Activité : cryptographie et architecture

Simon Abelard

Janvier 2026

Avertissement : ceci est un exercice créé de toutes pièces à partir d'un cas d'usage réel, cela signifie qu'aucun des choix présentés ici ne reflète l'architecture d'un système existant ou en cours de développement.

1 Contexte

Objectifs :

Élaborer une architecture de sécurité, c'est identifier :
- les composantes d'un système,
- les informations qui transitent entre elles,
- les liens nécessaires pour les faire transiter,
- les besoins de sécurité spécifique à chaque lien,
- les algorithmes cryptographiques permettant de remplir ses besoins,
- (la liste n'est pas exhaustive selon les projets, on peut ajouter : la gestion des clés, les tests, les procédures opérationnelles, la maintenance, etc.)

Description technique :

Nous souhaitons concevoir un système de communications sécurisées par satellite (pensez à la téléphonie ou à l'internet par satellites), composé des éléments suivants :
- Un centre de contrôle (CC)
- Une constellation de satellites (SAT)
- Des antennes permettant au centre de contrôle de communiquer avec les satellites
- Des terminaux utilisateurs (UT) permettant d'échanger des informations avec les satellites

Les informations échangées sont de plusieurs types :
- Échanges internes CC $\longleftrightarrow$ SAT : le CC peut envoyer des ordres aux satellites (corriger leur orbite, appliquer des patchs logiciels) et, réciproquement, les satellites envoient des informations au CC (acknowledgement, état interne du satellite, etc.)

— Échanges CC $\longleftrightarrow$ terminaux : le CC peut envoyer des mises à jour ou des informations (panne, maintenance) aux terminaux, les terminaux peuvent envoyer des requêtes au CC
— Échanges SAT $\longleftrightarrow$ SAT : les satellites peuvent échanger des informations entre eux (pour relayer des messages ou pour échanger des informations techniques relatives à l'état de la constellation)
— Échanges terminaux $\longleftrightarrow$ terminaux : les terminaux communiquent entre eux (c'est le but du service que fournit le système)

Question 1 : Faire un schéma du système incluant au moins deux satellites et deux terminaux utilisateurs. Avec ce schéma, décrire comment transitent les informations dans les cas listés ci-dessus. En utilisant ce schéma, listez tous les couples possibles de composantes échangeant des informations.

Question 2 : Mettons-nous un instant à la place de l'attaquant. Analysez comparativement les scénarios suivants en notant de 1 à 3 leur gravité (1= le moins grave, 3=le plus grave) et leur probabilité (1=le moins probable, 3=le plus probable). Pour vous étayer votre analyse, réfléchissez aux conséquences de chaque scénario et à comment il pourrait se produire.

— Un attaquant prend le contrôle d'un satellite
— Un attaquant prend le contrôle d'un terminal
— Un attaquant prend le contrôle du CC

Remarque : en cybersécurité, cette question à rapprocher des notions d'analyse de risque, de cible de sécurité, de threat model et de threat scenario. C'est une tâche complexe conduite par des ingénieurs spécialisés qui suivent des méthodes bien précises (ex : EBIOS).

Question 2b : Dans un projet bien conduit, l'analyse de risque et la cible de sécurité sont à faire au tout début du projet. Pourquoi ?

2 Sécurisation des liens

Question 3 : On suppose que toute information qui circule dans le système est potentiellement sensible, c'est-à-dire qu'une information que s'échangent deux composantes du système ne doit pas pouvoir être lue par les autres. En reprenant les questions précédentes, expliquer ce que cela implique en termes de clés partagées.

Question 4 : On considère plus spécifiquement deux composantes quelconques du système. Quels sont d'après vous les besoins de sécurité entre ces deux composantes ? Quels algorithmes proposeriez-vous ?

3 Gestion des clés (key management)

Question 5 : En matière de gestion de clés, les bonnes pratiques sont d'avoir une clé différente par lien et de renouveler régulièrement les clés (on parle de cryptopériode). Expliquez en quoi ces bonnes pratiques améliorent la sécurité, et réfléchissez à quels sont les paramètres qui peuvent influencer le choix de la cryptopériode.

