Attestation à distance de microprocesseurs vérifiée formellement

Jonathan CERTES †
Benoît Morgan ‡, Yamine Aït-Ameur ‡, Vincent Nicomette ◇

IRIT, Université Paul Sabatier, Université de Toulouse †
IRIT, INP-ENSEEIHT, Université de Toulouse ‡
LAAS-CNRS, INSA Toulouse, Universite de Toulouse ◇

16 décembre 2020

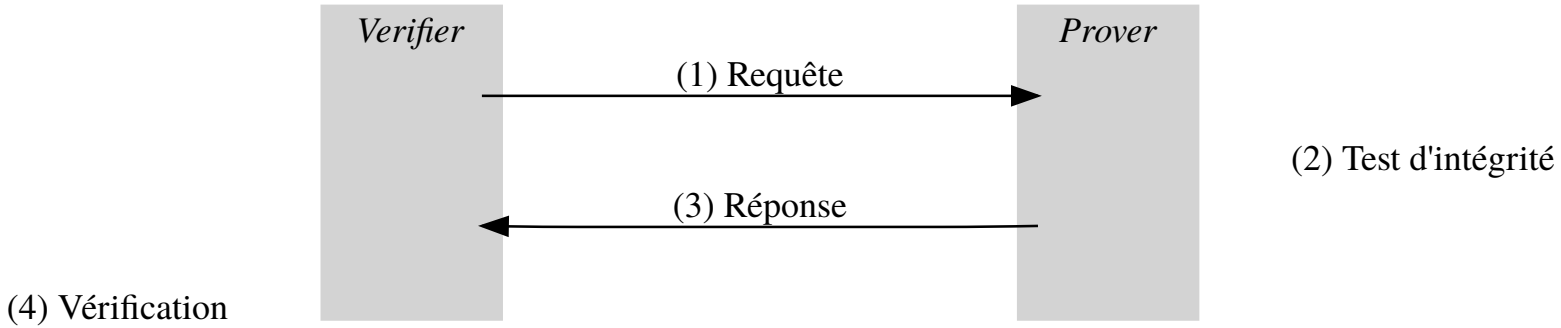
Objectif

Intégrité d'un algorithme et de son environnement d'exécution sur une machine "distante".

Modèle de menace fort

L'adversaire peut intégralement corrompre le code et les données de l'algorithme ainsi que son environnement d'exécution.

Protocole



1. $\mathcal{V}$rf envoie une requête ainsi qu'un challenge à $\mathcal{P}$rv.
2. $\mathcal{P}$rv calcule un test d'intégrité authentifié Σ sur son environnement et le challenge.
3. $\mathcal{P}$rv renvoie Σ à $\mathcal{V}$rf
4. $\mathcal{V}$rf vérifie Σ et décide s'il correspond à un état de $\mathcal{P}$rv valide

Intégrité de Σ

Basée sur un temps de réponse attendu

- pas de secret à protéger
- pas d'authentification de $\mathcal{P}$rv, donc hypothèse sur le temps

Σ dépendant d'un secret

- authentification possible de $\mathcal{P}$rv
- protéger un secret

Intégrité de Σ

Basée sur un temps de réponse attendu

- pas de secret à protéger
- pas d'authentification de $\mathcal{P}$rv, donc hypothèse sur le temps

Σ dépendant d'un secret

- authentification possible de $\mathcal{P}$rv
- protéger un secret

SMART ; VRASED

Contexte et hypothèses

- Intégrité de Σ par calcul de $f_k : c, m \mapsto \text{HMAC}(m||c, k) = \Sigma$. k secret partagé et m mémoire et environnement à attester.
- $\mathcal{P}$rv est un microcontrôleur open MSP430

Principe : moniteur matériel

Observation du bus d'adresse et du compteur ordinal

- LTL_1 : Contrôle de l'exécution atomique et la cohérence de f
- LTL_2 : Contrôle d'accès sur k : seule f peut lire k

Automate vérifié formellement (*model checking*)

Principe de la preuve de sécurité

$LTL_1 \wedge LTL_2 \rightarrow$ Théorème (par réécriture)

Objectifs :

- processeur pris sur étagère + FPGA (Zynq 7000)
- profiter des preuves de sécurité de l'attestation à distance sur Microcontrôleur

Enjeux :

- moyens détournés pour accéder aux informations d'exécution
- faire seulement confiance à l'interface de débug *CoreSight*

Questions ?