Security of the Electronic Transactions: Case of TLS

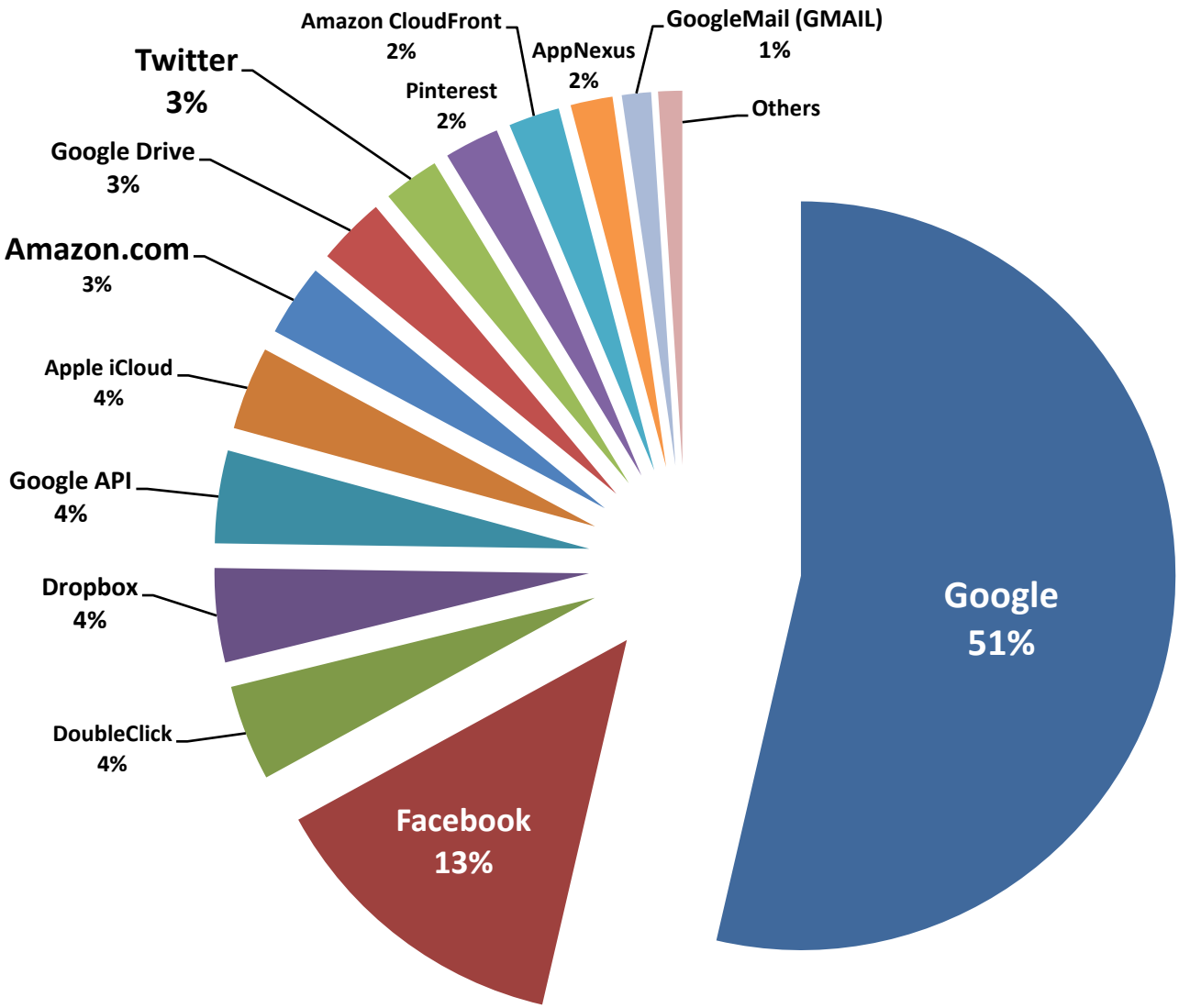
Dr. Eng. Nizar Ben Neji
IT Security Consultant

Wednesday, April 18th 2017

nizar.benneji @ gmail . com

10% Internet Traffic is Encrypted

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

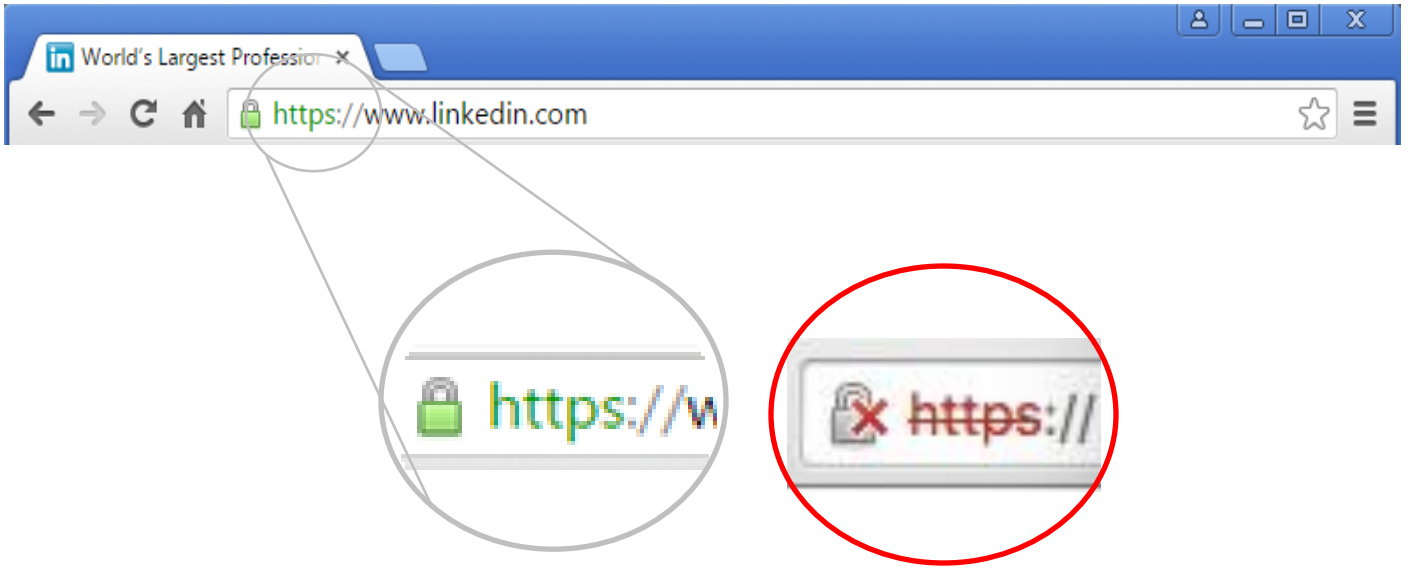
Not only Web

- **SSL/TLS** is used in several protocols not only with HTTP:
  - HTTP**S** (443)
  - LDAP**S** (636)
  - IMAP**S** (993)
  - POP**S** (995)
  - SMTP**S** (465)
  - …

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

LDAP Clients (JXPlorer, ….)

