



# Security of the Electronic Transactions: Case of TLS

**Dr. Eng. Nizar Ben Neji**  
**IT Security Consultant**

*Wednesday, April 18th 2017*  
*nizar.benneji @ gmail . com*

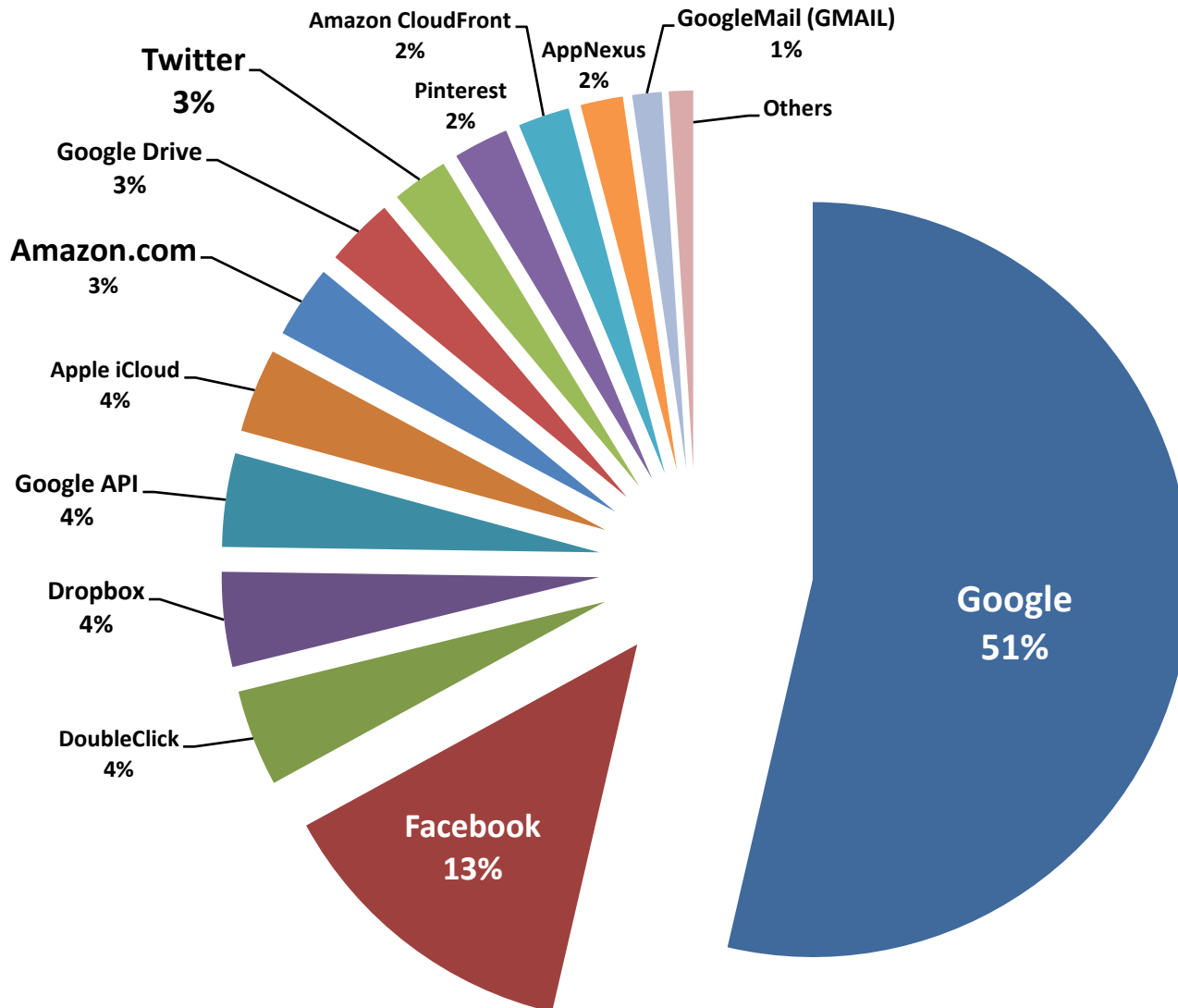
# 10% Internet Traffic is Encrypted

SSL comprises **1/3** of typical enterprise traffic

SSL traffic is growing **20%** per year



# Distribution of Encrypted Traffic



# Why SSL/TLS

- **Confidentiality** of data in transit over an un-trusted network connection (Internet)
- **Authentication** of the entity with which the transaction is being conducted (simple/double)
- It is best to **encrypt** sensitive data as **early** as possible and **decrypt** it as **late** as possible.
- Publicly **accessible** and **easy** to implement



# Not only Web

- **SSL/TLS** is used in several protocols not only with HTTP:

- HTTPS (443)

Web Browsers (Firefox, IE, Opera, Chrome, ....)

- LDAPS (636)

LDAP Clients (JXplorer, ....)

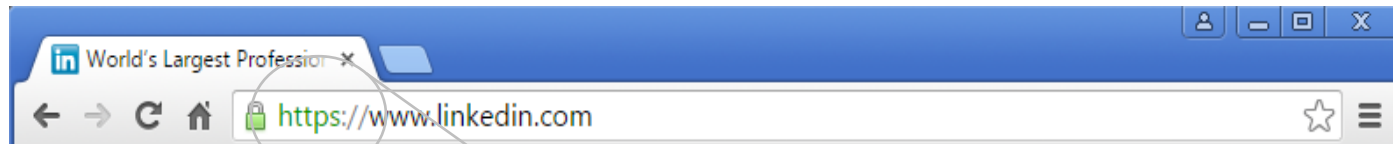
- IMAPS (993)

- POPS (995)

- SMTPS (465)

Messaging Client Tools (Thunderbird, MS Outlook, ...)

- ...

