Évaluation des attaques potentielles sur notre blockchain

Ce document vise à évaluer les attaques potentielles sur notre blockchain et à fournir une analyse de leur probabilité et de leur impact sur notre système. Comprendre les risques associés à la sécurité de notre blockchain est crucial pour maintenir l'intégrité de nos données et la confiance des utilisateurs.

- Les attaques surlignées en vert sont des attaques négligeables sur notre blockchain, à probabilités plus ou moins fortes.
- Les attaques surlignées en orange sont des attaques potentielles pour notre blockchain.
  Note : en réalité, puisque la blockchain opère dans un contexte de réseau privé
- **Les attaques mises en gras** sont des attaques liées à la nature même de l'algorithme de PoI, ou bien gérée spécifiquement par l'algorithme. Il peut s'agir d'attaques existantes sur d'autres types de consensus, mais qui peuvent être utilisées de manière spécifique afin de nuire au bon déroulement du consensus avec l'algorithme PoI.

1. Attaque de la porte dérobée (backdoor) : Cette attaque consiste à introduire une faille de sécurité dans la blockchain pour permettre à l'attaquant d'accéder à des informations sensibles ou de manipuler le réseau à sa guise.
   Si des failles de sécurité existent dans le système ou les protocoles utilisés, un attaquant pourrait potentiellement introduire une porte dérobée, permettant ainsi un accès non autorisé à des informations sensibles ou une manipulation du réseau. A notre niveau, nous n'avons pas repéré de potentielles failles de sécurité, il faudrait aller plus en profondeur en faisant appel à des professionnels de la sécurité pour analyser notre système.

2. Attaque de l'homme du milieu (Man-in-the-middle) : Cette attaque consiste à intercepter les communications entre deux parties de la blockchain pour pouvoir les manipuler ou les espionner.
   Bien que les blockchains privées impliquent généralement des participants connus et de confiance, il est toujours possible qu'un attaquant parvient à s'insérer entre deux parties de la communication sur la blockchain. L'attaquant pourrait intercepter et modifier les messages échangés, ce qui pourrait lui permettre de manipuler les transactions, d'espionner les informations confidentielles ou même de compromettre la sécurité des comptes. Sur notre blockchain, les communications ne sont pas sécurisées mais c'est quelque chose qui peut être amélioré.

3. Attaque par sabotage du réseau (Network Sabotage Attack) : Cette attaque consiste à perturber le fonctionnement de la blockchain en déconnectant des nœuds ou en empêchant la propagation de nouvelles transactions ou de nouveaux blocs.
   Cette attaque peut être moins probable sur une blockchain privée, car les nœuds du réseau sont généralement contrôlés par des entités de confiance et

les connexions réseau peuvent être sécurisées et surveillées de manière plus étroite.

4. **Attaque Sybil :** Cette attaque se produit lorsque l'attaquant crée plusieurs identités pour influencer le consensus sur la blockchain. Par exemple, il peut créer mettre en place des nœuds qui refusent de signer toutes les tentatives de signature de blocs venant d'un nœud spécifique. Cela l'empêcherait donc de faire valider ses blocs dans le cadre du PoI si des nœuds de l'attaquant sont dans son "chemin de signature".
   Bien que cette attaque puisse être possible dans certains cas sur une blockchain privée, elle est généralement moins préoccupante. Les blockchains privées ont un nombre limité de participants connus et vérifiés, ce qui limite la probabilité que ce genre d'attaques soient mises en place (sauf cas de piratage d'une partie des nœuds du réseau). Attention cependant à adresser ce point si l'algorithme tend à être modifié pour s'adapter à un contexte de blockchain publique.

5. Attaque des 51% : C'est l'une des attaques les plus courantes sur une blockchain. Elle se produit lorsqu'un groupe de mineurs contrôle plus de 51% de la puissance de calcul de la blockchain, ce qui leur permet de manipuler les transactions et d'invalider celles des autres utilisateurs.
   Cette attaque est moins probable sur une blockchain privée, car elle implique le contrôle de plus de la moitié de la puissance de calcul de la blockchain. Dans une blockchain privée, les participants sont généralement sélectionnés et de confiance, ce qui rend difficile l'obtention d'une telle majorité de contrôle (à nouveau, sauf cas de piratage informatique de plus de 50% des noeuds).

