Institut National des Sciences Appliquées de Lyon

Département Informatique, 4ème année, 2016-2017

Réseaux avancés et sécurité

(Documents manuscrits et copies des supports de cours autorisés)

A. Questions d'ordre général (5 points)

A.1 Que désigne une « adresse » dans Bitcoin ? Comment une adresse est-elle générée ? Par qui ?

>>> Dans Bitcoin, on appelle « addresse » (« *address* » en anglais) le hash d'une clef publique utilisé pour identifier un utilisateur (ou plutôt un « compte utilisateur ») qui va ainsi pouvoir recevoir et/ou dépenser des bitcoins. C'est l'utilisateur qui crée une paire clef publique/clef privée puis génère l'adresse par hachage de la première. Un utilisateur peut créer autant d'adresses qu'il le souhaite. Il n'y aura aucun lien entre ces adresses (à l'instar de comptes bancaires séparés).

A.2 Quels sont les composants d'un VPN (Virtual Private Network (Réseau Privé Virtuel)) ? Comment un VPN fonctionne-t-il ? Quelles sont les utilisations d'un VPN ?

>>> Un VPN (traduction de « Réseau Privé Virtuel ») est un « système » permettant de créer un lien sécurisé entre deux ordinateurs/réseaux reliés par une infrastructure partagée (typiquement Internet) (2 grandes classes : site2site (entre deux LANs) et remote access (entre 1 ordinateur et un LAN distant)). Un VPN de type « remote access » se compose d'un serveur côté LAN, d'un logiciel client (ou d'un navigateur travaillant en SSL) côté source et d'un protocole réseau (« tunnelling ») entre les deux. Tous les paquets échangés entre client et serveur (et réciproquement) sont préalablement chiffrés (« encapsulés ») avant leur émission sur le réseau d'interconnexion (typiquement Internet) puis déchiffrés et leur intégrité vérifiée à leur arrivée. Lors de la négociation initiale entre client et serveur (authentification du client), après authentification de l'utilisateur client (mot de passe, certificat, etc.), le serveur attribue une adresse IP locale temporaire au client. A leur arrivée sur le serveur, après déchiffrement et vérification d'intégrité, les paquets du client sont modifiés en remplaçant dans l'entête l'IP source par l'IP temporaire (l'opération inverse est réalisée lors de l'envoi de messages vers le client). On dit qu'un « tunnel » est créé entre le client et le serveur. Dans les VPN site2site, le même type d'approche est implémentée mais de manière permanente et symétrique entre les 2 serveurs d'entrée sur les LANs.

Protocoles utilisés : IPsec, PPTP, SSL, PPTP,

Utilisations : accès distant, mobilité, confidentialité, authentification.

B. Problème : Révolution énergétique (15 points + 2 points)

Nous sommes en train d'assister à une révolution de la production/consommation d'électricité. De plus en plus de personnes acquièrent des moyens de production personnelle d'électricité (panneaux photovoltaïques, éoliennes, micro-centrales hydro-électriques, etc.). L'électricité générée non-consommée est alors reversée dans le réseau électrique. Corollairement, des dispositifs tels que les véhicules électriques amènent à consommer de l'énergie de manière nouvelle et « distribuée », en se connectant à des bornes de rechargement, chez un ami ou dans un hôtel.

Ce double phénomène étant amené à fortement s'amplifier dans le futur, vous venez de vous voir confier la mission de concevoir le système d'information indispensable au juste paiement de l'électricité produite et consommée (ex : si Robert recharge sa voiture électrique chez son ami René, c'est Robert qui doit payer l'électricité consommée, pas l'ami René).

Félicitations !

Principales fonctionnalités du système visé (rq : vous êtes libres d'ajouter d'autres fonctionnalités si vous les jugez importantes) :

- Enregistrement des reversements d'électricité dans le réseau (reversement = envoi dans le réseau d'électricité produite par un particulier)
- Enregistrement des consommations personnelles d'électricité quel que soit le lieu de consommation : résidence principale, résidence(s) secondaire(s), véhicule(s) électrique(s) (dans un premier temps, on ne considérera que ces trois cas)
- Facturation, sur une base mensuelle, des productions et consommations d'électricité
- Consultation sur le Web en temps réel par les usagers producteurs et consommateurs (certains étant à la fois producteurs et consommateurs), des données (données électriques et crédits/débits financiers associés) les concernant