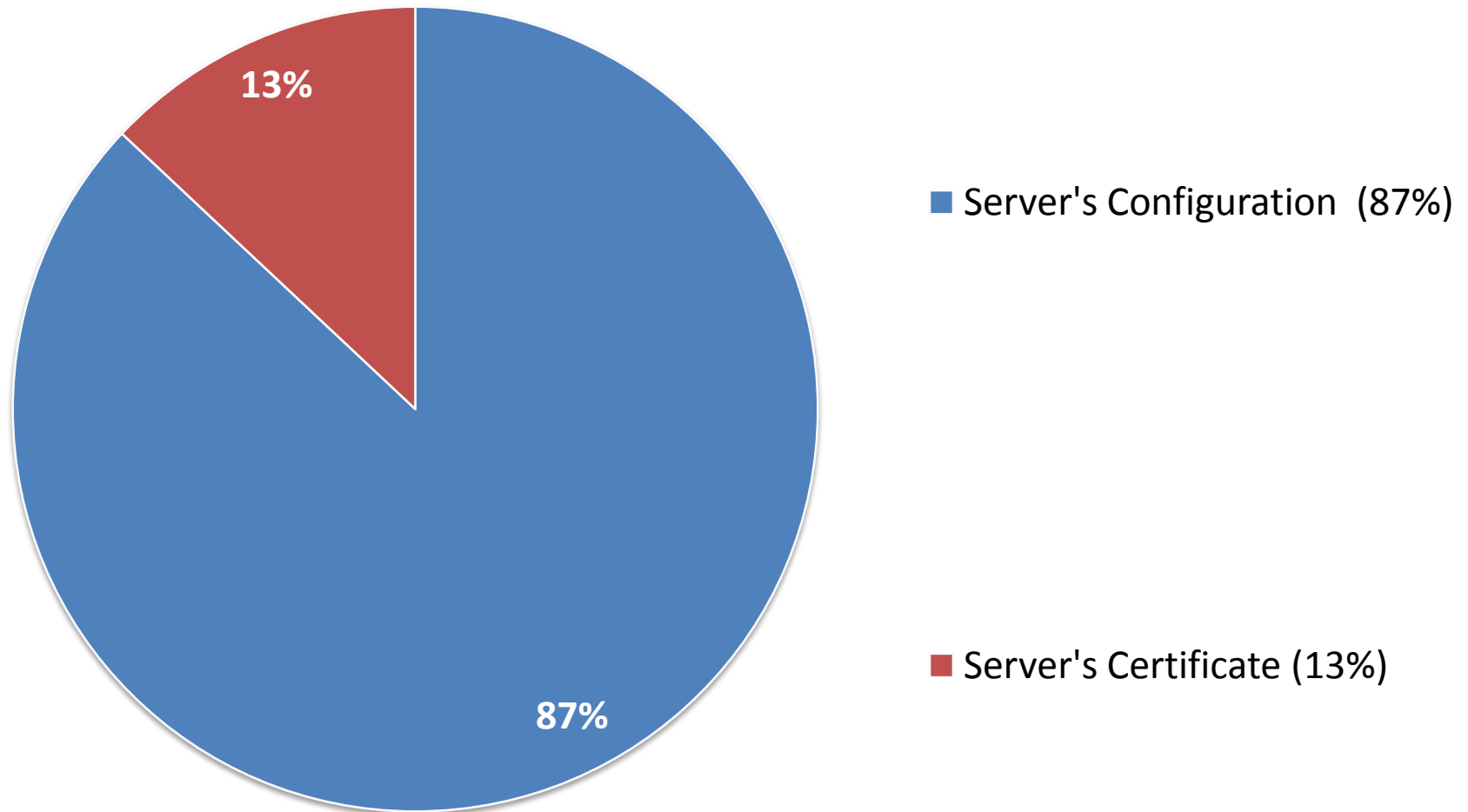


# Problems with TLS configuration

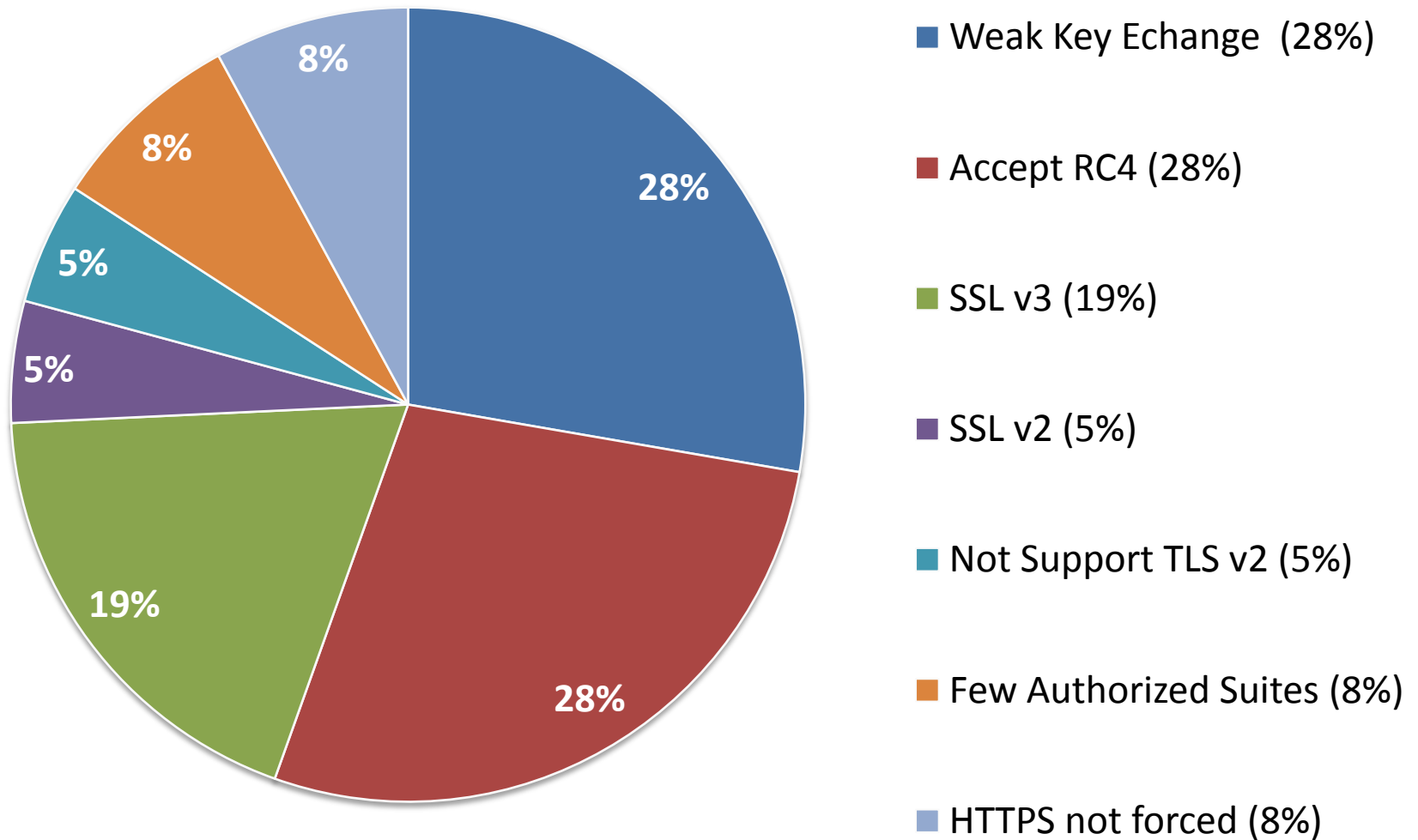
**20 Bank Websites** (Internet Banking Services) were SSL/TLS examined (Members of APTBEF Association)