Messaging Client Tools (Thunderbird, MS Outlook, …)

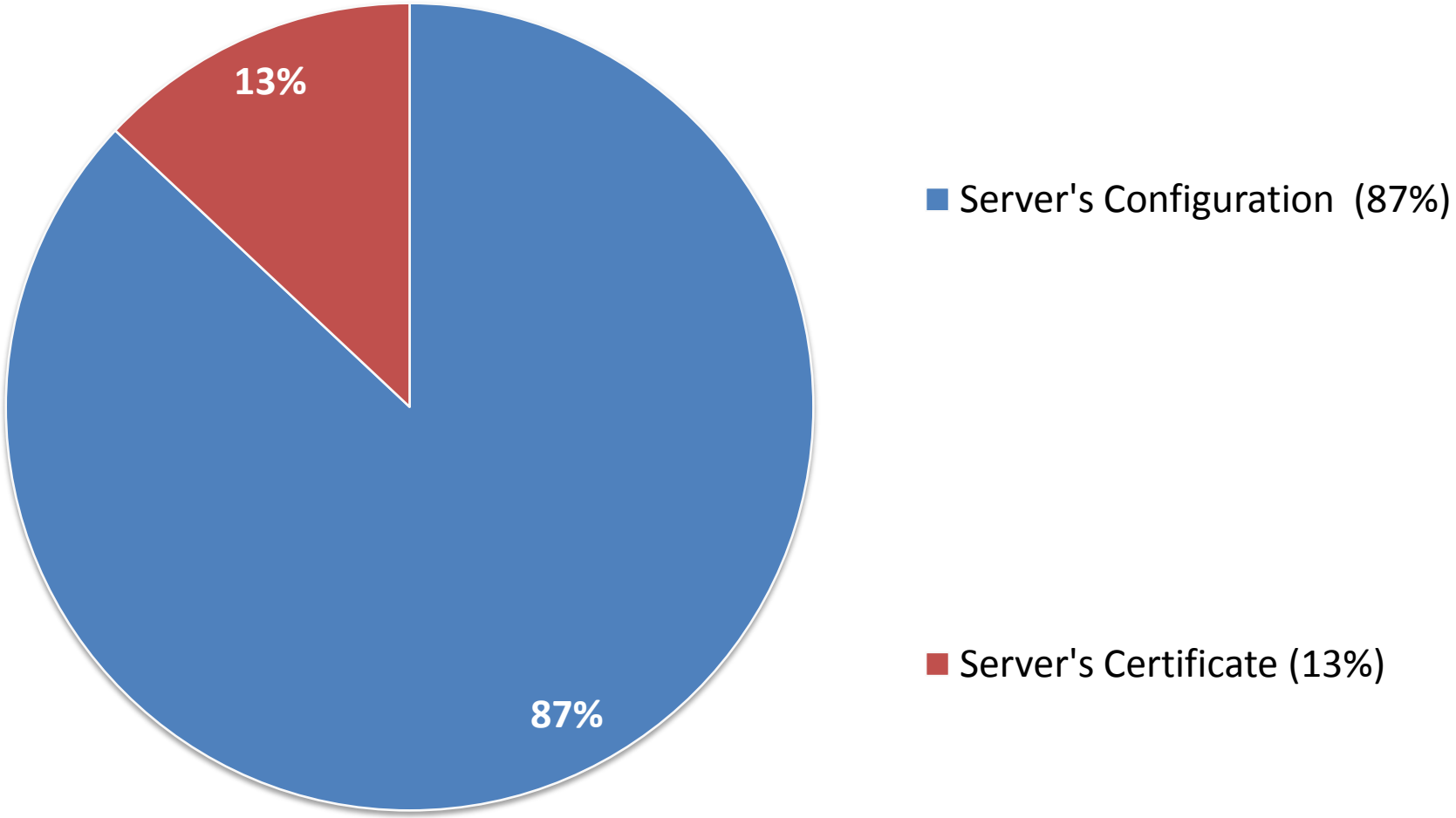


Problems with TLS configuration

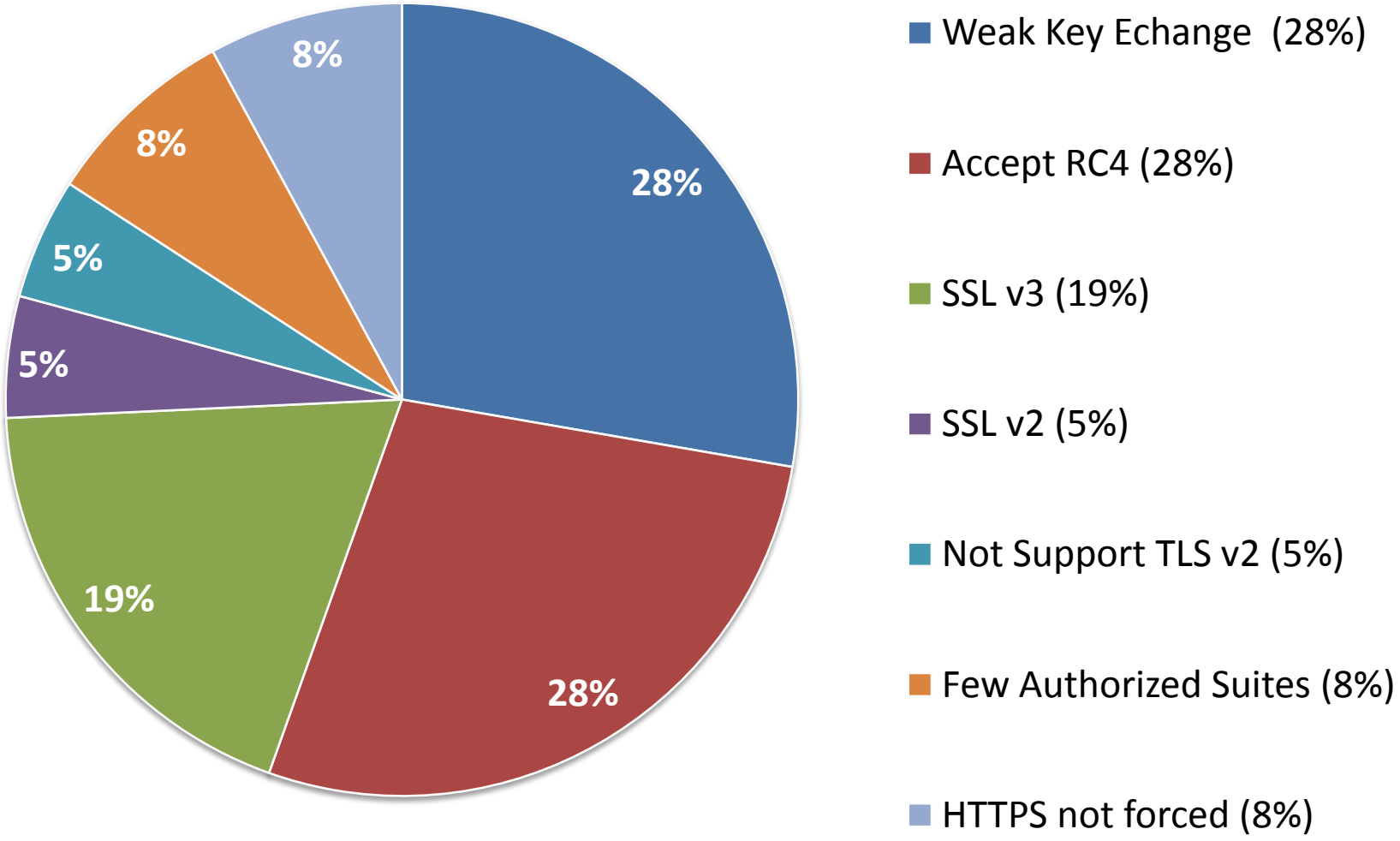
20 Bank Websites (Internet Banking Services) were SSL/TLS examined (Members of APTBEF Association)

	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3	Use of SSL v3 which is obsolete and unsecure	8
4	Use of SSL v2 which is obsolete and unsecure	2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

