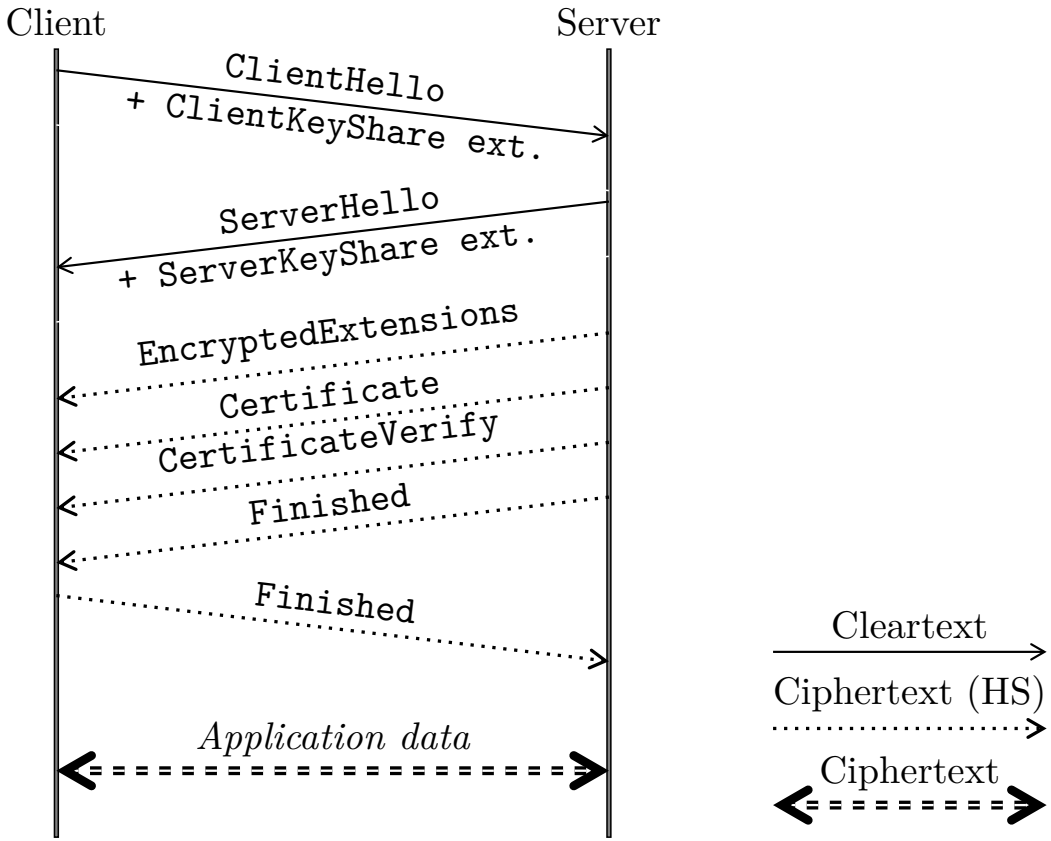
Analyse de l'implémentation d'un client TLS 1.3 en utilisant l'algorithme L ∗

