Retour d'expérience sur l'utilisation des challenges de sécurité durant un cours sur la sécurité des objets connectés

RESSI 2020 – 16 au 18 décembre 2020 – En ligne
Rendez-vous de la Recherche et de l'Enseignement
de la Sécurité des Systèmes d'Information

Session Enseignement

Christophe TILMANT - Maître de Conférences - ISIMA
christophe.tilmant@uca.fr

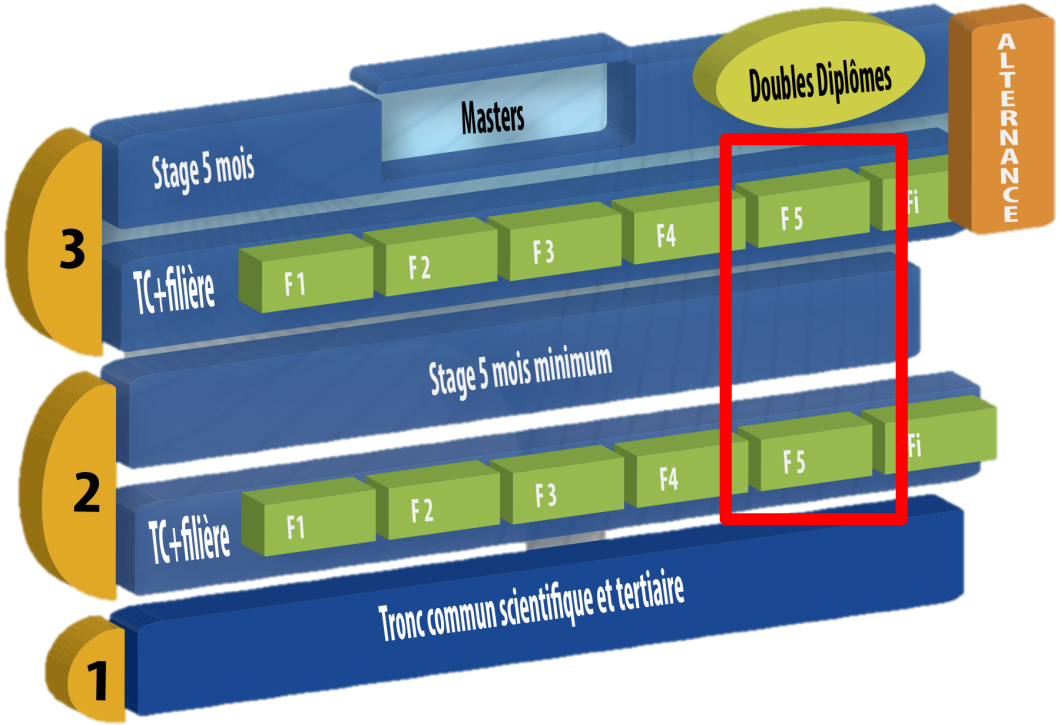
Jacques LAFFONT - Professeur agrégé - Polytech Clermont-Ferrand

Formation : Ou est enseignée la sécurité des objets connectés ?

ISIMA
Institut Supérieur d'Informatique de Modélisation et de leurs Applications

Institut Supérieur d'Informatique, de Modélisation et de leurs Applications

INSTITUT D'INFORMATIQUE
UNIVERSITÉ Clermont Auvergne



SecNumedu
ANSSI

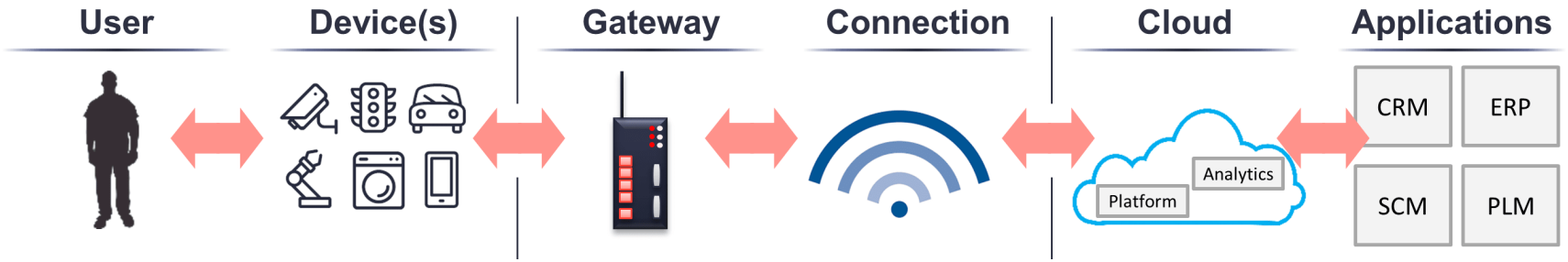
CyberEdu
La sécurité par l'enseignement supérieur des NTIC

F5 – Réseaux et sécurité informatique

https://www.isima.fr/f5-reseaux-et-securite/

Formation : Contenu pédagogique du cours

Contenu : présentation du principe de sécurité en profondeur avec un durcissement sur plusieurs niveaux



- Niveau réseau : en protégeant la sécurité physique du réseau utilisé ;
- Niveau transport : utilisation de SSL en tenant compte du problème de déploiement des certificats coté client ;
- Niveau applicatif : une authentification applicative simple, un chiffrement des données au niveau applicatif, le problème du cloisonnement entre utilisateurs ;
- Niveau matériel : accès à la mémoire et au protocole de communication entre périphériques.

