

Faculté des Sciences Exactes et de l'Informatique
Département de Mathématiques et d'Informatique
Filière : Informatique

MÉMOIRE DE FIN D'ETUDES
Pour l'Obtention du Diplôme de Master en Informatique
Option : **Ingénierie des Systèmes d'Information**

THÈME :

**SÉCURISATION DES LABORATOIRES À
DISTANCE (E-LAB)**

Etudiant : « **BEKIHAL Nouredine** »

Encadrant : « **MOUSSA MOHAMED** »

Année Universitaire 2017-2018

1. Liste des Figures

Figure 1: représentation schématique de l'expérience à distance.....	11
Figure 2: Types d'attaques DDoS - la seconde moitié de 2014.....	12
Figure 3: Dénis de service distribué.....	13
Figure 4: deni de service – smurf attack.....	14
Figure 5: SYN Flood.....	15
Figure 6: UDP attaque.....	16
Figure 7: Schéma d'attaque aux expériences de base.....	17
Figure 8: Schéma d'attaque aux expulsions complexes.....	18
Figure 9: schéma d'attaque à l'expérience scientifique.....	19
Figure 10: gestion de l'api de l'architecture désordonnée.....	27
Figure 11: Kong l' API Management.....	28
Figure 12: Avant et après le kong.....	28
Figure 13: kong architecture	29
Figure 14: Kong Workflow.....	31
Figure 15: Interaction Kong avec REST.....	32
Figure 16: JWT diagramme de sequence.....	35
Figure 17: CORS comment ça marche.....	37
Figure 18: limitation du débit dans les API payent.....	38

Liste des abréviations

Abréviation	Expression Complète	Page
TIC	technologies de l'information et de la communication	6
Ddos	les attaques par déni de service distribuées	11
RDP	Remote Desktop Protocol	12
WMI	Windows Management Instrumentation	12
FTP	protocole de transfert de fichier	12
ICMP	Internet Control Message Protocol	13
POD	ping of death	13
SYN	demande de synchronisation ou établissement de connexion	14
SYN-ACK	(acknowledgement)signale que le paquet est un accusé de réception	14
UDP	User Datagram Protocol	15
HTTP	Hypertext Transfer Protocol	15
SW	software	17
HW	hardware	20
IPS	Les systèmes de prévention d'intrusion	21
SOA	architecture orientée services	24
WSOA	<i>Web Services Oriented Architecture</i>	24
UDDI	<i>Universal Description Discovery and Integration</i>	24
WSDL	Web Services Description Language	24
W3C	World Wide Web Consortium	24
SOAP	<i>Simple Object Access Protocol</i>	24
API	application programming interface	24
RESTful	Representational State Transfer	25
JSON	JavaScript Object Notation	26
ESP	Extensible Service Proxy	27
JWT	JSON Web Token	29
RFC 7519	Request for Comments: 7519	30
HMAC	Hash-based Message Authentication Code	30
RSA	revenu de solidarité active	30
CORS	ressources d'origine croisée	30

2. Table des matières

1. RÉSUMÉ.....	7
2. INTRODUCTION GÉNÉRALE.....	8
3. LES LABORATOIRES À DISTANCE.....	10
3.1. Laboratoire à distance de base:.....	11
3.2. Laboratoire à distance complexes:.....	11
3.3. expériences scientifiques laboratoires à distance :	11
4. LES RISQUES GÉNÉRAUX DE SÉCURITÉ DES LABORATOIRE À DISTANCE.....	13
4.1. Aspect de la sécurité matérielle physique et informatique:.....	13
4.2. Aspect de sécurité dû à l'environnement:.....	14
4.3. Aspect de sécurité du logiciel informatique :	14
a) Risques logiciels des laboratoires distants :	14
b) Conséquences des attaques logicielles sur les laboratoires distants :	20
5. QUELQUE SOLUTIONS DE SÉCURITÉ.....	24
5.1. Sécurité des expériences à distance basiques:.....	24
5.2. Sécurité des expériences à distance complexes :	24
5.3. Sécurité des expériences scientifiques à distance :	25
a) Attaque au serveur (informatique HW) :	25
b) Attaque au matériel physique (Physical HW) :	27
6. ARCHITECTURE ORIENTÉE SERVICE.....	29
6.1. Principes généraux d'une architecture orientée service.....	29
6.2. Avantages d'une architecture orientée service.....	30
7. PRÉSENTATION DE LA SOLUTION KONG.....	32
7.1. Caractéristiques de la solutions Kong.....	33
a) Évolutif	33
b) Modulaire.....	33

a) Les clés API fournissent.....	36
7.4. JSON Web Token JWT.....	39
a) JWT Concept.....	39
7.5. CORS.....	41
7.6. Limitation de débit(Rate Limiting).....	42
a) Types de limites de débit.....	43
7.7. Package Lcapy.....	44
a) Installation de Lcapy pour Linux (Ubuntu et variantes).....	44
8. INSTALLATION DE LA SOLUTION KONG.....	45
a) 1- Installer Kong:.....	45
b) 2- Préparez votre base de données:.....	45
c) 3- Démarrer Kong:.....	46
d) 4- Utilisez Kong:.....	47
8.2. Configuration d'un service.....	48
a) Ajoutez votre service en utilisant l'API Admin.....	48
b) Ajouter un route pour le service.....	48
c) Transférer vos demandes via Kong.....	49
8.3. Configuration d'un API :.....	49
a) Ajoutez votre API à l'aide de l'API Admin.....	50
Récupérer l'API :.....	51
Mise à jour :.....	51
Supprimer l'API :.....	51
8.4. Ajouter des consommateurs.....	51
Récupérer le consommateur :.....	51
Supprimer le consommateur :.....	51
8.5. Activation des plugins.....	52
a) Configurer le plugin key-auth pour votre API.....	52
b) Fournissez les informations d'identification de clé pour votre consommateur:.....	53
9. CONCLUSION :.....	54

1. RÉSUMÉ

Nous nous sommes concentrés sur les laboratoires électroniques et leur sécurité. Dans l'introduction, les caractéristiques de base, les principes d'affaires modernes et cette nouvelle technologie des TIC sont décrits. Ce qui suit est notre réponse à la question: Quel est le laboratoire à distance? Et nous avons expliqué quelques solutions pour sécuriser cette technologie, notre thème principal est la question de la sûreté et de la sécurité des laboratoires électroniques, qui sont souvent vulnérables à la pénétration et les mesures de sécurité sont inadéquates et si elles tombent entre de mauvaises mains.

Pour des raisons faciles à suivre, les laboratoires électroniques sont divisés en trois groupes de travail en fonction de leur complexité. Une analyse de risque potentielle pouvant survenir du côté matériel et logiciel et des précautions potentielles pour éliminer ces risques est présentée.

2. INTRODUCTION GÉNÉRALE

De nos jours, les universités traditionnelles ou virtuelles proposent différents cours *on-line* basés sur des présentations multimédias. La technologie Web intégrant de l'information présentée sous forme de textes et d'images est enrichie par des séquences vidéo ou audio pour constituer des supports de cours. De tels supports sont de plus en plus nombreux. Ils complètent et enrichissent l'offre de formation traditionnelle. Ils donnent également une nouvelle dimension, voire une nouvelle orientation, au rôle des enseignants.

Ce n'est que récemment que le problème des aspects sécuritaires des e-laboratoires s'est posé. Comme la chaîne est toujours aussi forte que son maillon le plus faible, il faut partir de la sécurité du constituant de base du système et nous décrirons les précautions de sécurité de l'expérience lointaine des laboratoires distants lui-même. Les laboratoires distants sont en fait une véritable expérience dans un vrai laboratoire en utilisant de vrais instruments et équipements. Il peut être contrôlé par un enseignant, un étudiant ou tout autre utilisateur à partir de son ordinateur via Internet sur le schéma de contrôle général du serveur-client. Le contrôle des expériences est activé via l'interface Web, au moyen de laquelle l'utilisateur peut effectuer les paramètres appropriés, les options et démarrer ou arrêter l'expérience. Les données mesurées à partir de l'expérience sont transférées sur Internet et présentées via l'interface Web au client. La page Web peut inclure l'option d'exporter des données directement dans l'un des éditeurs de feuilles de calcul (le plus souvent Microsoft Excel) pour faciliter le traitement. La plupart des expériences incluent la caméra Web qui permet de surveiller l'expérience en cours en temps réel et / ou de communiquer avec l'instructeur.

De telles expériences sont principalement conçues sous les auspices des universités à des fins d'enseignement. Pour cette raison, l'utilisation de certains d'entre eux est seulement pour les étudiants de l'université en question et l'accès est sécurisé par le nom d'utilisateur et mot de passe (en particulier dans les universités américaines). En Europe et en Australie, plusieurs projets soutiennent la construction de laboratoires à distance ouverts - avec un accès gratuit, avec ou sans

3. LES LABORATOIRES À DISTANCE

Laboratoire à distance (également appelé laboratoire en ligne, établi à distance) est l'utilisation des télécommunications pour mener à distance des expériences réelles (par opposition à virtuelles), à l'emplacement physique de la technologie d'exploitation, tandis que le scientifique utilise la technologie à partir d'une localisation géographique distincte. Le laboratoire à distance comprend une ou plusieurs expériences à distance.

Les réseaux informatiques associés à des applications de plus en plus interactives et des interfaces mobiles et accessibles peuvent favoriser une utilisation innovante dans le domaine des formations pratiques scientifiques et techniques. Des alternatives aux formations en présentiel telles que les laboratoires à distance peuvent constituer une contribution pour résoudre le problème de la massification des étudiants en particulier dans les pays du Sud. Les travaux pratiques nécessaires aux formations scientifiques sont souvent sacrifiés en faveur d'enseignements purement théoriques. Ces systèmes distribués et répartis permettent le partage des ressources matérielles et humaines par la mise en ligne de travaux pratiques accessibles en temps réel. Ces laboratoires, utilisés de plus en plus de part le monde, sont des environnements informatiques complémentaires aux classiques formations à distance. Ils permettent aux apprenants de manipuler de vrais dispositifs (instruments de mesures ou d'analyses - des mécanismes réels ou robotiques, ...).

De telles installations permettent un enseignement pratique à un nombre croissant d'étudiants, malgré les ressources matérielles et d'encadrement souvent limitées. Elles peuvent aussi permettre le partage des manipulations entre plusieurs institutions académiques à l'échelle nationale, voire internationale, et faire profiter les différents partenaires de ressources coûteuses auxquelles ils n'auraient pas accès.