	TLS-Related Problems	Number of Entities
1	Weak Key Exchange ( < 128 bits )	12
2	Use of the insecure cipher algorithm RC4	12
3	Use of SSL v3 which is obsolete and unsecure	8
4	Use of SSL v2 which is obsolete and unsecure	2
5	Not supporting the best protocol TLS v1.2 (newest)	2
6	Few number of Authorized Cipher Suites	3
7	HTTPS not forced	3
8	Not trusted Server's Certificate	5
9	SHA 1 Certificate (Server or CA)	1
10	Not Valid Certificate (Expired, Revoked, ...)	0

# TLS Certificate vs Configuration Issues



# Configuration's Issues





# Common SSL/TLS Errors



https://www.ebankin[redacted].jsp

Ce site ne peut pas fournir de connexion sécurisée

www.ebankin[redacted] utilise un protocole incompatible.

ERR\_SSL\_VERSION\_OR\_CIPHER\_MISMATCH

MASQUER LES DÉTAILS

Protocole incompatible

ERR\_SSL\_VERSION\_OR\_CIPHER\_MISMATCH

# Common SSL/TLS Errors



Non sécurisé | [https://\[redacted\].com.tn](https://[redacted].com.tn)

**!**

## Votre connexion n'est pas privée

Il se peut que des pirates soient en train d'essayer de dérober vos informations sur le site [\[redacted\].com.tn](https://[redacted].com.tn) (par exemple, des mots de passe, des messages ou des informations sur vos cartes de paiement). **NET::ERR\_CERT\_AUTHORITY\_INVALID**

[Signaler automatiquement](#) les incidents de sécurité potentiels à Google. [Règles de confidentialité](#)

PARAMÈTRES AVANCÉS Retour à la sécurité

**NET::ERR\_CERT\_AUTHORITY\_INVALID**

# Common SSL/TLS Errors



Non sécurisé | <https://www.████████.com>

**Votre connexion n'est pas privée**

Il se peut que des pirates soient en train d'essayer de dérober vos informations sur le site [www.████████.com](https://www.████████.com) (par exemple, des mots de passe, des messages ou des informations sur vos cartes de paiement). **NET::ERR\_CERT\_COMMON\_NAME\_INVALID**