Objectif de ce cours (réalisé à l'aide de TP) :

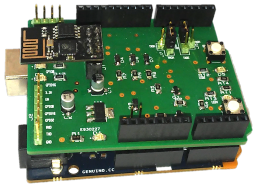
- Public : élève ingénieur en informatique en début de spécialisation en sécurité informatique (cours introductif) ;
- En complément d'un cours magistral sur les objets connectés (tronc commun de la formation) ;
- **Les IoT sont un magnifique terrain de jeu pour introduire les concepts de la sécurité informatique.**

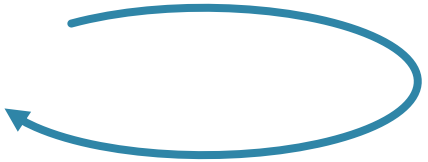
Formation : Contenu pédagogique du cours

Mise en place de l'application IoT

Mise en évidence des failles de sécurité

Durcissement du système





- Introduction - Mise en place de la plateforme de développement sous Arduino ;
- QCM - Introduction au protocole MQTT - Echange de messages avec un broker public ;
- Mise en place de l'application IoT/MQTT sur Arduino;
- QCM - Chaine de sécurité MQTT ;
- Challenge de sécurité n°1 ;
- Débriefing du challenge - Camouflage des informations et authentification ;
- QCM - Analyse réseau avec *tcpdump* et chiffrement ;
- QCM - Chiffrement symétrique AES ;
- Chiffrement du *payload* et mise en œuvre sur Arduino ;
- Challenge de sécurité n°2 ;
- Mise en œuvre SSL et sécurité bas-niveau (BusPirate).

Challenge de sécurité : Exemple d'un sujet de l'épreuve

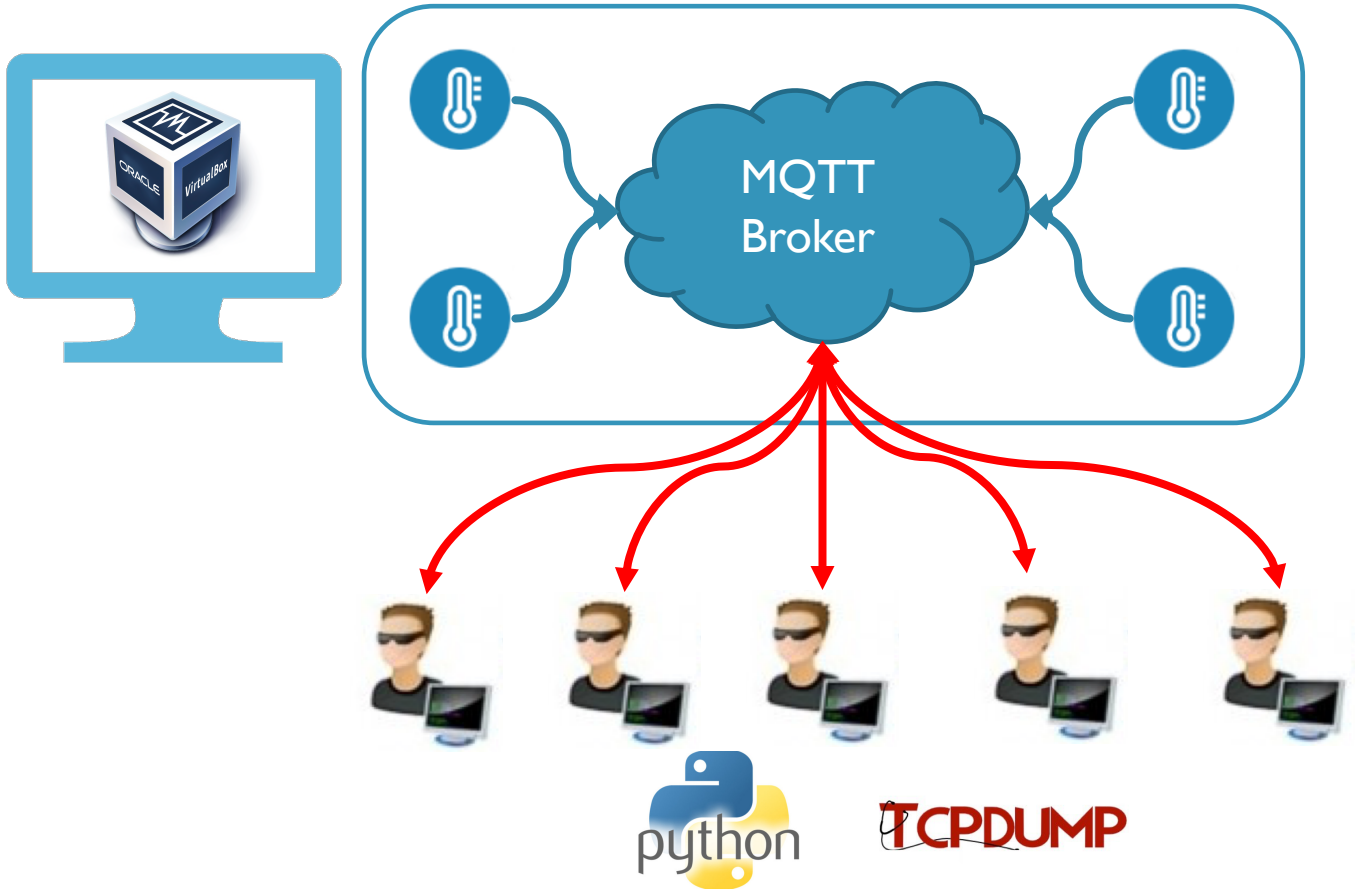
Objectif : Vous devez allumer les LEDs de l'objet connecté du professeur. Passage en mode attaquant (*Ethical Hacking*).

Moyens :

- Utilisation de *tcpdump;*
- Analyse des *payload* émis par la carte du professeur ➔ réaliser l'objectif.

Défis :

1. Récupération sur une communication non-sécurisé des paramètres d'authentification ;
2. Réussite par un simple rejet ;
3. Dix messages sont émis à tour de rôle : envoyer le bon ;
4. Chiffrement AES avec une clef de 2 bytes ;
5. Chiffrement AES avec une clef de 128 bits.



Challenge de sécurité : Notation

Evaluation :

- N pts / défis réussis ;
- M pts / classement en temps /défi réussi.

Intérêt :

- La partie de la notation « Défi » permet d'évaluer les compétences intrinsèques ;
- La partie de la notation « Temps » permet d'évaluer la réactivité, …
  mais surtout cela empêche la diffusion des résultats entre chaque groupe.