Les laboratoires à distance peuvent être divisés selon plusieurs critères. L'un d'entre eux est leur sophistication et la complexité du matériel physique qu'ils utilisent. De ce point de vue, les expériences peuvent être divisées en trois catégories en tant que risques de sécurité [1]

classiques de cette catégorie sont les stations météorologiques donnant au client l'accès aux données enregistrées (la température, la pression, l'intensité de la lumière solaire ou le fond radioactif).^[1]

3.2. Laboratoire à distance complexes:

Ces Laboratoire à distance nécessitent une communication bidirectionnelle entre un client et le serveur. L'utilisateur envoie des commandes de contrôle au serveur et reçoit la confirmation de la demande et des données mesurées. À titre d'exemple, nous pouvons donner l'expérience de caractérisation de cellule électrochimique, où l'utilisateur peut contrôler le volume de l'électrolyte et la concentration dans la cellule électrochimique.^[1]

3.3. expériences scientifiques laboratoires à distance :

très souvent basé sur un appareil commercial contrôlé par le logiciel auteur, livré par le producteur, et utilisé pour le contrôle à distance. Les services supplémentaires fournis par des expériences sophistiquées sont leurs caractéristiques coopératives; partage d'instruments et leur utilisation réservant. En particulier, ces laboratoires distants sont exposés à de nombreux dangers et dommages. L'instrumentation est généralement basée sur des équipements coûteux susceptibles d'être endommagés et des règles strictes d'exploitation pour le contrôle des expériences doivent être observées et des laboratoires éloignés doivent être protégés contre toute violation possible de ces règles d'exploitation des instruments. Le contrôle du télescope astronomique peut être un exemple de cette catégorie. Il convient de mentionner que des laboratoires éloignés, peu fiables ou dysfonctionnels, peuvent avoir un effet «psychologique» néfaste, en particulier sur les nouveaux venus dans le domaine, sur l'utilité de ce nouvel outil pédagogique et scientifique. Compte tenu de la maturité des e-laboratoires et de leur importance, il est surprenant de voir comment un peu d'attention a été consacrée aux risques de sécurité des laboratoires et des e-laboratoires distants. Nous voulons contribuer à ce domaine aigu en décrivant les risques de sécurité pour les laboratoires éloignés en généra.^[1]

4. LES RISQUES GÉNÉRAUX DE SÉCURITÉ DES LABORATOIRE À DISTANCE

Nous allons d'abord parler des aspects généraux de la sécurité qui s'applique pour tous les laboratoires à distance. Ces aspects peuvent être divisés selon les différentes parties constitutives d'un laboratoire à distance.

laboratoire à distance comprend toujours le matériel physique, le matériel informatique et les logiciels informatiques.

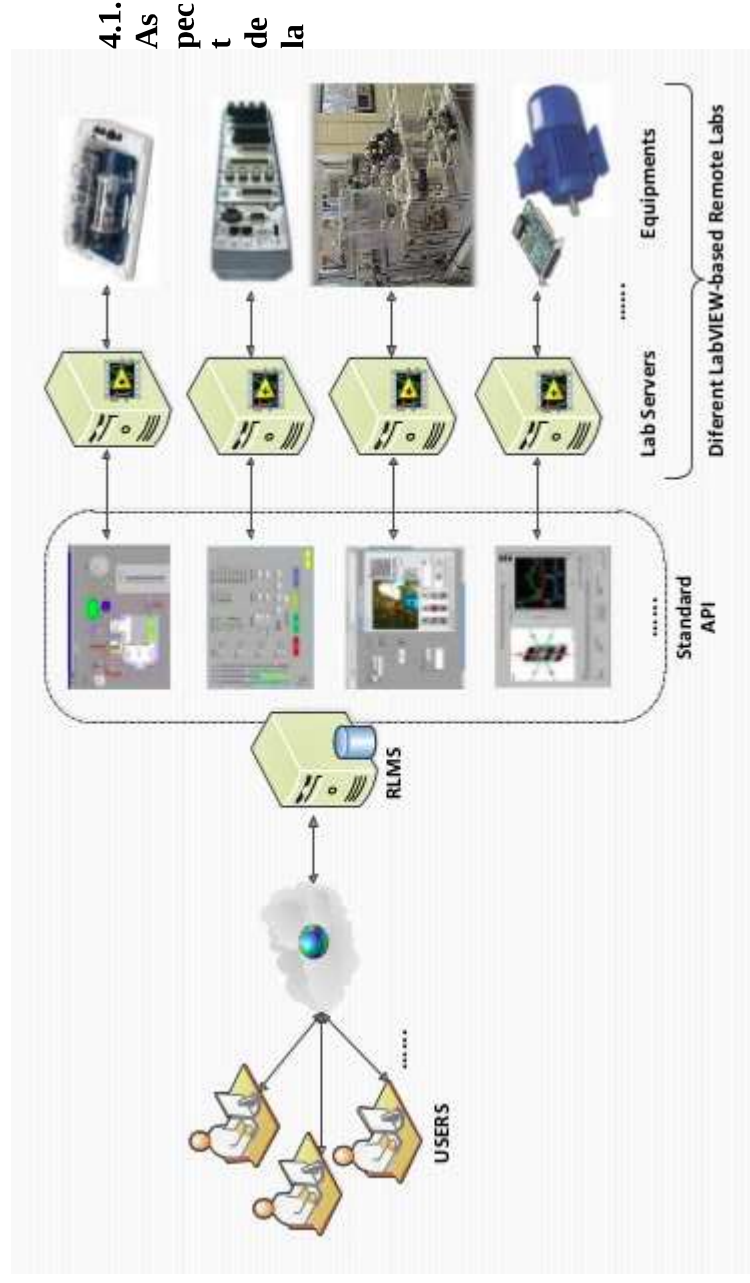


Figure 1: représentation schématique de l'expérience à distance sécurité matérielle physique et informatique:

cette catégorie comprend des dommages délibérés du matériel physique de l'expérience dans un bâtiment et dans une pièce fermée à clé.

4.2. Aspect de sécurité dû à l'environnement:

Cette catégorie comprend la défaillance de l'alimentation électrique (pannes de courant, pointes de tension et surtensions).

Le niveau de sécurité de ce dernier dépend bien sûr du coût de l'expérience. La protection contre les surtensions et les disjoncteurs sont généralement une sécurité adéquate pour des expériences simples, Mais les expériences utilisant des appareils de mesure coûteux nécessitent une sécurité complète via des sources d'alimentation sans coupure.

4.3. Aspect de sécurité du logiciel informatique :

Ceci est une attaque à l'expérience via un logiciel informatique principalement sur Internet.

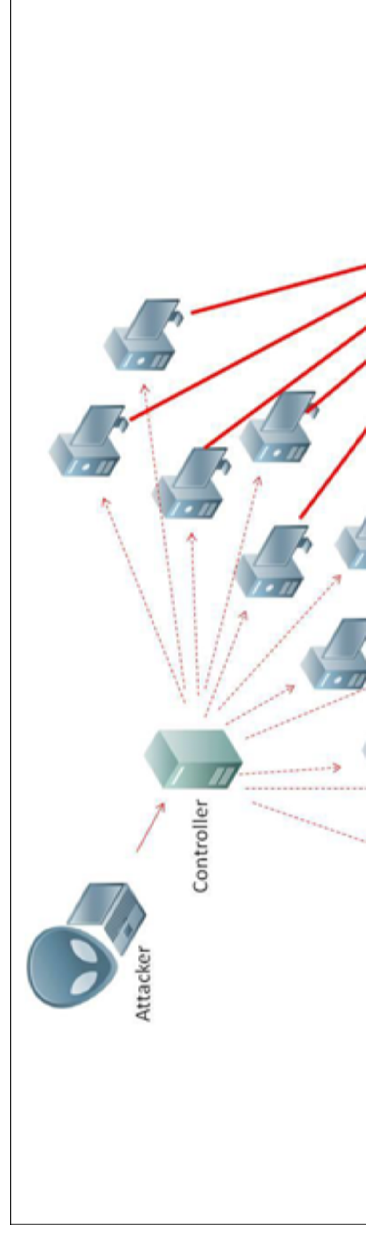
a) Risques logiciels des laboratoires distants :

Le principal problème des laboratoires à distance est l'accès à distance de n'importe où via Internet. Pour rendre cela possible, le serveur sur lequel l'expérience est exécutée doit avoir une adresse IP publique. Avec cette exigence vient toute une gamme de risques de sécurité. L'adresse IP publique permet de trouver et de tenter de se connecter au serveur à des attaquants potentiels non autorisés. Les attaques sur les serveurs ne sont pas un phénomène rare sur Internet. Il existe de nombreux types d'attaques qui menacent la fonctionnalité des serveurs Web. Récemment, nous avons rencontré le soi-disant type de DDoS de l'attaque la plus puissante dans les médias.

Nous pouvons voir que la plupart des attaques visaient des sites commerciaux tels que les magasins en ligne (25%) et les sites de commerce (20%). En fait, les attaques contre les laboratoires à distance n'étaient pas un problème aigu en 2011, mais elles peuvent facilement s'aggraver lorsque les laboratoires éloignés deviennent un outil d'expérimentation largement répandu dans les écoles et les universités. La (Figure 2) montre les types d'attaques DDoS les plus utilisés.^[1]

Ensuite, nous allons décrire les représentants typiques et la fonctionnalité des attaques DDoS et quelques autres types d'attaques de base que l'on pourrait rencontrer. Au risque de sécurité le plus souvent rencontré et évident appartient:

- Essayez de vous connecter à l'aide de RDP, WMI et FTP: L'accès au serveur permet la possibilité directe de contrôler le chargement expérimental aux dommages de l'expérience.
- Attaque par déni de service - (DoS attack) :est une tentative visant à rendre un ordinateur ou une ressource réseau indisponible pour ses utilisateurs. Bien que les moyens d'exécution, les motifs et les cibles d'une attaque de déni de service puissent varier, il s'agit généralement des efforts concertés d'une personne ou de plusieurs personnes pour empêcher un site ou un service Internet de fonctionner efficacement, temporairement ou indéfiniment. . [2]
- Déni de service distribué : fait référence à une variante d'attaques DoS où les attaques ne proviennent pas seulement d'un ordinateur, mais d'un grand nombre de canaux parallèles. Cela signifie qu'il y a des dizaines, des centaines et même des milliers de stations qui sont impliquées dans l'attaque. Les propriétaires de ces ordinateurs ne savent pas comment impliquer leur ordinateur dans une attaque. C'est possible à cause de logiciels malveillants (appelés zombies), qui sont installés sur leurs systèmes.



