Cryptosense

Romain Bardou

28 avril 2014

Cryptosense Analyzer

découverte automatique de failles de sécurité dans les appareils de gestion des clés cryptographiques

Motivation

recherche de failles de sécurité

à la main	Cryptosense Analyzer
requiert de l'expertise	presse-bouton
long	rapide
non-exhaustif	exhaustif

Idée générale

simuler un attaquant *raisonnable*
(sans faire de fuzzing)

- peut exécuter les commandes de l'API
- peut chiffrer et déchiffrer s'il connaît la clé
- peut utiliser ses propres clés

inspiré du modèle de Dolev-Yao

APIs de gestion des clés cryptographiques

HSMs : ordinateurs blindés pour :

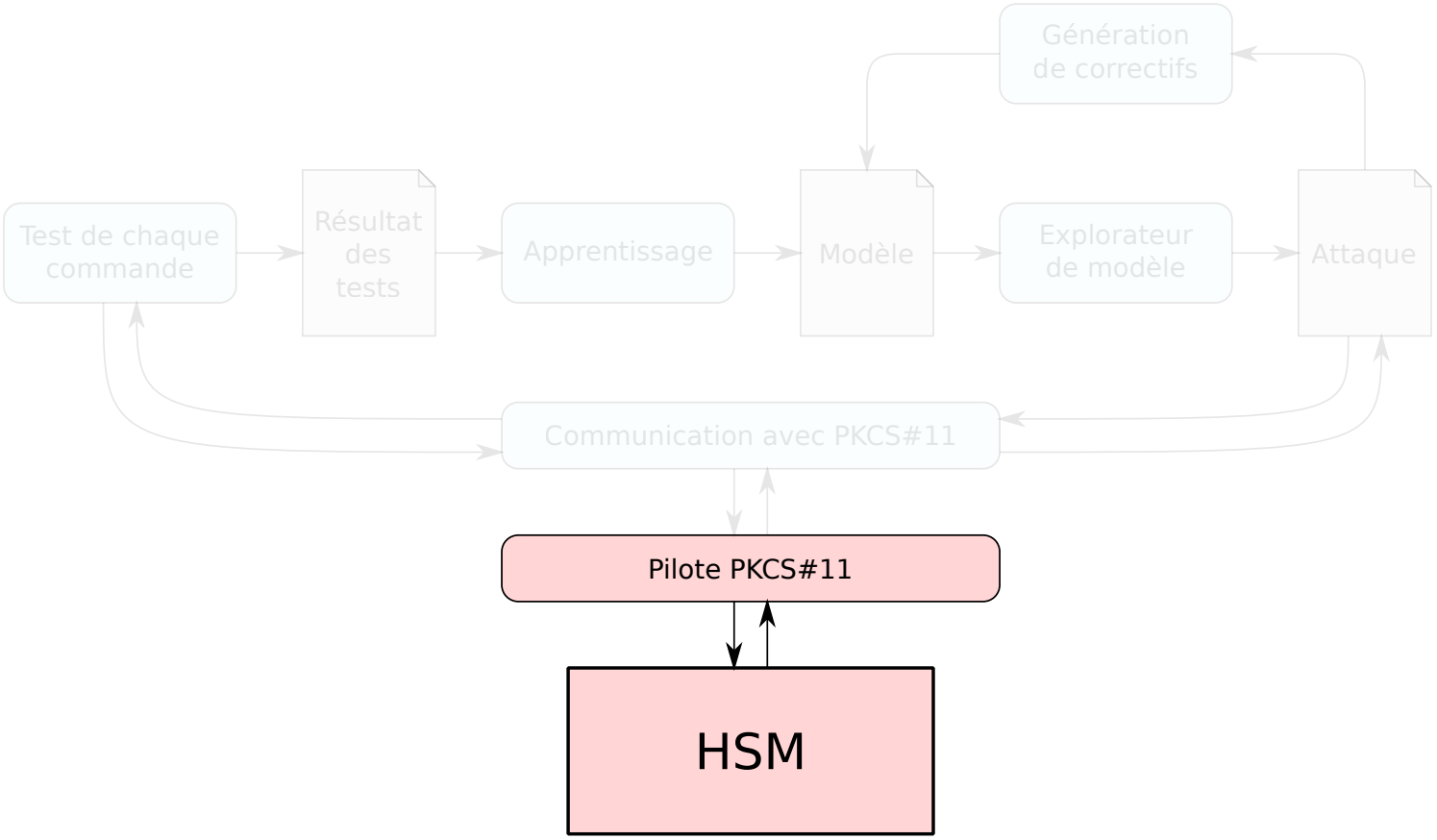
- générer des clés cryptographiques
- chiffrer / déchiffrer des données (e.g. codes PINs)
- exporter / importer ces clés (chiffrées)
- ...