Aina Toky Rasoamanana, Olivier Levillain

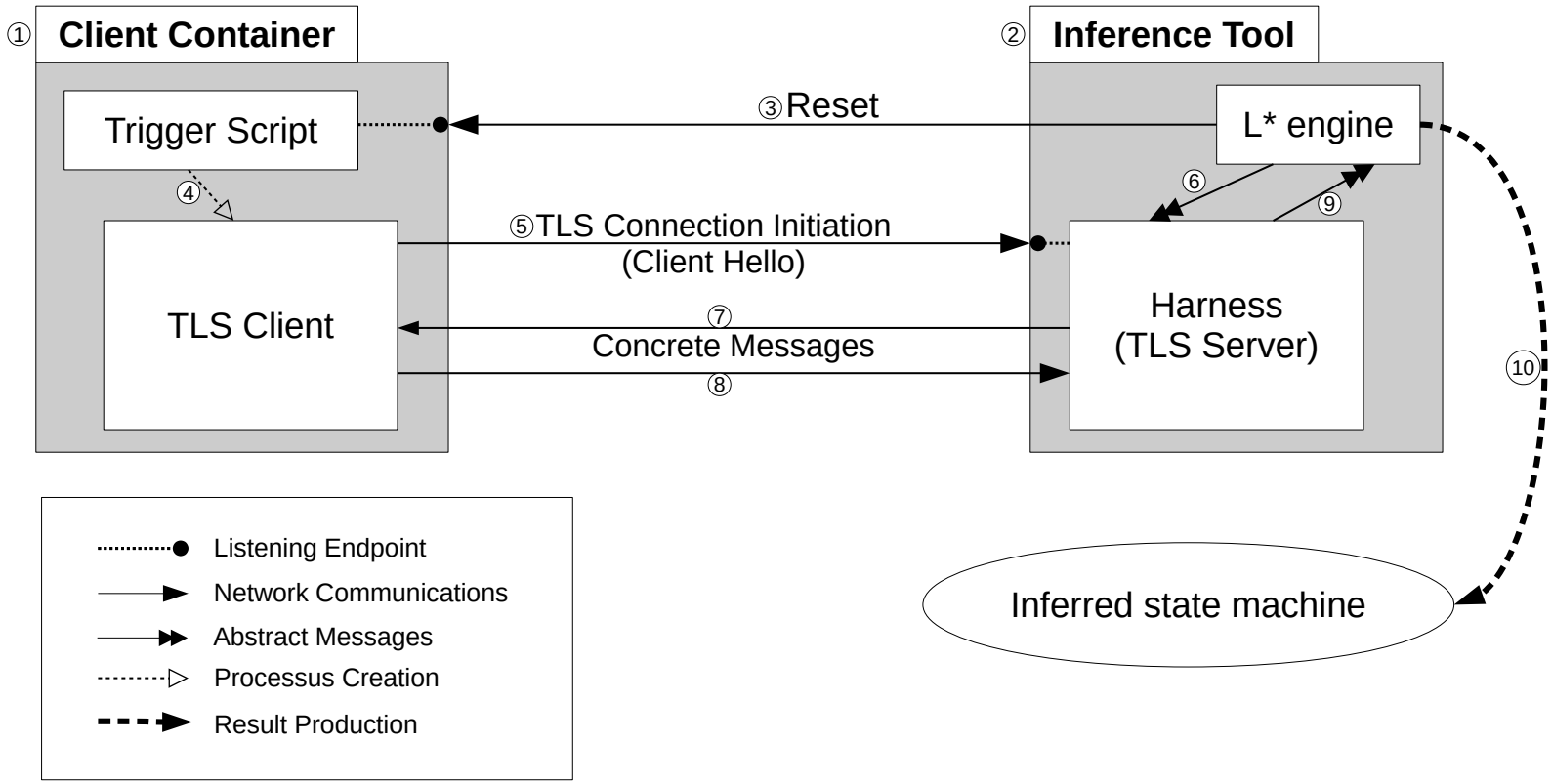
Département Réseaux et Services de Télécom
Télecom SudParis

11 mai 2021

Handshake protocol TLS 1.3



Architecture et algorithme L*



Méthodologie

- Vocabulaire utilisé :
  - les messages necessaires en mode normal (happy path)
  - `EmptyCertificate`, `ChangeCipherSpec`, `HelloRetryRequest`, message d'erreur non fatal

- Pile testée :
  - wolfSSL [1] : « Over 2 Billion applications and devices are secured with wolfSSL products. »