- ICMP flood - Ping of death - (abréviation "POD") : est un type d'attaque sur un ordinateur qui implique l'envoi d'un ping mal-formé ou malveillant à un ordinateur. Un ping a normalement une taille de 32 octets (ou 84 octets lorsque l'en-tête IP (Internet Protocol) est considéré); Historiquement, de nombreux systèmes informatiques ne pouvaient pas gérer un paquet ping supérieur à la taille maximale du paquet IPv4, qui est de 65 535 octets. L'envoi d'un ping de cette taille pourrait planter l'ordinateur cible. [3]
- ICMP flood - Ping of death est une variante particulière d'une attaque DoS flood sur l'Internet public. Il repose sur des périphériques réseau mal configurés qui permettent d'envoyer des paquets à tous les hôtes d'un réseau particulier via l'adresse de diffusion du réseau, plutôt qu'à une machine spécifique. Le réseau sert alors d'amplificateur smurf. Dans une telle attaque, les auteurs enverront un grand nombre de paquets IP avec l'adresse source falsifiée pour apparaître comme étant l'adresse de la victime. La bande passante du réseau est rapidement utilisée, ce qui empêche les paquets légitimes de parvenir à destination. Pour lutter contre les attaques par déni de service sur Internet, des services tels que le Smurf Amplifier Registry ont permis aux fournisseurs de services réseau d'identifier les réseaux mal configurés et de prendre les mesures appropriées, comme le filtrage [4].

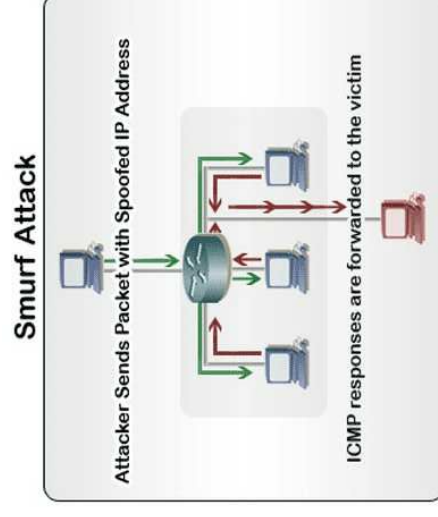


Figure 4: deni de service – smurf attack

- SYN flood :est une forme d'attaque par déni de service dans laquelle un attaquant envoie une succession de requêtes SYN au système d'une cible dans le but de consommer suffisamment de ressources serveur pour que le système ne réponde plus au trafic légitime. Cette attaque est basée sur la façon dont la connexion TCP / IP est établie. Cela fonctionne normalement comme ceci: Une application qui initie la session envoie des destinataires de synchronisation de paquets SYN. Le destinataire renvoie un paquet de confirmation au TCP SYN-ACK, l'initiateur répond par le paquet de confirmation ACK. Lorsqu'un attaquant SYN attaque inonde le système cible par une série de paquets TCP SYN. Chaque paquet amène le système cible à envoyer une réponse SYN ACK. Pendant que le système cible attend un accusé de réception, insère toute la réponse SYN-ACK en attente dans la file d'attente. Lorsque la file d'attente est pleine, le système ignore toutes les requêtes SYN entrantes. [5]

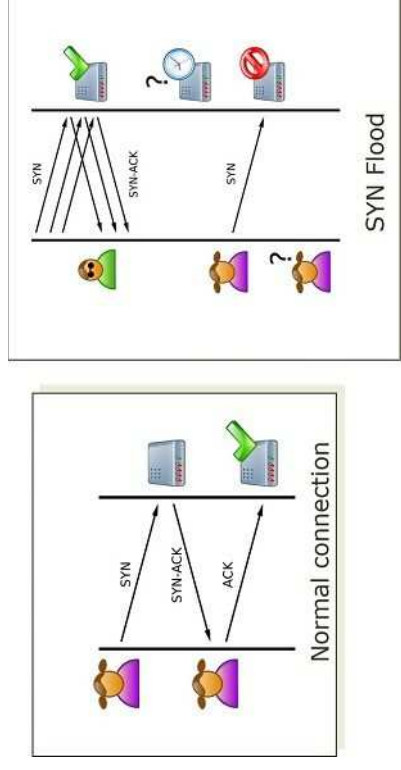


Figure 5: SYN Flood

➤ UDP flood - UDP Flood Attack :est l'une des attaques causant le déni de service basé sur l'hôte. UDP est un protocole sans connexion et ne nécessite aucune procédure de configuration de connexion pour transférer des données. Une attaque d'inondation UDP est possible lorsqu'un attaquant envoie un paquet UDP à un port aléatoire du système victime. Lorsque le système victime reçoit un paquet UDP, il détermine quelle application attend sur le port de destination. Quand il se rend compte qu'il n'y a aucune application qui attend sur le port, il va générer un paquet ICMP de destination inaccessible à l'adresse source falsifiée. Si suffisamment de paquets UDP sont remis aux ports sur la victime, le système va tomber.

[6]

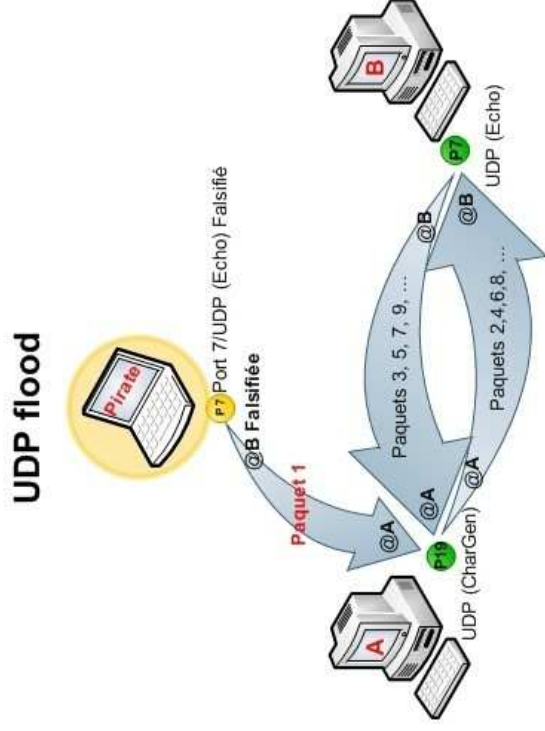


Figure 6: UDP attaque

[7]

➤ HTTP flood – HTTP:Ceci est le plus souvent utilisé pour attaquer les services Web et les applications. Sans mettre l'accent sur le trafic réseau à haut débit, cette attaque envoie des requêtes HTTP POST complètes et apparemment valides. Conçu spécifiquement pour

attaques qui impliquent de nombreuses tentatives de téléchargement d'un fichier sur le site.

Des attaques plus sophistiquées, dans lesquelles les cybercriminels tentent de masquer les robots en imitant le comportement des utilisateurs réels, ne sont menées que dans 10% des cas. [8] .

- Fausse identité : Pour les expériences plus complexes, la fausse identité peut conduire à un accès direct au contrôle de l'expérience. Cela peut entraîner des dommages de l'expérience.

b) Conséquences des attaques logicielles sur les laboratoires distants :

De la division des laboratoires distants, il est évident que les exigences de sécurité des trois groupes de laboratoires distants diffèrent en fonction de leur fonctionnalité. Toutes les attaques sur les laboratoires distants peuvent conduire à un arrêt contrôlé de laboratoires distants (dans le meilleur des cas) ou à un état indéfini de laboratoires distants (dans le pire des cas) et nécessitent donc des précautions de sécurité. Les mesures de sécurité dépendent du type d'expérience.

- laboratoire distant de base: L'attaque des laboratoires distants de base peut entraîner l'arrêt du serveur, empêchant ainsi leur utilisation correcte (Figure 7). Comme ce sont des expériences simples qui s'exécutent sans intervention de l'utilisateur et qui n'autorisent aucun contrôle, leur attaque ne causera aucun dommage supplémentaire. Les titres de base et l'externalisation utilisant l'accès à distance constituent le remède dans ce cas.



Figure 7: Schéma d'attaque aux expériences de base

- Complexes laboratoire distant: Comme dans le cas précédent, l'attaque peut entraîner l'arrêt du serveur et donc l'indisponibilité de l'expérience. En raison du matériel physique sophistiqué impliqué dans le programme de contrôle plutôt sophistiqué (informatique SW), il existe un autre risque. Le pirate peut endommager le logiciel de contrôle et, dans les cas extrêmes, même les composants matériels de l'expérience en attaquant le serveur. Lorsque le pirate prend le contrôle du serveur, il peut envoyer des commandes malveillantes qui peuvent endommager l'expérience (Figure 8). À titre d'exemple, nous pouvons mentionner «expérience de contrôle du niveau d'eau» (<http://195.178.94.32/>) lorsque l'écrasement des limites de contrôle peut entraîner un débordement du réservoir. Si l'expérience n'est pas protégée contre cette possibilité, cela pourrait provoquer une inondation, un court-circuit de l'électronique et même un incendie.



Figure 8: Schéma d'attaque aux expulsions complexes

➤ Les scientifiques: L'attaque de ces expériences implique les risques mentionnés pour les deux groupes précédents. Le risque avec les laboratoires distants scientifiques est augmenté par le coût des instruments de mesure sophistiqués utilisés dont le prix peut monter en flèche à des millions. L'endommagement de tels dispositifs, que ce soit une partie du logiciel ou même du matériel peut causer des dommages importants. Pour cette raison, ces expériences nécessitent les meilleurs soins et la sécurité pour toutes les perturbations possibles dues à des interférences externes. Certaines de ces expériences peuvent être contrôlées directement. Cela signifie que l'utilisateur envoie des commandes de contrôle directement à l'expérience. Cela crée un autre risque de sécurité, car le pirate peut truquer l'identité de l'utilisateur autorisé. Dans ce cas, il peut envoyer des commandes malveillantes qui peuvent endommager l'expérience (figure 9)

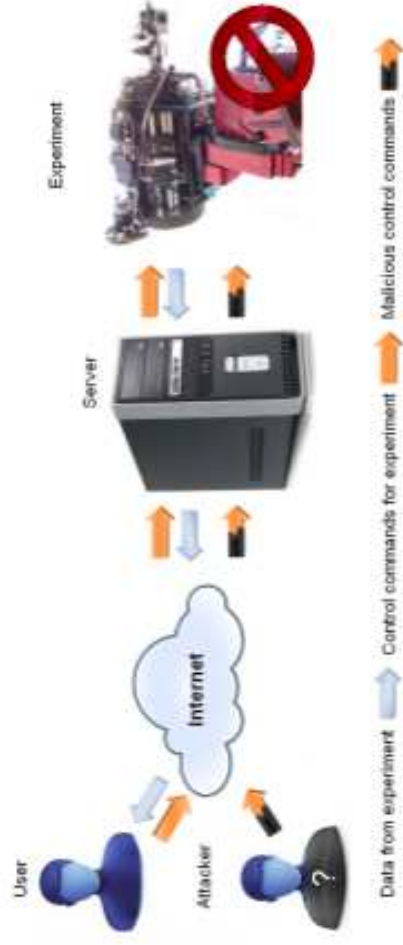


Figure 9: schéma d'attaque à l'expérience scientifique

5. QUELQUE SOLUTIONS DE SÉCURITÉ

Les sections suivantes concerneront la protection de sécurité des laboratoires distants contre les attaques de logiciels provenant de l'extérieur. Encore une fois, comme mentionné ci-dessus, le niveau de sécurité variera en fonction du type de sophistication des expériences donné ci-dessus.