clés sensibles jamais visibles en clair hors de l'appareil

utilisés notamment par les banques

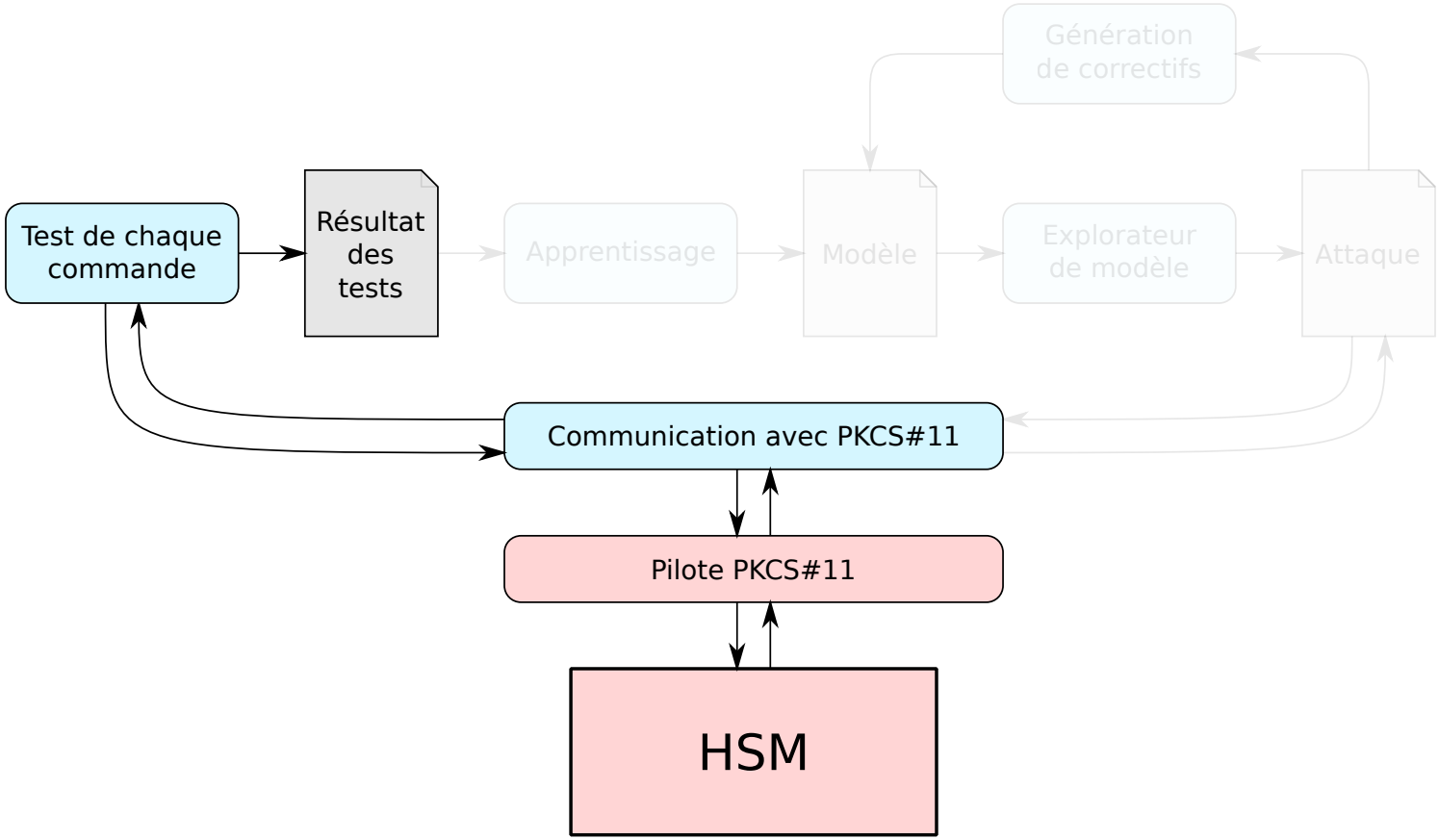
Hardware Security Modules (HSMs)

