: 4 UITS: Content: 4 UITS: Content: 4 Suite: TLS_ECHFL Suite: TLS_ECHFL Suite: TLS_EMPTV_I Ion Methods (1 methods n: server_name (1en: : ec_point_formats a 8b cc 30 80 11 5 0 00 80 06 00 00 cc c 65 55 cb b6 87 7	413a24e7382e70094f5a2ad RSA_NTTH_AES_256_GCM_SF RENEGOTIATION_INFO_SCSV 1 =17) (len=4) 9 fd 08 00 45 00 · 0· 0 a8 00 0f co a8 ···v 0 off a 59 50 18 ···v	ibd6dddb3fc5076290f44a9df6f IA384 (0xc030) / (0x00ff)		
0010 0020 0030	Session : Session : Cipher S: Cipher S: Cipher S: Compress: Compress: Compress: Extension Extension Extension C c 30 80 10 d 00 e8 76 f9 4 00 06 c 9 3b 0 02 01 82 48 00	ID Length: 32 ID: 7710abcca921643: uites Length: 4 uites (2 suites) - Suite: TLS_EKOHE_1 - Suite: TLS_EKPTY_1 ion Methods (1 m	413a24e7382e70094f5a2ad RSA_WITH_AES_256_GCM_SH RENEGOTIATION_INFO_SCSV 1 0 0 0 0 0 0 0 0 0 0 0 0 0	ibd6dddb3fc5076290f44a9df6f IA384 (0xc030)) ( (0x00ff) 		
0010 0020 0030 0040	Session : Session : Cipher S: Cipher S: Cipher Cipher Compress Extension Extension Compress Extension Compress Extension Compress Extension Compress Compress Extension Compress C	DD Length: 32 DD: 7710abccs321643. Uites Length: 4 Uites (2 suites) - Suite: TLS_ECMPE / - Suite: TLS_ECMPT / - Su	413a24e7382e70094f5a2ad RSA_MITH_AES_256_GCM_SA RENEGOTIATION_INFO_SCSV 1 1 1 1 1 1 1 1 1 1 1 1 1	ibd6dddb3fc5076290f44a9df6f IA384 (0xc030) / (0x00ff) 		
0010 0020 0030 0040 0050	Session : Session : Cipher S: Cipher S: Cipher S: Cipher S Cipher S Compress Extension Extension Compress Extension Extension Compress Compress Compr	ID Length: 32 ID: 7710abccs021643. uites Length: 4 uites (2 suites) r Suite: ILS_ECOHE_f suite: ILS_EMPTV_f ion Methods (1 methin su Length: 106 n: server_name (1en n: ec_point_formats a 6b cc 30 80 11 5 0 00 80 00 00 00 c cc 55 5 cb 50 87 0 00 16 03 10 00 5 sea f1 7b fd 2d 4 8 fc 7b 7b re 68 1d	413a24e7382e70094f5a2af RSA_WITH_AES_256_GCM_SH RENEGOTIATION_INFO_SCSV 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1	ibd6dddb3fc5076290f44a9df6f IA384 (0xc030) ( (0x00ff) 0		