5.1. Sécurité des expériences à distance basiques:

Ces expériences ne nécessitent pas de sécurité particulière. Nous devons simplement respecter les règles de sécurité de base telles que la mise à jour régulière de l'antivirus, le pare-feu système qui permet de verrouiller les ports et de sécuriser les services système appropriés. Une sécurité spéciale du serveur ou un accès sécurisé à l'expérience seraient coûteux en raison de la nature de l'expérience. La moindre des précautions devrait être l'avertissement que l'expérience est hors de la fonction et en réparation. Généralement, le SW de contrôle d'expériences même simples devrait avoir la propriété d'auto-guérison, soit de redémarrer dans les conditions de démarrage initial et / ou d'autre état défini permettant la poursuite de l'enregistrement des données après de simples coupures dues à des pannes ou autres interférences.

5.2. Sécurité des expériences à distance complexes :

Avec ce groupe de laboratoire distant , il est important de suivre les règles de sécurité de base comme dans le cas précédent. Parce que ce type de laboratoire distant ne peut pas être endommagé directement par les commandes de contrôle, il n'est pas nécessaire de sécuriser la connexion contre l'écoute indiscrete ou la confusion. Mais nous devrions couvrir tous les problèmes possibles découlant du fonctionnement de l'expérience à la fois le logiciel et le matériel (travail avec des fluides dans l'expérience <http://195.178.94.32/> - l'expérience est placée dans le réservoir où l'eau ne peut pas drainer à l'électricité dispositifs). Si l'on veut rendre l'expérience accessible uniquement à certains groupes d'utilisateurs, il convient d'organiser l'accès par nom d'utilisateur et mot de passe, ce qui conduit directement à une meilleure sécurité. Le plus grand risque potentiel est la procédure d'accès au serveur de l'expérience. Heureusement les attaques au serveur ne peuvent pas dans la majorité des cas conduire à l'endommagement du matériel physique, mais seulement à une indisponibilité de l'expérience. Comme mentionné dans l'introduction, le principal effet néfaste est

a) Attaque au serveur (informatique SW) :

Les attaques sur le serveur peuvent empêcher l'accès à l'expérience, ce qui peut entraîner des pertes matérielles. Les attaques les plus courantes contre le serveur sont les attaques DoS et DDoS avec des solutions simples à ce problème:

- Pare-feu, commutateurs et routeurs : Le bon choix et le bon réglage de ces dispositifs peuvent prévenir les types d'attaques de base. En utilisant des mécanismes tels que la liste de contrôle d'accès, la limitation de débit, la mise en forme du trafic, la liaison retardée (TCP), l'inspection approfondie des paquets et le filtrage Bogon, les attaques DoS peuvent être détectées et corrigées. Toutes ces mesures ne fonctionnent que tant que les mesures prises sont en faveur des attaques DoS en question. Par exemple, SYN flood peut être évité en utilisant une liaison retardée ou un épissage TCP. De même, le DoS basé sur le contenu peut être évité en utilisant une inspection approfondie des paquets. Les attaques provenant d'adresses sombres ou allant vers des adresses sombres peuvent être évitées en utilisant le filtrage Bogon. Cependant, si les attaques sont basées sur un principe différent, ces systèmes de sécurité sont inefficaces [9].
- Matériel frontal d'application : Le matériel frontal d'application est un matériel intelligent placé sur le réseau avant que le trafic n'atteigne les serveurs. Il peut être utilisé sur net / works en conjonction avec des routeurs et des commutateurs. Le matériel frontal de l'application analyse les paquets de données lorsqu'ils entrent dans le système, puis les identifie comme prioritaires, réguliers ou dangereux. Il y a plus de 25 fournisseurs de gestion de bande passante [10].
- Prévention basée sur IPS : Les systèmes de prévention d'intrusion (IPS) sont efficaces si les attaques ont des signes associés. Cependant, la tendance parmi les attaques est d'avoir un contenu légitime mais une mauvaise intention. IPS qui fonctionne sur la reconnaissance de contenu ne peut pas bloquer les attaques DoS basées sur le comportement. Un IPS basé sur

(telles que les inondations ICMP et les inondations SYN). À l'instar d'IPS, un système spécialement conçu, tel que les produits IPS Top Layer bien connus, peut détecter et bloquer les attaques par déni de service à une vitesse beaucoup plus proche de celle d'un système logiciel. [11]

- Tuyaux propres : C'est le service où tout le trafic est passé par un "centre de nettoyage" via un proxy, qui sépare le "mauvais" trafic (DDoS et autres attaques Internet courantes) et envoie seulement un bon trafic au serveur. Le fournisseur a besoin d'une connectivité centrale à Internet pour gérer ce type de service. Prolexic, Tata Communications et VeriSign sont des exemples de fournisseurs de ce service. [11]

L'accès au serveur peut également aider un attaquant à endommager l'expérience en envoyant des commandes de contrôle malveillantes directement sur l'appareil. Ce problème est déjà inclus dans la plupart des solutions de sécurité mentionnées ci-dessus.

b) Attaque au matériel physique (Physical HW) :

Un autre risque de sécurité apparaît en raison du fait que les expériences permettent un contrôle direct par des commandes de contrôle. Ils permettent à un attaquant d'attaquer directement l'expérience sans être influencé par les mesures de sécurité du serveur. En envoyant des commandes de contrôle malveillantes, des équipements sophistiqués peuvent être endommagés et des pertes financières importantes peuvent être causées. Il est évident qu'avec un matériel physique coûteux, il est nécessaire de donner accès à l'expérience uniquement aux utilisateurs autorisés.

La solution de ce problème peut être un accès sécurisé à l'expérience en utilisant le nom et le mot de passe de l'utilisateur. Cependant, cela peut s'avérer absolument insuffisant pour ce type de laboratoire distant. Un attaquant peut utiliser l'ingénierie sociale et le phishing pour accéder aux données. Il / elle peut également changer son identité Internet, c'est-à-dire rediriger le flux des données vers un faux ordinateur, pour ressembler à un utilisateur autorisé et ainsi avoir accès à l'expérience. Un bon remède est alors de sécuriser la connexion entre le serveur et le client en utilisant le chiffrement et l'authentification de l'identité des deux côtés. Pour ce faire, vous pouvez utiliser différents types de cryptage symétrique et asymétrique. Cependant, la couche application des protocoles réseau offre une solution complète à ce problème. C'est le protocole HTTPS (Hypertext Transfer Protocol Secure). [\[12\]](#)

HTTPS est une extension du protocole de réseau HTTP, qui permet une connexion sécurisée entre les navigateurs Web et le serveur Web à partir d'indiscrétions et de truquage de données. Il vérifie également l'identité de la contrepartie. Le protocole HTTPS utilise un cryptage asymétrique. Les deux parties doivent générer une paire de clés (privée et publique) avant la communication. Au début de la communication, les deux parties échangent des clés publiques, qui doivent être vérifiées par un canal de communication différent.

Le cryptage protège les communications contre les intrus, mais sans l'authentification des clés publiques, il y a des risques de communication d'un "Homme au milieu". Ce problème implique un

- La vérification peut être faite en vérifiant l'extrait de clé (hachage) par exemple en utilisant un appel téléphonique.
- Vous pouvez également utiliser le principe du "transfert de confiance"; La clé publique est signée numériquement dans ce cas. Cette signature est vérifiée par une autorité de certification à laquelle nous faisons confiance (par exemple, ViriSign).

6. ARCHITECTURE ORIENTÉE SERVICE

Une **architecture orientée services** (notée SOA pour *Services Oriented Architecture*) est une architecture logicielle s'appuyant sur un ensemble de services simples. L'objectif d'une architecture orientée services est donc de décomposer une fonctionnalité en un ensemble de fonctions basiques, appelées **services**, fournies par des composants et de décrire

finement le schéma d'interaction entre ces services. L'idée sous-jacente est de cesser de construire la vie de l'entreprise autour d'applications pour faire en sorte de construire une architecture logicielle globale décomposées en services correspondant aux processus métiers de l'entreprise.

Lorsque l'architecture SOA s'appuie sur des [web services](#), on parle alors de WSOA, pour *Web Services Oriented Architecture*).^[15]

6.1. Principes généraux d'une architecture orientée service

Il n'existe pas à proprement parler de spécifications officielles d'une architecture SOA,

néanmoins les principales notions fédératrices que l'on retrouve dans une telle architecture sont les suivantes :

- **La notion de service** : c'est-à-dire une fonction encapsulée dans un composant que l'on peut interroger à l'aide d'une requête composée d'un ou plusieurs paramètres et fournissant une ou plusieurs réponses. Idéalement chaque service doit être indépendant des autres afin de garantir sa réutilisabilité et son interopérabilité.
- **La description du service** : consistant à décrire les paramètres d'entrée du service et le format et le type des données retournées. Le principal format de description de services est WSDL (Web Services Description Language), normalisé par le W3C.
- **La publication et la découverte des services**. La publication consiste à publier dans un

6.2. Avantages d'une architecture orientée service

Une architecture orientée services permet d'obtenir tous les avantages d'une architecture client-serveur et notamment :

- Une modularité permettant de remplacer facilement un composant (service) par un autre
- Une ré utilisabilité possible des composants (par opposition à une système tout-en-un fait sur mesure pour une organisation).
- De meilleures possibilités d'évolution (il suffit de faire évoluer un service ou d'ajouter un nouveau service)
- Une plus grande tolérance aux pannes
- Une maintenance facilitée [\[15\]](#)

L'idée est d'appliquer SOA au laboratoire pour obtenir des micro-services (interface, gestion de paiement, les travaux pratique, base de donnée,etc...)chaque micro-services sont représentés par une API protégée