1. `https://www.wolfssl.com/`

Reproduction : CVE-2020-24613 et CVE-2020-12457

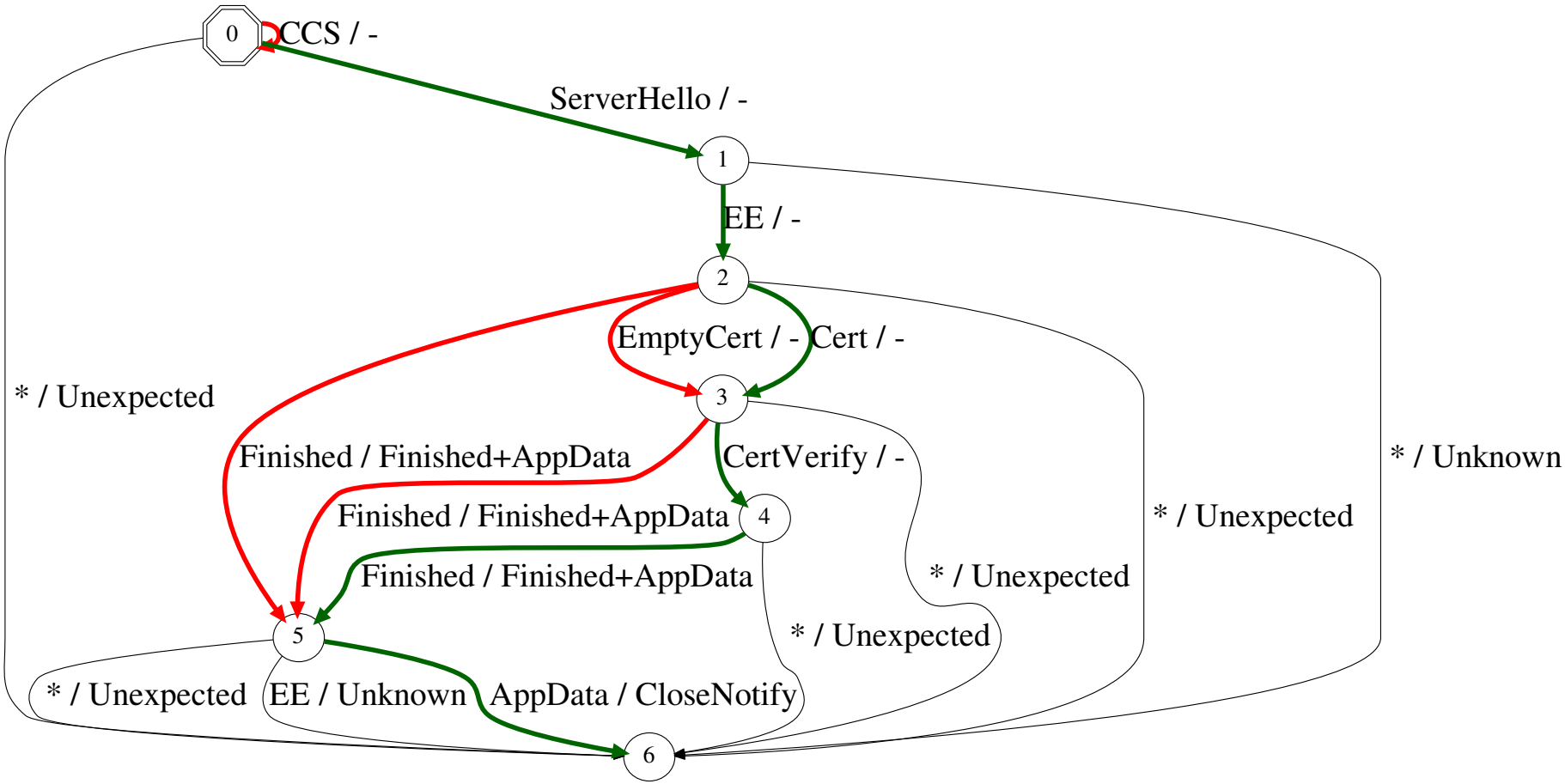


Figure – wolfSSL v4.4.0

Nouveau bug trouvé (CVE-2021-3336)