0010 0020 0030 0040 0050 0060	Session : Cipher S: Cipher S: Cipher Cipher Cipher S: Compress Extensio Extensio Extensio Compress Extensio Extensio Extensio 0 68 76 f9 4 60 68 76 f9 4 60 68 76 f9 4 60 88 76 f9 4 77 70 77 70 77 70 78 78 78 78 78 78 78 78 78 78 78 78 78	DD Length: 32 ID: 7710abcca921643: UD: 7710abcca921643: UD: 7210abcca921643: UD: 7210abcca921643: Suite: TLS_ECHF_J Suite: TLS_ECHF_J Suite	413a24e7382e70094f5a2ad RSA_WITH_AES_256_GCM_SF RENEGOTIATION_INFO_SCSV 0 d) =17) (len=4) 9 fd 80 00 45 00 -0- 0 0f fa 59 50 18 b 01 00 00 b7 031 1 ff 1c 5c ed f0 R- 5 f9 6c 6d 75 90 -% 3 a2 4e 73 82 e7 y w	bbd6dddb3fc5076290f44a9df6f (A384 (0xc030) / (0x00ff) 		
0010 0020 0030 0040 0050 0050 0060	Session : Session : Cipher S: Cipher S: Cipher S: Cipher S: Extension > Extension > Extension > Extension > Extension 0 00 6e 37 67 9 4 00 90 e 29 80 0 00 21 82 48 0 00 3 52 89 es 5 04 25 97 21 6 07 20 77 10 a 09 09 47 5 a 2 a	ID Length: 32 ID: 7710abccca921643. UD: 7710abccca921643. Uites Length: 4 uites (2 suites) r Suite: ILS_ECOHE_f: Suite: ILS_ENPTY_I ion Methods (1 methods n: server_name (1en n: ec_point_formats a &b cc 30 & 80 11 5 0 00 & 80 06 00 00 cc c 65 55 cb 61 87 0 00 16 03 01 00 b c 64 51 7b fd 2d 4 8 fc b7 b7 e6 81 d b cc a9 21 64 34 1 b dd 6d db 37 c 5	413a24e7382e70094f5a2at RSA_WITH_AES_256_GCM_SF RENEGOTIATION_INFO_SCSV a od) =17) (len=4) 9 fd 08 00 f5 00 ·0- 0 a8 00 of c0 a8 ···v 0 of fa 59 50 18 ···v b 01 00 00 h7 03 ···1 1 ff 1c 5c ed f0 ·R. 5 f9 6c 6d 75 90 ·% 3 a2 4e 73 82 e7 y w 0 76 29 0f 44 a9 ···v	ibid6dddb3fc5076290f44a9df6f         IA384 (0xc030) (0x00ff)		
0010 0020 0030 0040 0050 0050 0060	Session : Cioher S: Cipher S: Cipher S: Cipher S: Cipher S: Cipher S: Compress Extensio Extensio Extensio 0 00 48 76 54 0 00 48 76 54 0 00 48 76 59 0 22 99 20 77 10 a 0 09 44 75 22 a 0 46 77 10 a 0 46 79 04 75 20	DD Length: 32 ID: 7710abcca921643: UD: 7710abcca921643: UD: 7210abcca921643: UD: 7210abcca921643: Suite: TLS_ECHF_J Suite: TLS_ECHF_J Suite	413a24e7382e70094f5a2ad RSA_WITH_AES_256_GCM_SF RENEGOTIATION_INFO_SCSV 0 d) =17) (len=4) 9 fd 88 00 45 00 00 0 a8 00 0f c0 88 00 0 a8 00 0f c0 88 00 1 ff 1c 55 c6 df 0 8 5 f9 6c 6d 75 90 - % 3 a2 4e 73 82 e7 y w 0 76 29 0f 44 a9 00 0 6a 00 00 00 10 00	bbd6dddb3fc5076290f44a9df6f (A384 (0xc030) / (0x00ff) 		