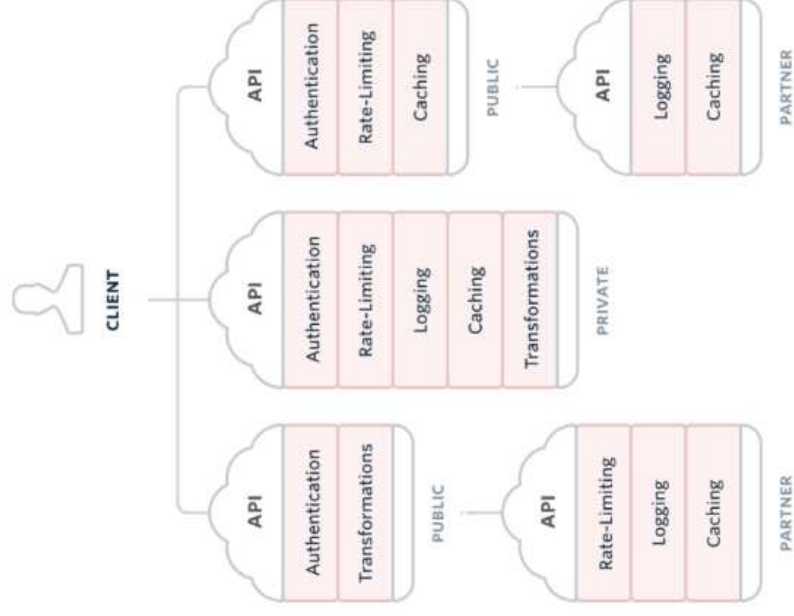


Figure 10: gestion de l'api de l'architecture désordonnée

7. PRÉSENTATION DE LA SOLUTION KONG

Kong est une couche d'API open source évolutive (également appelée API Gateway ou API Middleware). Kong s'exécute en amont de toute API RESTful et est étendu via les plugins, qui fournissent des fonctionnalités et des services supplémentaires au-delà de la plate-forme principale.

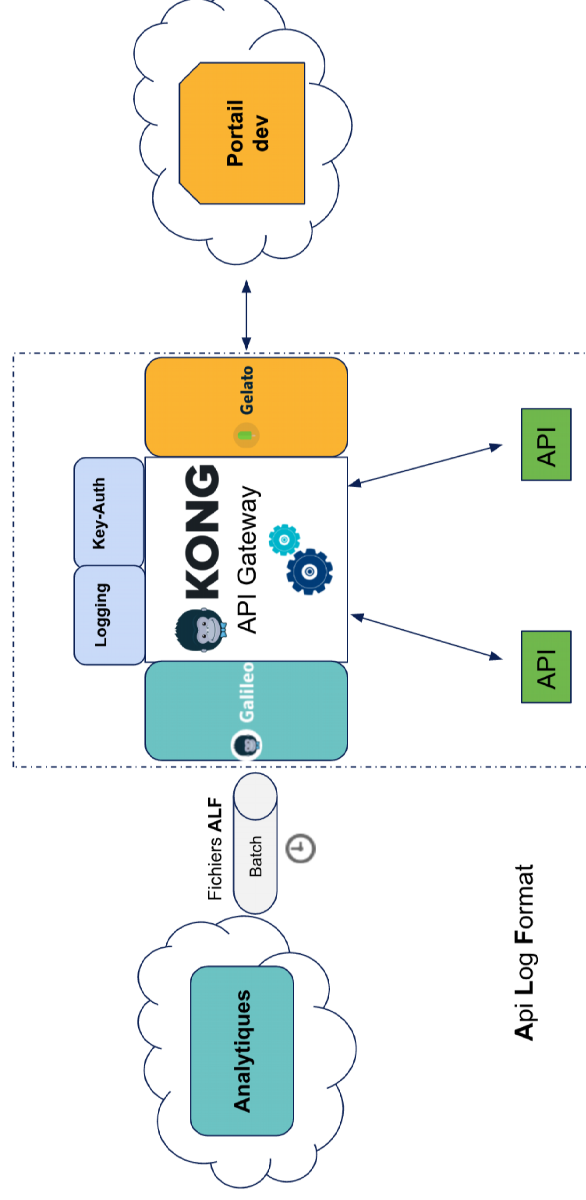


Figure 11: Kong l'API Management.

[17]

Kong a été conçu à Mashape pour sécuriser, gérer et étendre plus de 15 000 API et Microservices pour son API Marketplace, qui génère des milliards de demandes par mois pour plus de 200 000 développeurs. Aujourd'hui, Kong est utilisé dans des déploiements critiques pour les missions de petites et grandes organisations. [18]



[19]

7.1. Caractéristiques de la solutions Kong

a) Évolutif

Kong s'adapte facilement à l'horizontale en ajoutant simplement plus de machines, ce qui signifie que votre plate-forme peut gérer pratiquement n'importe quelle charge tout en gardant une faible latence.

b) Modulaire

Kong peut être étendu en ajoutant de nouveaux plugins, qui sont facilement configurés via une API RESTful Admin.

c) Fonctionne sur n'importe quelle infrastructure:

Kong court partout. Vous pouvez déployer Kong dans les environnements cloud ou sur site, y compris les configurations à un ou plusieurs centres de données, et pour les API publiques, privées ou à invitation uniquement.[18]

7.2. Aperçu de l'architecture

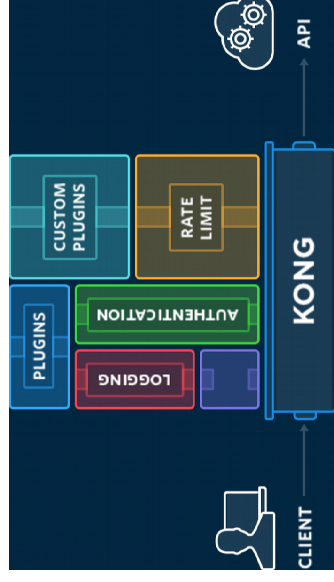


Figure 13: kong architecture .

a) API d'administration RESTful

➤ API HTTP JSON

- peut s'intégrer avec des services tiers
- c) **Mise en cluster et datastore:**
 - Soit cassandra ou PostgreSQL
 - En option Redis pour certains plugins
 - Clustering de centre de données unique ou multi
- d) **OpenResty:**
 - Moteur sous-jacent de Kong
 - Fournit des crochets pour le cycle de vie de la demande / réponse
 - étend NGINX sous-jacent
- e) **NGINX:**
 - la dépendance de base
 - gère les opérations de bas niveau
 - fondation solide et technologie connue

Kong s'appuie sur des technologies fiables comme NGINX et Apache Cassandra ou PostgreSQL, et vous fournit une API RESTful facile à utiliser pour faire fonctionner et configurer le système.[\[18\]](#)

7.3. Le Workflow selon la solution Kong

Pour mieux comprendre le système, il s'agit d'un workflow de requête type d'une API utilisant Kong:



Figure 14: Kong Workflow.

[18]

Une fois que Kong est en cours d'exécution, chaque requête envoyée à l'API touchera Kong en premier, puis sera transmise par proxy à l'API finale. Entre les demandes et les réponses, Kong exécutera tous les plugins que vous avez décidé d'installer, ce qui renforcera vos API. Kong devient effectivement le point d'entrée pour chaque demande d'API.

Kong simplifie et accélère la sécurisation, la gestion et l'orchestration des API microservice. C'est pourquoi il alimente des milliards de transactions API. C'est pourquoi les entreprises technologiques, les grandes banques, les innovateurs du commerce électronique et les agences gouvernementales placent Kong devant leurs charges de travail Web les plus importantes. Et les développeurs du monde entier apportent avec enthousiasme des innovations au sommet de la plateforme Kong. Voilà pourquoi j'utilise Kong. [18]

a) **Les clés API fournissent**

Pour décider quel schéma est le plus approprié, il est important de comprendre ce que les clés API et l'authentification peuvent fournir.

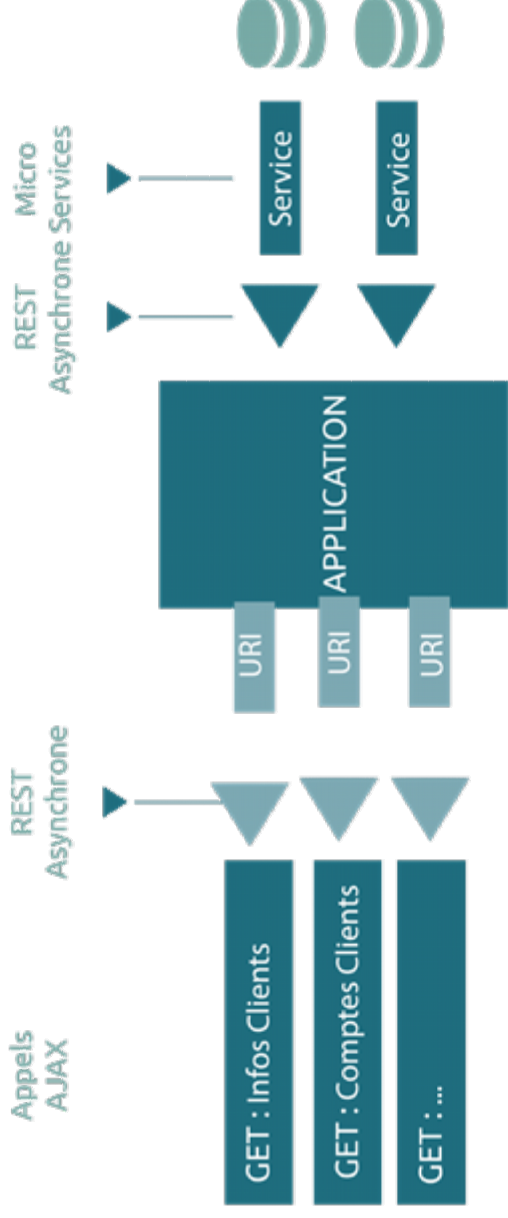


Figure 15: Interaction Kong avec REST

[20]

- **Identification du projet** - Identifiez l'application ou le projet qui appelle cette API
- **Autorisation de projet** - Vérifiez si l'application appelante a été autorisée à appeler l'API et a activé l'API dans son projet

Les clés d'API ne sont pas aussi sécurisées que les jetons d'authentification, mais elles identifient l'application ou le projet qui appelle une API. Ils sont générés sur le projet appelant et leur utilisation peut être limitée à un environnement spécifique tel qu'une plage d'adresses IP ou une application Android ou iOS spécifique.

