Mesures HTTPS par l'observatoire de la résilience de l'Internet français : compatibilité TLS et conformité des certificats

Maxence Tury
maxence.tury@ssi.gouv.fr

Agence nationale de la sécurité des systèmes d'information

11 juillet 2016

Quelques mots sur l'observatoire

Objectifs de l'observatoire

- Étudier en détail la résilience de l'Internet français
- Favoriser les échanges techniques entre acteurs de l'Internet
- Publier ses résultats anonymisés
- Publier des recommandations et diffuser des bonnes pratiques

http://www.ssi.gouv.fr/observatoire/

Les rapports annuels

Publiés chaque année depuis 2011

- Traduits en anglais depuis 2013

Indicateurs techniques

- Méthodologies de collecte
- Analyses vis-à-vis de la France

Trois protocoles étudiés

- BGP
- DNS
- TLS

Les outils pour reproduire les résultats

http://github.com/ANSSI-FR/mabo

- Mabo : détection des conflits d'annonces

http://github.com/ANSSI-FR/tabi

- Tabi : transformation des archives BGP en JSON

Résultats BGP

Usurpations de préfixe

- 6392 conflits d'annonces détectés
- 26 usurpations avérées détectés

Couverture des préfixes par des objets route

- IPv4 : la situation continue de s'améliorer +6.6 %
- IPv6 : la situation se dégrade -3.2 %

RPKI

- La situation stagne
- 65 % des préfixes français sont couverts
- La France fait partie des pays déclarant le plus de ROA

Résultats DNS

Dispersion des serveurs DNS faisant autorité

- 41 % des zones ne sont accessibles qu'en IPv4
- 83 % des zones sont hébergées par un seul AS

DNSSEC

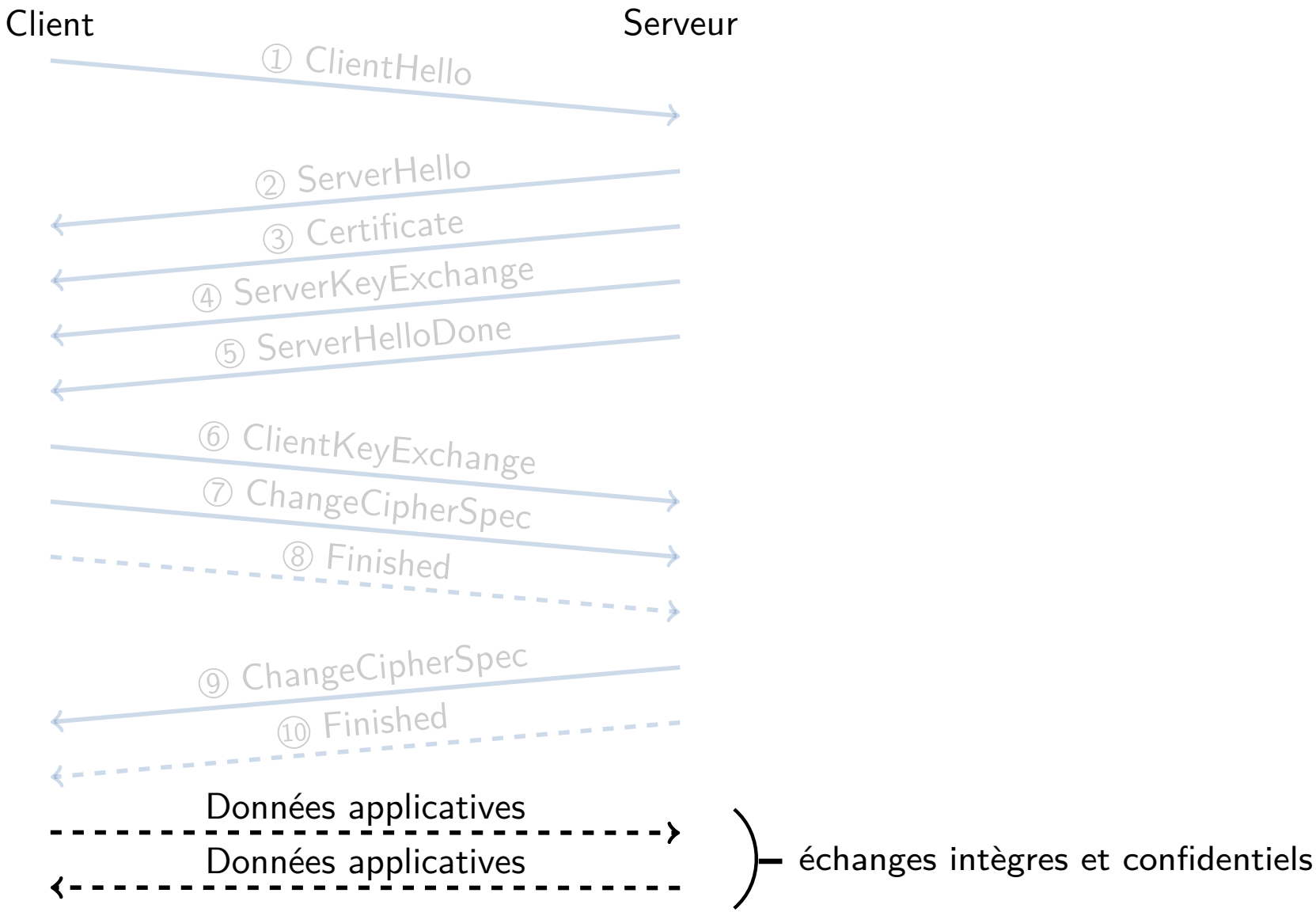
- 92 % des DS des zones utilisent SHA-1
- 98 % des zones utilisent SHA-2 pour la chaîne de confiance