No.	Time	Source	Destination	Protocol Length Info	
	23 12,066082	192.168.0.14	192.168.0.15	TLSv1.2 214 Client Hello	
_	24 12,069261	192.168.0.15	192.168.0.14	TLSv1.2 968 Server Hello, Co	etif
	25 12.073010	192.168.0.14	192.168.0.15	TLSv1.2 180 Client Key Excha	
	26 12.075570	192.168.0.15	192.168.0.14	TISVI 2 105 Change Cipher St	
	27 12.079737	192.168.0.14	192.168.0.15	TLSv1.2 113 Application Data	<b>•</b> ••
	28 12.103280	192.168.0.15	192.168.0.14	TLSv1.2 106 Application Data	
	20 12.105200	192.100.0.15	192.100.0.14	TESVI.2 100 Application baca	
				ed (1712 bits) on interface \Device	\NPF
				VAI0_11:59:fd (cc:30:80:11:59:fd)	
> In	nternet Protocol	Version 4, Src: 19	2.168.0.14, Dst: 192.1	168.0.15	
> Tr	ransmission Cont	rol Protocol, Src P	ort: 60804, Dst Port:	3782, Seq: 1, Ack: 1, Len: 160	
✓ Tr	ransport Layer S	ecurity			
~	' TLSv1.2 Record	Layer: Handshake P	rotocol: Client Hello		
	Content Type	e: Handshake (22)			
	Version: TL	S 1.0 (0x0301)			
	Length: 155				
	✓ Handshake P	rotocol: Client Hell	lo		
	Handshake	e Type: Client Hello	) (1)		
	Length: :	151			
	Version:	TLS 1.2 (0x0303)			
	> Random: 4	Beb0c6e9fe3f7070fd41	81b1661f655632402c60f	b568be833fca8b058c206c1	
	Session 3	ID Length: 0			
	Cipher S	uites Length: 4			
	✓ Lipher St	uites (2 suites)			
	Cipher	Suite: TLS_ECDHE_E	CDSA_WITH_AES_128_GCM	_SHA256 (0xc02b)	
	Cipher	Suite: TLS_EMPTY_F	ENEGOTIATION_INFO_SCS	V (0x00ff)	
		ion Methods Length:	1		
	ompress				
		ion Methods (1 metho	od)		
	> Compress:		od)		
	> Compress: Extension	ion Methods (1 metho	,		
	> Compress: Extension > Extension	ion Methods (1 metho ns Length: 106	-17)		
	> Compress: Extension > Extension > Extension > Extension	ion Methods (1 metho ns Length: 106 n: server_name (len=	:17) (len=4)		
0000	<pre>&gt; Compress: Extension &gt; Extension &gt; Extension &gt; Extension</pre>	ion Methods (1 metho ns Length: 106 n: server_name (len- n: ec_point_formats n: supported_groups	:17) (len=4) (len=28)	V. 0	
	<pre>&gt; Compress: Extension &gt; Extension &gt; Extension &gt; Extension &gt; cc 30 80 11 55</pre>	ion Methods (1 metho ns Length: 106 n: server_name (1en- n: ec_point_formats n: supported_groups 9 fd cc 30 80 10 di	:17) (len=4) (len=28) a 8b 08 00 45 00 0	-Υ··0 ·····Ε· ·@··	
0010	<ul> <li>Compress: Extension</li> <li>Extension</li> <li>Extension</li> <li>Extension</li> <li>Extension</li> <li>cc 30 80 11 50</li> <li>00 c8 77 14 40</li> </ul>	Ion Methods (1 metho ns Length: 106 n: server_name (len: ec_point_formats n: supported_groups 9 fd cc 30 80 10 dd 0 00 80 06 01 ae cd	-17) (len=4) (len=28) a 8b 08 00 45 00 0 a 8b 08 00 c0 a8 00 0	r.@	
0010 0020	<ul> <li>Compress: Extension</li> <li>Extension</li> <li>Extension</li> <li>Extension</li> <li>Extension</li> <li>Cc 30 80 11 50</li> <li>00 68 77 14 44</li> <li>00 0f ed 84 00</li> </ul>	ion Methods (1 metho ns Length: 106 n: server_name (1en- n: ec_point_formats n: supported_groups 9 fd cc 30 80 10 di	<pre>17) (len=4) (len=28) a 8b 08 00 45 00 0 0 a 80 00 c0 a8 0 0 l 1e 55 21 50 18 0 0 0 0</pre>		
0010 0020 0030	<pre>&gt; Compress: Extension &gt; Extension &gt; Extension &gt; Extension &gt; cc 30 80 11 5 0 00 c8 77 14 4 0 00 0f ed 84 0 0 100 3e 21 0</pre>	ion Methods (1 metho ns Length: 106 n: server_name (len n: supported_groups 9 fd cc 30 80 10 di 0 00 80 06 01 ae cc e cc 26 d6 65 da 22	117)         (len=4)         (len=28)         a 8b 08 00 45 00         a 8b 08 00 c6 a8         b 12 5 21 50 18         0 01 00 00 97 03	··@··· ···&· e·!·U!P·	
