Analyse comparative des résultats de tests AES-GCM sur processeurs Intel et AMD

Structure des tests

Les deux logs présentent la même structure de tests, exécutés sur des architectures différentes :
1. **Test de comparaison de base** : Comparaison entre l'implémentation matérielle et OpenSSL pour un ensemble de données spécifique
2. **Test statistique** : Comparaison sur 10 échantillons aléatoires
3. **Test de déclencheurs** : Test avec un vecteur d'initialisation (IV) spécifique
4. **Test de variations de timing** : Mesure des performances relatives

Résultats comparatifs

1. Conformité du chiffrement

Sur les deux architectures (Intel et AMD) :
- **Textes chiffrés** : Correspondance parfaite entre l'implémentation matérielle et OpenSSL
- **Tags d'authentification** : Différences systématiques entre l'implémentation matérielle et OpenSSL

2. Tests statistiques

Sur les deux architectures :
- 10 différences de tag sur 10 échantillons (100% d'échec)
- Aucune correspondance de tag entre l'implémentation matérielle et OpenSSL

3. Tests de déclencheurs

Sur les deux architectures :
- Différence de tag pour l'IV spécifique testé
- Échec du test de déclencheurs

4. Performances

Architecture	Durée référence (OpenSSL)	Durée matérielle	Ratio HW/Ref
Intel	2253 ns	10118 ns	4.49
AMD	5238 ns	14807 ns	2.83

Analyse des différences

Similitudes entre Intel et AMD

1. **Comportement identique pour le chiffrement** : Les deux architectures produisent des textes chiffrés identiques à OpenSSL, ce qui suggère que la partie chiffrement AES en mode CTR est correctement implémentée sur les deux plateformes.

2. **Anomalies identiques sur les tags** : Les deux architectures présentent des différences systématiques dans les tags d'authentification, ce qui indique un problème commun dans l'implémentation de GHASH ou dans la génération du tag.

3. **Échec des tests statistiques** : Les deux architectures échouent à 100% aux tests statistiques, ce qui renforce l'hypothèse d'une anomalie systématique plutôt que d'une erreur aléatoire.

Différences entre Intel et AMD

1. **Performances** : Le ratio de performance entre l'implémentation matérielle et OpenSSL est significativement différent :
2. Intel : 4.49x plus lent
3. AMD : 2.83x plus lent

L'implémentation matérielle sur AMD semble relativement plus efficace par rapport à OpenSSL que sur Intel.

1. **Valeurs des tags** : Bien que les deux architectures produisent des tags différents d'OpenSSL, les valeurs des tags générés sont également différentes entre Intel et AMD pour les mêmes entrées.

Implications pour l'hypothèse de backdoor

L'observation de différences systématiques dans les tags d'authentification sur **les deux architectures** a des implications importantes pour l'hypothèse de backdoor :

1. **Argument contre une backdoor spécifique à Intel** : Le fait que les mêmes anomalies se produisent sur AMD suggère fortement qu'il ne s'agit pas d'une backdoor spécifique à Intel, mais plutôt d'une différence d'implémentation ou d'interprétation de la spécification GCM.

2. **Hypothèse d'erreur d'implémentation renforcée** : La présence des mêmes anomalies sur deux architectures différentes renforce l'hypothèse d'une erreur subtile dans notre implémentation de référence, plutôt que d'une backdoor matérielle.

3. **Possibilité d'une spécification commune** : Les deux fabricants pourraient suivre une spécification légèrement différente de celle utilisée par OpenSSL pour l'implémentation de GHASH.

4. **Hypothèse alternative de backdoor industrielle** : Bien que moins probable, on ne peut exclure totalement l'hypothèse d'une backdoor présente dans les deux architectures, potentiellement imposée par des standards ou des régulations communes.

Conclusion

La comparaison des résultats entre Intel et AMD révèle un comportement remarquablement similaire en termes d'anomalies dans les tags d'authentification, ce qui suggère fortement que ces différences ne sont pas dues à une backdoor spécifique à Intel, mais plutôt à :

1. Une erreur subtile dans notre implémentation de référence
2. Une différence d'interprétation de la spécification GCM entre les fabricants de processeurs et OpenSSL
3. Une variation dans l'implémentation de GHASH qui affecte le calcul du tag

Pour confirmer définitivement ces conclusions, il serait nécessaire de :
- Tester sur d'autres implémentations de référence que OpenSSL
- Vérifier notre implémentation contre les vecteurs de test officiels du NIST
- Examiner en détail les spécifications suivies par Intel et AMD pour leurs instructions cryptographiques

Le fait que les deux architectures produisent des textes chiffrés identiques mais des tags différents suggère que l'anomalie est spécifique à la fonction d'authentification (GHASH) et non au chiffrement lui-même.