HYPERFORM franchit sa première étape dans la protection post-quantique des données

Le démonstrateur du consortium français de cybersécurité protège les données au repos et en transit

CYBERSÉCURITÉ

POSTÉ LE 01.29.26

Le consortium HYPERFORM, une initiative collaborative menée par IDEMIA Secure Transactions en partenariat avec cinq leaders de la cybersécurité (CryptoNext Security, PRIM'X, Synacktiv, le CEA et l'INRIA) et avec l'Agence Nationale de Sécurité des Systèmes d'Information (l'ANSSI) a démontré avec succès son prototype de protection post-quantique des données. Cette avancée constitue un progrès significatif pour la sécurisation des données sensibles en Europe et ouvre la voie à un avenir résilient face au quantique.

Vers une souveraineté européenne renforcée en matière de cybersécurité

Avec pour objectif de développer la première plateforme de référence française, le consortium HYPERFORM, financé par France 2030 et l'Union européenne, se concentre sur des cas d'usage concrets pour évaluer, tester et démontrer des solutions de cryptographie post-quantique. Ces cas d'usage couvrent la vérification des documents d'identité électroniques, les transactions bancaires sécurisées, l'archivage à long terme de documents confidentiels, le travail collaboratif sur des données sensibles et la sauvegarde de données dans un cloud souverain. En parallèle de ces applications concrètes, le projet intègre une analyse proactive de la sécurité et le développement de contre-mesures afin que la solution soit, in fine, résiliente non seulement face aux ordinateurs quantiques, mais aussi contre les attaques sophistiquées déjà existantes.

Avec ce premier prototype, le consortium HYPERFORM fait la démonstration concrète d'une solution de chiffrement capable de protéger les données confidentielles tout au long de leur cycle de vie, de leur création (données en transit) à leur stockage à long terme (données au repos). Pour ce faire, le prototype remplace les clés de protection à long terme par des clés hybrides résistantes aux ordinateurs quantiques et intègre des algorithmes conformes aux standards du NIST dans le cadre d'un environnement collaboratif.

Le succès de cette démonstration constitue une avancée majeure pour sécuriser les échanges de données confidentielles dans les environnements de travail sensibles et leur archivage à long terme. En offrant une protection immédiate et durable, cette solution répond directement à la menace qui consiste à collecter les données maintenant, pour les déchiffrer plus tard (« *harvest now, decrypt later* »).

Démonstration de l'interopérabilité post-quantique

L'un des principaux succès de la démonstration est d'avoir démontré l'interopérabilité des composants clés de la solution. Le projet a ainsi validé que les librairies cryptographiques IDEMIA Sphere (exécutées au sein de l'élément sécurisé) peuvent interopérer sans friction avec la librairie de CryptoNext Security (utilisée pour la PKI et intégrée au logiciel de chiffrement de PRIM'X). Il s'agit d'une étape essentielle, prouvant qu'il est possible de mettre en place un écosystème robuste faisant intervenir plusieurs fournisseurs, ce qui évitera toute dépendance à un acteur unique et rendra la solution applicable à grande échelle. Les prochaines étapes du projet incluront le développement d'un élément sécurisé post-quantique de nouvelle génération, l'intégration d'une autre famille d'algorithmes cryptographiques post-quantiques et la démonstration de la crypto-agilité de la solution.

Tous les éléments réunis pour le chiffrement post-quantique des données

Le démonstrateur HYPERFORM repose sur des solutions européennes de pointe pour le chiffrement des données, combinées au stockage robuste des clés dans des éléments sécurisés et à des techniques de chiffrement avancées.

- PRIM'X a fait évoluer **deux de ses logiciels de chiffrement** afin de prendre en charge la cryptographie post-quantique hybride dans le cadre de la démonstration : ZONECENTRAL, qui chiffre le poste de travail de l'utilisateur et garantit que seuls les utilisateurs autorisés peuvent accéder aux données confidentielles, et ZED!, qui sécurise la collaboration entre deux utilisateurs au moyen de conteneurs chiffrés.
- IDEMIA Secure Transactions a fourni un **composant sécurisé résistant aux ordinateurs quantiques**, intégrant des accélérateurs matériels spécialement conçus pour la cryptographie post-quantique. Celui-ci assure la protection des clés à long terme de la solution et embarque la librairie cryptographique IDEMIA Sphere afin de fournir des fonctionnalités cryptographiques résistantes au quantique.
- La **librairie cryptographique** de CryptoNext Security intègre, entre autres, des implémentations de ML-KEM et ML-DSA à temps constant, renforcées contre les attaques par canaux auxiliaires. Elle a été certifiée par Synacktiv dans le cadre du projet HYPERFORM. Elle est utilisée par les différentes solutions logicielles du projet pour la protection des données et la PKI, lorsqu'il n'est pas nécessaire de recourir à un élément sécurisé matériel.

L'importance stratégique de projets tels qu'HYPERFORM pour l'Europe réside dans le développement de solutions souveraines résistantes au quantique pour la protection des données critiques telles que des archives stratégiques, des données souveraines et des secrets industriels. Ces solutions seront essentielles pour instaurer une confiance numérique durable à l'ère post-quantique et préserver l'indépendance européenne en matière de cybersécurité.