➤ **Autorisation de l'utilisateur** - Vérifiez si l'utilisateur doit avoir accès à cette demande

Les schémas d'authentification fournissent un moyen sécurisé d'identifier l'utilisateur appelant. Cloud Endpoints vérifie également le jeton d'authentification pour vérifier qu'il est autorisé à appeler une API. Sur la base de cette authentification, le serveur API décidera d'autoriser une demande.[\[18\]](#)

Alors que les clés API identifient le projet appelant, elles n'identifient pas l'utilisateur appelant. Par exemple, si vous avez créé une application qui appelle une API, une clé API identifie l'application qui effectue l'appel, mais pas l'identité de la personne qui utilise l'application.

Sécurité des clés API

Les clés API ne sont généralement pas considérées comme sécurisées; ils sont généralement accessibles aux clients, ce qui permet à quelqu'un de voler une clé API facilement. Une fois la clé volée, elle n'a pas d'expiration, elle peut donc être utilisée indéfiniment, sans que le propriétaire du projet révoque ou régénère la clé. Bien que les restrictions que vous pouvez définir sur une clé API atténuent cela, il existe de meilleures approches pour l'autorisation.[\[18\]](#)

7.4. JSON Web Token JWT

JSON Web Token (JWT) est un standard ouvert (RFC 7519) qui définit une manière compacte et autonome de transmettre de manière sécurisée des informations entre des parties en tant qu'objet JSON. Cette information peut être vérifiée et fiable car elle est signée numériquement. Les JWT peuvent être signés en utilisant un secret (avec l'algorithme HMAC) ou une paire de clés publique / privée utilisant RSA.

Bien que les fichiers JWT puissent être cryptés pour assurer également le secret entre les parties, nous nous concentrerons sur les jetons signés. Les jetons signés peuvent vérifier l'intégrité des réclamations qui y sont contenues, tandis que les jetons chiffrés cachent ces réclamations à d'autres parties. Lorsque des jetons sont signés à l'aide de paires de clés publiques / privées, la signature certifie également que seule la partie qui détient la clé privée est celle qui l'a signée.

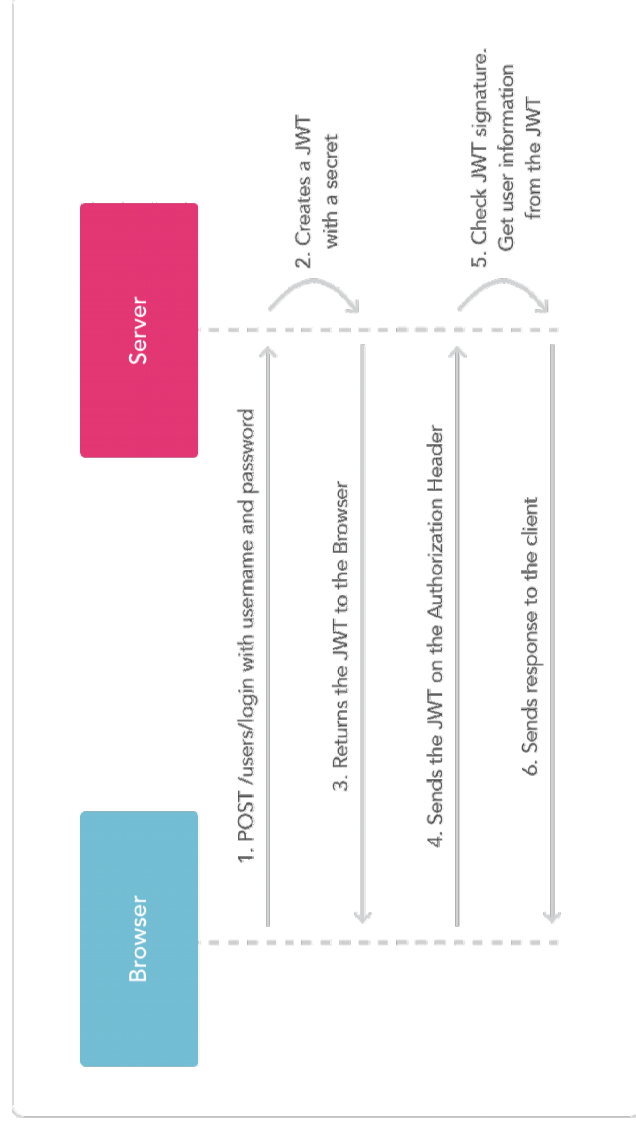


Figure 16: JWT diagramme de sequence

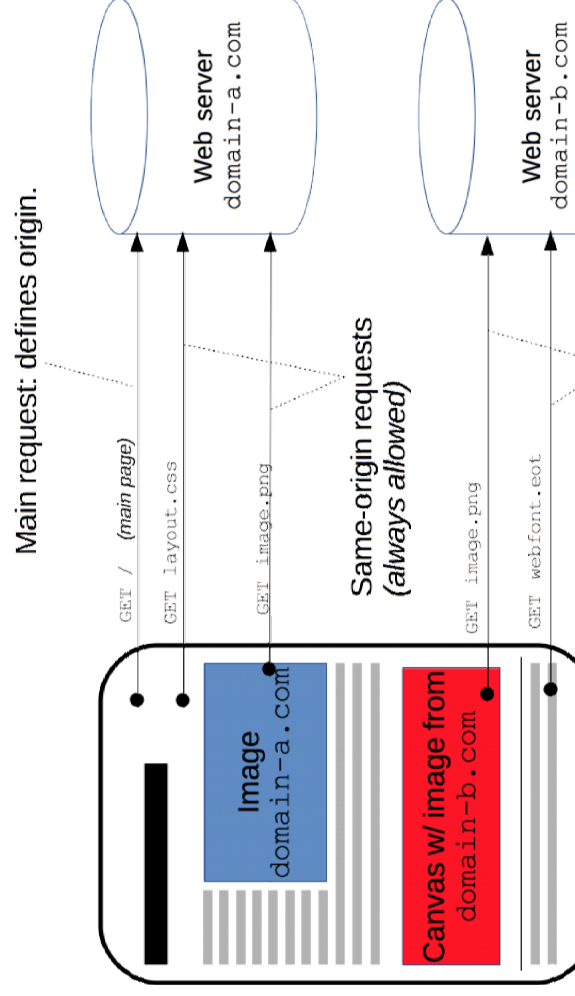
Authentification: C'est le scénario le plus courant pour utiliser JWT. Une fois l'utilisateur connecté, chaque requête ultérieure inclura le JWT, permettant à l'utilisateur d'accéder aux routes, services et ressources autorisés avec ce jeton. Single Sign On est une fonctionnalité qui utilise largement JWT de nos jours, en raison de sa faible surcharge et de sa capacité à être facilement utilisé dans différents domaines.

Échange d'informations: Les jetons Web JSON sont un bon moyen de transmettre des informations en toute sécurité entre les parties. Étant donné que les JWT peuvent être signés (par exemple, en utilisant des paires de clés publiques / privées), vous pouvez être sûr que les expéditeurs sont ceux qu'ils prétendent être. De plus, comme la signature est calculée à l'aide de l'en-tête et de la charge utile, vous pouvez également vérifier que le contenu n'a pas été altéré [21]

7.5. CORS

La politique de même origine est un concept de sécurité important mis en œuvre par les navigateurs Web pour empêcher le code Javascript de faire des demandes contre une origine différente (par exemple, un domaine différent) que celle à partir de laquelle il a été servi. Bien que la politique d'origine identique empêche efficacement les ressources d'origines différentes, elle prévaut également les interactions légitimes entre un serveur et des clients d'origine connue et fiable.

Supposons que vous ayez besoin de partager Données JSON avec une autre application ou un autre service. Si tout est hébergé sur un domaine, c'est un jeu d'enfant. Mais si les données sont sur un autre domaine, la politique "même origine" du navigateur vous arrête froid. Le partage de ressources d'origine croisée (CORS) est une nouvelle norme Web qui permet un accès interdomaine sécurisé sans code complexe côté serveur. La maîtrise de CORS permet aux applications Web et mobiles de partager des données simplement et en toute sécurité.[\[22\]](#)



7.6. Limitation de débit(Rate Limiting)

La limitation de débit est utilisée pour contrôler la quantité de trafic entrant et sortant vers ou depuis un réseau. Par exemple, supposons que vous utilisez l'API d'un service particulier configuré pour autoriser 100 requêtes / minute. Si le nombre de requêtes dépasse cette limite, une erreur sera déclenchée. Le raisonnement derrière la mise en œuvre des limites de débit est de permettre un meilleur flux de données et d'accroître la sécurité en atténuant les attaques telles que les attaques DDoS.

La limitation de débit est également utile si un utilisateur particulier sur le réseau fait une erreur dans sa requête, demandant ainsi au serveur de récupérer des tonnes d'informations qui peuvent surcharger le réseau pour tout le monde. Avec la limitation de débit en place cependant, ces types d'erreurs ou d'attaques sont beaucoup plus gérables.[23]

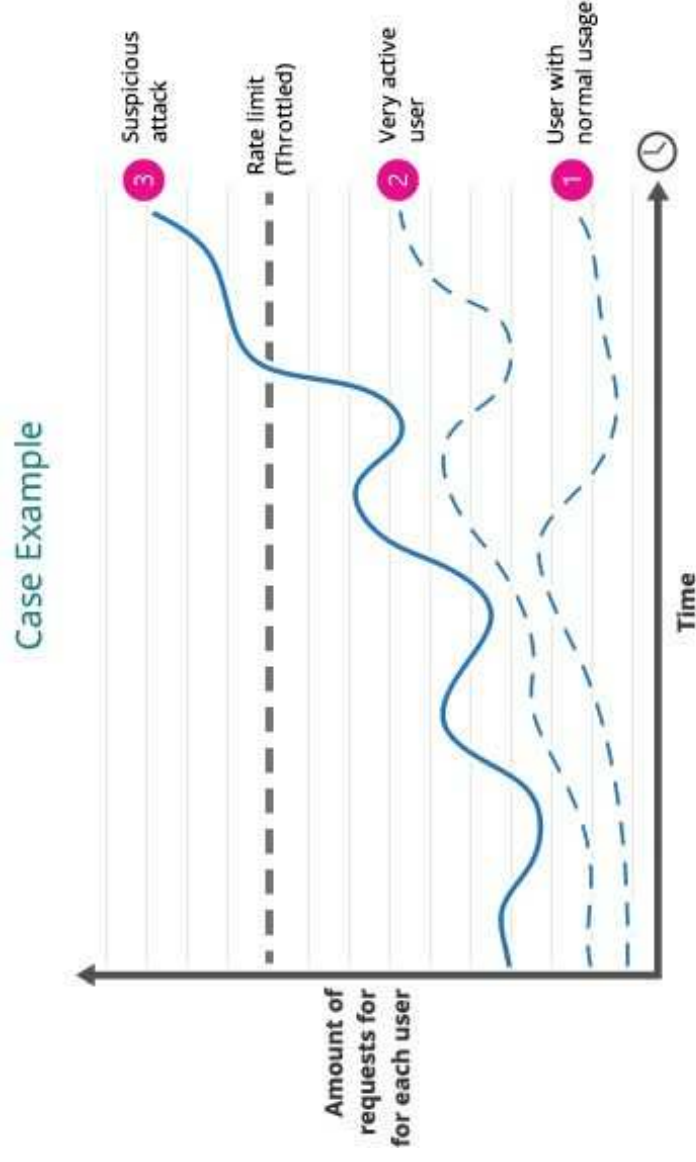


Figure 18: limitation du débit dans les API peuvent

a) Types de limites de débit

Il existe différentes méthodes et paramètres qui peuvent être définis lors de la définition des limites de débit. La méthode de limite de taux qui devrait être utilisée dépendra de ce que vous voulez réaliser ainsi que de la façon dont vous voulez être restrictif. La section ci-dessous présente trois types différents de méthodes de limitation de débit que vous pouvez implémenter.