On fera les hypothèses suivantes :

- A l'interface entre dispositif de production et réseau électrique, est placé un dispositif de mesure intelligent. Celui-ci permet (i) de mesurer de manière précise la quantité d'électricité envoyée dans le réseau ; (ii) d'envoyer au système d'information que vous êtes chargé de concevoir (dénoté SI), via Internet et de manière périodique, cette quantité d'électricité (rq : certains onduleurs sont capables de faire cela)
- Les habitations sont toutes équipées de compteurs intelligents capables de communiquer au SI la consommation d'électricité (au niveau de l'ensemble de l'habitation) sur une période définie (cf. compteurs Linky)
- Les véhicules électriques disposent d'un compteur électrique intelligent capable de communiquer au SI l'électricité consommée après chaque rechargement (ou de manière périodique)

Outre les besoins fonctionnels décrits plus haut, il vous est demandé de veiller, dans vos propositions, à garantir la sécurité du système (ex : protection contre les intrusions), sa fiabilité/disponibilité (disponibilité proche de 100%), son efficacité (affichage en temps réel de l'état des consommations/productions), la protection des données personnelles (données de production et consommation incluses).

Note importante : vous êtes libre, dans vos réponses aux questions ci-dessous, de faire des hypothèses additionnelles dès lors que vous les justifiez.

B.1 Solution centralisée (6 points) Une première solution envisageable est d'utiliser un serveur centralisé. Décrivez l'architecture du SI ainsi que les mécanismes et protocoles à mettre en œuvre (cf. besoins fonctionnels listés plus haut). Note : n'oubliez pas les objectifs non-fonctionnels (ex : sécurité, disponibilité, etc.) décrits ci-dessus. Quels sont les avantages et inconvénients de cette solution ?

>>> Serveur central (avec serveur transactionnel, BDD et courriel) en redondance active avec équilibrage des charges, firewall/antivirus/IDS. Communication des infos par VPN (cf. A.2) ou API REST SSL (https). Comptes clients (login/mdp ou plutôt certificat (cf. plus bas)). Proxy http si pas fourni par le firewall.

Enregistrement des reversements d'électricité : de manière périodique (ex : toutes les nuits à heure fixe), le dispositif envoie un message avec comme données : l'id du dispositif, le n° de message (chaque message envoyé par un dispositif reçoit de celui-ci un n° d'ordre => ordre total), la date d'envoi, les dates de mesure de la consommation (en toute logique, si les messages sont ordonnés, date fin de mesure su message n = date de début de mesure du message n+1 ; on pourrait donc supprimer la date de début ; voir cependant si celle-ci peut être utile en cas de crash ou de contestation), la consommation mesurée entre ces dates. Enregistrement dans les logs du serveur et mise à jour du compte client (solde). Envoi d'un ACK par le serveur. A la réception du ACK, deux approches : (i) le dispositif archive temporairement ce message dans un cache ; (ii) ou le dispositif détruit le message. Si on peut avoir un peu de mémoire, l'option (i) est préférable. Le serveur vérifie aussi que le message précédent a bien été reçu et archivé. Si non et si option (i) plus haut, demande du ou des messages perdus. Si on ne reçoit pas de ACK ou si coupure réseau, on réessaie après un temps aléatoire ; si toujours pas de ACK, 2 approches : écrire dans le cache et renvoyer le message avec le message en attente avec le prochain message ; détruire le message et envoyer plus tard un message de consommation portant sur une période plus longue (agrégation des consommations de 2 ou n périodes).

Côté serveur, régulièrement, sauvegarde des données (comptes clients + logs) sur support distant pour archivage légal et sauvegarde. De même détection de possibles anomalies (données reçues suspectes), qui pourraient être le signe d'un dysfonctionnement soit du dispositif de production, soit du dispositif de mesure.

Cette approche est de type push (le « producteur » envoie les infos). Une approche inverse, de type pull, consisterait à faire initier la transaction par le serveur (le fonctionnement (ex : structure des messages) reste le même). On peut aussi faire du push/pull en cas de réseau très mauvais (pas le cas en France).

