Mesures HTTPS : compatibilité TLS et conformité des certificats

Maxence Tury
maxence.tury@ssi.gouv.fr

Agence nationale de la sécurité des systèmes d'information

23 novembre 2016

L'observatoire de la résilience de l'Internet français

Objectifs de l'observatoire

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

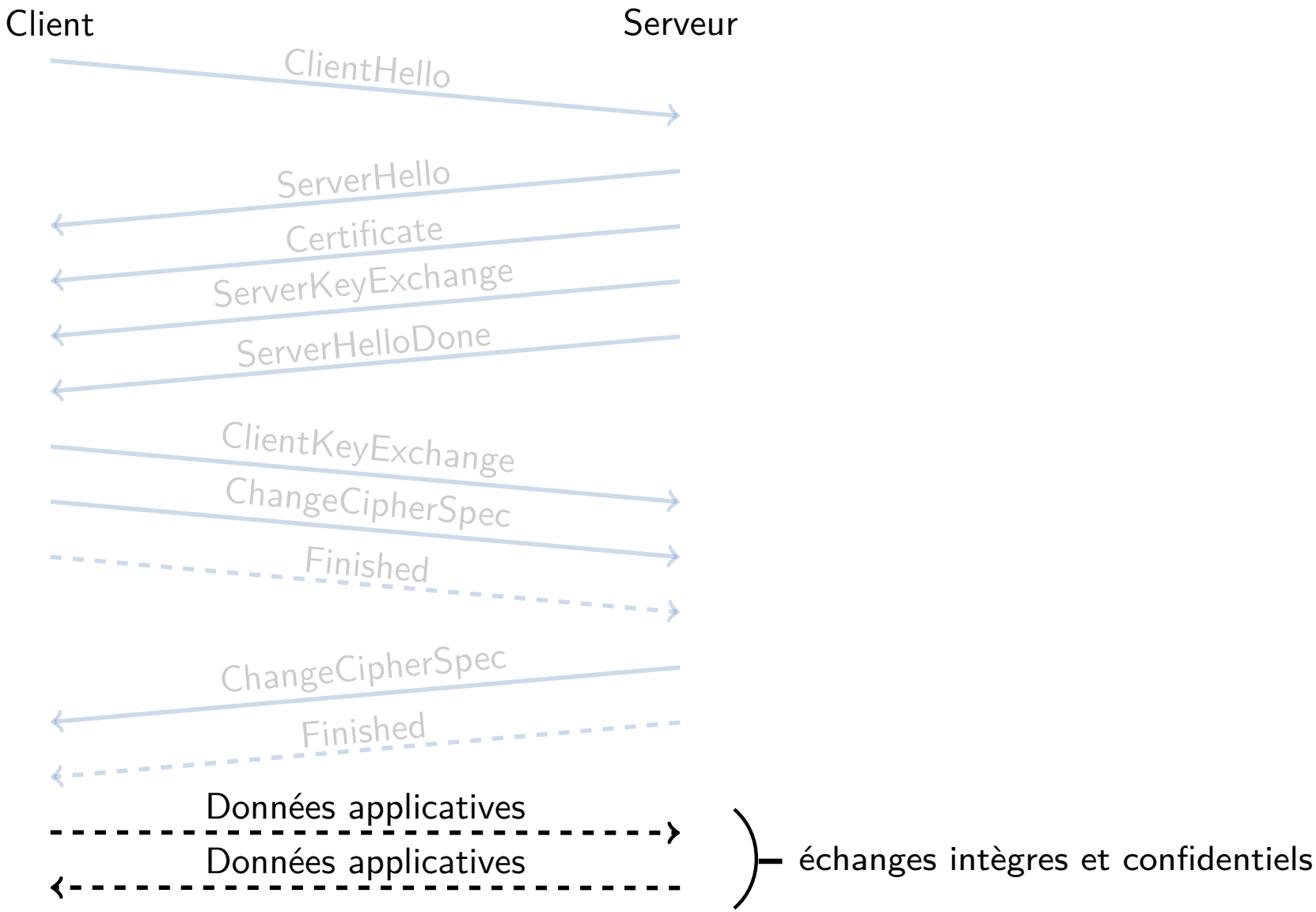
Trois protocoles étudiés

- BGP
- DNS
- TLS

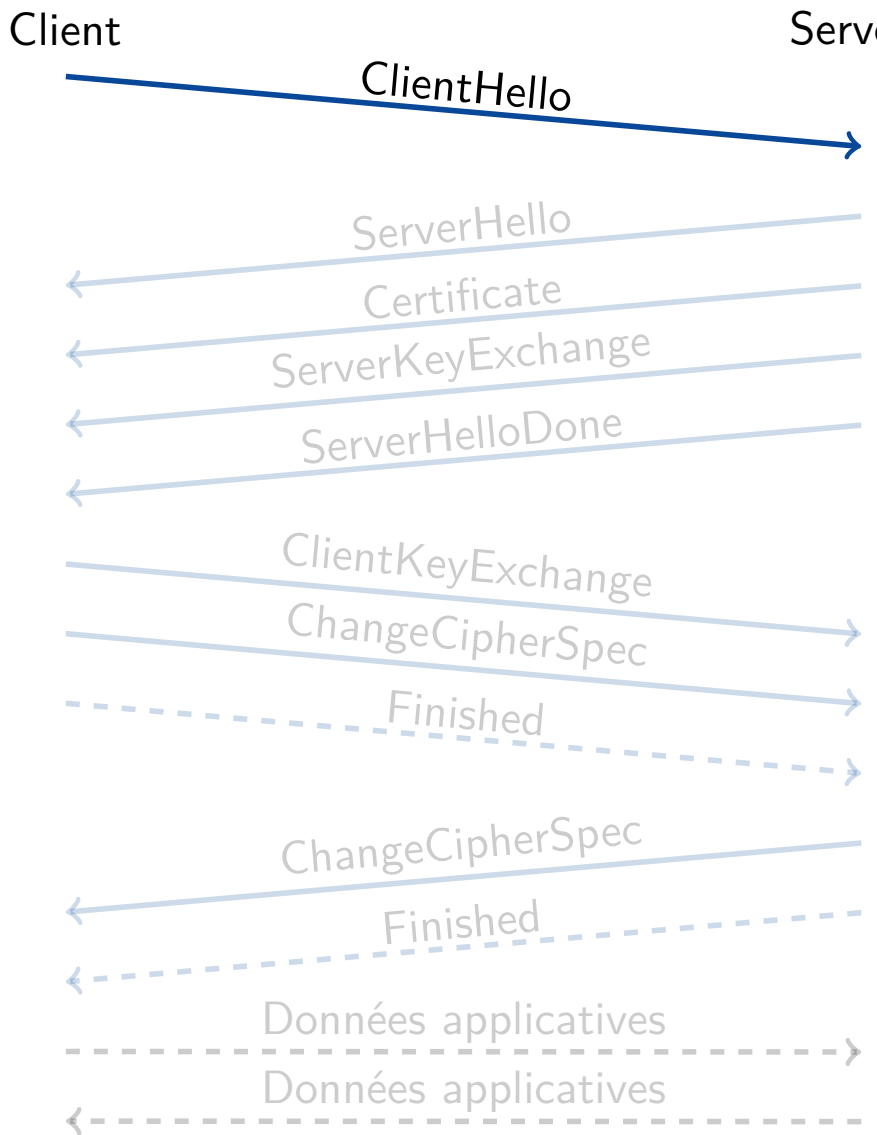
https://www.ssi.gouv.fr/observatoire/

Serveurs SSL/TLS : que veut-on mesurer ?

