

A Generic Approach to Secure Network Protocols

GASP

anr ©
agence nationale
de la recherche

Appel : AAPG

Année : 2019

Instrument : JCJC

Contact :

olivier.levillain@telecom-sudparis.eu

COORDINATEUR : Olivier Levillain

PARTENAIRES
Télécom SudParis

Résumé (3 lignes max) :

Les protocoles réseau sont omniprésents dans nos échanges quotidiens. Les vulnérabilités affectant ces briques de base de nos systèmes peuvent avoir des conséquences graves (p. ex. Heartbleed, FREAK). Pour améliorer leur sécurité, GASP vise à automatiser l'implémentation et l'évaluation des piles protocolaires.

CONTEXTE ET OBJECTIFS

Les protocoles réseau d'aujourd'hui sont omniprésents et d'une grande complexité. Il est donc compliqué de les implémenter de manière fiable et sécurisée.

Exemple de vulnérabilités liées aux implémentations TLS

- Heartbleed (divulgaration d'informations sensibles) ;
- FREAK (vulnérabilité de la machine à états) ;
- Berserk (usurpation serveur via des signatures contrefaites).

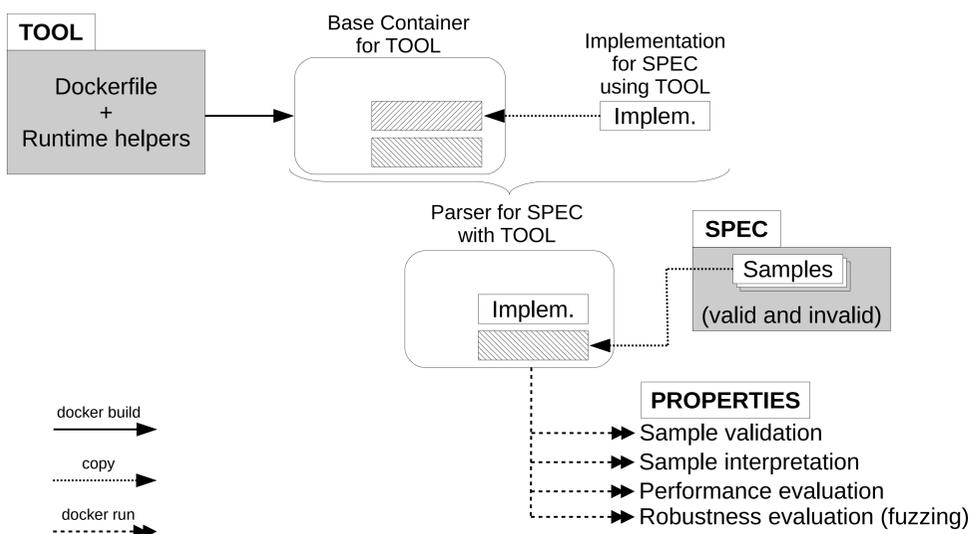
GASP propose trois axes pour améliorer cette situation

- La génération automatique des *parsers* à partir d'une description dans un langage dédié (DSL) ;
- La génération automatique d'implémentations à partir d'une description dans un langage dédié ;
- L'analyse en boîte noire d'implémentations existantes pour détecter des défauts dans les machines à état.

MÉTHODOLOGIE ET RÉSULTATS

Étude des générateurs de *parsers* à l'aide d'une plateforme comparant l'expressivité, la robustesse et la performance.

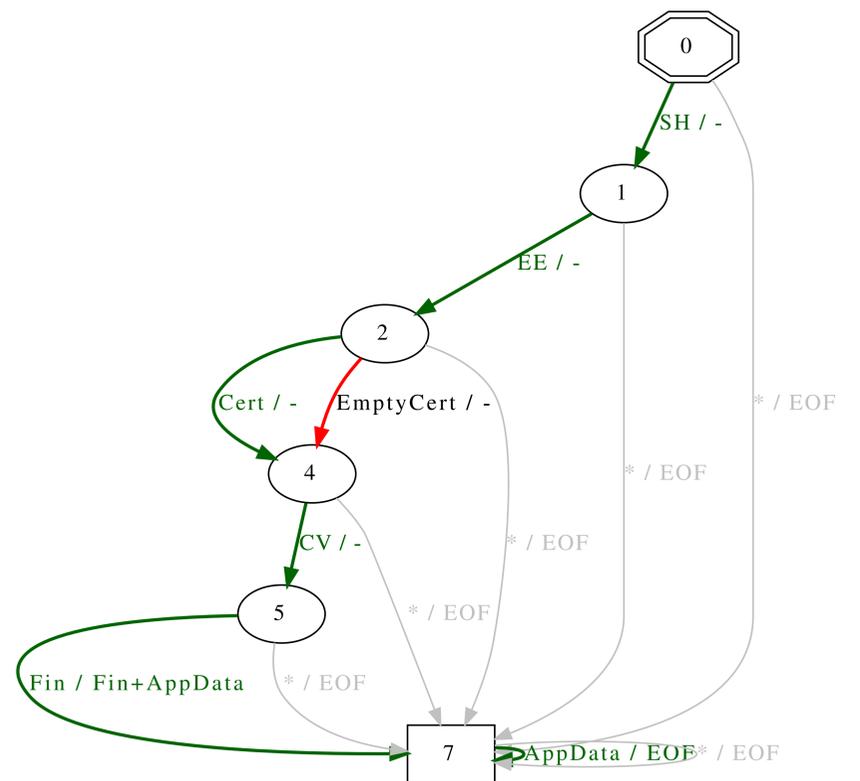
Langsec-PF est une plateforme intégrant des outils (Hammer, Kaitai-Struct, Nail, Nom, Parsifal) via des conteneurs Docker.



Analyse des machines à états par inférence en boîte noire d'implémentations existantes, avec application à TLS et SSH

TLS Inferer est un outil pour inférer la machine à état d'implémentations en utilisant l'algorithme L*.

Exemple de vulnérabilité mise au jour dans wolfssl (CVE-2021-3336) : contournement de l'authentification serveur dans les clients TLS 1.3.



La figure décrit la machine à état du client TLS 1.3 de wolfssl (versions antérieures à 4.7). La transition en rouge, suivie d'un message CV (CertificateVerify) arbitraire, permet à un attaquant de contourner l'authentification du serveur.

Publication prochaine de l'outil
Soumission des résultats en cours

Travaux à venir sur la génération d'implémentations, par généralisation des travaux sur TLS et SSH.

Dépôt : <https://gitlab.com/pictyeye/langsec-pf> (logiciel libre)

Publication : Naud, Levillain et Rasoamanana - *Towards a Platform to Compare Binary Parser Generators* - LangSec 2021



25 et 26
JANVIER

2022



UNIVERSITÉ DE BORDEAUX