- **Limitation du débit utilisateur:** Le type de limitation de débit le plus courant est la limitation du débit utilisateur. Cela associe le nombre de requêtes effectuées par un utilisateur à sa clé API ou à son adresse IP (en fonction de la méthode utilisée). Par conséquent, si l'utilisateur dépasse la limite de débit, toutes les autres demandes seront refusées jusqu'à ce qu'elles atteignent le développeur afin d'augmenter la limite ou d'attendre que le délai de limite de débit soit réinitialisé.
- **Limitation du taux géographique:** Pour accroître encore la sécurité dans certaines régions géographiques, les développeurs peuvent fixer des limites de taux pour des régions particulières et des périodes particulières. Par exemple, si un développeur sait que de minuit à 8h00 les utilisateurs d'une région particulière ne seront pas aussi actifs, ils peuvent définir des limites de débit inférieures pour cette période. Cela peut être utilisé comme mesure préventive pour aider à réduire davantage le risque d'attaques ou d'activités suspectes.

- **Limitation du débit du serveur:** Si un développeur a défini certains serveurs pour gérer certains aspects de son application, il peut définir des limites de débit au niveau du serveur. Cela donne aux développeurs la liberté de réduire les limites de trafic sur le serveur A tout en l'augmentant sur le serveur B (un serveur plus communément utilisé).

La limitation du débit peut être une excellente méthode pour lutter contre les attaques d'infrastructure et bloquer d'autres types d'activités suspectes. Comme mentionné, il existe différentes méthodes que vous pouvez utiliser pour implémenter la limitation de débit que ce soit au

7.7. Package Lcapy

Lcapy est un paquet Python pour l'analyse de circuit linéaire. Il ne résoudra que les réseaux linéaires invariants dans le temps. En d'autres termes, les réseaux constitués de composants de circuit de base (R, L, C, etc.) qui ne varient pas avec le temps.

Les réseaux et les circuits peuvent être décrits en utilisant des listes de réseaux ou des combinaisons d'éléments de réseau. Ceux-ci peuvent être dessinés semi-automatiquement.

Lcapy ne peut pas analyser directement des dispositifs non linéaires tels que des diodes ou des transistors bien qu'il supporte des opamps simples sans saturation. Néanmoins, il peut les dessiner!

Lcapy utilise SymPy (symbolique Python) pour ses valeurs et expressions et ainsi l'analyse du circuit peut être effectuée symboliquement.

Avant de pouvoir utiliser Lcapy, vous devez installer le paquet Lcapy ou configurer PYTHONPATH pour trouver les fichiers sources de Lcapy. [24]

a) Installation de Lcapy pour Linux (Ubuntu et variantes)

Vous devez installer le paquet SymPy:

```
$ sudo apt-get install python-sympy
```

Pour le traçage, vous avez besoin des paquets Matplotlib et NumPy:

```
$ sudo apt-get install python-numpy python-matplotlib
```

Pour le dessin schématique, vous avez besoin de pdflatex, du paquetage circuitkz, de imagemagick et de ghostscript.

```
$ sudo apt-get install texlive-latex-base texlive-pictures texlive-standalone imagemagick ghostscript
```

Lcapy peut être installé en utilisant:

```
$ cd lcapy
$ sudo python setup.py install
```

8. INSTALLATION DE LA SOLUTION KONG

a) 1- Installer Kong:

Commencez par télécharger le package correspondant à votre configuration: j'utilise ubuntu 16.04 xenial

alors vous pouvez exécuter les commandes suivantes

```
$ sudo apt-get update
$ sudo apt-get install openssl libpcre3 procps perl
$ sudo dpkg -i kong-community-edition-0.12.3.xenial.all.deb
```

b) 2- Préparez votre base de données:

Configurez Kong pour qu'il puisse se connecter à votre base de données. Kong prend en charge PostgreSQL 9.5+ et Cassandra 3.x.x en tant que banque de données.

➤ Installations de postgresQL9.5 :

```
$ sudo apt-get install postgresql postgresql-contrib
```

Si vous utilisez Postgres, veuillez provisionner une base de données et un utilisateur avant de démarrer Kong

J'utilise postgres donc je devrais créer un utilisateur et une base de données

```
$ cd etc/kong

postgres=# CREATE USER diden;
postgres=# CREATE DATABASE kongdata OWNER diden;
postgres=# ALTER USER diden WITH PASSWORD 'aze';
```

Si tout s'est bien passé, vous devriez voir un message (Kong started) vous informant que Kong est en cours d'exécution.

```
$ sudo kong start -c /etc/kong/kong.config
[sudo] Mot de passe de diden :

2018/06/06 22:02:54 [warn] ulimit is currently set to "1024". For better
performance set it to at least "4096" using "ulimit -n"
Kong started
```

Par défaut Kong écoute sur les ports suivants:

: **8000** sur lequel Kong écoute le trafic HTTP entrant de vos clients et le transmet à vos services en amont.

: **8443** sur lequel Kong écoute le trafic HTTPS entrant. Ce port a un comportement similaire à celui du port **8000**, sauf qu'il n'attend que le trafic HTTPS. Ce port peut être désactivé via le fichier de configuration.

: **8001** sur lequel l'API Admin utilisée pour configurer Kong écoute.

: **8444** sur lequel l'API d'administration est à l'écoute du trafic HTTPS.

d) 4- Utilisez Kong:

Kong est en cours d'exécution :

dans le terminal peut utiliser curl

```
$ curl -i http://localhost:8001/
```

dans le navigateur, vous pouvez consulter l'adresse

<http://localhost:8001/>



8.2. Configuration d'un service

Dans cette section, vous allez ajouter une API à Kong. Pour ce faire, vous devez d'abord ajouter un service; C'est le nom que Kong utilise pour se référer aux API amont et aux microservices qu'il gère.

Pour ce faire, nous devons créer un service pointant vers l'API des laboratoires. Avant de pouvoir commencer à faire des demandes à l'encontre du service, vous devez ajouter un itinéraire. Les routes spécifient comment (et si) les demandes sont envoyées à leurs services après qu'elles aient atteint Kong. Un seul service peut avoir plusieurs itinéraires.

Après avoir configuré le service et l'itinéraire, vous serez en mesure de faire des demandes via Kong en les utilisant.

Kong expose une API Admin RESTful sur le port: 8001. Kong est la configuration, y compris l'ajout de services et de routes, est faite via des demandes sur cette API. Je ne l'ai pas parce que je travaille dans l'hôte local, donc je vais passer cette étape

a) Ajoutez votre service en utilisant l'API Admin

Ajoutez votre service en utilisant l'API Admin

Émettez la requête cURL suivante pour ajouter votre premier service à Kong:

```
$ curl -i -X POST \
  --url http://localhost:8001/services/ \
  --data 'name=example-service' \
  --data 'url=http://mockbin.org'
```

b) Ajouter un route pour le service

```
$ curl -i -X POST \
  --url http://localhost:8001/services/example-service/routes \
  --data 'hosts[]=example.com'
```

c) Transférer vos demandes via Kong

Emettez la requête cURL suivante pour vérifier que Kong transmet correctement les demandes à votre service. Notez que Kong gère par défaut les requêtes proxy sur le port: 8000:

```
$ curl -i -X GET \
  --url http://localhost:8000/ \
  --header 'Host: example.com'
```

Une réponse réussie signifie que Kong redirige maintenant les requêtes effectuées vers `http://localhost:8000` vers l'URL que nous avons configurée à l'étape 1, et nous renvoie la réponse. Kong sait faire cela via l'en-tête défini dans la requête cURL ci-dessus

8.3. Configuration d'un API :

Dans cette section, je vais ajouter votre API à la couche Kong. C'est la première étape pour que Kong gère mon API. Pour ce faire, j'ajoute mon API à Kong,

Kong expose une API Admin RESTful sur le port 8001 pour la gestion de la configuration de votre instance ou cluster Kong.

a) **Ajoutez votre API à l'aide de l'API Admin**

Emettez la requête cURL suivante pour ajouter mon API à Kong:

```
$ curl -i -X POST \
  --url http://localhost:8001/apis/ \
  --data 'name=my_api' \
  --data 'hosts=my_api.com' \
  --data 'upstream_url=http://localhost:5000/'
```

Vous devriez voir une réponse similaire de cette requête:

```
HTTP/1.1 201 Created
Date: Wed, 06 Jun 2018 21:36:51 GMT
Content-Type: application/json; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Origin: *
Server: kong/0.12.3

{"created_at":1528325996575,"strip_uri":true,"id":"a97de123-274b-4ce0-8ca1-147e7f2ff8bf","hosts":["my_api.com"],"name":"my_api","http_if_terminated":false,"preserve_host":false,"upstream_url":"http://localhost:5000/","upstream_connect_timeout":60000,"upstream_send_timeout":60000,"upstream_read_timeout":60000,"retries":5,"https_only":false}
```

Emettez la requête cURL suivante pour vérifier que Kong transmet correctement les demandes à votre API. Notez que Kong gère par défaut les requêtes proxy sur le port: 8000:

```
$ curl -i -X GET \
  --url http://localhost:8000/ \
  --header 'Host: my_api.com'
```

Une réponse réussie signifie que Kong redirige maintenant les requêtes faites à `http://localhost:8000` vers le fichier `upstream_url` que nous avons configuré à l'étape 1, et nous renvoie la réponse. Kong sait faire cela via l'en-tête défini dans la requête cURL ci-dessus

➤ **Récupérer l'API :**

en utilisant l'identifiant unique ou le nom de l'API pour récupérer

```
$ curl -i -X GET \
  --url http://localhost:8001/apis/my_api
```

➤ **Mise à jour :**

```
$ curl -i -X PATCH \
  --url http://localhost:8001/apis/my\_api
```

➤ **Supprimer l'API :**

```
$ curl -i -X DELETE \
  --url http://localhost:8001/apis/my\_api
```

8.4. Ajouter des consommateurs

Dans cette section, nous allons apprendre comment ajouter des consommateurs à mes instances de Kong. Les consommateurs sont associés à des personnes utilisant mon API et peuvent être utilisés pour le suivi, la gestion des accès, etc.