Négociation TLS

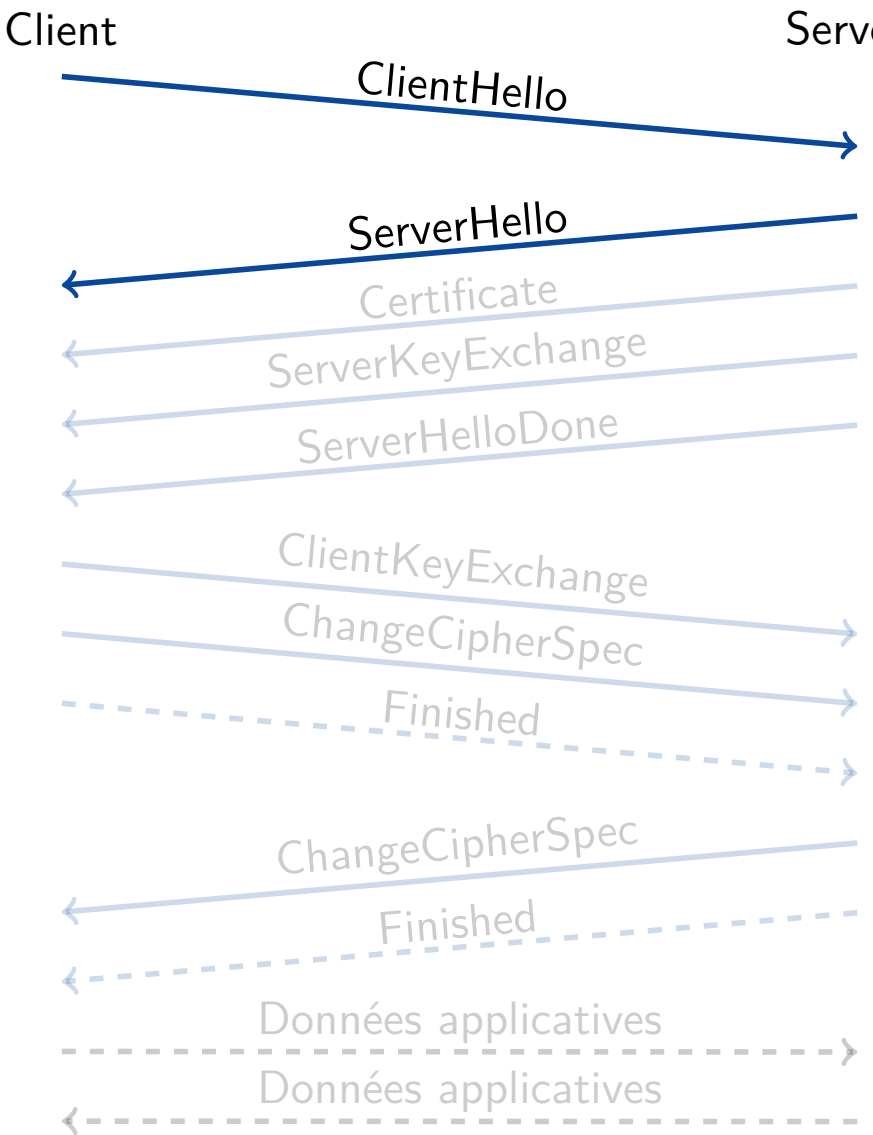


Négociation TLS



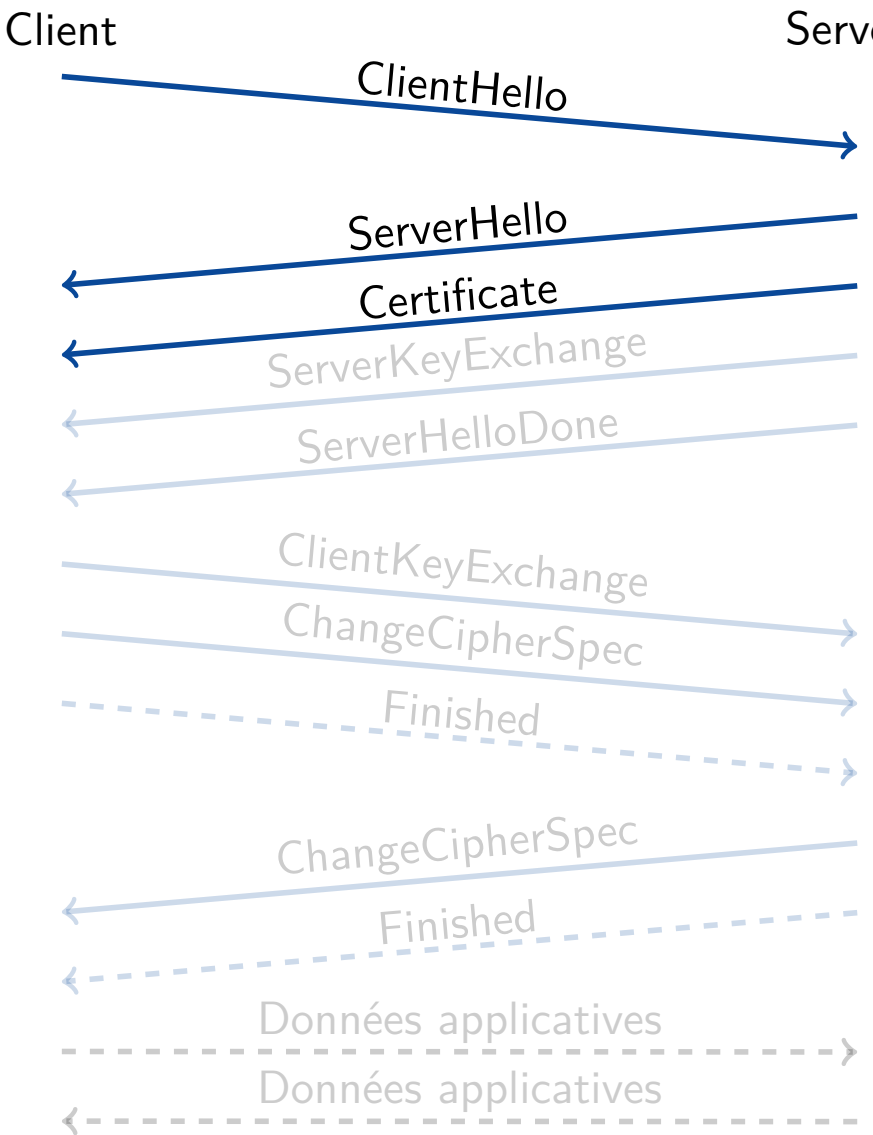

```
###[ TLS Handshake - Client Hello ]###
  msgtype    = client_hello
  msglen     = 88
  version    = TLSv1.2
  gmt_unix_time= Thu, 26 Apr 1979 07:58:23 +0000 (293961503)