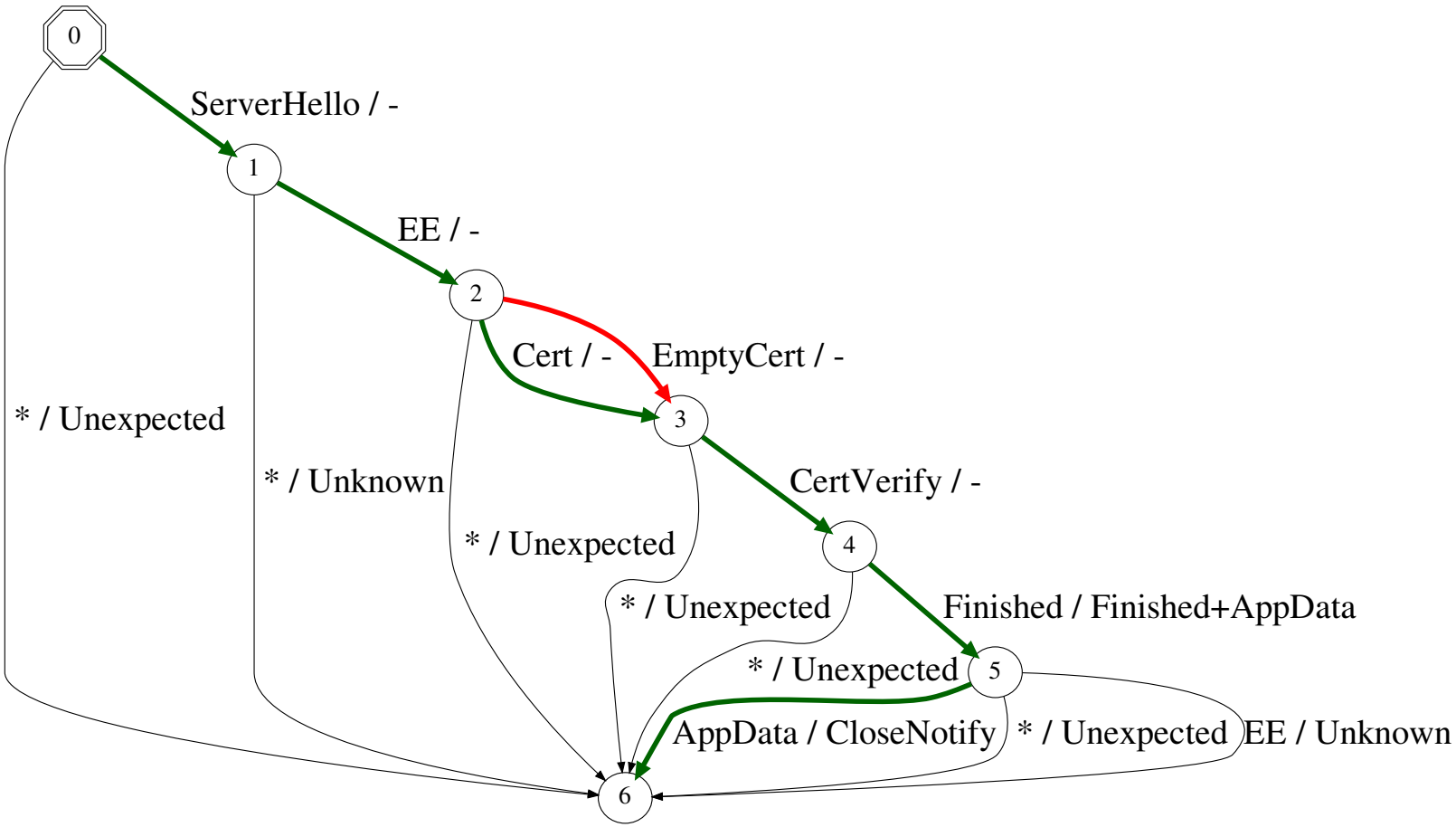


Figure – wolfSSL v4.6.0

Conclusion

- Reproduction des bugs : CVE-2020-24613 et CVE-2020-12457
- Nouveau bug affectant toutes les versions wolfSSL antérieures à 4.6.0

- Réflechir sur différents messages qui peuvent mener à un court-circuit/boucle
- Analyser de manière systèmatique des piles TLS

Merci pour votre attention !

OpenSSL 1.1.1j