Messagerie (MX)

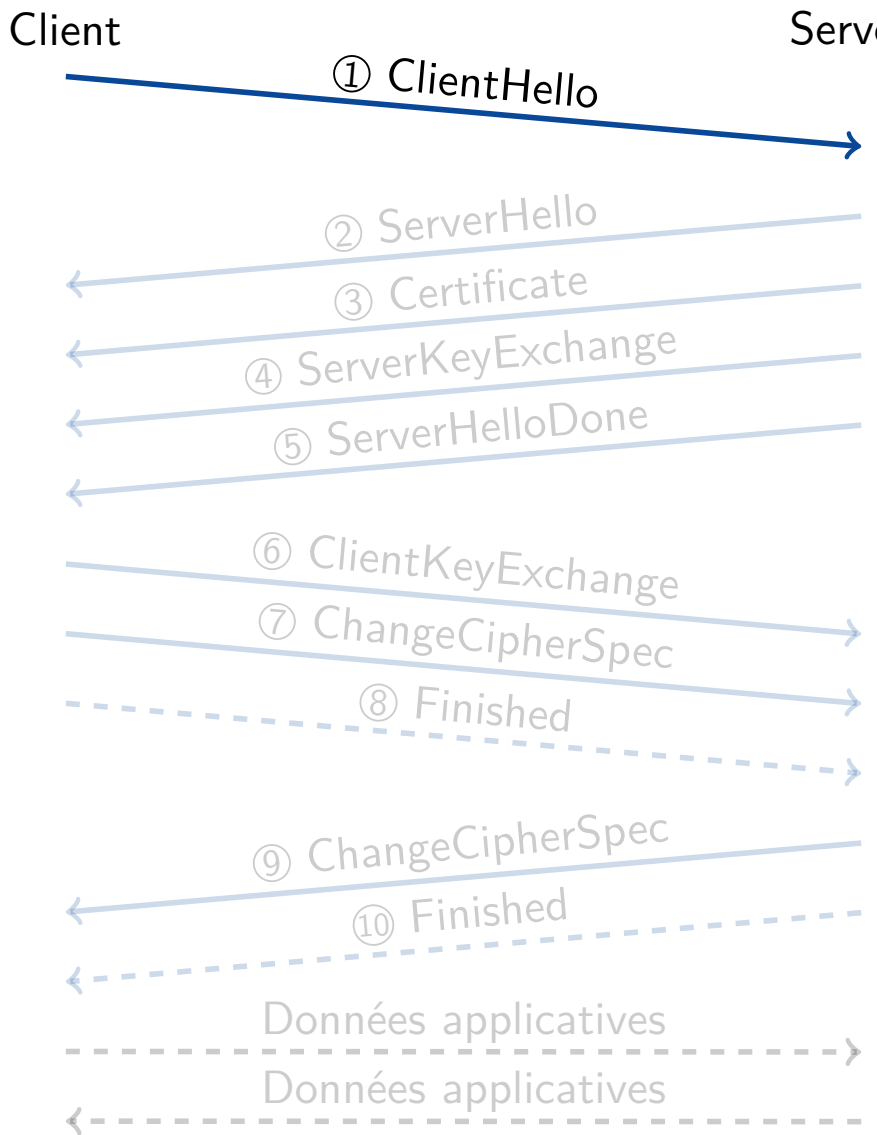
- 38 % des zones n'ont qu'une seul IP de relais déclarée
- 11 % des domaines ont au moins un enregistrement IPv6
- 69 % des relais de messagerie ont une IP hébergée en France

Serveurs SSL/TLS : que veut-on mesurer ?