0010 0020 0030 0040	<pre>&gt; Compress: Extension &gt; Extension &gt; Extension &gt; Extension &gt; Extension 0 cc 30 80 11 57 0 00 c6 77 14 41 0 00 0f ed 84 0 0 01 00 3e 21 00 0 38 b0 c6 ef</pre>	ion Methods (1 metho ns Length: 106 n: server_name (lene n: ec_point_formats n: supported_groups 9 fd cc 30 80 10 di 8 00 80 66 01 ae ci e c6 26 d6 65 da 22 0 00 16 03 01 00 91	117) (len=4) (len=28) a 80 08 00 45 00 00 b 80 00 00 c0 a8 00 l 10 55 21 50 18 00 0 1 00 00 97 03 00 81 b1 66 1f 65 000	1-@ &- e-!-∪!P- -!	
0010 0020 0030 0040 0050 0060	<ul> <li>Compress: Extension</li> <li>Extension</li> <li>Extension</li> <li>Extension</li> <li>Extension</li> <li>Cc 30 80 11 55</li> <li>00 c8 77 14 4</li> <li>00 0f ed 84 0</li> <li>01 00 3e 21 0</li> <li>03 8e b0 c6 e7</li> <li>56 32 40 2c 66</li> <li>c1 00 00 04 cc</li> </ul>	ion Methods (1 metho ss Length: 106 i: server_name (len- n: ec_point_formats : supported_groups 9 fd cc 30 80 10 d 0 00 80 06 0 al ac ct c c 26 d6 65 da 2 0 00 16 06 30 40 09 9 fe 3f 70 70 fd 4; 0 fb 56 8b e3 33 f 0 2b 00 ff 0 40 00 00	177) (len=4) (len=28) a 8b 08 04 5 00 b 8b 09 6 c 8a b 12 55 21 59 18 0 10 00 09 7 03 a 8 b 05 8 c 2 06 V2g 5 6a 00 09 00 11	r@··· ···?a· e·!·U!P· ···?p p·A··F·e ),`·V···3···X· ·+···j···	
0010 0020 0030 0040 0050 0060 0070	<pre>&gt; Compress: Extension &gt; Extension &gt; Extension &gt; Extension &gt; Extension 0 00 c8 77 14 4 0 00 fed 84 0 01 00 38 eb 0c6 ef 03 8e b0 c6 ef 03 8e b0 c6 ef 0 c1 00 00 04 cc</pre>	ion Methods (1 metho ss Length: 106 is server_name (len- is server_name (len- is upported_groups 9 fd c 30 80 10 di 0 00 80 06 01 me ci 0 c 62 66 65 da 22 0 06 16 03 01 00 91 9 fe 37 70 76 dd 4 0 fb 56 8b e 33 fi 0 2b 00 ff 01 00 00 0 fb 36 b e 33 fi 0 2b 00 ff 01 00 00 0 fb 37 20 22 81 31	117) (len=4) (len=28) a 8b 08 00 45 00 -00 b 86 00 0e c0 86 -w l 16 55 215 018 b 01 00 00 97 03 ->- 181 b1 66 1f 65 a 8b b9 58 c2 06 V2g 6 6 a0 00 00 11 5 38 2e 30 2e 31	γ@····· ···· ···· ···· ···· ···· ···· ·	
0010 0020 0030 0040 0050 0060 0070 0080	<pre>&gt; Compress: Extension &gt; Extension &gt; Extension &gt; Extension &gt; Extension &gt; Extension &gt; 00 c6 714 44 000 off ed 84 00 010 00 fed 80 00 01 00 fed 80 00 01 00 fed 80 00 01 00 fed 80 00 01 00 fed 80 00 00 fed 80 00 00 00 fed 80 00 00 00 00 fed 80 00 00 00 00 00 fed 80 00 00 00 00 00 00 00 00 00 00 00 00</pre>	ion Methods (1 metho ss Length: 106 i: server_name (len- n: ec_point_formats s: supported_groups 9 fd cc 30 80 10 d 0 00 80 06 01 ae ci c c 26 d6 65 da 2; 0 00 16 06 30 10 00 99 9 ff af 70 70 fd 4; 0 15 66 8b e6 33 f 0 2b 00 ff 01 00 00 c 31 39 32 2e 31 3; 4 03 00 01 0 00 00 00	17.7)           (len=4)           (len=28)           a bb 08 00 45 00           b b 08 00 45 00           a bb 09 c c 08 0           b 10 00 07 03           b 10 16 07 03           c 8 b 05 8 c 2 06           c 8 00 58 c 2 06           c 8 00 08 01           c 8 2 09 2 2 31           o 8 00 10 00	··ê···· ···ê···· ···?pp p.A··f·e j··V· -3···X·· ···192 .168.0.1	
0010 0020 0030 0040 0050 0060 0070 0080 0090	Compress: Extension > Extension > Extension > Extension > Extension > Extension > Extension > 00 60 7 14 40 00 60 7 24 40 00 60 7 24 40 01 60 62 24 40 26 03 86 40 66 60 03 60 40 60 40 35 60 60 60 60 35 60 60 60 80 35 60 90 90 80	ion Methods (1 metho ss Length: 106 i: server_name (len- i: server_name (len- i: supported_groups 9 fd c 30 80 10 di 0 00 80 06 01 me ci 0 c 62 66 65 da 22 0 06 16 03 01 00 91 9 fe 37 70 76 dd 4 0 fb 56 8b e 33 fi 0 2b 00 ff 01 00 00 0 fb 36 b e 33 fi 0 2b 00 ff 01 00 00 0 fb 37 20 28 13	17)       (len=4)         (len=28)	γ@····· ···· ···· ···· ···· ···· ···· ·	