Consommation d'électricité : pour les habitations, approche similaire ; pour les voitures, la difficulté est d'identifier à la fois la voiture concernée (qu'il s'agisse de la voiture d'un tiers (Robert) ou d'une des voitures possédées par le client) et l'habitation concernée. Idées (rappel : les dispositifs sont considérés comme fiables et non malicieux) :

- Si la voiture ne communique pas avec le serveur, faire signer la « facture » par la voiture. La prise électrique (plutôt que le véhicule comme le suggère le sujet) (si la prise électrique est intelligente, sinon, le compteur de l'habitation s'il sait parler à la voiture, sinon, cette solution ne marche pas) rédige un message de consommation et le fait signer numériquement par la voiture. Processus : authentification de la voiture par la prise de rechargement via un challenge-réponse type Diffie-Helmann ; création du message (« facture ») par la prise de rechargement (id de la prise de rechargement, id de la voiture, date de rechargement, consommation) ; signature du message par la voiture ; vérification de la signature par la prise de rechargement ; envoi du message (via VPN) ; vérification de la signature ; débit du compte de la voiture, crédit du compte de la prise (pour que l'opération soit neutre pour cette dernière)

- Si la voiture peut communiquer avec le serveur, et sous l'hypothèse que la voiture peut identifier l'habitation (prise intelligente), on procède de manière similaire : soit, comme précédemment, création de la facture par la voiture ou l'habitation, signature de la facture par la prise ou le compteur (si faisable), envoi par la voiture au serveur ; soit, création de de la facture par la voiture et envoi directement au serveur. En l'absence de possibilité d'identifier l'habitation, on peut soit utiliser la position

GPS, soit demander au propriétaire de la maison de rentrer un code d'identification sur l'ordinateur de la voiture (=> nécessité d'embarquer une application dédiée)

Dans tous les cas, cela suppose que chaque dispositif reçoive un couple clef privée/clef publique et un certificat signée par l'AC du service comprenant sa clef publique.

En outre, chaque dispositif est associé à un utilisateur (une personne privée ou morale qui va payer les factures/recevoir l'argent de sa production).

Rq : le premier protocole ne permet pas d'interdire à un automobiliste d'interrompre le rechargement et de partir sans payer (i.e., sans signer la facture), à l'instar de ce qui peut se passer actuellement dans les stations-service. Une solution, similaire à une procédure mise en place par les stations-service, consisterait à faire signer, avant le rechargement, le message (« facture ») qui sera envoyé au serveur à l'issu du rechargement. Cela suppose que la prise de rechargement soit fiable. Si tel n'est pas le cas, la seule solution semble de mettre un dispositif de mesure côté prise, un dispositif de mesure côté voiture et, en cas de contestation, d'aller devant les tribunaux qui pourront demander une expertise.

Facturation : simple. Afficher pour chaque dispositif associé à un utilisateur son état courant (consommation/production depuis la dernière période). Les logs de consommation/production peuvent également être listés.

Consultation : accès à une page Web dédiée (authentification par login/mdp) en https.

B.2 Solution à base de blockchain publique (6 points) Une deuxième solution envisageable est d'utiliser une blockchain publique. Dans un premier temps, on s'intéressera à Bitcoin. Décrivez les mécanismes et protocoles à mettre en œuvre (même remarque que précédemment concernant les objectifs non-fonctionnels). Quels sont les avantages et inconvénients de cette solution ? Quels seraient les avantages et inconvénients d'une blockchain intégrant la notion de smart contracts (contrats intelligents), telle qu'Ethereum ?

>>> Question très proche du TD Blockchain.

Affectation, par le service, d'une clef publique/clef privée (et donc, d'une « adresse » au sens de la question A.1) à chaque dispositif.

Enregistrement des reversements d'électricité : de manière périodique, le dispositif de production envoie un message authentifié au serveur pour recevoir un nombre minimum de satoshis (nécessaire pour créer une transaction) ; il crée ensuite une transaction du montant de ces satoshis du même type que dans l'exercice 2 du TP (typiquement mettre le n° de message, (le codage de) la date de fin de mesure et le montant (+ éventuellement une estampille) dans OP_RETURN).

Consommation d'électricité : pour les habitations, approche similaire ; pour les voitures, si la voiture sait communiquer,, approche similaire. Si on a supposé en B1 que la voiture ne communique pas, on est assez proche de l'exercice 5 du TD mais avec la contrainte du temps réel => solutions possibles : utiliser un système de séquestre (« *escrow* »), utiliser une « adresse verte » (« *green address* »), utiliser une double signature (avant le rechargement, création d'une transaction envoyant l'argent de la voiture du futur rechargement à la prise envoi et une coin d'un montant minimal de la prise à voiture ; le premier transfert vire l'argent du rechargement de la voiture vers la prise et le deuxième atteste que cette dernière est d'accord pour recharger la voiture).