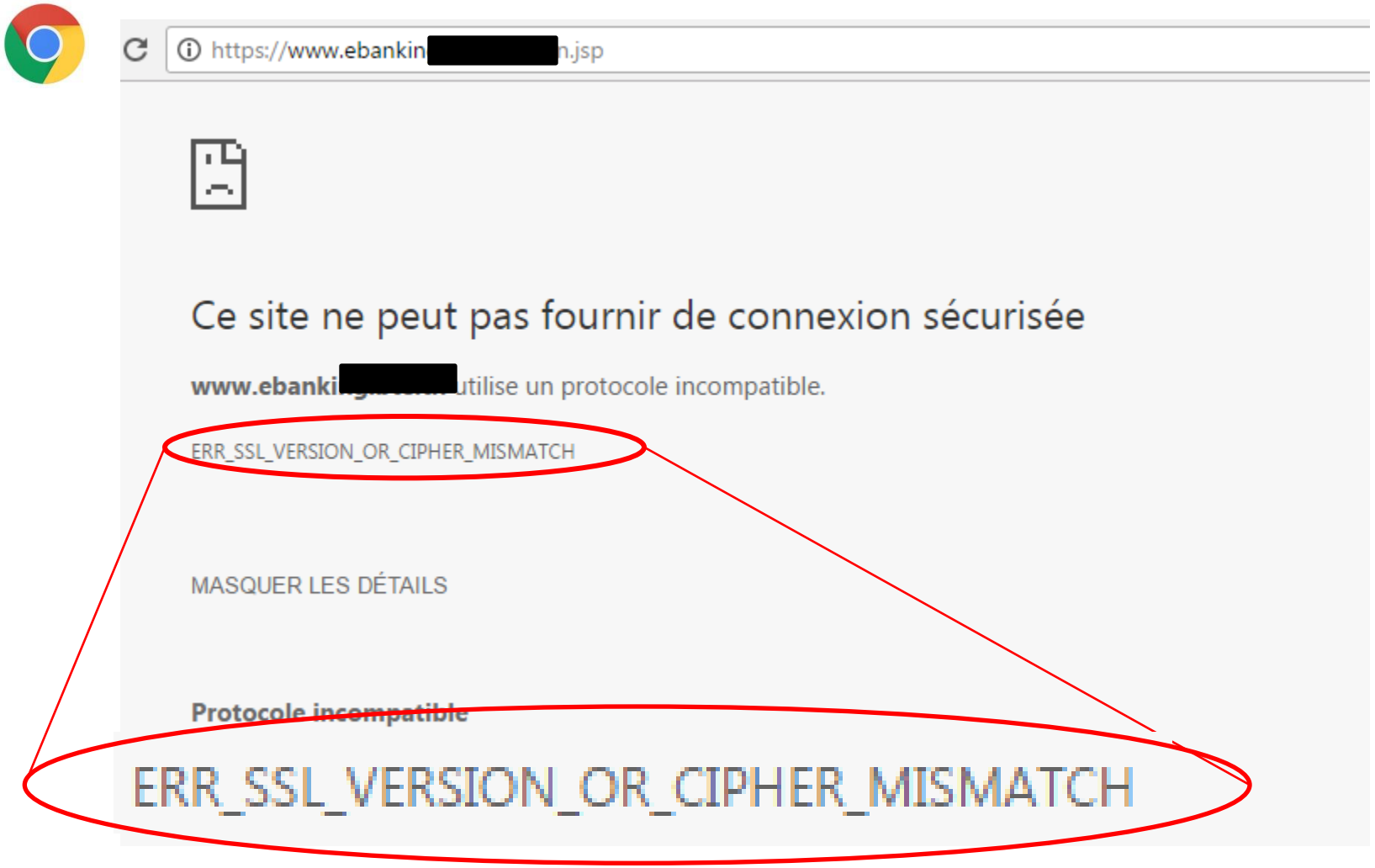
TLS Certificate vs Configuration Issues



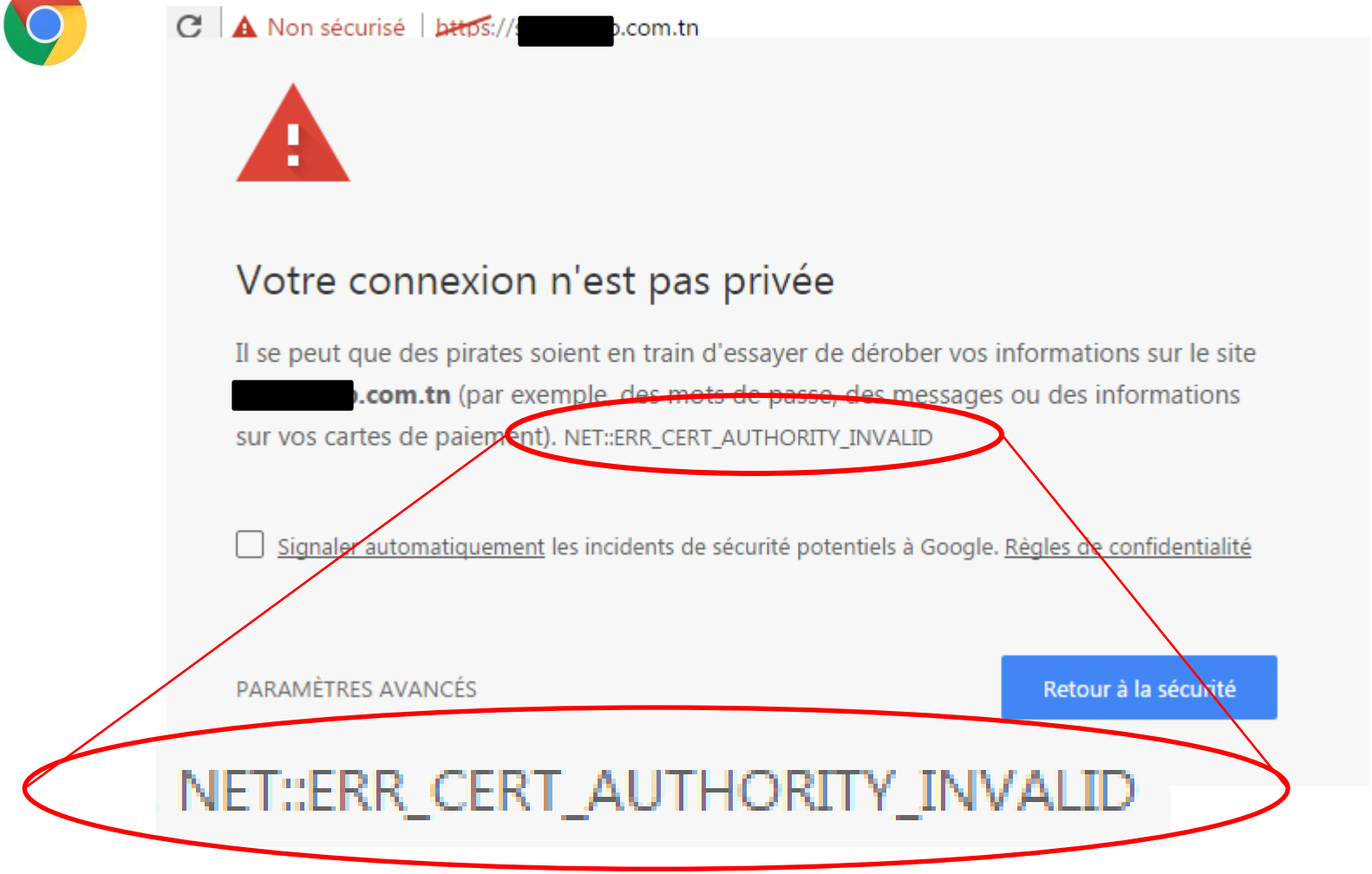