L'objectif de cette séance est de résoudre un challenge de sécurité qui est décomposé en 5 défis. Le niveau de difficulté va croître de défi en défi. Afin de commencer un nouveau défi, vous devez avoir résolu les défis précédents.

Afin de vous évaluer sur ce challenge, votre groupe récoltera des points pour chaque défi réussi:

- défi 1 réussi = **2 points;**
- défi 2 réussi = **2 points;**
- défi 3 réussi = **2 points;**
- défi 4 réussi = **2 points;**
- défi 5 réussi = **2 points.**

De plus, dans le domaine de la sécurité informatique le temps de réaction doit être le plus court possible, donc des points supplémentaires seront affectés suivant le temps que vous mettez pour résoudre ces défis. Si vous résolvez un défi, votre classement en temps (= temps pour résoudre le défi, en prenant comme début le moment où vous récupérez les renseignements) vous permettra de récolter des points supplémentaires:

Exemple si 12 groupes participent au challenge

- Groupe 1 = **2 points** (le plus rapide);
- Groupe 2 = 2*(1 - 1/11) = **1,82 points** (le deuxième plus rapide);
- Groupe 3 = 2*(1 - 2/11) = **1,64 points** (le troisième plus rapide);
- Groupe 4 = 2*(1 - 3/11) = **1,45 points**;
- Groupe 5 = 2*(1 - 4/11) = **1,27 points**;
- Groupe 6 = 2*(1 - 5/11) = **1,09 points**;
- Groupe 7 = 2*(1 - 6/11) = **0,9 point**;
- Groupe 8 = 2*(1 - 7/11) = **0,73 point**;
- Groupe 9 = 2*(1 - 8/11) = **0,55 point**;
- Groupe 10 = 2*(1 - 9/11) = **0,36 point**;
- Groupe 11 = 2*(1 - 10/11) = **0,18 point;**
- Groupe 12 = 2*(1 - 11/11) = **0 point**.

Nous attirons votre attention que ce travail est individuel (au sens du groupe) et qu'**il est interdit de diffuser sa solution auprès des autres groupes**. Si vous êtes tentés de le faire, il y a de forte chance que votre groupe baissera dans le classement en temps, et donc moins de points. De plus, à chaque défi résolu, vous devrez déposer votre script python qui sera évalué par les enseignants et analysé par le logiciel d'anti-plagiat de l'université (*compilatio*).

Garde fou :

- Préparation à la maison de fonctions de base à l'aide d'un squelette de code et de plusieurs tests unitaires ;
- Durant la séance, les groupes peuvent demander des indices aux enseignants en contrepartie de points.

Challenge de sécurité : Déroulement du côté apprenant

Préparation :

Fonctions Python préparatoires au challenge 2

Compléter les différentes fonctions décrites dans le fichier python.

Vous pouvez vous assurer du bon fonctionnement de vos fonctions en utilisant les tests unitaires proposés.

Squelette application de hack pour le challenge 2

A analyser de préférence avant le début du challenge.

```python
def EncodeAES(chaine,key):
    """ Chiffrement AES 128 bits de chaine avec key comme clef.
        La taille de chaine est quelconque et sera complétée par le
        caractère espace si nécessaire. Key est un tableau 16 éléments."""

def DecodeAES(chaine,key):
    """ Déchiffre chaine. La clef key est un tableau de 16 éléments.
        Les caractères espace en fin de la chaine résultatante seront supprimés."""

def Contient(aiguille,chaine):
    """ Résultat True si le paramètre chaine contient la chaine aiguille."""

def EstImprimable(caractere):
    """ Liste des caractères imprimables :
        0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ """

def Remplace(chaine,avant,apres):
    """ Remplace les occurrences de avant par apres dans chaine."""

def Extraire(chaine,separation,n):
    """ Retourne la valeur du nième champ de chaine.
        Les champs sont séparés par le caractère séparation."""

def Format(n):
    """ Retourne une chaine de caractères de 4 caractères pour tout nombre entier de 0 à  9999
        Les valeurs seront précédées de 0."""

def main():
    """ Tests, toutes les lignes sont correctes (résultat : True). Compléter les fonctions."""
    print (Xor(" $-_.","A")=="Hello")
    print (Xor("-/-43","ABA")=="Bonjour")
    print (Indice([1,2,3,4,5,6],3)==2)
    print (EncodeBase64(b"Une Chaine")==b"VW51IENoYWluZQ==")
    print (DecodeBase64(b"VW51IENoYWluZQ==")==b"Une Chaine")
    print (EncodeAES(b"Elements",[2,2,2,3,3,3,4,4,4,5,5,5,6,6,6,6])==b"\xcb[q(\x07\xe70\xff\x13D\xfe\xf9\x9eQ\x08!")
    print (DecodeAES(b"\xcb[q(\x07\xe70\xff\x13D\xfe\xf9\x9eQ\x08!",[2,2,2,3,3,3,4,4,4,5,5,5,6,6,6,6])==b"Elements")
    print (Contient("OK","Le resultat est OK !")==True)
    print (Contient("OK","Le resultat est Ok !")==False)
    print (EstImprimable("A")==True)
    print (EstImprimable("\x07")==False)
    print (EstImprimable(" ")==True)
    print (Remplace("Ceci est une string typique","string","chaine")=="Ceci est une chaine typique")
    print (Extraire("ROUGE,0034,4EF563",",",1)==34)
    print (Format(3)=="0003")
    print (Format(123)=="0123")
    return
```

```python
import time
import paho.mqtt.client as mqtt
import time
import base64
from Crypto.Cipher import AES

IP="172.16.32.7"
PORT=1080X
GROUPE="GROUPE_XX_YY_ZZ"

def EncodeXor(tabMessage,tabKey):
    tabKey=tabKey*(len(tabMessage)//len(tabKey)+1)
    return bytes([a^b for a,b in zip(tabMessage,tabKey)])

def DecodeXor(tabMessage,tabKey):
    tabKey=tabKey*(len(tabMessage)//len(tabKey)+1)
    return bytes([a^b for a,b in zip(tabMessage,tabKey)])

#Le travail commence ici
def newMessage(client,userData,msg):
    print ("\n",msg.topic,"\t\t",msg.payload,end=' ')
    if "LED2_HACKED" in msg.topic and GROUPE in msg.topic:
            print("\nWell done !")
            raise KeyboardInterrupt

    #Construction du nouveau payload ICI

    if False:#si construction payload OK :
        topic=msg.topic
        topic=topic.replace("GROUPE_XX",GROUPE)
        topic=topic.replace("LED1","LED2")
        client.publish(topic,newpayload)

def mqttConnect():
    mqttClient=mqtt.Client(GROUPE)
    mqttClient.username_pw_set("TOBEDETERMINED","TOBEDETERMINED")
    mqttClient.connect(IP,PORT)
    mqttClient.on_message=newMessage
    mqttClient.subscribe("TOBEDETERMINED")
    return mqttClient

def main():
    try:
        mqttClient=mqttConnect()
        while True:
            mqttClient.loop()
            time.sleep(0.5)
            print (".",end='')
    except KeyboardInterrupt:
        pass
    mqttClient.disconnect()
```

