Faculté des Sciences & Techniques — Université de Limoges

Master 1ère année

Sécurité des Usages TIC

Examen — mai 2021

Durée : 1h30 — Tous documents autorisés

PKI — 15 points

1 – DSI : qu'est-ce que l'approche Zero Trust, et comment la mettre en place ?

15pts *Par Timothée Brogniart, SSL247 Modifié le mercredi 28 avril 2021 à 11:00*

Les **données** représentent désormais une mine d'or pour les hackers, forçant les professionnels de la sécurité à considérer tout le trafic et le flux de données comme potentiellement dangereux. Ce nouveau paradigme nécessite de **nombreuses strates d'authentification**, autant au niveau de l'utilisateur que de l'appareil ou de l'application utilisés, et une dynamique de **sécurité constante**❶. Pour endiguer ce problème, les entreprises à la recherche d'un **modèle d'authentification efficace** adoptent majoritairement l'approche dite « *Zero Trust* », afin de garantir un niveau de sécurité avancé. Dans ce modèle, la confiance n'est **jamais accordée implicitement** ❷ mais doit au contraire être réévaluée en permanence. Voici les règles d'or et étapes à garder à en tête si vous envisagez d'adopter cette approche...

Le Zero Trust est un concept, pas une technologie en soit

Le concept de « *Zero Trust* » réside avant tout sur un **ensemble de principes**, et non sur des produits ou services d'un fournisseur en particulier. Bien que la technologie soit une condition sine qua non de son bon fonctionnement et de sa mise en application, ce n'est qu'une partie d'une stratégie plus large qui nécessite un **changement radical** dans la façon dont les utilisateurs, les appareils et les applications se connectent les uns aux autres❸.

L'approche de « *Zero Trust* » est un concept d'**identité numérique** qui crée une **authentification mutuelle forte**, octroyant accès et autorisations à chaque utilisateur, appareil et processus du réseau de manière individuelle. Grâce à ce modèle, les organisations peuvent ensuite mettre en œuvre les capacités d'autorisation, d'assurance, d'analyse et d'administration nécessaires pour mettre en œuvre une architecture d'identité cohérente, et **100%sécurisée**.

L'infrastructure à clé publique (ou PKI) : le principe technique fondateur du Zero Trust

L'authentification des utilisateurs et des appareils est le point de départ. Si les entreprises se tournaient auparavant vers des exigences de mot de passe plus complexes ou une **authentification multifacteur** (MFA) afin de fournir une mesure de sécurité supplémentaire, ces méthodes ont malheureusement prouvé leur vulnérabilité❹.

Le PKI est quant à lui la référence en matière d'**authentification** et de **cryptage d'identité**. Selon le dernier rapport du « *National Institute of Standards and Technology* » (NIST) paru en août 2020 (« *Zero Trust Architecture* »), le PKI est l'un des principes fondateurs du « *Zero Trust* ». Avec cette technologie, les entreprises peuvent garantir le plus haut niveau d'authentification des utilisateurs et des appareils sans affecter la productivité des employés ou l'expérience utilisateur❺.

Elle permet aux entreprises de sécuriser des activités sans interruption, en **remplaçant** les **mots de passe** par des **certificats utilisateurs**, et en remplaçant la MFA traditionnelle par une **identification instantanée**. Enfin, cette technique permet d'automatiser le **cycle de vie** de tous les certificats d'identité❻.

Ce point n'est pas à négliger, car **l'automatisation** est l'un des éléments clé de la réussite d'une stratégie « *Zero Trust* ». À chaque nouvelle demande d'accès à un réseau, ou à une application par exemple, les contrôles doivent pouvoir être effectués automatiquement pour appliquer les politiques de l'entreprise en fonction de l'utilisateur, du groupe, du type d'appareil, de l'emplacement… Tout cela afin de **délivrer le plus rapidement possible** les autorisations d'accès. En bref : une authentification transparente pour les utilisateurs finaux, qui peut être facilement déployée sur chaque appareil à l'aide d'outils automatisés, et prêts à l'emploi ❼.

Centraliser gouvernance et application pour réussir sa transition

Cependant, il est certain que fournir un **haut degré de sécurité et d'authentification** à l'écosystème de son entreprise n'est pas une tâche simple. Cela repose non seulement sur les nouveaux principes de gouvernance et les nouvelles règles, mais aussi sur les modes d'application de ces principes. Plus qu'un changement dans la technologie, l'approche « *Zero Trust* » constitue également une culture d'entreprise en soi.

Les équipes IT doivent s'assurer qu'**aucun accès n'est accordé implicitement**, et ce dans l'intégralité des architectures réseau de plus en plus complexes, qui incluent des environnements de cloud privés, hybrides et de multiples clouds publics... En outre, chaque utilisateur et chaque terminal doivent se voir attribuer une **identité**, qui doit ensuite être **authentifiée** sur le réseau dans lequel ils se trouvent. Les équipes IT sont enfin responsables de veiller sur l'ensemble du **cycle de vie de ces identités**.