Configuration's Issues



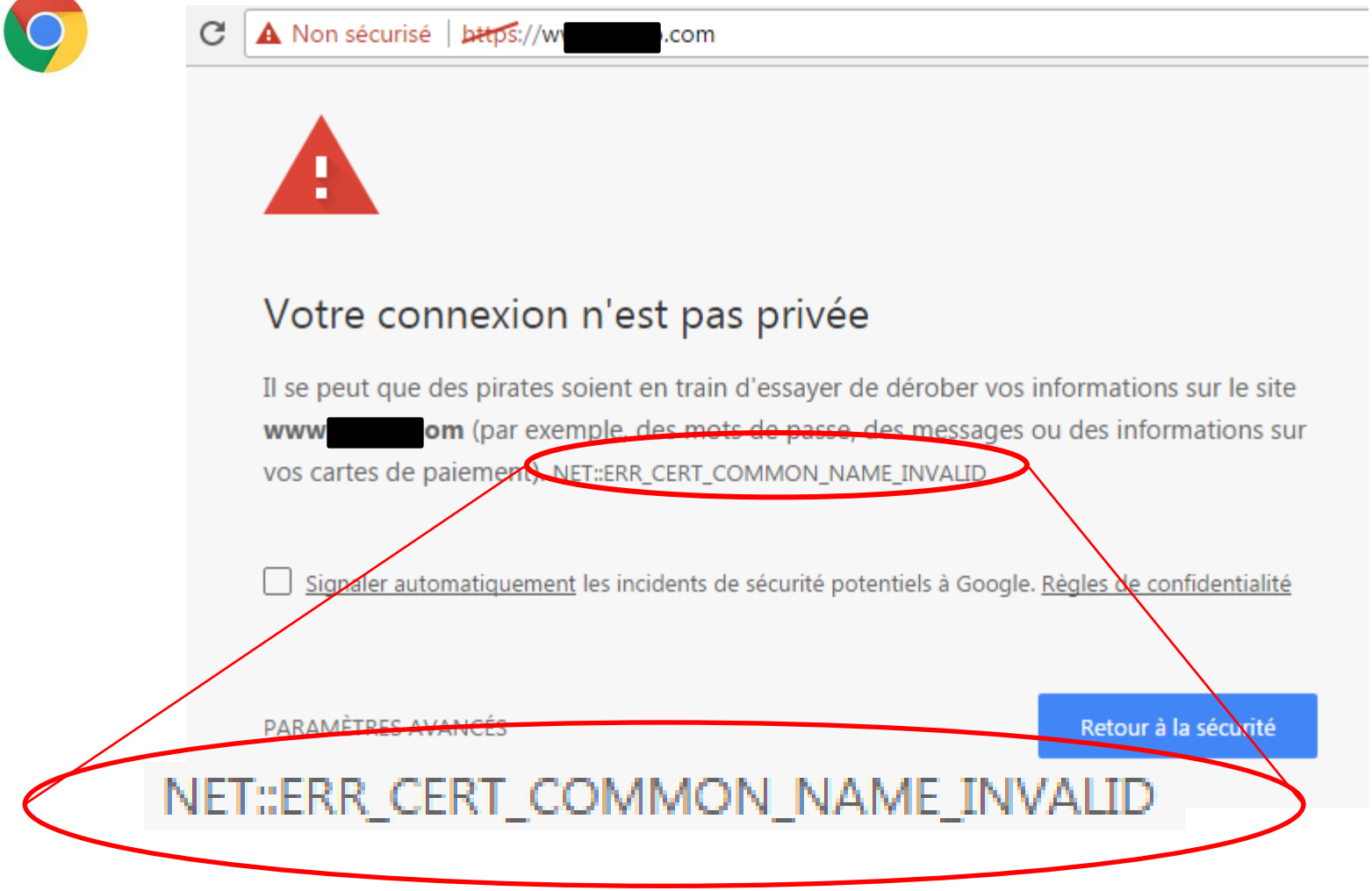
Common SSL/TLS Errors



Common SSL/TLS Errors

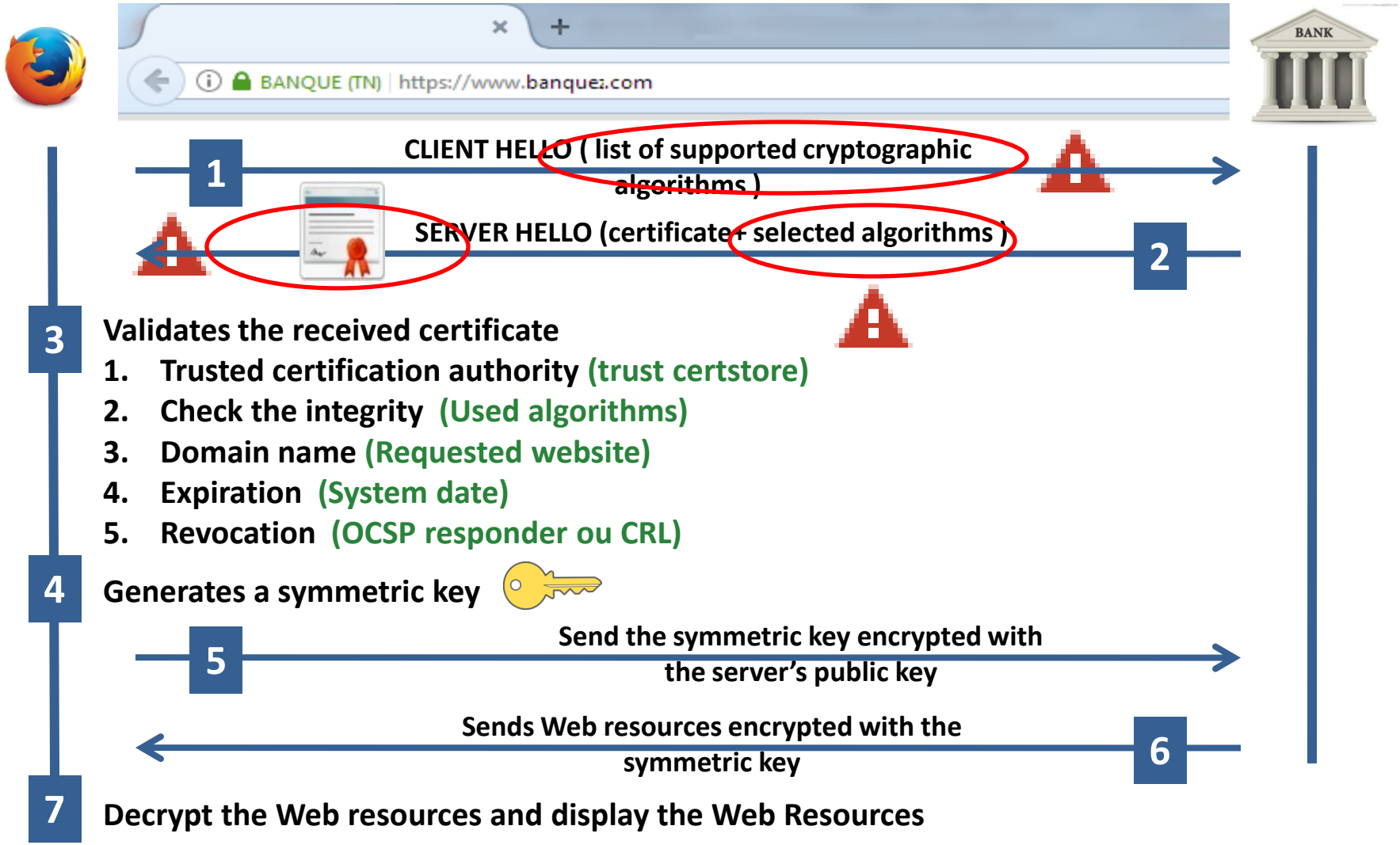