Signaler automatiquement les incidents de sécurité potentiels à Google. [Règles de confidentialité](#)

PARAMÈTRES AVANCÉS

[Retour à la sécurité](#)

**NET::ERR\_CERT\_COMMON\_NAME\_INVALID**

# Common SSL/TLS Errors



Non sécurisé | <https://www.████████.com>

**!**

## Votre connexion n'est pas privée

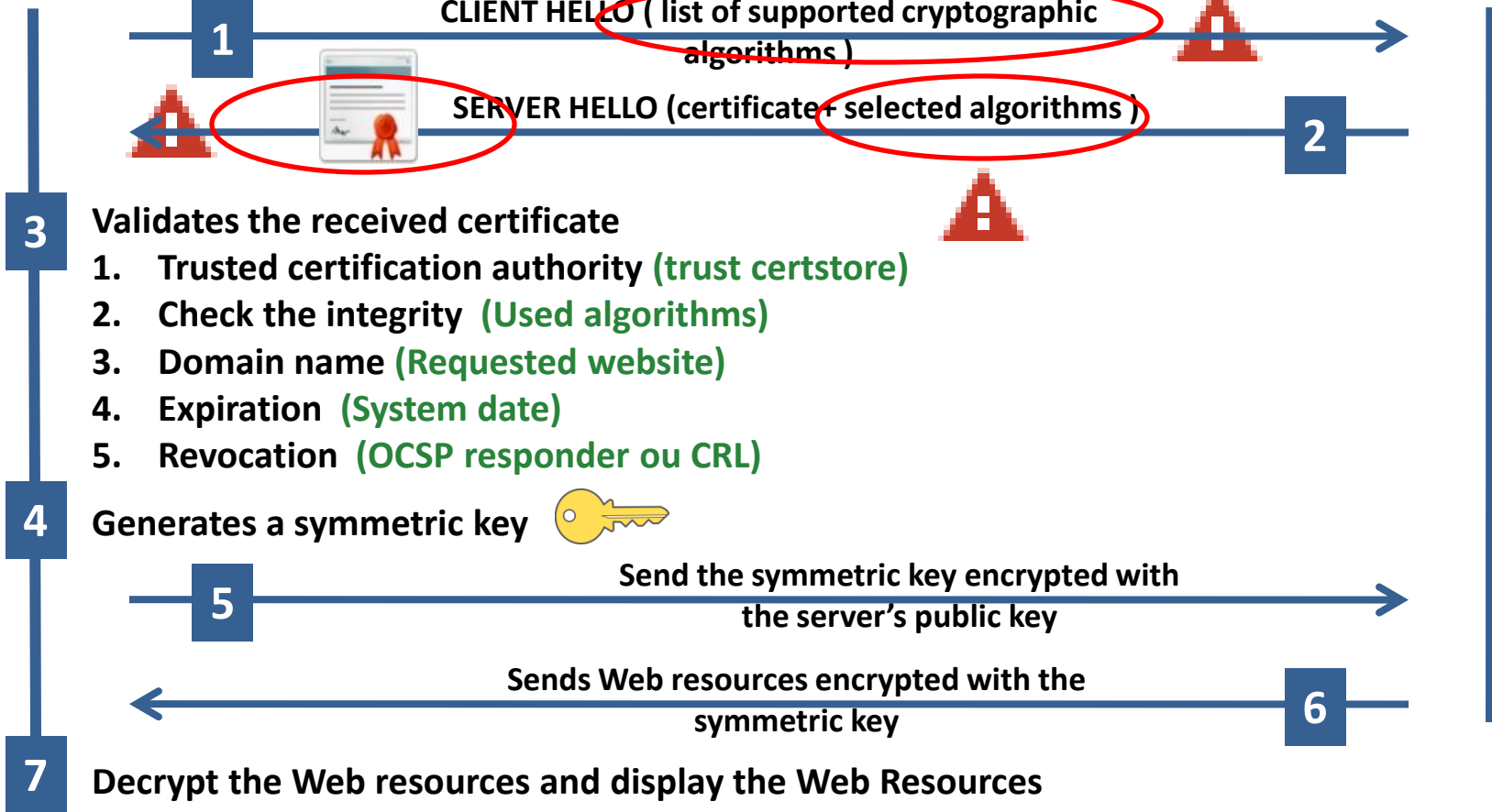
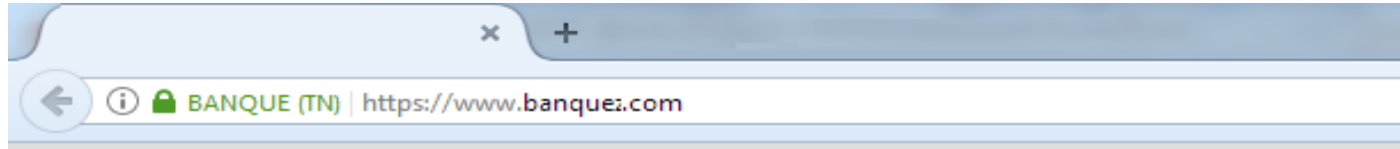
Il se peut que des pirates soient en train d'essayer de dérober vos informations sur le site [www.████████.com](https://www.████████.com) (par exemple, des mots de passe, des messages ou des informations sur vos cartes de paiement). **NET::ERR\_CERT\_WEAK\_SIGNATURE\_ALGORITHM**