Migrer vers le Zero Trust en douceur

Mais même avec l'aide de la technologie PKI et de l'automatisation du traitement des identités numériques, la migration de toute une entreprise vers le Zero Trust peut paraître décourageante. Heureusement, les entreprises n'ont pas à mettre en œuvre ces certificats en masse, en une seule fois. Les équipes IT peuvent choisir de faciliter cette transition en mettant en œuvre un processus étape par étape.❽

Ci-dessous une liste pour aider à ne rien oublier lors de la transition vers l'accès réseau « *Zero Trust* », ou ZNTA (« *Zero Trust Network Access* ») :

- **Sécuriser les serveurs et les applications** : utiliser des certificats SSL / TLS pour sécuriser les serveurs web et app, y compris ceux des environnements DevOps et des environnements cloud.
- **Points de terminaison d'accès réseau sécurisés** : utiliser des certificats numériques pour protéger les équipements réseau sur lesquels vous comptez, notamment les pare-feu, le filtrage Web, les applications de messagerie, les réseaux privés virtuels et les passerelles Wi-Fi.
- **Sécuriser les points de terminaison des appareils** : utiliser des certificats d'appareil pour authentifier l'identité de tous les ordinateurs, ordinateurs portables, tablettes et appareils mobiles provisionnés, ainsi que des appareils BYOD.
- **Protéger les emails** : utiliser des certificats S / MIME pour protéger et authentifier le contenu des e-mails et des signatures d'e-mail sur différents appareils et points d'accès réseau ;
- **Remplacer les mots de passe par des certificats utilisateurs** : utiliser des certificats numériques soutenus par PKI pour fournir le plus haut degré d'authentification à chacun des collaborateurs

Pour relever ce défi au mieux et gérer les vulnérabilités internes à votre réseau, il peut être également pertinent de s'entourer des bons experts, notamment en effectuant des **tests d'intrusion** afin d'identifier les portes d'entrées potentielles.

Questions :

a. Quels sont les éléments à protéger ❶ ? *(1pt)*

b. À quoi correspond « *la confiance accordé implicitement* » ❷ ? *(1pt)*

c. Pourquoi les identités existantes comme les adresses matérielles et les login/mdp ne sont pas suffisants et qu'il faut un **changement radical** ❸ ? *(1pt)*

d. Donner des exemples de MFA ❹ et de vulnérabilités. *(1pt)*

e. Quelles sont les **composantes d'une PKI** que doit posséder/gérer l'entreprise en « *Zero Trust* »❺ ? *(1pt)*

f. Quels sont les risques liés à ces composantes **présentes dans l'entreprise** par rapport aux PKIs « *courantes* » que tout le monde utilise ? *(1pt)*

g. Comment réaliser de l'**authentification mutuelle** avec des certificats ? *(1pt)*

h. Est-ce que **tous les éléments liés à cette authentification** sont protégeables ? *(1pt)*

i. Quel est le « *cycle de vie* » du certificat ❻ ? Comment peut-on **rapidement** autoriser ou bloquer un appareil/individu pour l'accès au système d'information à l'aide de la PKI ? *(2pts)*
Quels sont les **éléments techniques** à utiliser ?

j. À quoi ressemblent les outils permettant une « *automatisation* » comme décrit en ❼ ? *(1pt)*

k. Quels est ce processus « *étape par étape* » dont on parle en ❽ ? *(1pt)*

l. Quels sont les risques contre lesquels l'approche « *Zero Trust* » n'a pas de réponse et peut même créer des problèmes supplémentaires ? *(1pt)*

m. Quel est **votre avis** sur l'approche « *Zero Trust* » ? *(1pt)*

n. Quelles sont **vos recommendations** pour éviter ce genre de problèmes ? *(1pt)*

Protocoles sécurisés – 5 points

2 – 3pts

a. Concernant les protocoles cryptographiques, expliquer la différence entre **l'authentification de message** et **l'authentification d'agent**. *(1pt)*

Considérez l'échange ci-dessous, K_{AB} est une clé symétrique connue seulement de A et de B, N_A est un nonce.

- $A \rightarrow B : A, N_A$
- $B \rightarrow A : \{B, N_a, \text{"4u2c"}\}K_{ab}$

b. Cet échange permet-il **l'authentification du second message** ? *(1pt)*

c. Cet échange permet-il **l'authentification d'un agent** par un autre (si oui lequel ou lesquels) ? *(1pt)*

3 – 2pts

a. Qu'est-ce que la « *freshness* » ? Pourquoi est-ce important ? *(1pt)*

b. Pourquoi l'ajout de contrôle d'intégrité est important dans un protocole d'échange chiffré ? *(1pt)*