Common SSL/TLS Errors

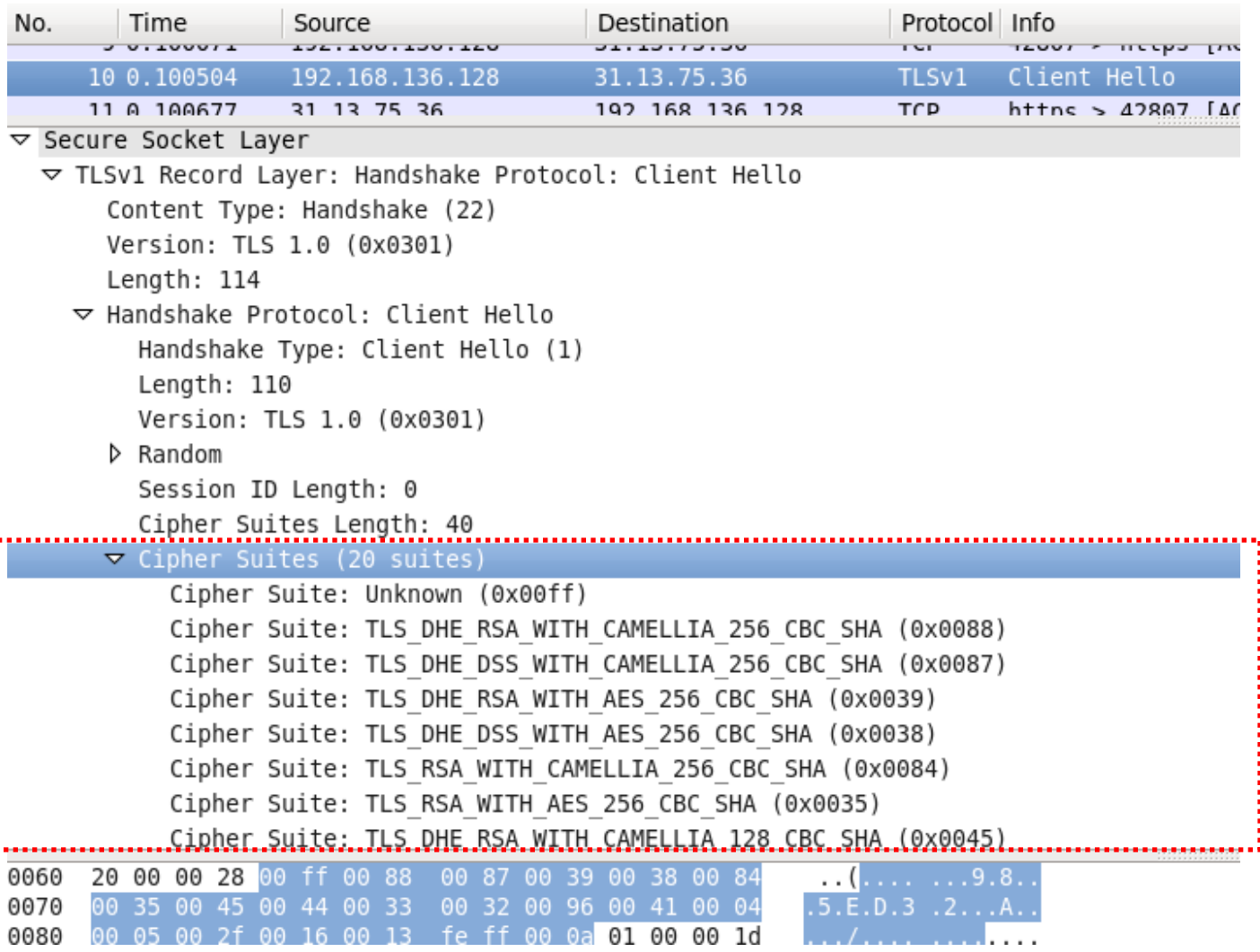


Common SSL/TLS Errors

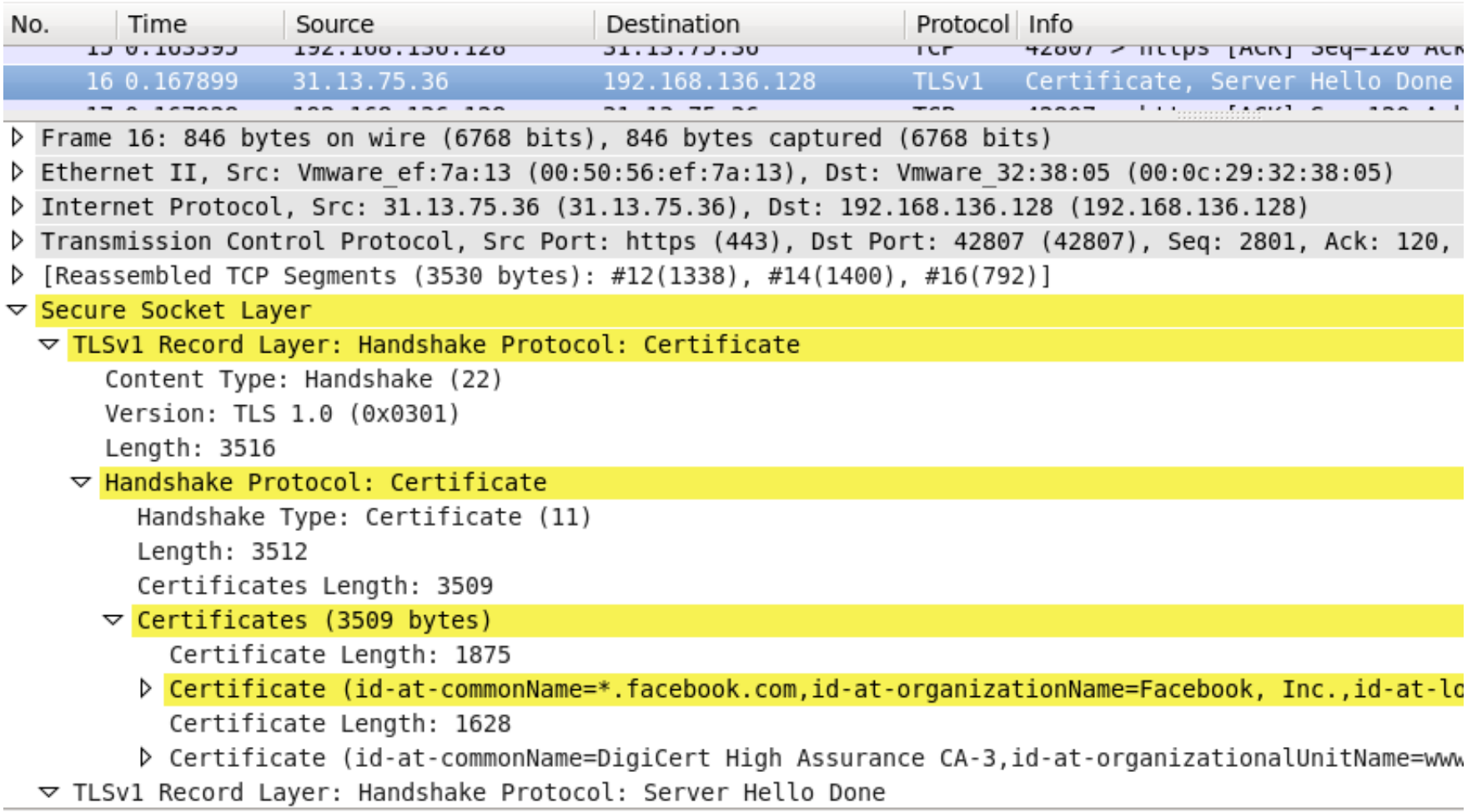