Négociation TLS

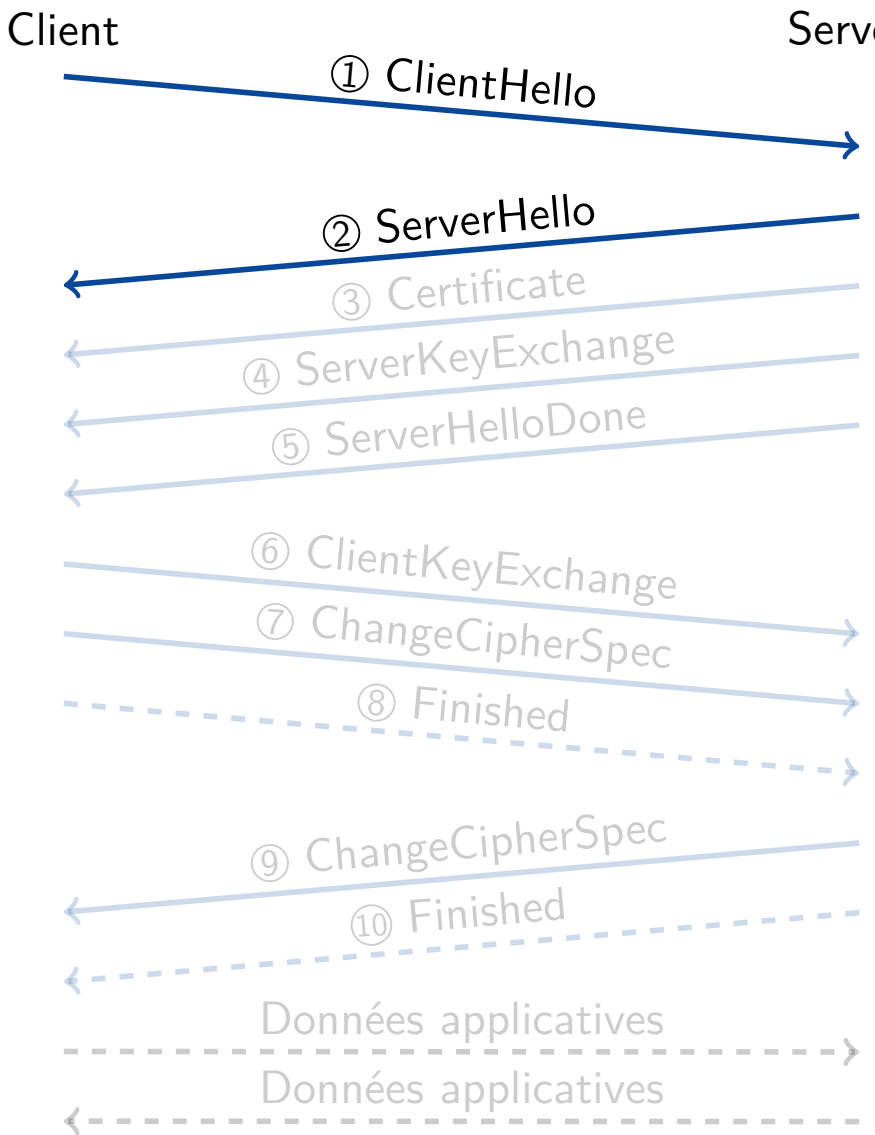


Négociation TLS



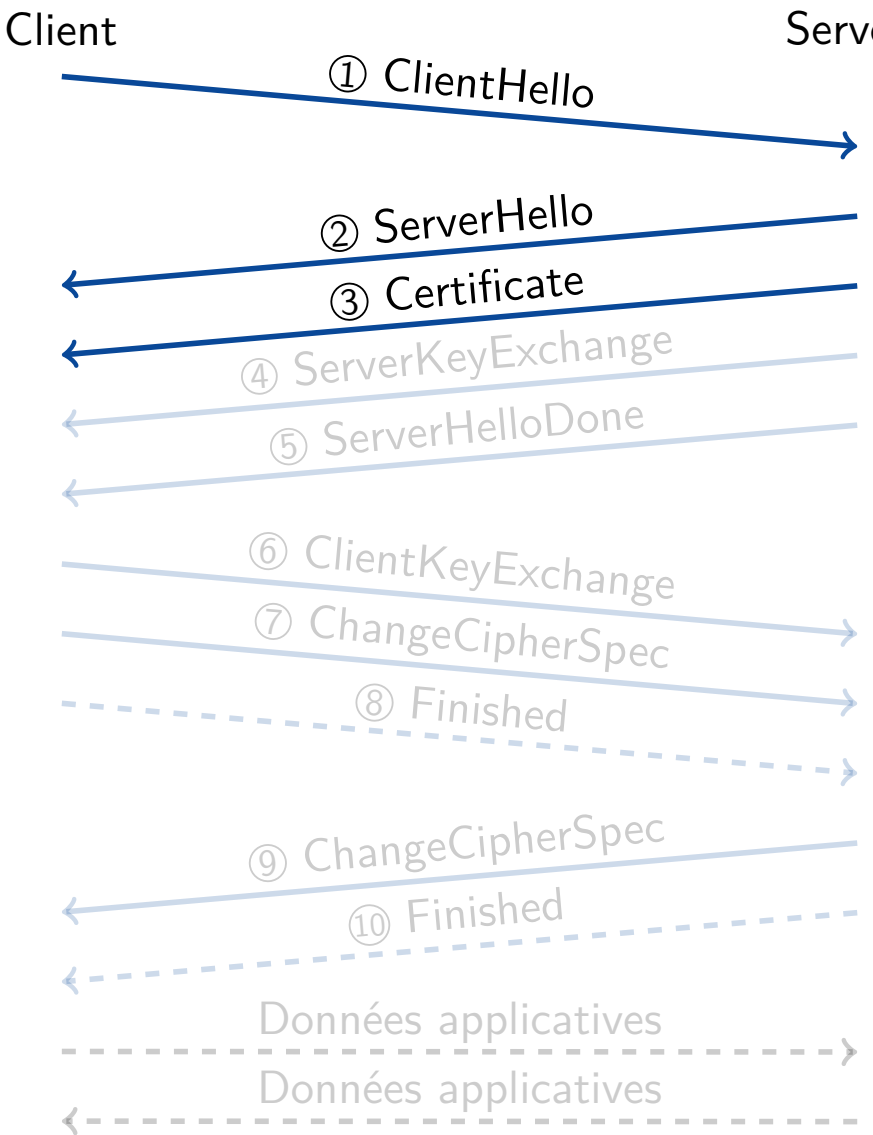

```
###[ TLS Handshake - Client Hello ]###
  msgtype   = client_hello
  msglen    = 88
  version   = TLSv1.2
  gmt_unix_time= Thu, 26 Apr 1979 07:58:23 +0000 (293961503)
  random_bytes= dce3af01fe96ab59d017faac0740083a46259789a744a339d27f6e8b
  sidlen    = 0
  sid       = ''
  cipherslen= 8
  ciphers   = [TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
               TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
               TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
               TLS_RSA_WITH_AES_128_GCM_SHA256]
  complen   = 1
  comp      = null
  extlen    = 39
  \ext       \
   |###[ TLS Extension - Server Name ]###
   |  type      = server_name
   |  len       = 15
   |  servernameslen= 13
   |  \servernames\
   |   |###[ ServerName ]###
   |   |  nametype  = host_name
   |   |  namelen   = 10
   |   |  name      = 'github.com'
   |###[ TLS Extension - Supported Elliptic Curves ]###
   |  type      = elliptic_curves
   |  len       = 8
   |  ecllen    = 6
   |  ecl       = [secp256r1, secp384r1, secp521r1]
   |###[ TLS Extension - Signature Algorithms ]###
   |  type      = signature_algorithms
   |  len       = 4
   |  sig_algs_len= 2
   |  \sig_algs  \
   |   |###[ Signature and Hash Algorithm ]###
   |   |  hash      = sha256
   |   |  sig       = rsa
```