[Signaler automatiquement](#) les incidents de sécurité potentiels à Google. [Règles de confidentialité](#)

[PARAMÈTRES AVANCÉS](#) [Retour à la sécurité](#)

**NET::ERR\_CERT\_WEAK\_SIGNATURE\_ALGORITHM**

# Handshake SSL/TLS



# Client Hello

No.	Time	Source	Destination	Protocol	Info
10	0.100504	192.168.136.128	31.13.75.36	TLSv1	Client Hello
11	0.100677	31.13.75.36	192.168.136.128	TCP	https > 42807 [ACK]

## Secure Socket Layer

### TLSv1 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 114

### Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 110

Version: TLS 1.0 (0x0301)

#### Random

Session ID Length: 0

Cipher Suites Length: 40

#### Cipher Suites (20 suites)

Cipher Suite: Unknown (0x00ff)

Cipher Suite: TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA (0x0088)

Cipher Suite: TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA (0x0087)

Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0039)

Cipher Suite: TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA (0x0038)

Cipher Suite: TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA (0x0084)

Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)

Cipher Suite: TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA (0x0045)



```

0060 20 00 00 28 00 ff 00 88 00 87 00 39 00 38 00 84 ..(. ....9.8..
0070 00 35 00 45 00 44 00 33 00 32 00 96 00 41 00 04 .5.E.D.3 .2...A..
0080 00 05 00 2f 00 16 00 13 fe ff 00 0a 01 00 00 1d /.....

```

# Server Hello

No.	Time	Source	Destination	Protocol	Info
15	0.163393	192.168.136.128	31.13.75.36	TCP	42807 → https [ACK] Seq=120 Ack=...
16	0.167899	31.13.75.36	192.168.136.128	TLSv1	Certificate, Server Hello Done
17	0.167899	192.168.136.128	31.13.75.36	TCP	42807 → https [ACK] Seq=120 Ack=...