Créons un utilisateur nommé diden en émettant la requête suivante:

```
$ curl -i -X POST \
  --url http://localhost:8001/consumers/ \
  --data "username=diden"
```

➤ **Récupérer le consommateur :**

en utilisant l'identifiant unique ou le nom de consommateur pour récupérer

```
$ curl -i -X GET \
```

```
--url http://localhost:8001/consumers/diden
```

➤ **Supprimer le consommateur :**

```
$ curl -i -X DELETE \
  --url http://localhost:8001/consumers/diden
```

8.5. Activation des plugins

Dans cette section, je vais configurer les plugins Kong. L'un des principes de base de Kong est son extensibilité à travers les plugins. Les plugins vous permettent d'ajouter facilement de nouvelles fonctionnalités à votre API ou de faciliter la gestion de votre API.

Dans les étapes ci-dessous, je vais configurer le plugin key-auth pour ajouter une authentification à l'API. Avant l'ajout de ce plugin, toutes les demandes à mon API seraient transmises par proxy en amont.

Une fois que j'aurai ajouté et configuré ce plugin, seules les requêtes avec les clés API correctes seront transmises par proxy, toutes les autres demandes seront rejetées par Kong, protégeant ainsi votre service en amont contre une utilisation non autorisée.

a) Configurer le plugin key-auth pour votre API

Emettez la requête cURL suivante sur l'API précédemment créée nommée my_api:

```
$ curl -i -X POST \
--url http://localhost:8001/apis/my_api/plugins/ \
--data 'name=key-auth'

HTTP/1.1 201 Created
Date: Wed, 06 Jun 2018 21:44:57 GMT
Content-Type: application/json; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Origin: *
Server: kong/0.12.3

{"created_at":1528322799000,"config":
{"key_in_body":false,"run_on_preflight":true,"anonymous":"","hide_credentials":false,"key_names":["apikey"]},"id":"4c69546e-3509-45cd-b9cd-3211925afa8d","name":"key-auth","api_id":"a97de123-274b-4ce0-8ca1-147e7f2ff8bf","enabled":true}
```

Emettez la requête cURL suivante pour vérifier que le plug-in key-auth a été correctement configuré sur l'API:

```
--data 'key=UnivMosta2018'
```

```
HTTP/1.1 201 Created
Date: Wed, 06 Jun 2018 22:08:11 GMT
Content-Type: application/json; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Origin: *
Server: kong/0.12.3
```

```
{"id":"d776021f-9e42-4fca-ba36-
07c69b418327","created_at":1528322892000,"key":"UnivMosta2018","consumer_id":
"d7a5f8b8-a56e-4576-8e6c-6206568c898c"}
```

Nous pouvons maintenant émettre la demande suivante pour vérifier que les informations d'identification de notre diden Consumer sont valides:

```
$ curl -i -X GET \
--url http://localhost:8000 \
--header "Host: my_api.com" \
--header "apikey: UnivMosta2018"
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 5188
Connection: keep-alive
Access-Control-Allow-Origin: *
Server: Werkzeug/0.14.1 Python/2.7.12
Date: Wed, 06 Jun 2018 22:10:47 GMT
X-Kong-Upstream-Latency: 8
X-Kong-Proxy-Latency: 40
Via: kong/0.12.3
```

➤ **Mise à jour :**

```
$ curl -i -X PATCH \
--url http://localhost:8001/apis/my\_api/plugins/93e1b9aa-6fa4-4e1c-9451-
```

[abe6c55b3840](http://localhost:8001/apis/my_api/plugins/93e1b9aa-6fa4-4e1c-9451-abe6c55b3840)

➤ **Supprimer plugin :**

```
$ curl -i -X PATCH \
--url http://localhost:8001/apis/my\_api/plugins/93e1b9aa-6fa4-4e1c-9451-
```

[abe6c55b3840](http://localhost:8001/apis/my_api/plugins/93e1b9aa-6fa4-4e1c-9451-abe6c55b3840)

9. CONCLUSION :

Les laboratoires à distance dans les e-laboratoires deviennent modernes et tendent vers l'enseignement au niveau scolaire et universitaire. Malheureusement, avec cela viennent les menaces d'attaques possibles. Les attaques peuvent varier en fonction du type d'expérience et du but pour lequel elles sont exécutées, de même, la défense varie également.

Les attaques peuvent être dirigées vers les serveurs de contrôle d'expériences conduisant généralement à la fermeture de l'expérience et à l'impossibilité d'accès. L'interférence DoS est utilisée principalement pour ces attaques. Ces attaques peuvent être appliquées à n'importe quel serveur sur Internet. Ce problème est décrit de manière adéquate dans la littérature et différents types de défense peuvent être utilisés. Les mesures de protection les plus sûres sont basées sur une base matérielle elle-même. Toutes ces solutions sont plutôt chères; par conséquent, leur utilisation est rarement trouvée avec des expériences simples. [2]

La sécurité des laboratoires distants est beaucoup plus sensible à l'attaque visant le matériel d'expérimentation. Ces attaques conduisent à endommager des équipements coûteux entraînant une perte financière substantielle. Les attaques peuvent être exécutées par l'accès aux serveurs ou directement par l'envoi de commandes de contrôle malveillantes aux laboratoires distants. Une solution possible de cette situation consiste à sécuriser l'expérimentation par nom d'utilisateur et mot de passe. Cependant, cette approche est susceptible d'être interceptée ou de créer une confusion d'identité chez l'utilisateur. Par conséquent, il est approprié d'utiliser une connexion cryptée entre l'utilisateur et l'expérience, basée sur le protocole HTTPS dans ce cas. Ce protocole assure une sécurité de connexion suffisante et vérifie l'identité de l'utilisateur s'il est utilisé correctement. Cette solution comporte également des risques de sécurité. Il y a une possibilité d'interception de clés publiques éliminées en utilisant des certificats validés par une autorité de certification. [12]

10. RÉFÉRENCE

- [1] [František Schauer, František Lustig, Miroslava Ošvoldová: Internet Natural Science Remote e-Laboratory (INRe-L) for Remote Experiments /In: Innovations 2011: World Innovations in Engineering Education and Research (USA), iNEER / ed. W. Aung, et al. - (2011), s.51-68.,]
- [2] Yuval, Fedel. Uri, Kanonov. Yuval, Elovici. Shlomi, Dolev. Chanan,. "Google Android: A Comprehensive Security Assessment". IEEE Security & Privacy Vol 8 Issue 2 March-April 2010 pp35 – 44
- [3] Ping of death. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 10 October 2011 [Read: 2012-02-06]. http://en.wikipedia.org/wiki/Ping_of_death
- [4] Denial-of-service attack: ICMP flood. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 1 February 2012 [Read: 2012-02-06]. http://en.wikipedia.org/wiki/Denial-of-service_attack
- [5] SYN flood. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 22 January 2012 [Read: 2012-02-06]. http://en.wikipedia.org/wiki/SYN_flood
- [6] UDP Flood Attack. In: Javvin [online]. 2011 [cit. 2012-02-27]. <http://www.javvin.com/networksecurity/UDPFloodAttack.html> [15] GOPI, Midhun. Distributed Denial of Service Attack (DDoS). In: Security Research [online]. November 21, 2011 [Read: 2012-02-27]. <http://securityresearch.in/index.php/tutorials/how-to/distributed-denial-of-service-attack-ddos/>
- [7] imperva incapsula DDoS protection center <http://www.incapsula.com/ddos/ddos-attacks/>
- [8] Gamaeva, Maria a Yury Namestnikov. DDoS attacks in H2 2011. In: Securelist [online]. 22 Feb 2012 [Read: 2012-02-27]. http://www.securelist.com/en/analysis/204792221/DDoS_attacks_in_H2_2011
- [9]GOPI, Midhun. Distributed Denial of Service Attack (DDoS). In: Security Research [online]. November 21, 2011 [Read: 2012-02-27]. <http://securityresearch.in/index.php/tutorials/howto/distributed-denial-of-service-attack-ddos/>
- [10]Denial-of-Service Attacks. In: Webhosting Depot [online]. © 2001- 2012 [Read: 2012-02-27]. <http://www.webhosting-depot.com/articles/ddos-attacks.php>
- [11] DoS Attack: Prevention And Response. In: Serving History [online]. 2012 [Read: 2012-02-27]. <http://www.webhosting-depot.com/articles/ddos-attacks.php>
- [12] The World Wide Web Security FAQ: Securing against Denial of Service attacks. W3C: Security [online]. 1.7. W3C, 2003, 2003/02/23 [Read: 2012-02-06].

- [16] Simpler data streaming for greater everything.
<https://streamdata.io/blog/developing-an-helloworld-kong-plugin/>
- [17] Kong, le gorille de l'API Management vu de près
<https://blog.octo.com/kong-le-gorille-de-l-api-management-vu-de-pres/>
- [18] what is kong <https://getkong.org/about/>
- [19] IT Consultant @CarbonParis, #java #search #data #craft #devops #stream
<https://medium.com/@d3rwan/r%C3%A9gnez-sur-vos-apis-avec-kong-c48f600883f7>
- [20] Les nouvelles architectures du Web 06 May 2014 architectures web, Single Page Application by Aurelie Magniez <http://www.it-expertise.com/les-nouvelles-architectures-du-web/>
- [21] get the [JWT Handbook for free](https://jwt.io/introduction/) and learn JWTs indepth! <https://jwt.io/introduction/>
- [22] Cross-origin resource sharing (CORS)
<https://developer.mozilla.org/fr/docs/Web/HTTP/CORS>
- [23] PERFMATTERS [FreeTestAccount](#) Supercharge your Website with KeyCDN
HTTP/2 - Free SSL - RESTful API - Instant Purge
<https://www.keycdn.com/support/rate-limiting/>
- [24] [Lcapy 0.26.0 documentation](#) © Copyright 2014--2017, Michael Hayes. Created using [Sphinx](#) 1.3.6. <http://lcapy.elec.canterbury.ac.nz/tutorial.html#plotting>