Jour J :

Déroulement du challenge :

Ce challenge est constitué de 5 défis.

Chaque défi vous octroie des points additionnés de points bonus dès qu'il est résolu.

Chaque défi vous apporte 2 points. Les points bonus sont calculés comme en fonction de votre rang. Le premier à avoir validé le défi emporte 2 points, le deuxième : 2.(1-1/N), et de façon générale pour le groupe de rang i le bonus sera : 3.(1-(i-1)/N). N étant le nombre de groupes ayant réussi le défi.

Chaque groupe ayant réalisé le défi aura donc un bonus, par contre la valeur du bonus dépendra du nombre de personnes ayant validé le défi (sauf pour le premier groupe).

Le temps pris en compte est le temps depuis le début du challenge, puis le temps depuis la validation du défi précédent.

Objectif :

Pour chaque défi, vous devez allumer la LED2 d'un IOT.

Pour allumer la LED2, il faut qu'un message ayant un payload correct et contenant "ON" soit reçu sur un topic de cette forme :

- ISIMA/SECRET_ZZZ/CHALLENGE_2/DEFI_Y/**GROUPE_NOM1_NOM2/LEDS/LED2**
  - ZZZ est à déterminer pendant le défi
  - Y correspond au numéro du défi (1 à 5)
  - GROUPE_NOMS_ETUDIANTS : Corresponds aux noms des étudiants du groupe en majuscule sans caractères accentués.
    - Cette chaine doit être strictement identique au clientID utilisé lors de la connexion au broker.

Attention si le topic ne correspond pas à cette structure vous ne serrez pas en mesure de valider le défi !

Informations générales:

Vous pourrez souscrire aux messages de commande de la LED1.

Un utilisateur externe (XX) publie alternativement des payloads contenant "ON" et "OFF" sur le topic de la LED1

- ISIMA/SECRET_ZZZ/CHALLENGE_2/DEFI_Y/**GROUPE_XX**/LEDS/LED1

Il vous appartient d'analyser les messages et de construire une attaque permettant d'allumer la LED2.

GROUPE_XX est le nom de cet utilisateur, il est fixé et non modifiable.

L'accès au broker est protégé (les accès anonymes sont interdits).

Pour pouvoir vous connecter, vous devez avoir accès au login / mot de passe du client ayant l'ID "user_x_y". Avec x correspondants au numéro du challenge (2) et y au numéro du défi (1 à 5).

Attention : pour le fonctionnement du système, un autre utilisateur ("monitor_x_y") est susceptible de se connecter au réseau. L'utilisation de ses identifiants est interdite. Si une telle activité est détectée, toutes vos tentatives seront rejetées.

Les payloads sont systématiquement encodés en base64.

Connexion au broker :

La connexion au broker doit impérativement être faire avec :

- un clientID du type GROUPE_NOM1_NOM2,
- un login correspondant au login du client user (chaine constituée de caractères majuscules),
- un mot de passe correspondant au mot de passe du client "user" (chaine constituée de caractères majuscules).

Challenge de sécurité : Déroulement du côté apprenant

Défis à réaliser durant la séance :

Défi No 1

Nous avons très peu d'informations à fournir concernant ce défi.

Le port du broker serait 10801.

Bonne chance.

Le document à rendre aura la forme suivante :

```
------------------------------------ Informations sur le Hack --------------------------------------

Détaillez succinctement dans cette partie votre analyse et la méthode utilisée

------------------------------------ Proof of Concept ----------------------------------------------

Code Python utilisé pour réaliser l'attaque.

------------------------------------------------------------------------------------------------------
```

Défi No 3

Enfin un défi à la hauteur des compétences du service.

Notre valeureux espion a réussi à déterminer que la clef de chiffrement était semblable au code d'une carte bleue. C'est à dire 4 chiffres de 0 à 9.

Le payload lui semble être constitué uniquement des caractères suivants "ON","OFF", espace " ", point "." et des caractères de 0 à 9 "0123456789".

Le port du broker est 10803.

Le document à rendre aura la forme suivante :

```
------------------------------------ Informations sur le Hack --------------------------------------

Détaillez succinctement dans cette partie votre analyse et la méthode utilisée

------------------------------------ Proof of Concept ----------------------------------------------

Code Python utilisé pour réaliser l'attaque.
```

Défi No 2

L'équipe de développement s'est fait vertement tancer, la qualité de la protection mise en place dans le défi précédent étant très faible.

C'est après être allé voir "Un jour sans fin" au cinéma que ce nouveau schéma de protection a été mis en place.

L'équipe de développeurs ayant complètement disparu ensuite, là encore les services de renseignement n'ont aucune information à donner sur ce défi.

On sait que le port du broker est le 10802.

Bon courage !