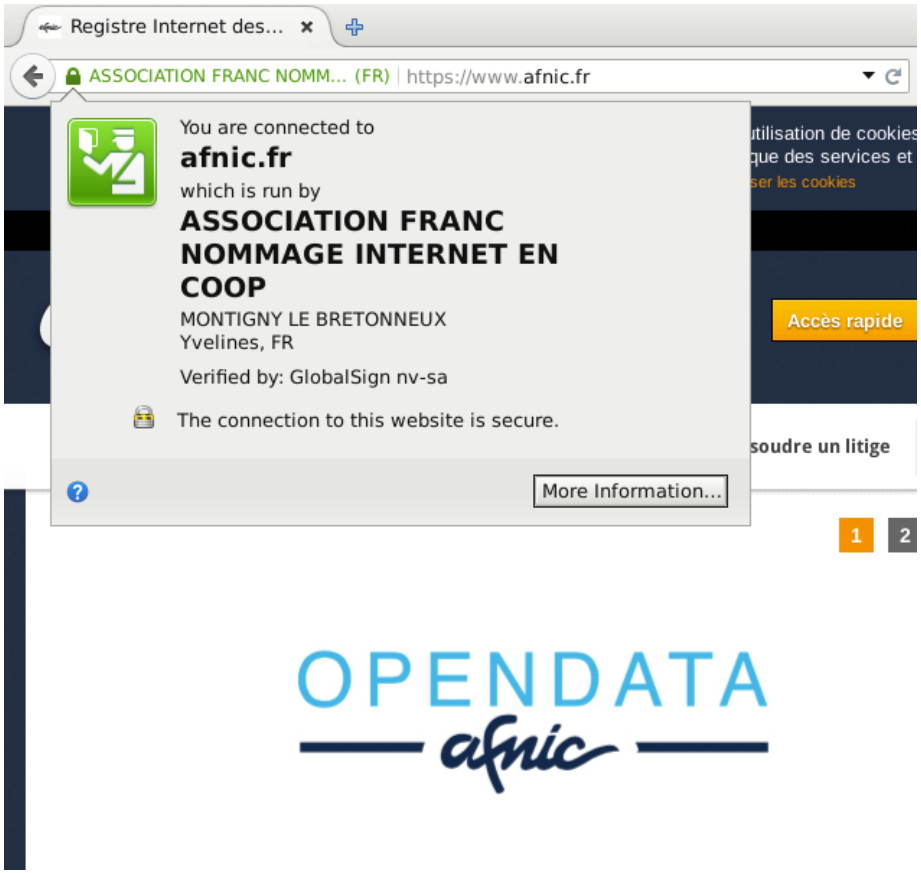
Négociation TLS



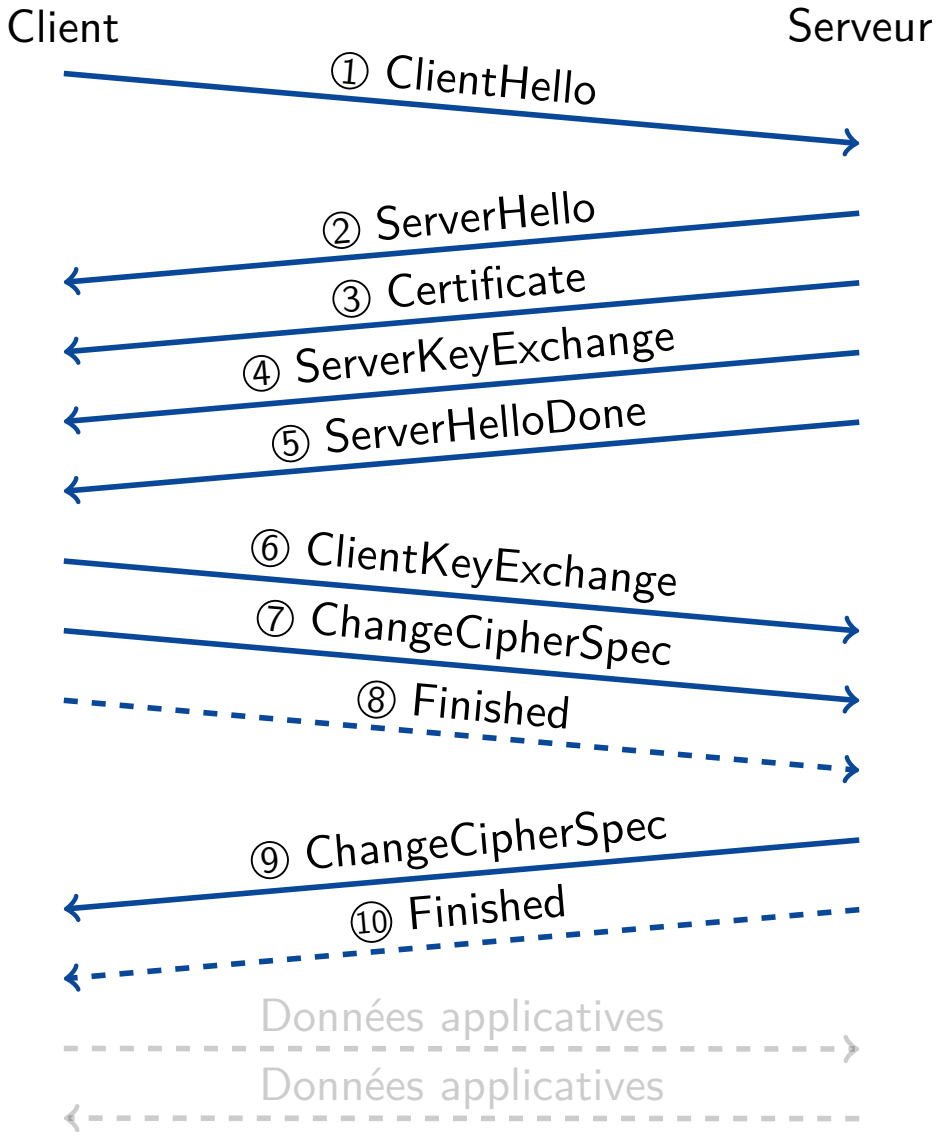

```
###[ TLS Handshake - Server Hello ]###
  msgtype    = server_hello
  msglen     = 76
  version    = TLSv1.2
  gmt_unix_time= Thu, 30 Jun 2016 15:59:34 +0000 (1467302374)
  random_bytes= 9fe47d74a5ca5b332d6ca9e2b198d37cd5450fbb278994a7d11ee7ef
  sidlen     = 32
  sid        = 067c12c1e5ce13c7d7c03fcaa7b7bd6a34983528a6374b50d8838788763f82a4
  ciphers    = TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  comp       = null
  extlen     = 4
  \ext        \
   |###[ TLS Extension - Server Name ]###
   |  type      = server_name
   |  len       = 0
   |  servernameslen= None
   |  \servernames\
```