▷ Frame 16: 846 bytes on wire (6768 bits), 846 bytes captured (6768 bits)

▷ Ethernet II, Src: Vmware\_ef:7a:13 (00:50:56:ef:7a:13), Dst: Vmware\_32:38:05 (00:0c:29:32:38:05)

▷ Internet Protocol, Src: 31.13.75.36 (31.13.75.36), Dst: 192.168.136.128 (192.168.136.128)

▷ Transmission Control Protocol, Src Port: https (443), Dst Port: 42807 (42807), Seq: 2801, Ack: 120, [Reassembled TCP Segments (3530 bytes): #12(1338), #14(1400), #16(792)]

▽ Secure Socket Layer

▽ TLSv1 Record Layer: Handshake Protocol: Certificate

- Content Type: Handshake (22)
- Version: TLS 1.0 (0x0301)
- Length: 3516

▽ Handshake Protocol: Certificate

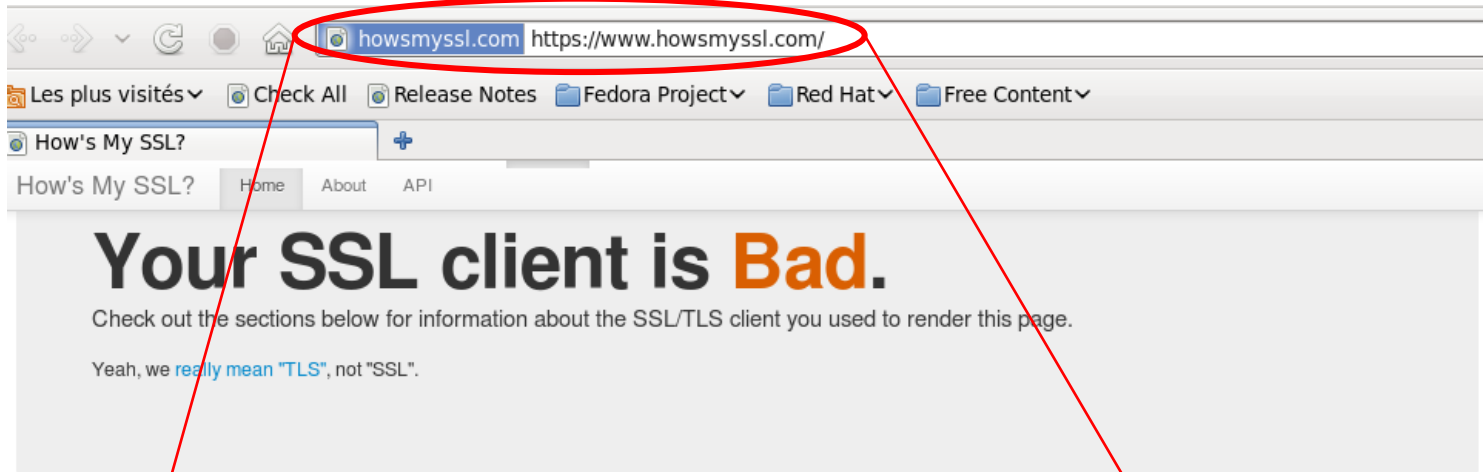
- Handshake Type: Certificate (11)
- Length: 3512
- Certificates Length: 3509

▽ Certificates (3509 bytes)

- Certificate Length: 1875
- ▷ Certificate (id-at-commonName=\*.facebook.com,id-at-organizationName=Facebook, Inc.,id-at-lo...  
Certificate Length: 1628
- ▷ Certificate (id-at-commonName=DigiCert High Assurance CA-3,id-at-organizationalUnitName=www...

▽ TLSv1 Record Layer: Handshake Protocol: Server Hello Done

# Evaluate your TLS Client



- 
- 
- 

## Version

**Bad** Your client is using TLS 1.0, which is very old, possibly susceptible to the BEAST attack, and doesn't have the best cipher suites available on it. Additions like AES-GCM, and SHA256 to replace MD5-SHA-1 are unavailable to a TLS 1.0 client as well as many more modern cipher suites.