HSM = hardware + firmware + pilote + configuration
$\Rightarrow$ chaque HSM est unique



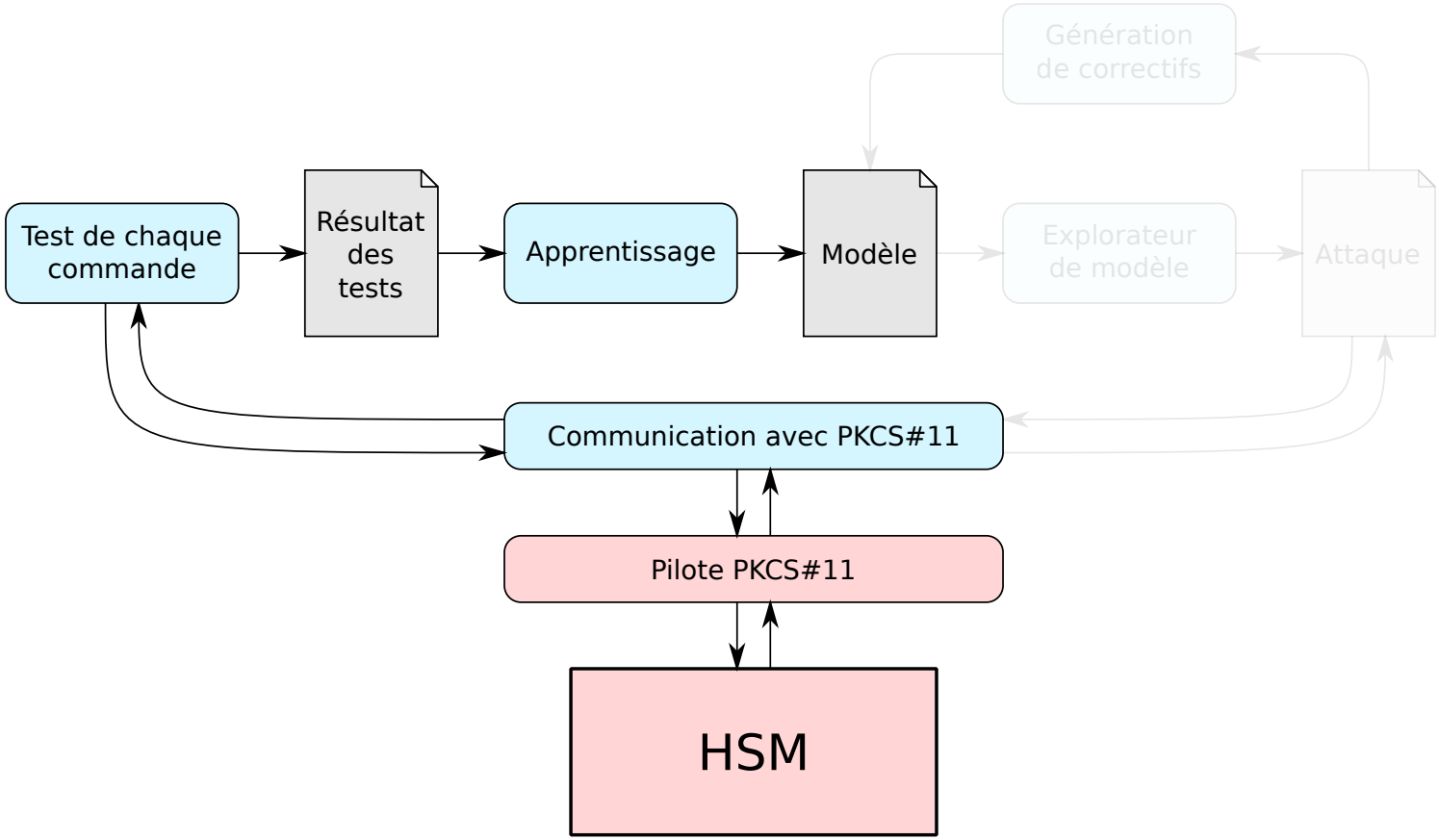
Comment ça marche ?

