Attestation à distance de microprocesseurs vérifiée formellement

Jonathan CERTES

Benoît Morgan, Yamine Aït-Ameur, Vincent Nicomette

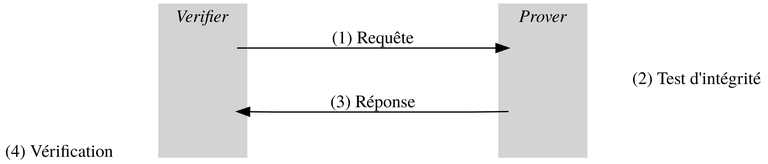
Contexte : attestation à distance

Objectif

Vérifier l'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.



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

Intégrité de Σ

Calcul de $\boldsymbol{f_k : c, m \mapsto \text{HMAC}(m||c, k) = \Sigma}$.

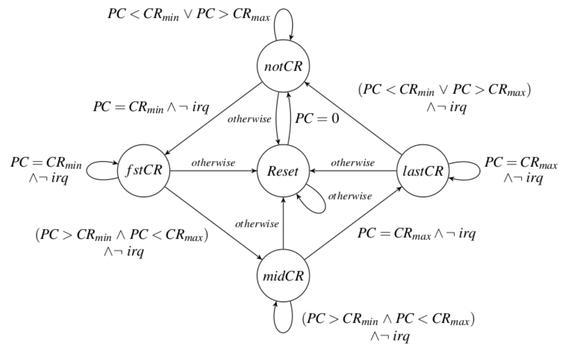
- c : challenge, permet d'emêcher le re-jeu d'une réponse
- m : mémoire et environnement à attester
- k : secret partagé

Protection du secret : support matériel pour les contrôles d'accès

Vérification formelle (extrait de *VRASED : A Verified Hardware-Software Co-Design for Remote Attestation*)

Intégrité de Σ, élimination de vulnérabilités :

- modélisation du système (automate)
- spécification formelle (invariants, propriétés temporelles)
- *model-checking* : vérification des propriétés
- preuve de sécurité : absence de vulnérabilité



$$\mathbf{G}\{\neg reset \wedge \neg(PC \in CR) \wedge \mathbf{X}(PC \in CR) \rightarrow PC = CR_{min} \vee \mathbf{X}(reset)\} \quad (1)$$

$$\mathbf{G}\{\neg reset \wedge (PC \in CR) \wedge \neg\mathbf{X}(PC \in CR) \rightarrow PC = CR_{max} \vee \mathbf{X}(reset)\} \quad (2)$$

$$\mathbf{G}\{irq \wedge (PC \in CR) \rightarrow reset\} \quad (3)$$

$$\mathbf{G}\{\neg(PC \in CR) \wedge R_{en} \wedge (D_{addr} \in KR) \rightarrow reset\} \quad (4)$$

Preuve de sécurité :

$$LTL_1 \wedge LTL_2 \wedge LTL_3 \wedge LTL_4 \rightarrow Theorem$$

Problématique

Pas de modification lourde du cœur :

- accès aux bus d'adresse (D_{addr})
- accès au compteur ordinal (PC)

Solution proposée

Architecture :

- processeur pris sur étagère + FPGA (Zynq 7000)
- profiter des preuves de sécurité de *VRASED*, attestation à distance sur microcontrôleur

Transducteur vers alphabet d'entrée du moniteur :

- esclave AXI pour socker k et f (D_{addr})
- décodeur de traces *CoreSight* + instructions spécifiques (PC)