6. Attaque par déni de service (DDoS) : Cette attaque consiste à submerger la blockchain avec un grand nombre de requêtes, ce qui peut entraîner un ralentissement ou une interruption complète du réseau.
   Cette attaque peut toujours être possible sur une blockchain privée, mais elle est moins probable, car les participants sont généralement connus et peuvent être contrôlés de manière plus étroite. Les mesures de sécurité peuvent être mises en place pour détecter et atténuer les attaques DDoS.

7. Attaque par atténuation de la difficulté (Difficulty Retargeting Attack) : Cette attaque consiste à manipuler la difficulté de minage de la blockchain afin de rendre le minage plus facile et ainsi prendre le contrôle du réseau.
   Cette attaque est moins probable sur une blockchain privée car la difficulté de minage est généralement configurée de manière centralisée et contrôlée par l'entité qui gère la blockchain. Cela limite la possibilité de manipulation de la difficulté par des acteurs malveillants.

8. **Attaque de blocs invalides (Invalid Block Attack) :** Cette attaque consiste à créer des blocs invalides ou à invalider des blocs existants dans le but de perturber le fonctionnement de la blockchain.
   Un mécanisme de pénalité est en place dans l'algorithme de PoI afin de détecter et réprimander les nœuds qui émettront des blocs dans le but de nuire

au bon déroulement du consensus. Notamment, si un noeud reçoit plusieurs fois le même bloc venant d'un autre noeud, cela signifie que ce dernier essaie de "bruteforcer" les générations aléatoires de chemin jusqu'à en trouver un qui l'arrange, par exemple qui ne passe pas par un certain noeud lors du parcours.

9. Attaque par usurpation d'identité des mineurs (Mining Identity Spoofing Attack) :
   Cette attaque consiste à usurper l'identité d'un mineur de la blockchain pour prendre le contrôle de la puissance de calcul du réseau.
   Si les mécanismes d'authentification sont faibles ou si des vulnérabilités existent dans le processus de sélection des mineurs, la probabilité d'une attaque d'usurpation d'identité des mineurs peut augmenter.
   Les mineurs sont authentifiés et validés sur notre blockchain, cette sécurité prévient les usurpations, la probabilité de cette attaque est donc relativement faible.

Dans le cadre de cette analyse des attaques potentielles sur notre blockchain, il est important de souligner que cette étude n'a pas eu d'impact sur le développement actuel de notre système.

En résumé, toutes les attaques mentionnées peuvent potentiellement se produire sur notre blockchain si des mesures de sécurité adéquates ne sont pas mises en place. Il est donc essentiel de mettre en œuvre des protocoles de sécurité solides pour protéger notre blockchain. Pour atténuer les risques, des mesures de sécurité appropriées doivent être mises en place, comme l'utilisation de protocoles de communication sécurisés, de techniques de chiffrement, d'authentification forte et de mécanismes de vérification d'identité robustes pour minimiser les risques.

Cela dit, notre blockchain étant privée, une majorité de ces attaques ont une probabilité négligeable de se produire. Mais si les mesures de sécurité sont négligées ou mal implémentées, même une blockchain privée peut être vulnérable à certaines des attaques mentionnées.

La sécurité de notre blockchain dépend aussi du niveau de confiance accordé aux participants et de la solidité des contrôles d'accès et des protocoles de sécurité mis en œuvre. Nous ne sommes pas experts en sécurité, il est donc important de consulter des experts en sécurité blockchain et de suivre les meilleures pratiques pour garantir une protection adéquate.

Références

https://www.senat.fr/rap/r17-584/r17-58416.html
https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors
https://www.researchgate.net/publication/348485529_Blockchain_Security_Attacks_Challenges_and_Solutions_for_the_Future_Distributed_IoT_Network
https://www.spiceworks.com/it-security/vulnerability-management/articles/top-five-blockchain-attacks/
https://journalducoin.com/encyclopedia/principaux-vecteurs-d-attaques-sur-ethereum-et-methodes-de-defense/
https://cryptoweek.fr/les-attaques-de-blockchain-expliquees-comprendre-les-vulnerabilites-du-reseau
https://www.bitpanda.com/academy/fr/lecons/quest-ce-quune-attaque-a-51-et-comment-leviter/
https://www.horizen.io/academy/blockchain-attacks/
https://securitypilgrim.com/7-blockchain-security-issues-in-2022/