Note : éventuellement envisageable de chiffrer les données de consommation avec la clef publique du « service de facturation » ou une clef partagée (pb : si on change la clef, il faut garder en mémoire la clef devenue obsolète).

Note : quid si la voiture est vendue à un autre propriétaire ? Cf. TD Blockchain. La « coin » représentant la voiture est passée au nouveau propriétaire.

Facturation et consultation : cf. exercice 7 du TP : il suffit de parcourir la blockchain pour retrouver la trace de toutes les transactions. Il faut cependant connaître l'ensemble des dispositifs associés à un utilisateur. Cette information peut être stockée dans une « petite BDD centralisée » (on est un peu B.3 !) ou dans la blockchain (assignation d'un dispositif à un utilisateur => 1 transaction) => dans ce cas, analyser la blockchain pour retrouver les dispositifs du client.

Une solution sans doute plus simple serait d'utiliser un contrat intelligent (« *smart contract* ») qui va vérifier que la voiture est OK pour payer un rechargement grâce à la prise (existence d'une transaction ad hoc dans la chaîne) et que la prise est bien OK pour recharger la voiture ; quand la prise a fini le chargement, elle écrit dans la chaîne une transaction correspondant au rechargement, le contrat alors écrit dans la chaîne une transaction attestant du rechargement.

Une approche complètement différente (full bitcoin ») serait de réaliser directement des transferts de bitcoins au lieu de stocker des reversements/consommations :

- Reversement : le réseau électrique envoie des bitcoins (ex : après chaque tranche de kWatts ou après chaque tranche de temps) sur le compte du client producteur
- Consommation habitation : le compteur envoie des bitcoins sur le compte du réseau électrique
- Consommation voiture : la voiture envoie des bitcoins sur le compte du propriétaire de l'habitation

Problème quand même : prévoir un mécanisme pour changer d'adresse Bitcoin + les clients doivent avoir des comptes Bitcoin avec des sous.

Avantages/risques : cf. cours (ex : non-répudiabilité, permanence/immutabilité, infrastructure existante... vs privacy, non-temps réel, bande passante de transactions faible, énergie...). Pb majeur : Bitcoin pas fait pour ça => risque de saturer le réseau => contre-mesures des mineurs.

B.3 Solution mixte (3 points) Une troisième solution envisageable (il y en a encore plusieurs autres mais nous nous arrêterons là !) est d'essayer de combiner les avantages (... sans en combiner les inconvénients !) d'une blockchain publique ou privée (à vous de réfléchir à la meilleure solution) et d'une base de données centralisée. Quelle architecture proposez-vous ? Décrivez le fonctionnement général de cette solution. Quels en sont les avantages et les inconvénients ?

>>> L'intérêt de la blockchain est de stocker de manière immuable les transactions. Sa limitation est que l'enregistrement des transactions ne se fait du tout en temps réel. L'intérêt d'une base de données est un peu l'inverse : excellente en termes de temps de réponse mais sujette à des attaques. On peut par exemple combiner les deux en mettant à jour les comptes des dispositifs dans une base de données et en stockant les logs des consommations/reversements dans la blockchain.

B4. Question subsidiaire – Suite B3 (2 points) Décrivez les protocoles et mécanismes à mettre en œuvre dans la solution proposée en B3.

>>> Le principal point est de synchroniser la base de données et la blockchain. Une idée simple est d'utiliser une adresse verte i.e., un serveur de confiance qui, quand on lui soumet une opération va, à la fois, écrire dans la base de données des comptes et créer des transactions dans la blockchain.

Encore un petit (enfin... sérieux !) effort en PLD (lâchez-vous et soyez cré atifs !)... et vous êtes en stage puis en vacances (ou l'inverse) puis en 5IF puis ingénieur... puis à la retraite, alors... « allons cueille cueille//les roses les roses//roses de la vie//et que leurs pétales//soient la mer étale//de tous les

bonheurs//allons cueille cueille//si tu le fais pas//ce que tu te goures//[]//ce que tu te goures » (R. Queneau).