Négociation TLS

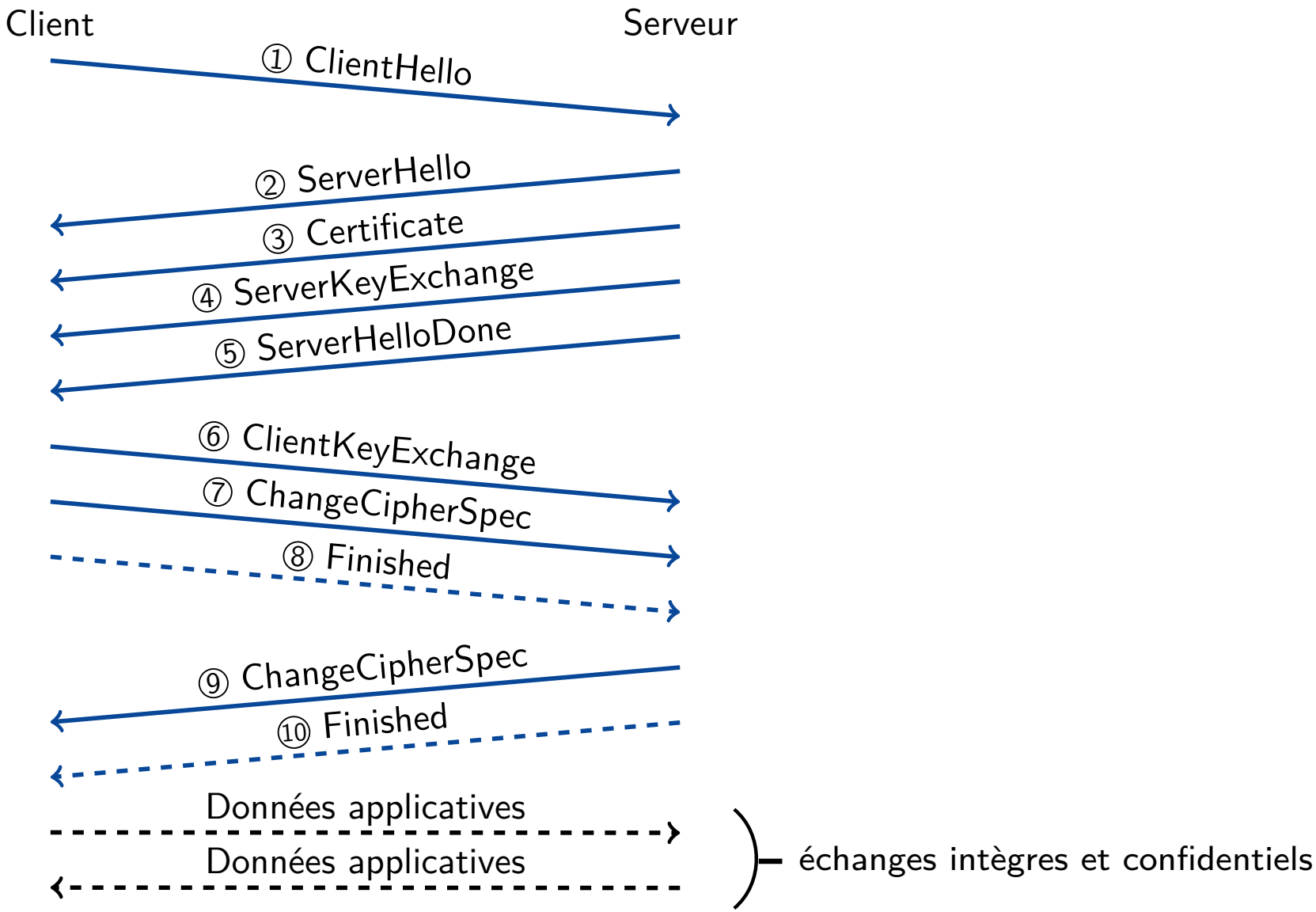




Négociation TLS



Négociation TLS



Principaux paramètres d'intérêt

			
Version	TLS 1.2	TLS 1.1, 1.0	SSLv3, SSLv2
Échange de clés	PFS (DHE, ECDHE)	sans PFS	anonyme
Chiffrement	AES	3DES	RC4
Motif d'intégrité	avec SHA-2	avec SHA-1	
Signature de certificat	avec SHA-2	avec SHA-1	avec MD5