test d'un grand nombre d'instances de chaque commande de l'API



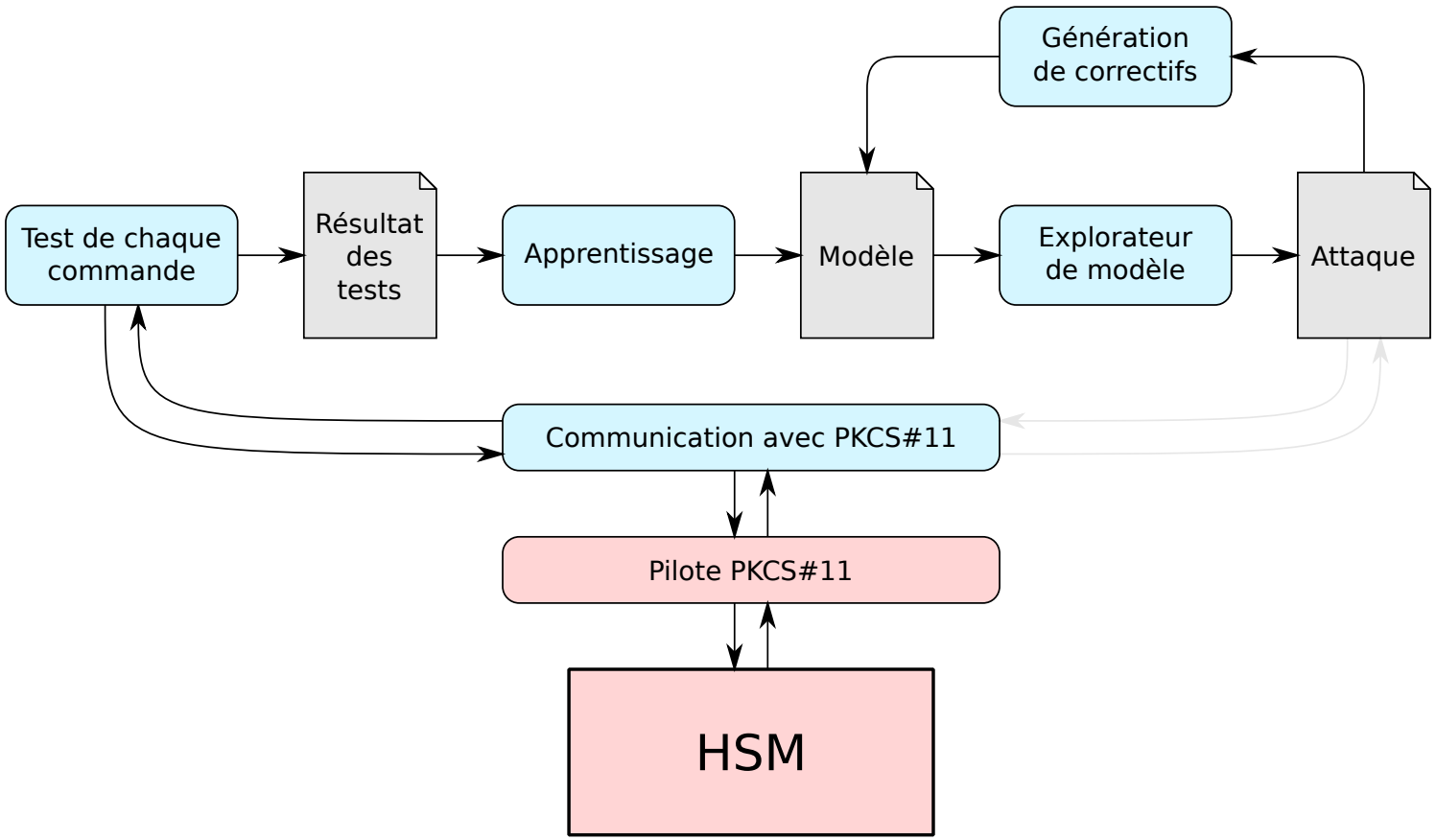
Comment ça marche ?

apprentissage du comportement de l'appareil cryptographique pour obtenir un modèle