Handshake SSL/TLS



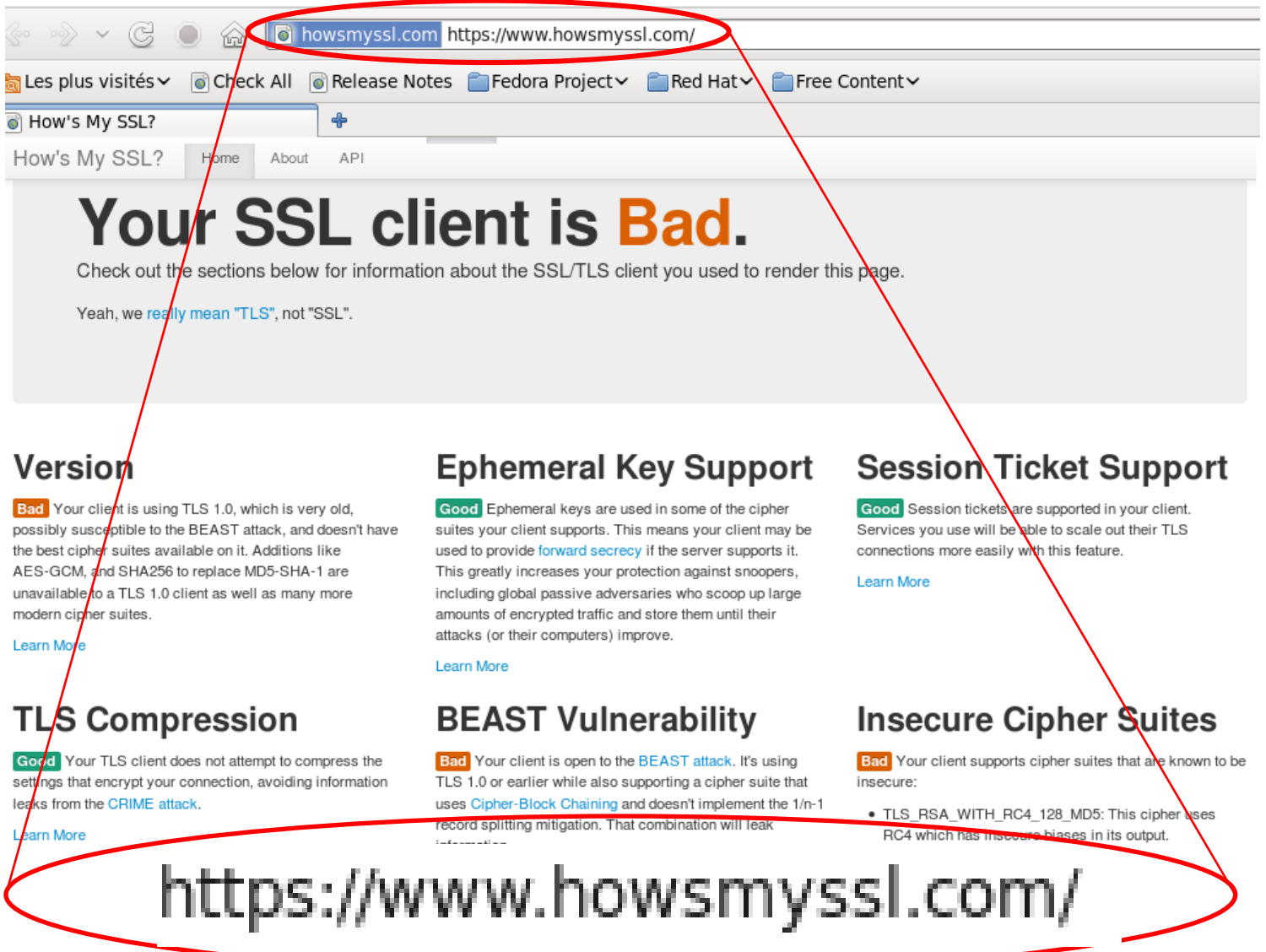
Client Hello



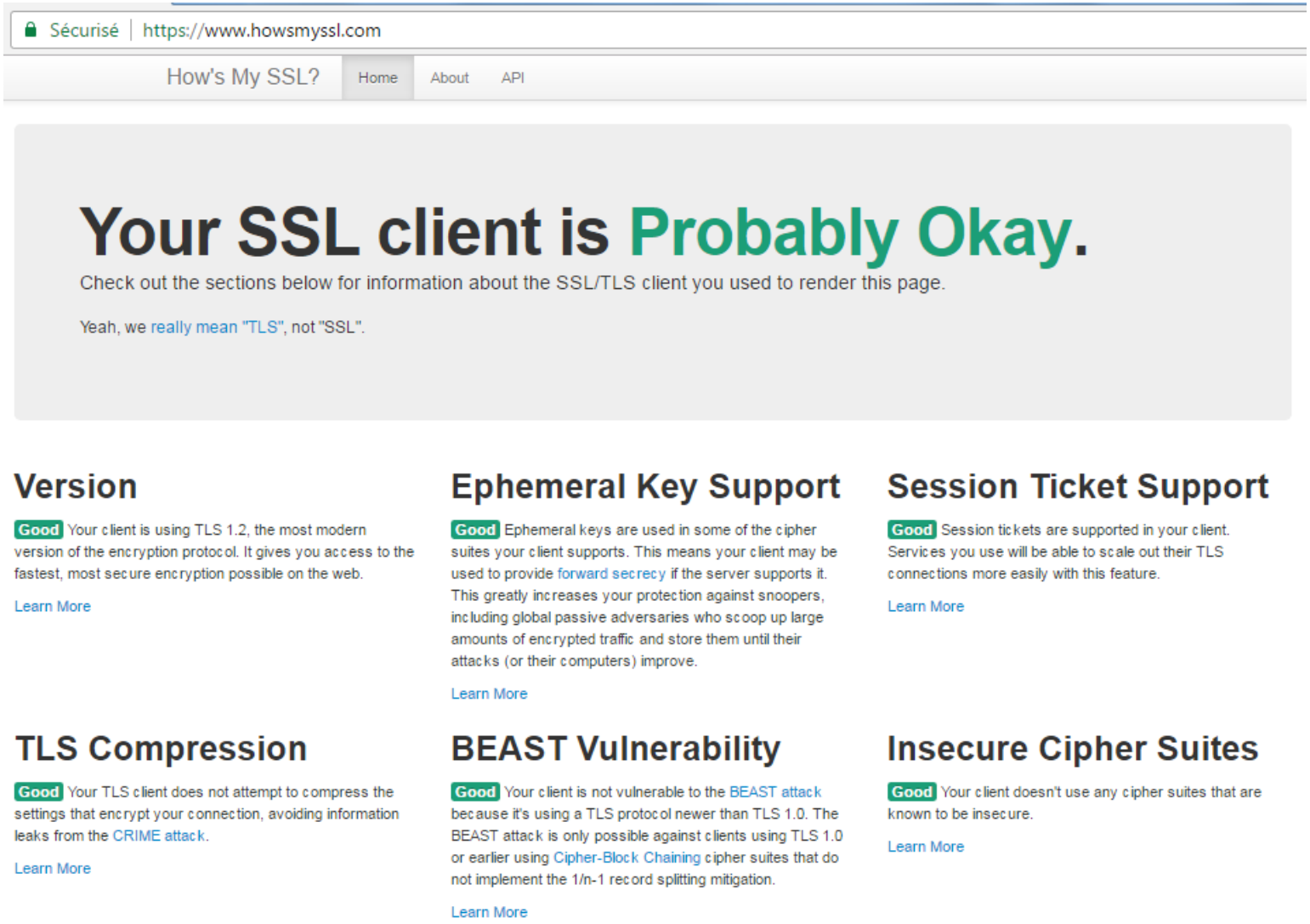