Principaux paramètres d'intérêt

			
Version	TLS 1.2	TLS 1.1, 1.0	SSLv3, SSLv2
Échange de clés	PFS (DHE, ECDHE)	sans PFS	anonyme
Chiffrement	AES	3DES	RC4
Motif d'intégrité	avec SHA-2	avec SHA-1	
Signature de certificat	avec SHA-2	avec SHA-1	avec MD5

Méthodologie

Extraction des indicateurs pour un serveur

- ServerHello et Certificate du handshake ?
- Envoi d'un ClientHello (pas d'état à maintenir !)
- Ou plutôt plusieurs ClientHello
  - Différentes versions de protocole acceptées
  - Différentes suites cryptographiques acceptées
  - Au total, une dizaine de « stimulus » envoyés

Périmètre des mesures

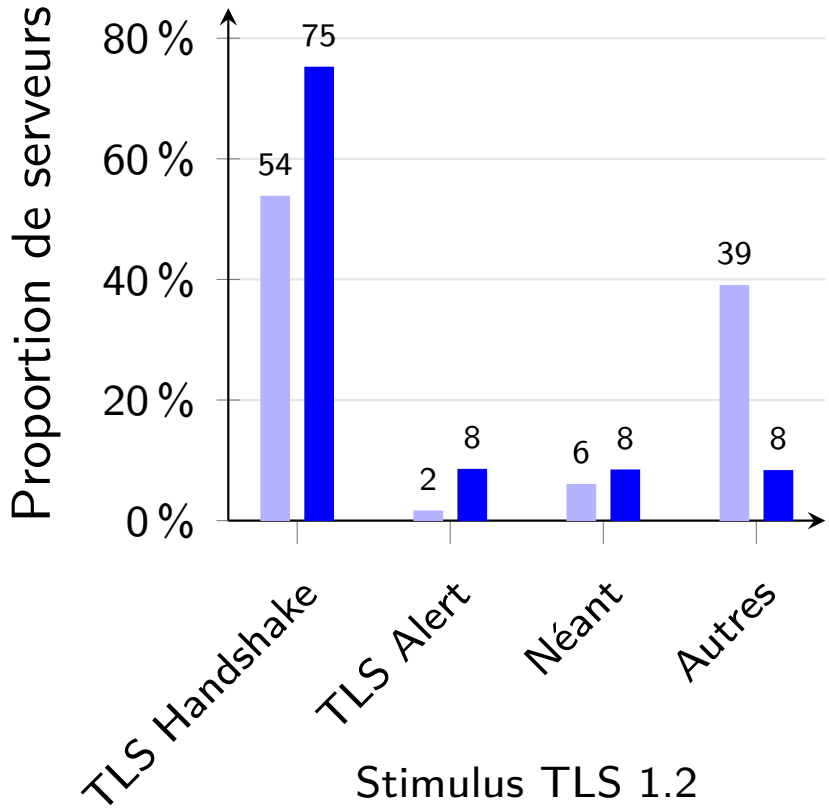
1. Extraction de la zone `.fr`
2. Ajout du préfixe `www.`
3. Résolution DNS
4. Randomisation des IP
5. Si le port 443 est ouvert :
6. Envoi des différents ClientHello

Traitement des données

- `parsifal`, un logiciel par Olivier Levillain :
  - parse les messages TLS bruts
  - isole les données notables
- Puis insertion en base SQL :
  - facilite l'historisation des différentes campagnes de mesure
  - facilite les requêtes d'agrégation et les statistiques