Fig. 13. TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256.

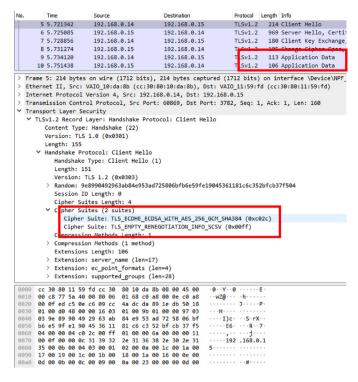


Fig. 14. TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384.

as unsecured MMS messages have different certificate and ADE sizes. An interesting finding is that all cipher suites had ADE sizes smaller than the unsecured MMS message. Reported certificate sizes vary, last two suites yielding the smallest size. That being said, certificates are only exchanged during TLS sessions establishment and is not used during IEC 61850 MMS exchanges. Their impact is not significant.

#### 4. Conclusions

All cipher suites recommended by IEC 62351-4 have been implemented on IEC 61850 MMS messages and secure information exchanges have been demonstrated. TLS 1.2 has been used for creating a secure communication channel between the client and the server while X.509 certificates have been used for authentication purposes. Lab experiments have been conducted and real MMS messages secured with different cipher suites have been captured.

The results are presented in terms of full message bodies as well as different certificate and message sizes. It is found that use of cipher suites may decrease ADE size to 46.1% of unsecured message size. It is also discovered that cipher suite selection is critical as some suites have 29.67% smaller certificate size than others.

Table 2. Performance results for recommended cipher suites.

Cipher suites	Certificate size (bytes)	ADE size (bytes)
None	N/A	245
TLS_RSA_WITH_AES_128_CBC_SHA256	903	139
TLS_DH_RSA WITH_AES_128_CBC_SHA256	835	139
TLS_DH_RSA_ WITH_AES_128_GCM_SHA256	838	113
TLS_DHE_RSA_ WITH_AES_128_GCM_SHA256	903	113
TLS_DH_RSA_ WITH_AES_256_GCM_SHA384	838	113
TLS_ECDHE_RSA_ WITH_AES_128_GCM_SHA256	903	113
TLS_ECDHE_RSA_ WITH_AES_256_GCM_SHA384	903	113
TLS_ECDHE_ECDSA_ WITH_AES_128_GCM_SHA256	635	113
TLS_ECDHE_ECDSA_ WITH_AES_256_GCM_SHA384	635	113

In addition to validating cybersecurity recommendations of IEC 62351-4, this paper also gives application insights about how these recommendations impact IEC 61850 MMS sizes and performances. These results are useful for pretesting security recommendations for MMS messages before the deployment is planned in the field. Both researchers and engineers active in this field will benefit from these application details and test results.