Server Hello



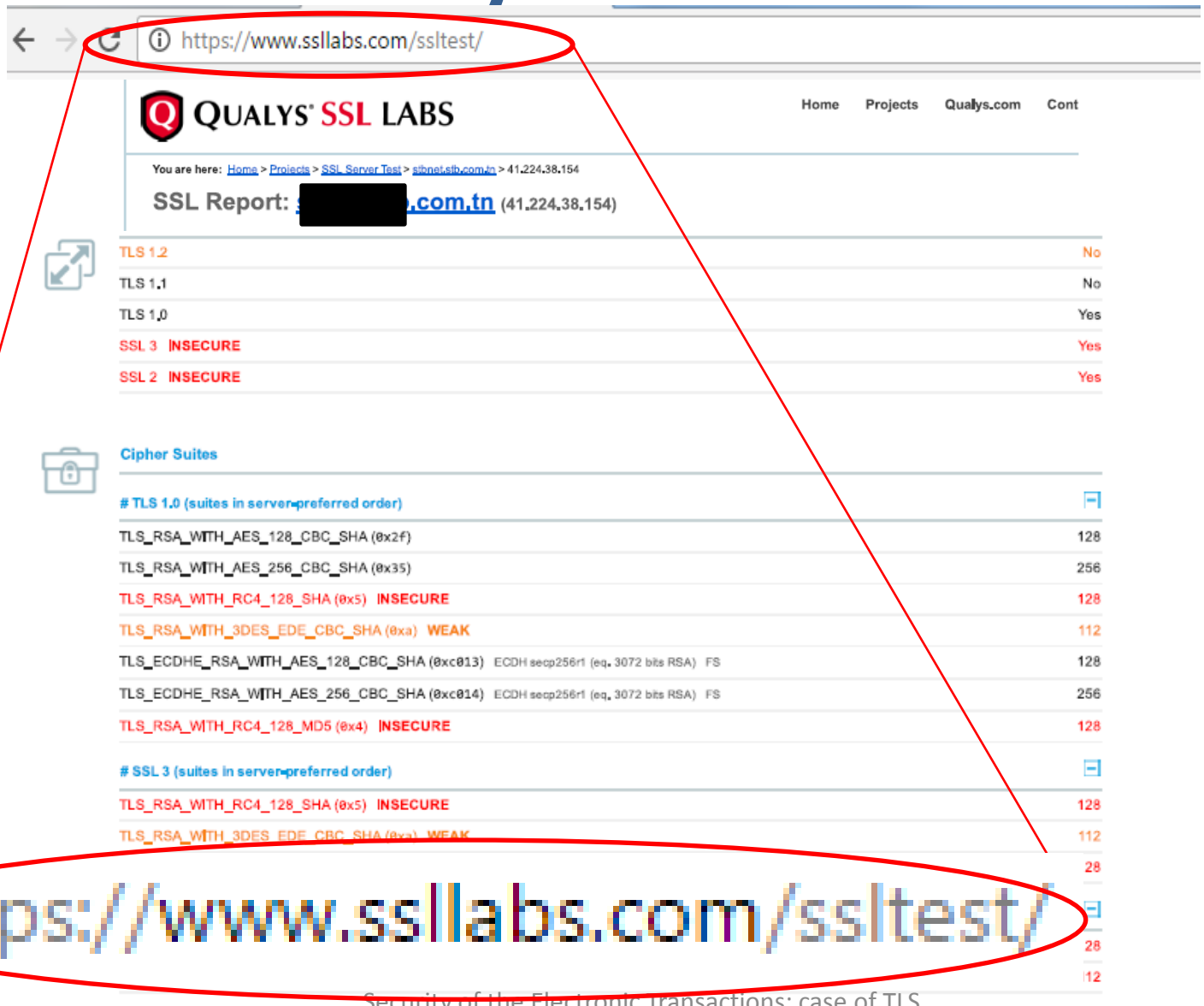
Evaluate your TLS Client



Evaluate your TLS Client



Evaluate your TLS Server



THANK YOU FOR YOUR ATTENTION

Dr. Eng. Nizar Ben Neji
IT Security Expert
nizar.benneji@gmail.com /+216 99 207 377