Stage Master : Mise en œuvre d'une attaque par canaux de test et proposition de contre-mesures au niveau RTL

Collaboration : Defacto Technologies (defactotech.com/) / LCIS (lcis.grenoble-inp.fr/)

Les besoins en sécurité des systèmes embarqués ne cessent de croître. Si de nombreuses solutions logicielles sont proposées pour sécuriser ces systèmes, leur efficacité peut être amoindrie si la cible matérielle n'est pas adaptée. Notamment, les techniques de conception en vue du test utilisées pour accroitre l'observabilité et la contrôlabilité des systèmes pour leur test et leur debug peuvent constituer des failles de sécurité importantes. Ainsi les concepteurs de System-on-Chip doivent intégrer des solutions de sécurisation matérielles de ces structures de test intégrés pour adresser les applications sécurisées. Si ces techniques sont maîtrisées par des équipes de conception spécialisées dans la sécurité, elles sont plus difficiles à appliquer pour des équipes de concepteurs non spécialistes de la sécurité. Or les besoins en sécurité ne se limitent plus à des circuits spécifiques type smartcard, les circuits génériques nécessitant désormais un minimum de sécurité. Dans ce projet, nous souhaitons donc développer un outil permettant de faciliter la sécurisation des structures de test dans les circuits intégrés.

Le travail consistera à développer une méthode permettant d'évaluer la vulnérabilité et d'accroitre la robustesse des circuits en s'appuyant sur les outils de conception en vue du test au niveau RTL développée par Defacto. Les attaques par chaîne de scan seront donc simulées au niveau RTL. En effet, il existe de nombreuses contre-mesures contre ce type d'attaque mais elles nécessitent souvent d'intervenir tardivement dans le flot de conception au risque d'avoir des effets de bord sur d'autres paramètres du circuit (taux de couverture, consommation…). Les vérifications sont alors longues et fastidieuses et peuvent nécessiter de reprendre la conception du circuit ce qui impacte le temps de développement et le coût. Ainsi, on proposera des techniques permettant d'insérer ces contres mesures automatiquement et très tôt dans le flot de conception au niveau RTL.

Le stagiaire devra donc dans un premier temps mettre en œuvre une attaque par canaux cachés profitant des vulnérabilités liées aux structures de test intégré (notamment les chaînes de scan). Ensuite, après avoir recensé les principales contre-mesures, le stagiaire intégrera automatiquement au niveau RTL l'une de ces contre-mesures en adaptant les outils de Defacto Technologies. Finalement, une analyse de la robustesse de la contre-mesure proposée sera réalisée.

Afin de mener à bien ce travail, le candidat aura de solides connaissances en conception numérique et notamment : VHDL, C, microélectronique.

Lieux : LCIS (Valence) et Defacto Technologies (Grenoble) (Frais de mission entre Grenoble et Valence pris en charge)

Merci de transmettre votre candidature (CV, cursus suivis, liste des matières étudiées, lettre de motivation, lettre de recommandation) par email à:

David HELY
Grenoble INP LCIS
50 rue Barthélémy de Laffemas BP 54 - 26902 Valence Cedex 9 - France
Tel : +33 4 75 75 94 73 david.hely@esisar.grenoble-inp.fr