  random_bytes= dce3af01fe96ab59d017faac0740083a46259789a744a339d27f6e8b
  sidlen     = 0
  sid        = ''
  cipherslen= 8
  ciphers    = [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

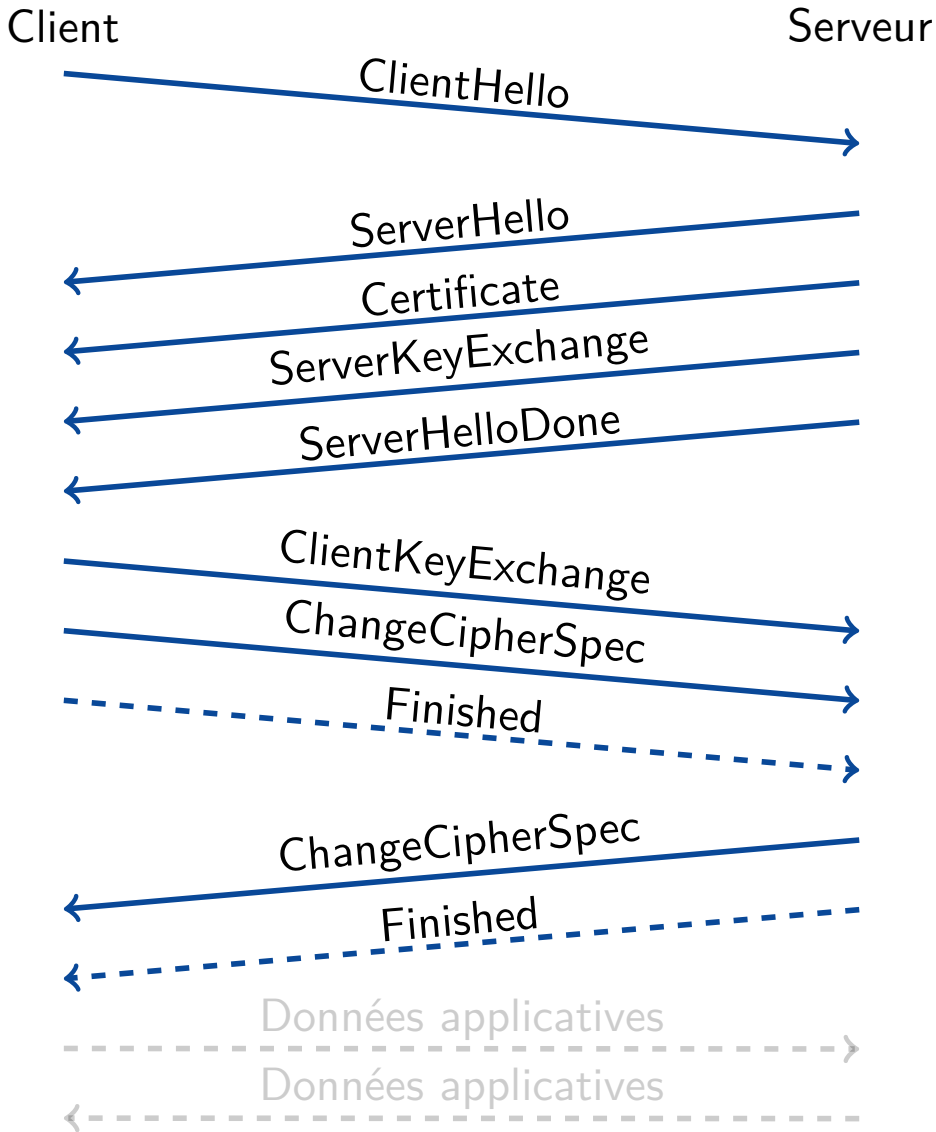