Le document à rendre aura la forme suivante :

```
------------------------------------ Informations sur le Hack --------------------------------------

Détaillez succinctement dans cette partie votre analyse et la méthode utilisée

------------------------------------ Proof of Concept ----------------------------------------------

Code Python utilisé pour réaliser l'attaque.
```

Défi No 4

Changement de méthode de l'équipe de renseignement. L'équipe de développeurs a dû suivre une formation sérieuse et complète.
En utilisant la ruse et la persuasion, quelques informations ont été obtenues.
Le mot de passe est plus long (10 caractères au maximum). Il n'est constitué que de lettres majuscules.
Le payload est constitué des caractères suivants "ONF .0123456789" il contiendrait de plus une partie constituée d'un nombre codé en hexadécimal ("0123456789ABCDEF").
Le port du broker est 10804.

Le document à rendre aura la forme suivante :

Défi No 5

Bonne nouvelle, nous avons à notre disposition le micrologiciel utilisé. Par contre aucune information sur le mot de passe utilisé. Le payload doit toujours avoir la même structure, on est à peu près certains qu'il est constitué des caractères suivants: "ONF .0123456789". Si le chiffrement utilisé est AES, il est évident que les recommandations de l'ANSSI auront été respectées (clef 128 bits).

Le port du broker est 10805.

Au cas où, une librairie permettant de faire du chiffrement AES en python est fournie.

Le document à rendre aura la forme suivante :

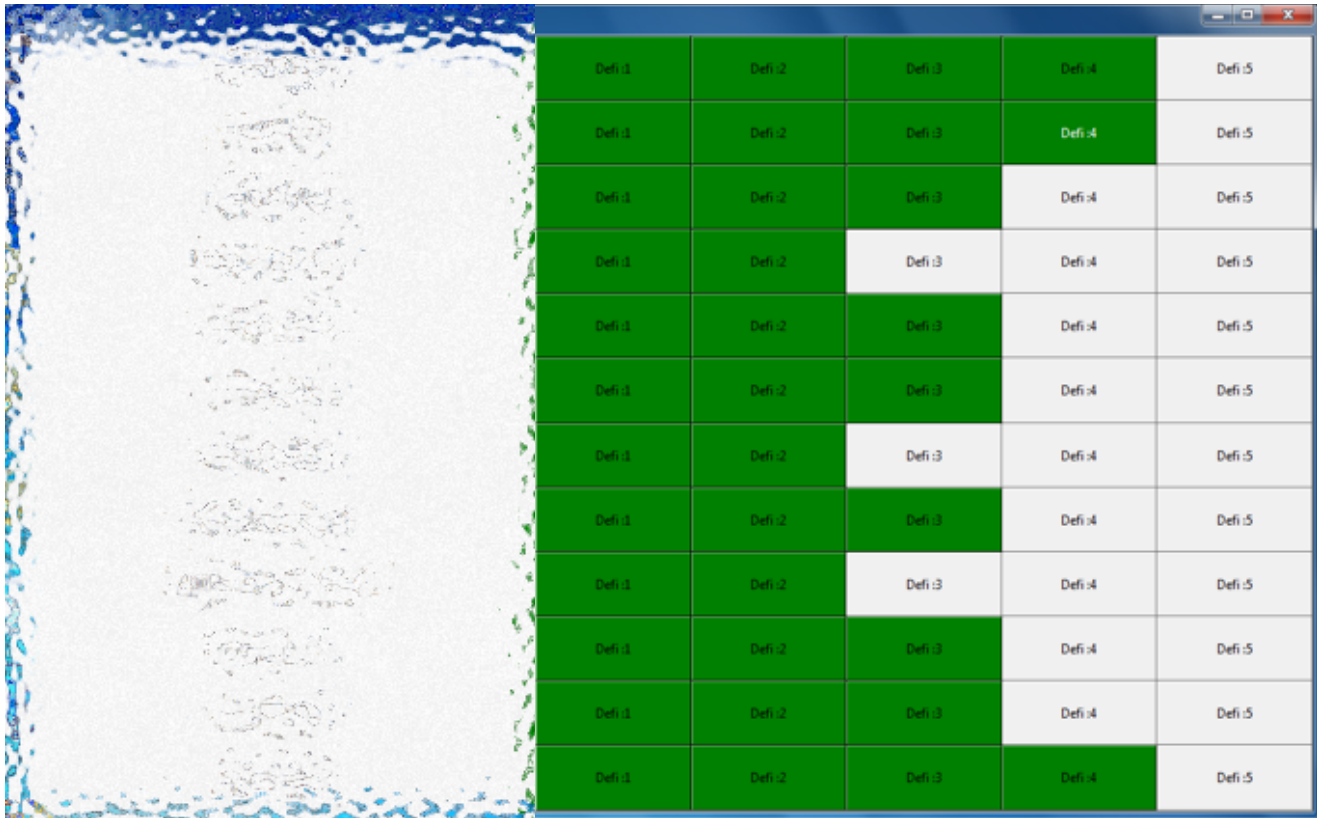
```
------------------------------------ Informations sur le Hack --------------------------------------

Détaillez succinctement dans cette partie votre analyse et la méthode utilisée

------------------------------------ Proof of Concept ----------------------------------------------

Code Python utilisé pour réaliser l'attaque.

------------------------------------------------------------------------------------------------------
```

Challenge de sécurité : Déroulement du côté enseignant

Visualisation en live des résultats : crée un réel enthousiasme dans l'implication des étudiants dans les challenges avec un bon esprit compétitif où les étudiants se challengent entre eux en oubliant la partie notation.