#### **Declaration of competing interest**

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

#### References

- [1] Ali I, et al. Communication modeling for differential protection in IEC-61850-based substations. IEEE Trans Ind Appl 2018;54:135-42.
- [2] Hussain SMS, et al. IEEE 1609 WAVE And IEC 61850 standard communication based integrated EV charging management in smart grids. IEEE Trans Veh Technol 2018;67(8):7690–7.
- [3] Aftab MA, et al. IEC 61850 And XMPP communication based energy management in microgrids considering electric vehicles. IEEE Access 2018;6:35657–68.
- [4] Hussain SMS, et al. Communication modeling of solar home system and smart meter in smart grids. IEEE Access 2019;6:16985-96.
- [5] Farooq SM, et al. S-GoSV: FRamework for generating secure IEC 61850 GOOSE and sample value messages. Energies 2019;12(13):2536.
- [6] Cyber-Attack Against Ukrainian Critical Infrastructure. Industrial control systems cyber emergency response team (ICSCERT). Incident report. 2016.
- [7] Communication networks and systems for power utility automation. 2.0. IEC 61850, IEC. 2013.
- [8] Power systems management and associated information exchange Data and communications security Part 4: Profiles including MMS and derivatives. 1.0. IEC 62351-4, IEC. 2018.
- [9] S.M.S. Hussain, Ustun TS, Kalam A. A review of IEC 62351 security mechanisms for IEC 61850 message exchanges. IEEE Trans Ind Inf 2020;16(9):5643–54. http://dx.doi.org/10.1109/TII.2019.2956734.
- [10] R. Schlegel, Obermeier S, Schneider J. A security evaluation of IEC 62351. J Inf Secur Appl 2017;34(2):197-204.
- [11] Power systems management and associated information exchange Data and communications security Part 6: Security for IEC 61850, 1.0. IEC 62351-6, IEC. 2007.
- [12] Farooq SM, et al. Performance evaluation and analysis of IEC 62351-6 probabilistic signature scheme for securing GOOSE messages. IEEE Access 2019;7:32343–51.
- [13] F. Hohlbaum, Braendle M, Fernando F. Cyber security practical considerations for implementing IEC 62351. In: PAC world conference. 2010.
- [14] D. Ishchenko, Nuqui R. Secure communication of intelligent electronic devices in digital substations. In: IEEE/PES transmission and distribution conference and exposition. 2018.
- [15] Hussain SMS, et al. Analysis and implementation of message authentication code (MAC) algorithms for GOOSE message security. IEEE Access 2019;7:80980–4.
- [16] S.M.S. Hussain, Farooq SM, Ustun TS. A method for achieving confidentiality and integrity in IEC 61850 GOOSE messages. IEEE Trans Power Deliv 2020;35(5):2565–7. http://dx.doi.org/10.1109/TPWRD.2020.2990760.
- [17] Mikel Rodríguez, et al. A fixed-latency architecture to secure GOOSE and sampled value messages in substation systems. IEEE Access 2021;(9):51646–58.
- [18] T.S. Ustun, Hussain SMS. An improved security scheme for IEC 61850 MMS messages in intelligent substation communication networks. J Mod Power Syst Clean Energy 2020;8(3):591–5.
- [19] J. Zhang, Li J, Chen X, Ni M, Wang T, Luo J. A security scheme for intelligent substation communications considering real-time performance. J Mod Power Syst Clean Energy 2019;7(4):948–61.
- [20] T.S. Ustun, Hussain SMS. IEC 62351-4 security implementations for IEC 61850 MMS messages. IEEE Access 2020;8:123979-123985.