```
###[ TLS Handshake - Server Hello ]###
  msgtype    = server_hello
  msglen     = 76
  version    = TLSv1.2
  gmt_unix_time= Thu, 30 Jun 2016 15:59:34 +0000 (1467302374)
  random_bytes= 9fe47d74a5ca5b332d6ca9e2b198d37cd5450fbb278994a7d11ee7ef
  sidlen     = 32
  sid        = 067c12c1e5ce13c7d7c03fcaa7b7bd6a34983528a6374b50d8838788763f82a4
  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\
```

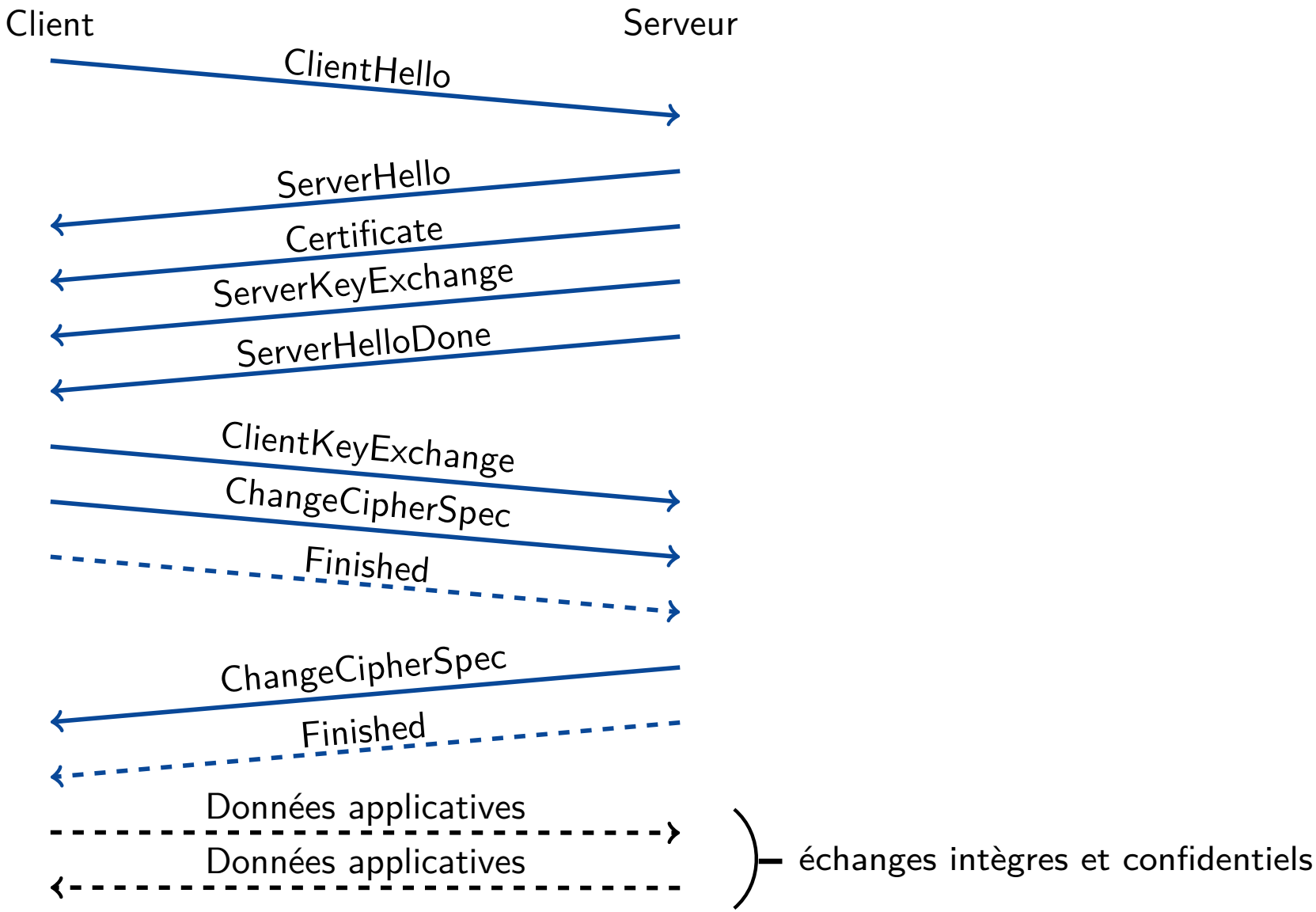
Négociation TLS



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

Voir le guide de l'ANSSI « **Recommandations de sécurité relatives à TLS** »