Programme tournant sur le poste enseignant et gérant automatiquement le challenge :

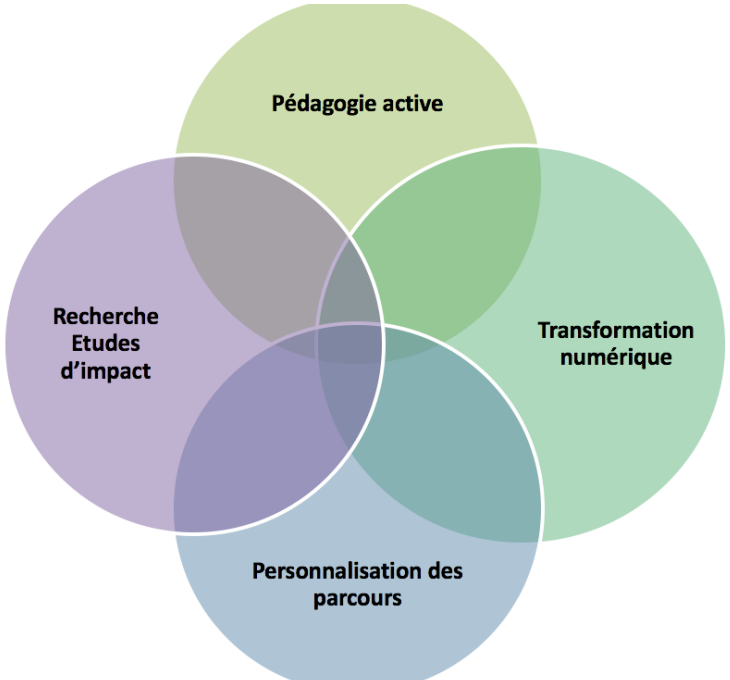
```
        if groupe==None:groupe=self.groupe
        return "/"+self.prefix+"/SECRET_"+secret+"/CHALLENGE_"+str(self.challenge)+"/DEFI_"+str(self.defi)
            +"/"+groupe+"/"+suffix

    def Polling(self,timeout=None):
        if timeout==None:
            timeout=self.timeOut
        self.hackClient.loop_read()
        self.hackClient.loop_write()
        return (time.time()-self.startTime)<timeout

    def PollingHack(self,timeout=None):
        return self.Polling(timeout) and not self.hacked and not self.gotHack

    def PollingHacked(self,timeout=None):
        return self.Polling(timeout) and not self.hacked

    def Hack(self,timeout=None):
        if not self.gotHack:
            return self.Polling(timeout) and not self.hacked
        else:
            self.sendHack()
            return self.PollingHacked(timeout)

    def __repr__(self):
        return "{} {defi} {groupe}->".format(self.__class__.__name__,**self.__dict__)

def main():
    print (Defi.__doc__)
    pass

if __name__ == '__main__':
    main()
```

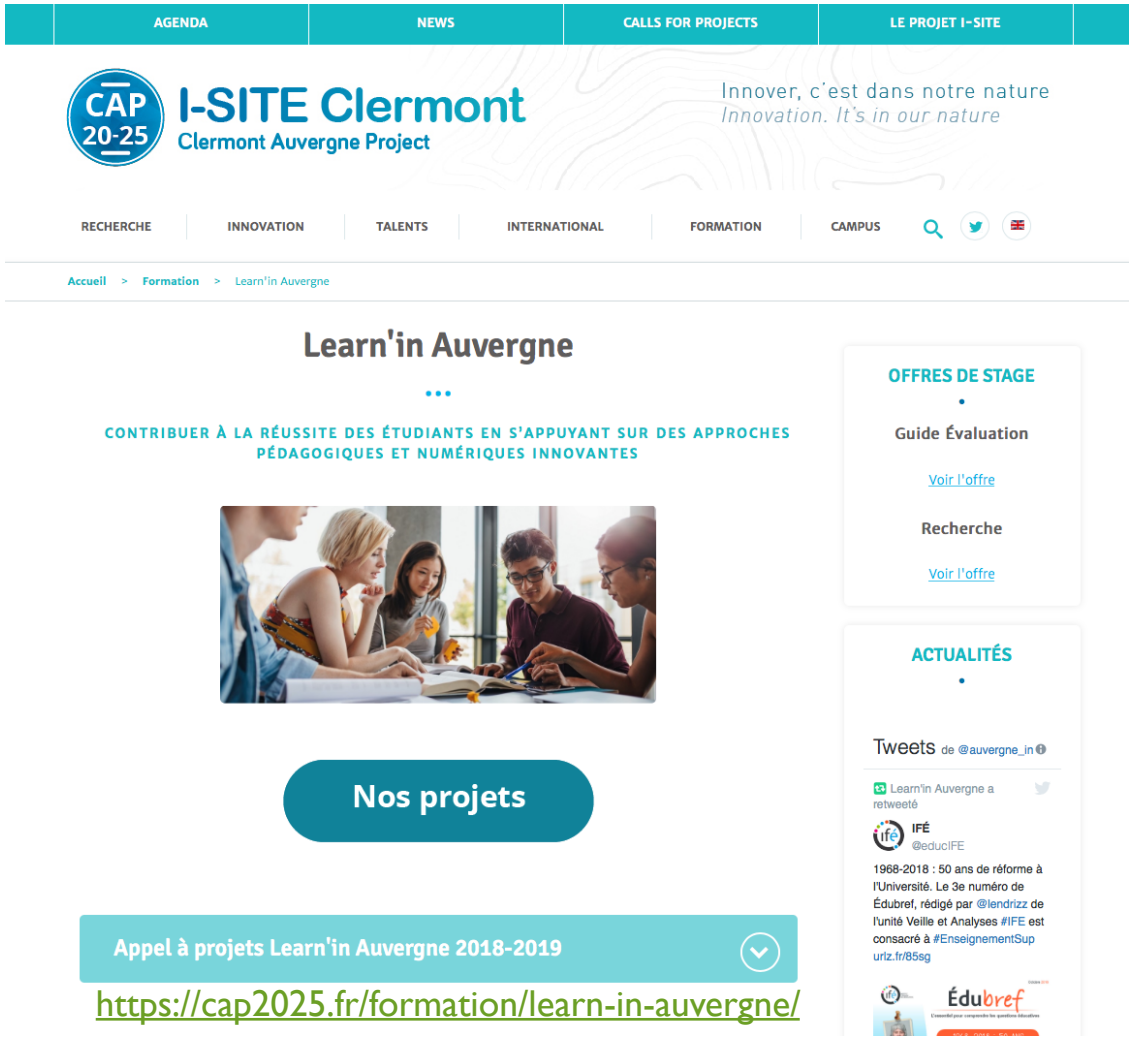


Dispositif d'évaluation : Learn'in Auvergne (LIA)

Programme transverse du programme CAP 20-25
Objectifs de Learn'in Auvergne (LIA)

- Accompagner la transformation pédagogique et numérique du site ;
- Evaluer les effets de ces transformations.