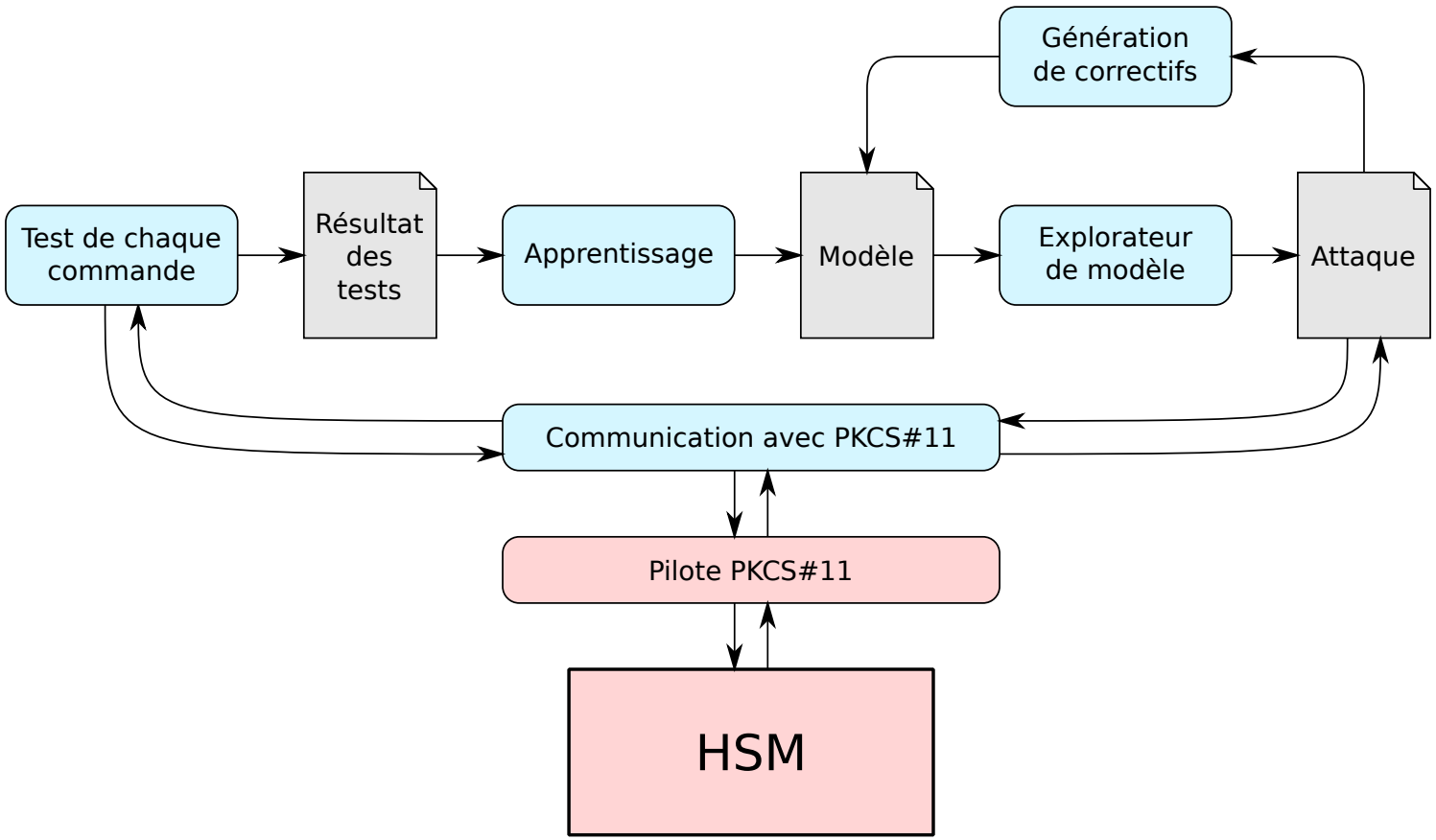
Comment ça marche ?

recherche de séquences de commandes compromettant des clés cryptographiques dans le modèle



Comment ça marche ?

exécution des attaques pour éliminer les faux positifs et génération d'un rapport de vulnérabilités

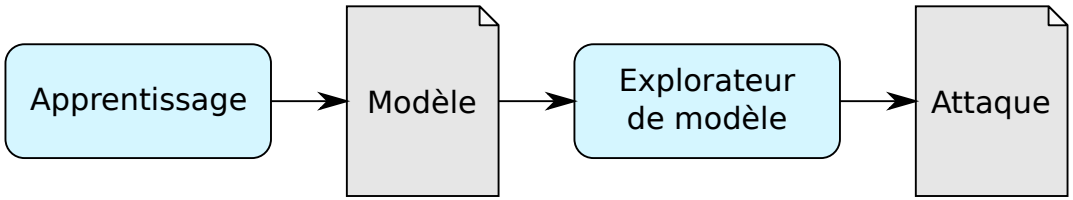


Conclusion

cœur de notre technologie :

- apprentissage
- exploration de modèles (*model-checking*)

en OCaml



`http://cryptosense.com`