https://www.ssi.gouv.fr/nt-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

Voir le guide de l'ANSSI « **Recommandations de sécurité relatives à TLS** »
https://www.ssi.gouv.fr/nt-tls/

Méthodologie

Extraction des indicateurs pour un serveur

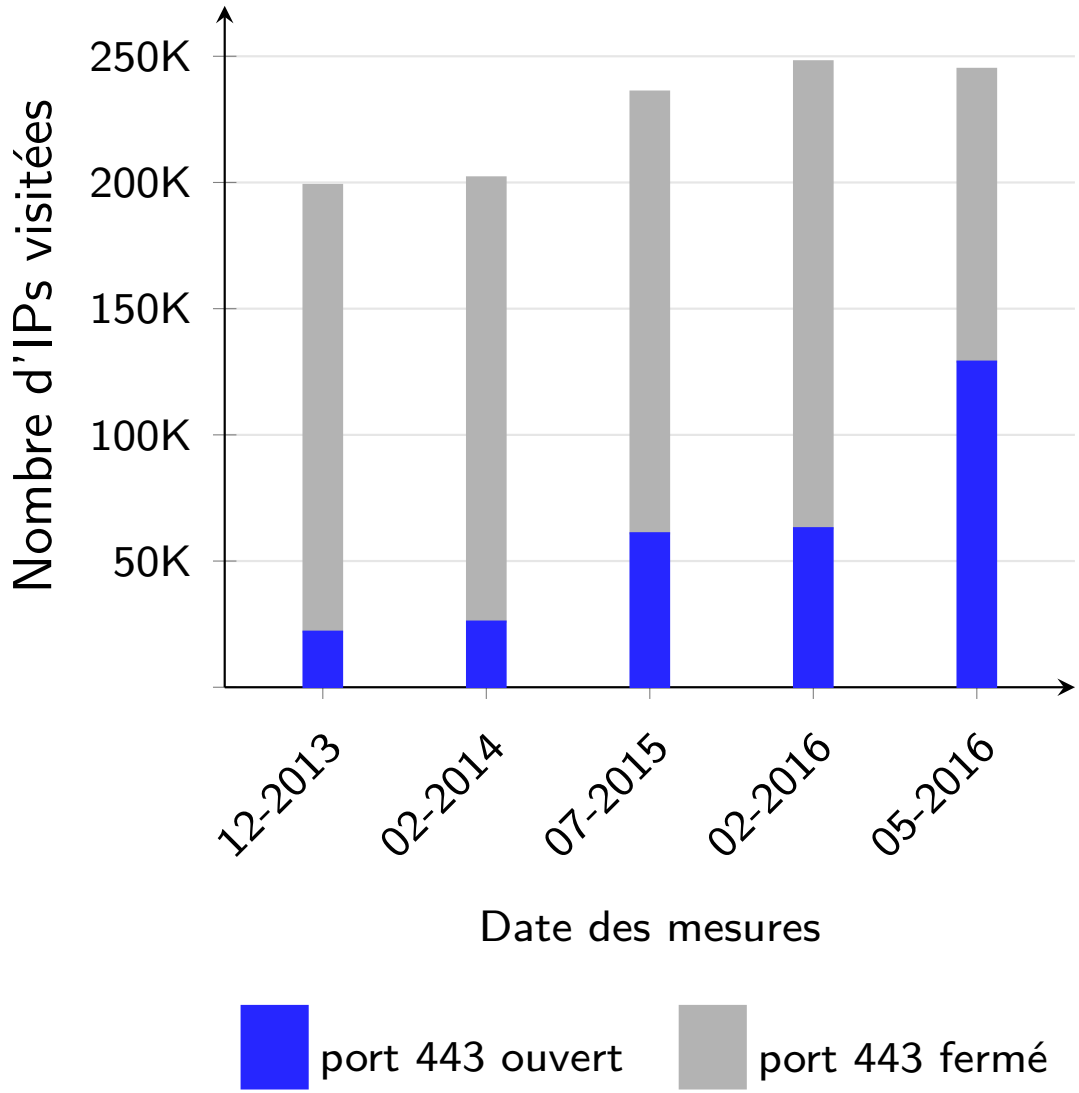
- ServerHello et Certificate du handshake ?
- Envoi d'un ClientHello (pas d'état à maintenir !)
- Ou plutôt plusieurs ClientHello
  - Chaque ClientHello teste une seule version et une seule suite
  - Au total, une dizaine de « stimulus » envoyés par serveur

Périmètre des mesures