Dispositif d'évaluation : Mise en place

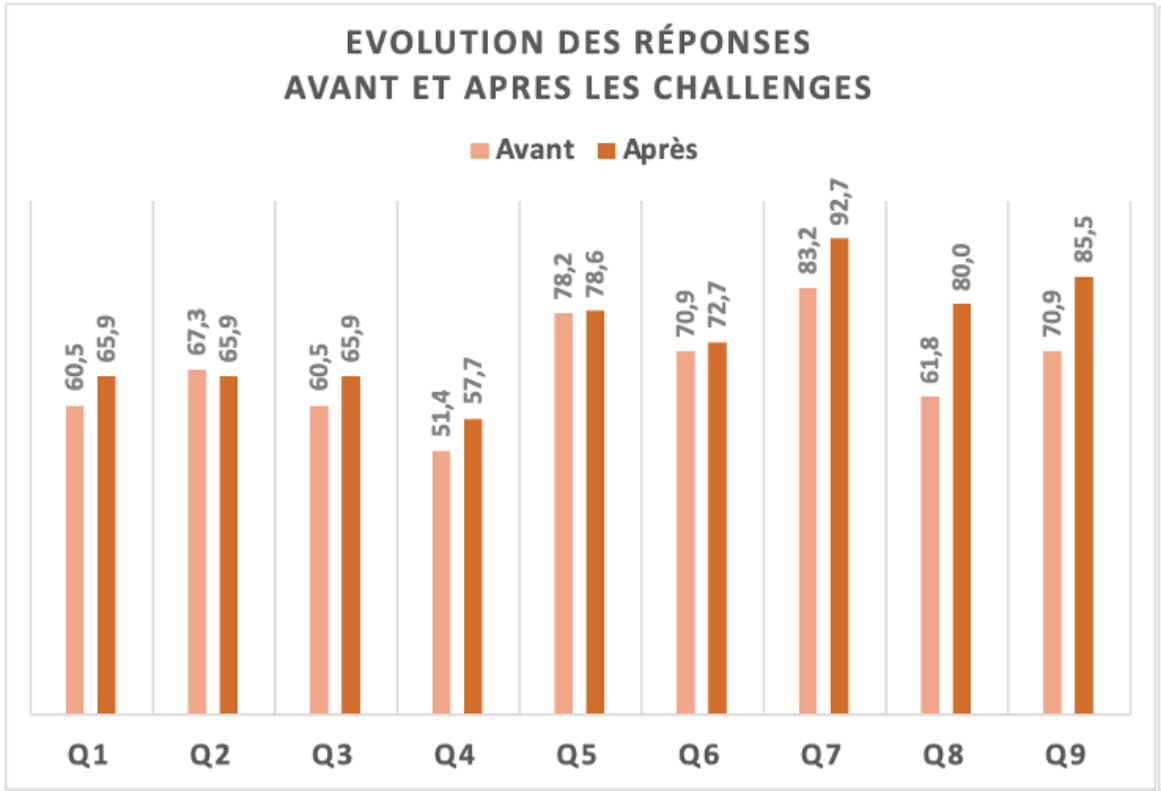
- Comment être sûre que notre approche a des **effets bénéfiques** pour les étudiants ?
- Identification des compétences (techniques et transversales), méthode d'évaluation (questionnaire, auto-évaluation), définition des cohortes (groupes témoin et test) ?
- Ethiquement ⇒ dur de créer des groupes test/témoin (⇔ autoriser ou non des étudiants à suivre les challenges).
- Conclusion : mise en place d'un questionnaire d'auto-évaluation avant et après les deux challenges :
  - **G1 :** *Evaluer une montée en compétences sur les aspects techniques :* Identification et exploitation de vulnérabilités, contremesure, programmation C et Python, cryptographie, protocole MQTT, Obfusctation – Salage, Analyse d'un firmware, sniffeur réseau (tcpdump), …
  - **G2 :** *Evaluer une montée en compétences sur les aspects transversales :* accès à l'information rapidement et efficacement, gestion du stress dans un environnement contraint, partage du travail sous des contraintes de temps, …
  - **G3 :** *Evaluation de l'enseignement :* Forme du cours et des challenges, …