Question 6 : Pour renouveler les clés il faut d'abord les générer puis les distribuer. Comment conseillez-vous de procéder pour la génération de clés ?

Question 7 : Expliquer en quoi la distribution de clés est différente selon qu'on utilise de la cryptographie symétrique ou asymétrique. Insister sur les mesures de protection à mettre en place pour protéger la nouvelle clé que l'on distribue.

Question 8 : Pour la distribution des clés secrètes, donnez votre avis sur les avantages et les inconvénients des méthodes ci-dessous :

- Envoyer la nouvelle clé secrète chiffrée par l'ancienne clé secrète
- Injecter la nouvelle clé secrète dans l'appareil via une connexion physique (par exemple avec une clé USB)

Question 9 : Proposer une solution utilisant la cryptographie asymétrique.

Question 10 : Une menace pour le système est le vol d'équipement cryptographique afin d'en extraire des clés. Pour cela, les équipements intègrent parfois une fonction d'effacement d'urgence qui détruit les clés. Pour chaque composante (CC, SAT, UT), dire s'il est pertinent d'inclure cette fonction et justifier.

4 Cryptographie asymétrique

Question 11 : on veut que chaque composante puisse renouveler ses clés à distance. Proposer un mécanisme utilisant la cryptographie asymétrique.

Question 12 : Expliquez la différence entre clés statiques et éphémères, en insistant sur l'impact en cas de compromission de clés.

Question 13 : Pour chaque composante du système (CC, SAT, UT), dressez la liste de toutes les clés qu'il doit stocker. On suppose que toutes les composantes sont capable de faire de la cryptographie asymétrique et qu'elles utilisent des clés éphémères lorsque c'est possible. Si cela vous aide, vous pouvez vous limiter au cas où il y a deux satellites et deux terminaux.

Question 14 : Pour chaque fonctionnalité cryptographique, proposer un choix d'algorithme (et éventuellement de paramètres). Vous pouvez vous aider des documents de l'ANSSI `https://messervices.cyber.gouv.fr/documents-guides/anssi-guide-mecanismes_crypto-2.04.pdf` ou de la NSA `https://en.wikipedia.org/wiki/Commercial_National_Security_Algorithm_Suite`

Question 15 : Pour chaque composante du système (CC,SAT, UT), dressez la liste de tous les algorithmes cryptographiques qu'il doit pouvoir éxécuter. Pourquoi cette question est-elle importante ? Faut-il garder cette liste secrète ?

5 Infrastructure à clés publiques (PKI)

Question 16 : Rappelez (brièvement) le principe d'une attaque de l'homme du milieu (man in the middle). Et expliquez comment s'en prémunir.

Question 17 : Selon vous, pourquoi serait-il pertinent d'avoir deux PKI différentes pour les clés des UT et des satellites ?

Question 18 : Pourquoi pourrait-on envisager une PKI plus simple pour les satellites ? En regardant la norme X509, identifiez quels champs on pourrait supprimer ou simplifier.

6 Pour aller plus loin

Question 19 : Pour résister au brouillage, on sécurise les liens SAT $\longleftrightarrow$ UT avec une clé symétrique propre à chaque satellite. Quel impact sur l'architecture de sécurité ?

Question 20 : dérivation de clés Entre deux entités, la cryptographie asymétrique permet de négocier une clé de session K_s. Pour en déduire plusieurs clés, on utilise une fonction pour générer plusieurs clés $K_i = \mathrm{KDF}(K_s, FixedInfo_i)$. Justifier l'intérêt d'un tel mécanisme. Quelles sont les propriétés de sécurité que l'on attend pour la fonction KDF ?

Question 21 : séparation de domaines Est-ce une bonne chose d'utiliser les mêmes algorithmes pour toutes les composantes du système ? Pourquoi ? Peut-on faire en sorte d'utiliser les mêmes algorithmes tout en faisant en sorte d'avoir un cloisonnement entre le service (les communications entre UT) et la gestion de la constellation ?

Question 22 : crypto-agilité Admettons que l'on doive modifier certains algorithmes cryptographiques sans interrompre le service. Comment feriez-vous ? Si on souhaite le faire par une mise à jour à distance, comment sécuriseriez-vous cette fonctionalité ?