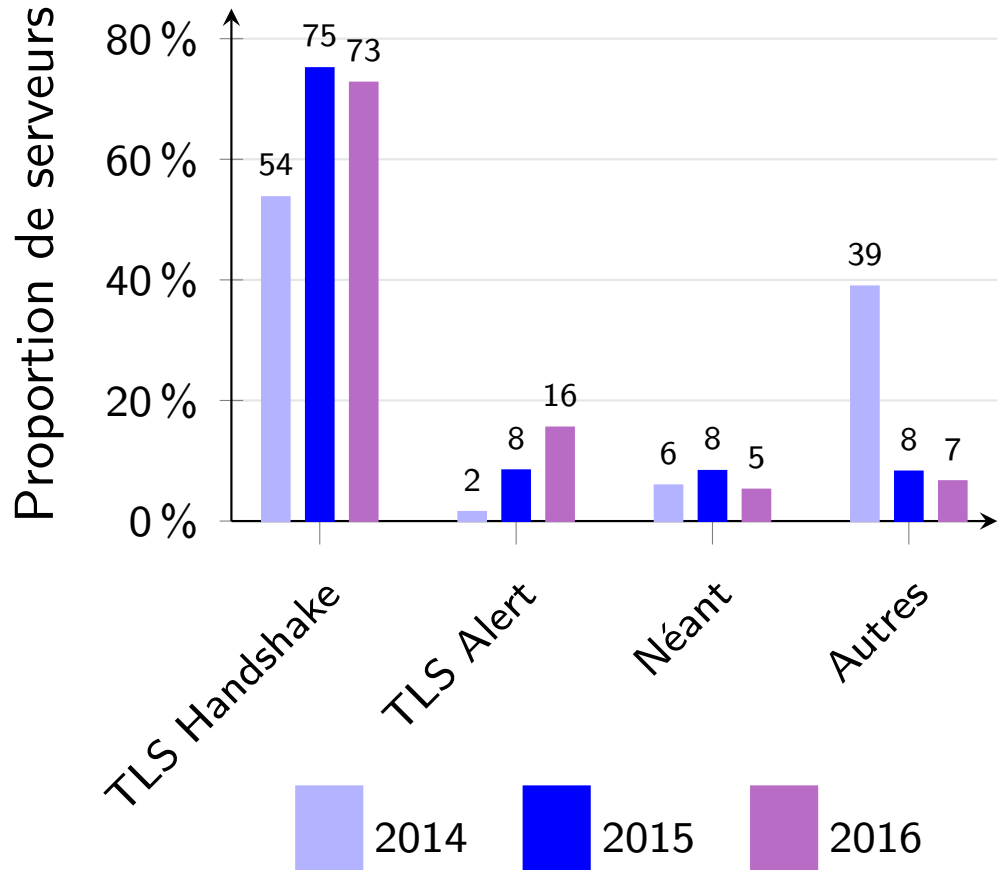
1. Extraction de la zone `.fr`
2. Résolution DNS
3. Suppression des IP redondantes, puis randomisation
4. Test d'ouverture du port 443
5. Envoi des différents ClientHello

Résultats

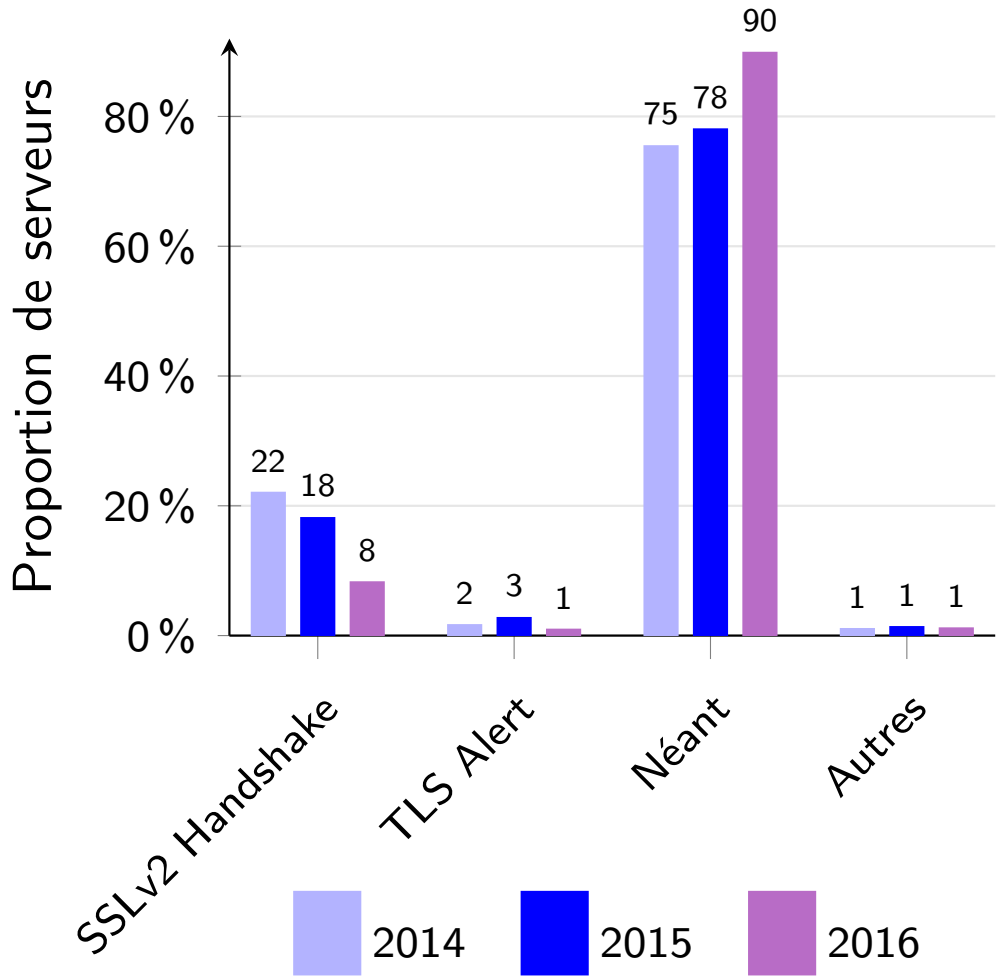
Quantification du périmètre de mesures



Réponses au stimulus TLS 1.2

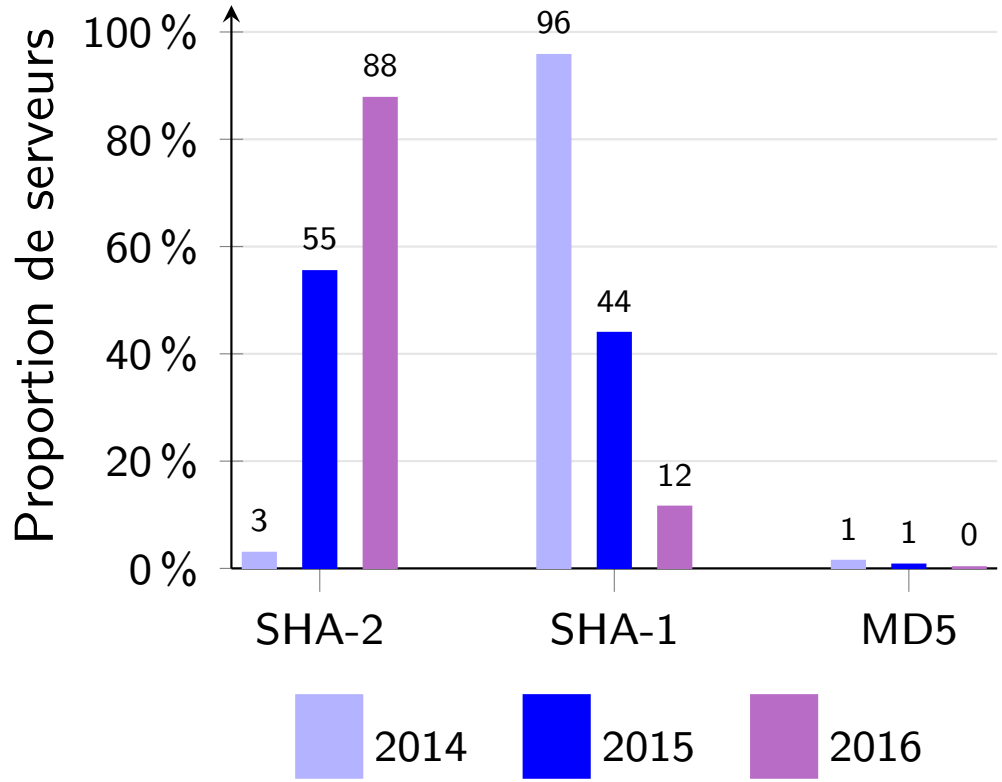


Réponses au stimulus SSLv2



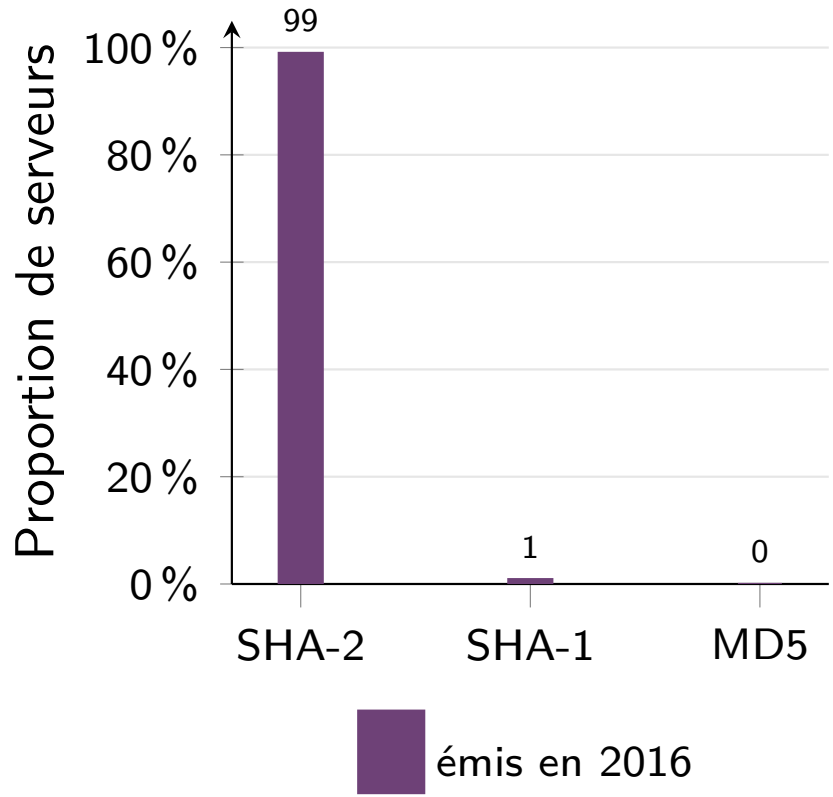
SSLv2 persiste sur les déploiements existants.
Cette version doit être abandonnée —de même que SSLv3.

Signatures des certificats