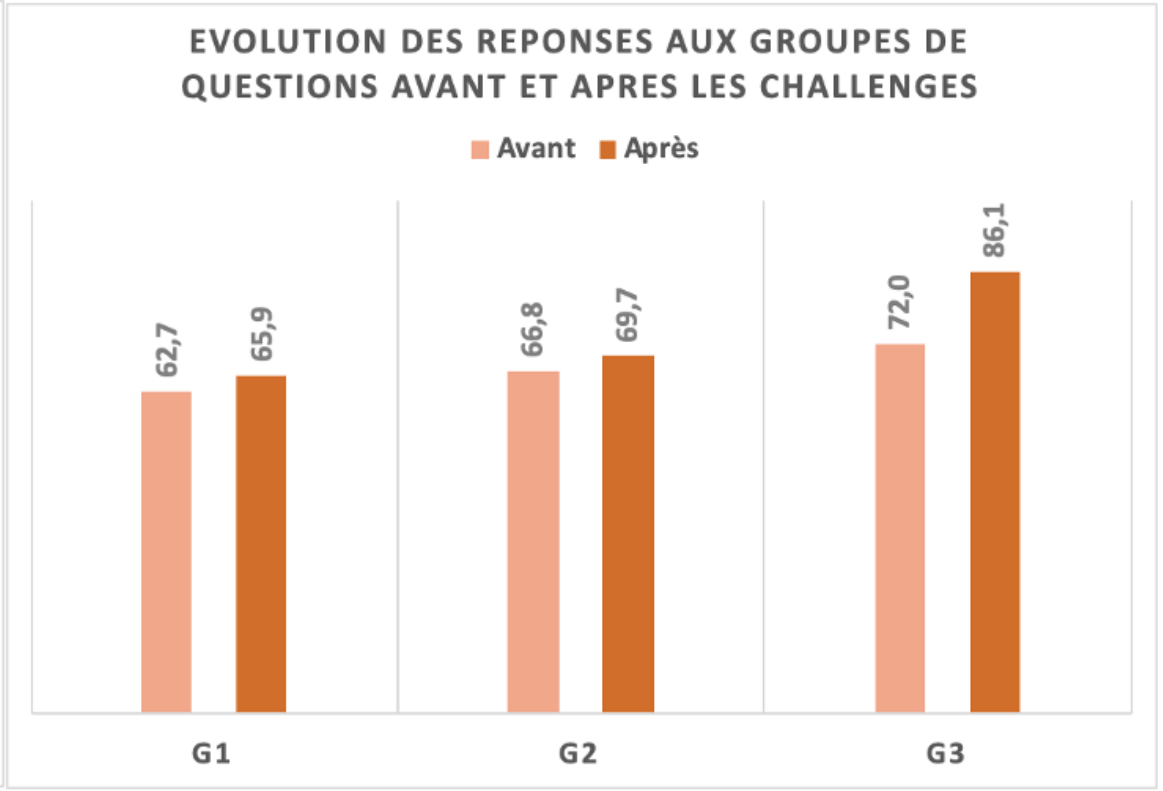
Dispositif d'évaluation : Mise en place

		Questions	Réponses possibles			
G1	Q1	Comment évaluez-vous votre aisance à trouver facilement et rapidement des informations pertinentes ?	Très difficilement	Difficilement	Facilement	Très facilement
	Q2	Comment évaluez-vous votre aisance à l'utilisation d'outils informatiques en lien avec la sécurité ?	Très difficilement	Difficilement	Facilement	Très facilement
	Q3	Comment évaluez-vous votre aisance à mobiliser des raisonnements et des outils mathématiques ?	Très difficilement	Difficilement	Facilement	Très facilement
G2	Q4	Comment évaluez-vous votre aisance à travailler efficacement dans un environnement stressant ?	Très difficilement	Difficilement	Facilement	Très facilement
	Q5	Comment évaluez-vous votre aisance à travailler en équipe ?	Très difficilement	Difficilement	Facilement	Très facilement
	Q6	Comment évaluez-vous votre aisance à répartir les tâches et à collaborer ?	Très difficilement	Difficilement	Facilement	Très facilement
G3	Q7	Pensez-vous qu'une évaluation basée sur des challenges de sécurité est pertinente ?	Pas du tout	Un peu	Plutôt pertinent	Très pertinent
	Q8	Pensez-vous que ce type d'évaluation soit intéressante dans le cadre d'autres enseignements ?	Pas du tout	Probablement pas	Plutôt	Tout à fait
	Q9	Quel est votre sentiment sur l'évaluation par challenge de sécurité ?	Très négatif	Négatif	Positif	Très positif

Dispositif d'évaluation : Mise en place

Effectif de 26 étudiants : taux de réponse de 73 % pour le 1er questionnaire et de 92 % pour le 2ième





Calcul d'une évolution moyenne des réponses : pour la réponse la plus positive on a attribué une valeur de 100 % et une décroissante linéaire jusqu'à la réponse la plus négative à 0%.

Dispositif d'évaluation : Discussions

- Une évolution globale et positive des réponses des étudiants aux 3 groupes de questions (G1, G2, G3) ;
- Certaines variabilités (exemples):
  - ↗ Question Q1 (« la recherche pertinente d'informations »), question Q3 (« mobiliser des raisonnements ») et la question Q4 (« travailler dans un environnement stressant ») : choses prévisibles.
  - → Question Q5 (« aisance à travailler en équipe ») : cadre de travail très courant (binôme) pour des étudiants en bac+4 donc on comprend que cela ne leur a pas apporté de nouvelles compétences.
  - ↘ Question Q2 (« l'utilisation d'outils informatiques en lien avec la sécurité ») : idée fausse de la sécurité et plus particulièrement sur la difficulté de mise en place d'un mécanisme sécurisé. Les étudiants ont pris conscience de cette difficulté après les challenges.
- Analyse quantitative de l'impact pédagogique (retours directs des étudiants par les délégués):
  - Retour des étudiants a été enthousiaste avec une émulation autour de faire un « jeu » ;
  - Certains mauvais retours : ce type de séances a créé un énorme stress car la forme est très différente des séances de cours classiques. Néanmoins ces compétences peuvent être plus qu'indispensable dans le monde de la sécurité informatique.

Conclusion

- Mise en place d'un **cours de sécurité des objets connectés** dans une formation **d'ingénieur en informatique** (niveau Bac+4) dans une spécialité « Réseaux et Sécurité Informatique » ;
- **Intérêt pédagogique** : Initiation à la chaine de sécurité et à la sécurité des IoT mais aussi une initiation à l'informatique embarquée et à ses contraintes ;
- **Pédagogie innovante** basée sur une classe inversée, ≃ l'échec productif (*Productive failure*), évaluation par des challenges de sécurité (*Serious Game*) ;
- **Soutien** par un programme transverse CAP 20-25 : Learn'in Auvergne ;
- **Evaluation de l'approche pédagogique**

ISIMA
INSTITUT D'INFORMATIQUE
Université Clermont Auvergne

CAP 20-25
I-SITE CLERMONT
Clermont Auvergne Project
INVESTISSEMENTS D'AVENIR

Avez-vous des questions?

QXZlei12b3VzIGRlcyBxdWVzdGlvbnM/

Yv0RW5uH/1hSJQosR9B8I/0ZayGRJtz+n4FV9ZOmhFg=