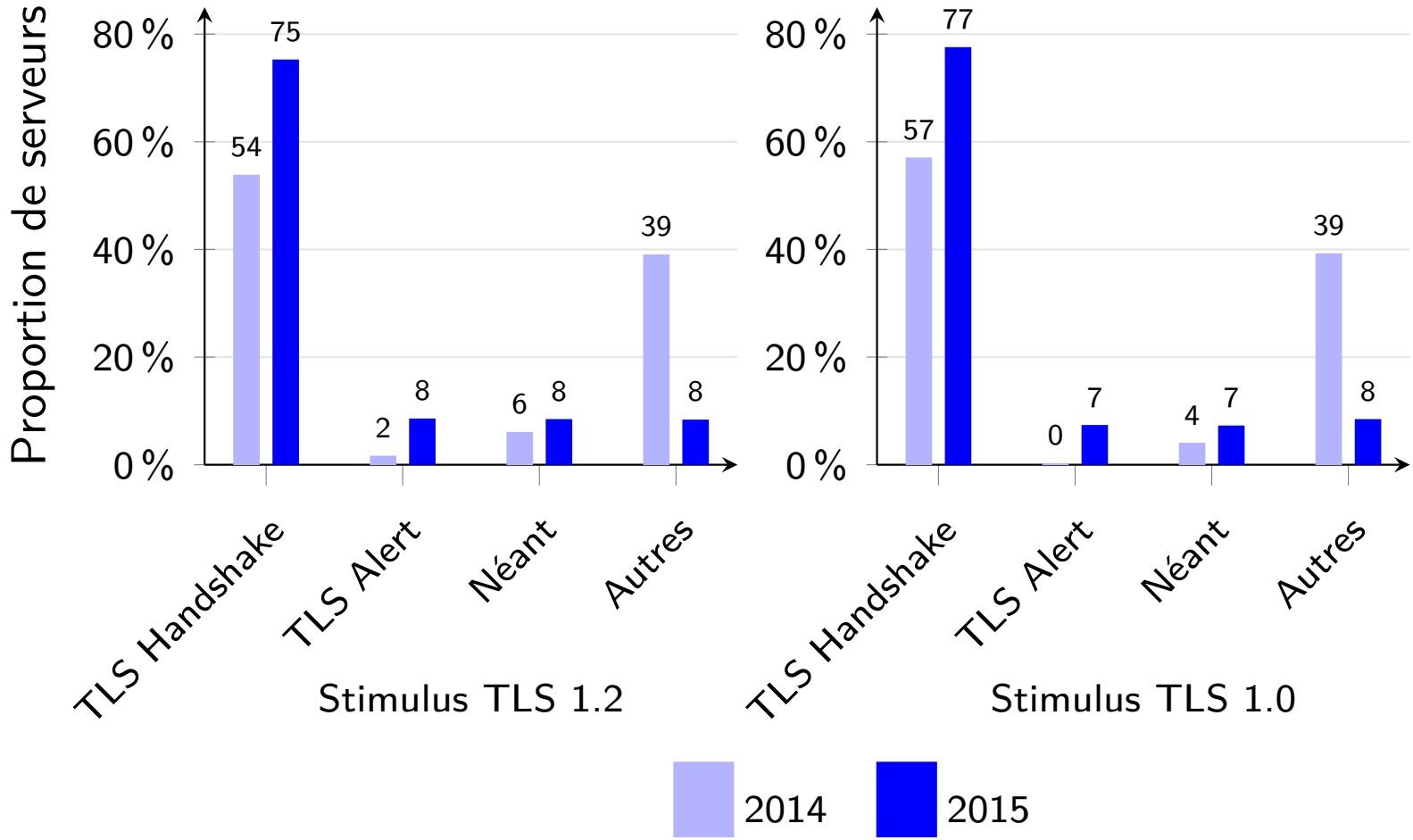
Résultats

TLS 1.2


Proportion de serveurs
80 %
60 %
40 %
20 %
0 %
75
54
8
2
8
6
39
8
TLS Handshake
TLS Alert
Néant
Autres
Stimulus TLS 1.2

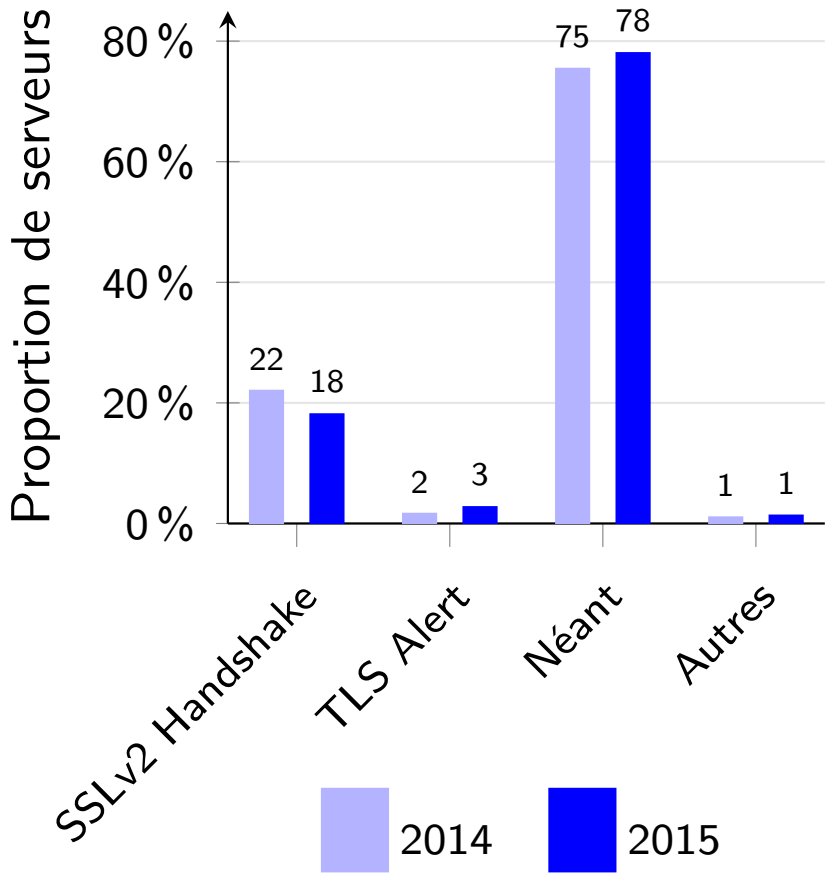

2014
2015

TLS 1.2



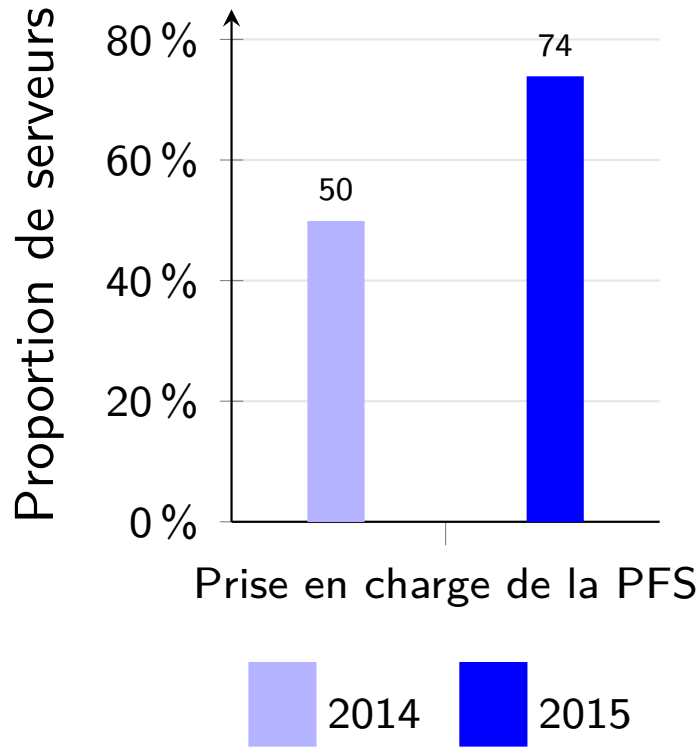
Les serveurs qui font du TLS 1.0 font aussi du TLS 1.2.