Les signatures exploitant SHA-1 sont bien en cours de disparition.

Signature des *nouveaux* certificats



Presque tous les nouveaux certificats sont bien signés avec SHA-2.

Perspectives – Nouvelle méthodologie

1. Extraction de la zone `.fr`
2. Résolution DNS
3. **Évaluation du nombre de domaines hébergés par IP**
   - si 100+ domaines : sélection d'un échantillon aléatoire
4. Test d'ouverture du port 443
5. **Insertion du nom de domaine dans chaque ClientHello**
6. Envoi des différents ClientHello

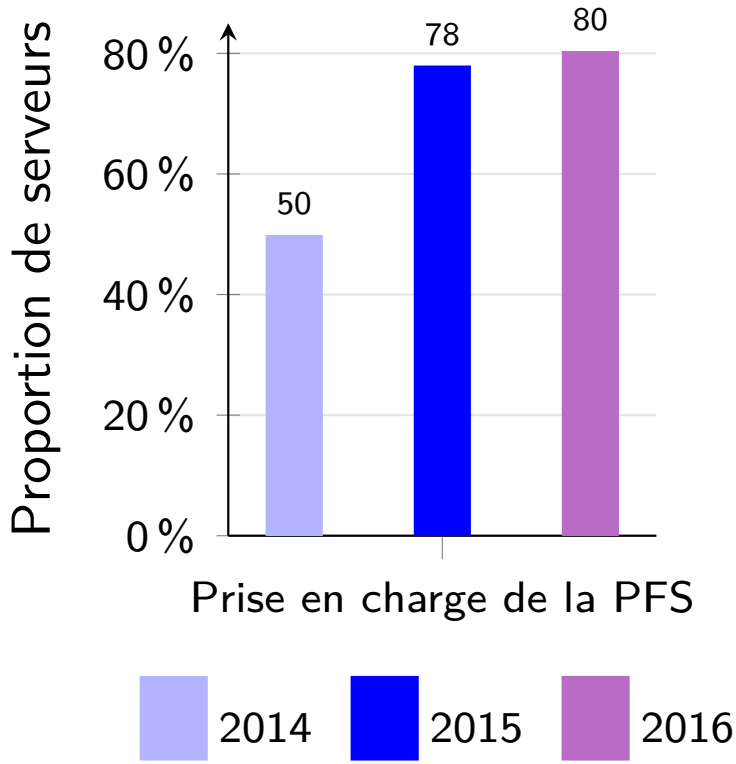
Conclusion

- Observations
  - SSLv2 et SSLv3 persistent encore