[Learn More](#)

## Ephemeral Key Support

**Good** Ephemeral keys are used in some of the cipher suites your client supports. This means your client may be used to provide [forward secrecy](#) if the server supports it. This greatly increases your protection against snoopers, including global passive adversaries who scoop up large amounts of encrypted traffic and store them until their attacks (or their computers) improve.

[Learn More](#)

## Session Ticket Support

**Good** Session tickets are supported in your client. Services you use will be able to scale out their TLS connections more easily with this feature.

[Learn More](#)

## TLS Compression

**Good** Your TLS client does not attempt to compress the settings that encrypt your connection, avoiding information leaks from the [CRIME attack](#).

[Learn More](#)

## BEAST Vulnerability

**Bad** Your client is open to the [BEAST attack](#). It's using TLS 1.0 or earlier while also supporting a cipher suite that uses [Cipher-Block Chaining](#) and doesn't implement the 1/n-1 record splitting mitigation. That combination will leak information.

## Insecure Cipher Suites

**Bad** Your client supports cipher suites that are known to be insecure:

- TLS\_RSA\_WITH\_RC4\_128\_MD5: This cipher uses RC4 which has insecure biases in its output.

<https://www.howssmyssl.com/>



# Evaluate your TLS Client

🔒 Sécurisé | <https://www.howssmyssl.com>

How's My SSL?

Home

About

API

## Your SSL client is **Probably Okay.**

Check out the sections below for information about the SSL/TLS client you used to render this page.

Yeah, we **really mean** "TLS", not "SSL".

### Version

**Good** Your client is using TLS 1.2, the most modern version of the encryption protocol. It gives you access to the fastest, most secure encryption possible on the web.

[Learn More](#)

### Ephemeral Key Support

**Good** Ephemeral keys are used in some of the cipher suites your client supports. This means your client may be used to provide **forward secrecy** if the server supports it. This greatly increases your protection against snoopers, including global passive adversaries who scoop up large amounts of encrypted traffic and store them until their attacks (or their computers) improve.

[Learn More](#)

### Session Ticket Support

**Good** Session tickets are supported in your client. Services you use will be able to scale out their TLS connections more easily with this feature.

[Learn More](#)

### TLS Compression

**Good** Your TLS client does not attempt to compress the settings that encrypt your connection, avoiding information leaks from the **CRIME attack**.

[Learn More](#)

### BEAST Vulnerability

**Good** Your client is not vulnerable to the **BEAST attack** because it's using a TLS protocol newer than TLS 1.0. The BEAST attack is only possible against clients using TLS 1.0 or earlier using **Cipher-Block Chaining** cipher suites that do not implement the 1/n-1 record splitting mitigation.

[Learn More](#)

### Insecure Cipher Suites

**Good** Your client doesn't use any cipher suites that are known to be insecure.

[Learn More](#)

# Evaluate your TLS Server

← → <https://www.ssllabs.com/ssltest/>

**QUALYS<sup>®</sup> SSL LABS** Home Projects Qualys.com Cont

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [sibnet.sib.com.tn](#) > 41.224.38.154

**SSL Report:** [sibnet.sib.com.tn](#) (41.224.38.154)

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3 <b>INSECURE</b>	Yes
SSL 2 <b>INSECURE</b>	Yes

**Cipher Suites**

# TLS 1.0 (suites in server-preferred order)	
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_RC4_128_SHA (0x5) <b>INSECURE</b>	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) <b>WEAK</b>	112
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq, 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq, 3072 bits RSA) FS	256
TLS_RSA_WITH_RC4_128_MD5 (0x4) <b>INSECURE</b>	128
# SSL 3 (suites in server-preferred order)	
TLS_RSA_WITH_RC4_128_SHA (0x5) <b>INSECURE</b>	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) <b>WEAK</b>	112

<https://www.ssllabs.com/ssltest/>



**THANK YOU FOR YOUR ATTENTION**

**Dr. Eng. Nizar Ben Neji**

IT Security Expert

[nizar.benneji@gmail.com](mailto:nizar.benneji@gmail.com) /+216 99 207 377