SSLv2



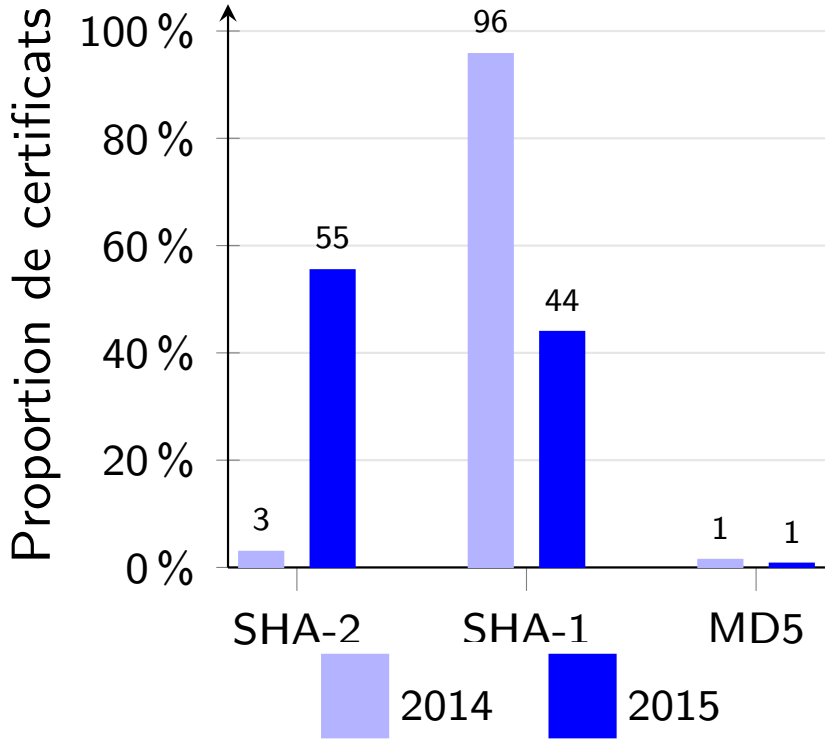
Un serveur sur cinq persiste à faire du SSLv2.

Confidentialité persistante (PFS)



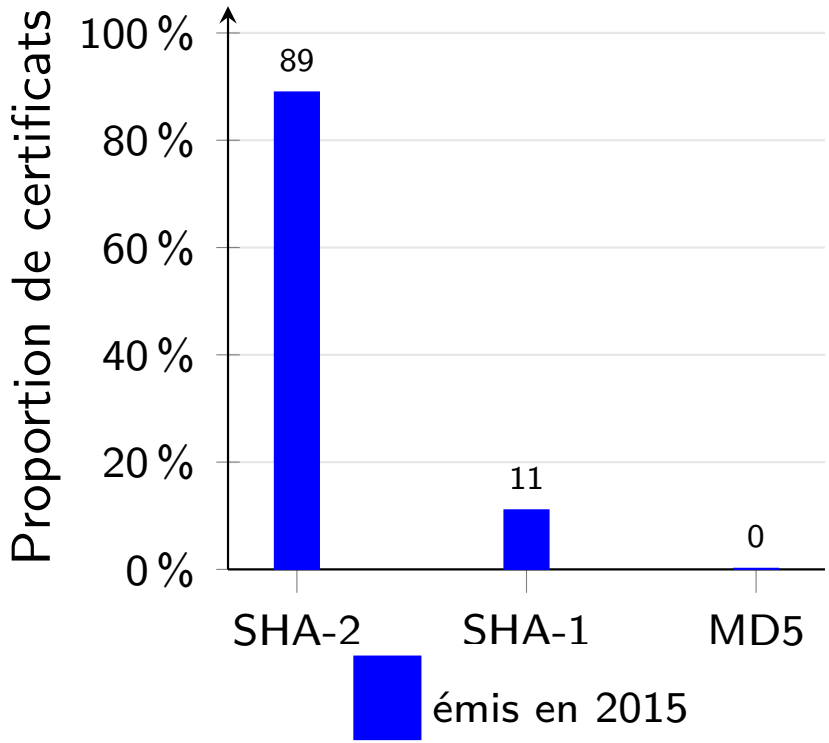
Une large majorité de serveurs offre la possibilité de PFS.

Signatures des certificats



Mi-2015, la moitié des certificats restait signée avec SHA-1.

Signatures des certificats



L'essentiel des nouveaux certificats est bien signé avec SHA-2.

Conclusion

Conclusion

- Nombreux paramètres à observer pour juger d'un serveur TLS
- SSLv2 persiste alors qu'il faut l'abandonner (comme SSLv3)
- TLS 1.2, DHE et les signatures SHA-2 se répandent bien

Perspectives

- Automatisation des mesures
- Prise en charge précise des suites cryptographiques
- Guide de recommandations de sécurité pour TLS
- Reversement Scapy-TLS

Questions ?

http://www.ssi.gouv.fr/observatoire/
rapport.observatoire@ssi.gouv.fr