  - TLS 1.2 et SHA-2 sont largement répandus
- Recommandations
  - Vérifier que TLS 1.2 est prioritaire
  - Interdire l'utilisation de SSLv2 et SSLv3
  - Déployer des certificats signés avec SHA-2

Questions ?

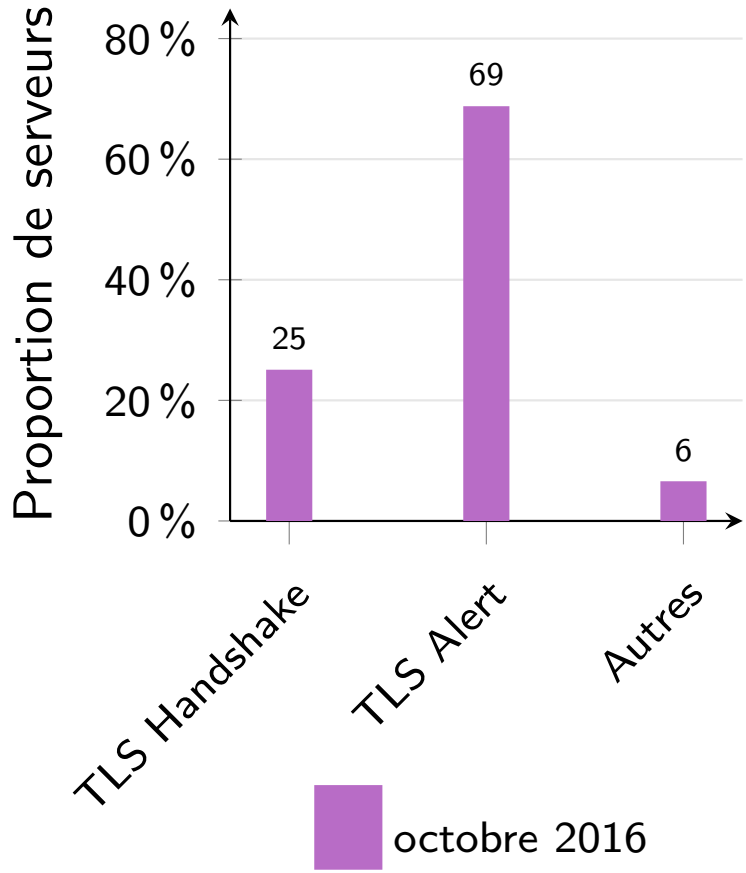
https://www.ssi.gouv.fr/nt-tls/
https://www.ssi.gouv.fr/observatoire/
rapport.observatoire@ssi.gouv.fr

Confidentialité persistante (PFS)



Parmi les serveurs permettant un handshake, la PFS stagne.

SSLv3


Proportion de serveurs
80 %
60 %
40 %
20 %
0 %
25
69
6
TLS Handshake
TLS Alert
Autres
octobre 2016

Mutualisation