Séance 1
Séance Introductive

Objectifs de la séance

- Mise en oeuvre du premier environnement d'expérimentation (deux utilisés au total durant ces 13 séances de CI)
- Prise en main de cet environnement et identification des différents éléments qui le composent
- Etude théorique annexe - Side Channel Attacks

A. Mise en place de l'environnement

Au cours de cette séance et des séances à venir, un environnement virtualisé sera utilisé. Ceci offrira différents bénéfices : simplicité de déploiement, simplicité de réplication notamment.

Pour ce faire, il vous est demandé de réaliser les étapes suivantes (si elles n'ont pas déjà été effectuées sur vos machines) :

1. Téléchargement du premier Lab d'expérimentation utilisé durant ces séances de CI. Celui-ci est accessible ici : https://filesender.renater.fr/?s=download&token=cb001a82-1340-48d2-a702-425732d659b3

2. Téléchargement et installation de VirtualBox (dans l'idéal dans un environnement Linux, des difficultés ont été rencontrées l'année dernière par des élèves déployant l'environnement dans un environnement Windows) - Afin de gagner du temps, cette étape peut-être réalisée en parallèle de la première

Note : cette étape devrait prendre un certain temps, il vous est donc demandé de réaliser les parties B et C en attendant que l'installation soit effectuée.

B. Attaques par canaux auxiliaires (Side-channel attack)

Dans cette partie, au travers d'une étude théorique, nous allons nous intéresser aux attaques pouvant être menées au niveau de l'objet/de l'équipement terminal/de l'équipement réseau lui-même (attaques matérielles). Plus particulièrement, nous allons nous intéresser aux attaques par canaux auxiliaires.

Q.1 Qu'est ce qu'une attaque par canaux auxiliaires ? Que cherche-t-on généralement à deviner ? Quelles valeurs peuvent être mesurées ?

(Source potentielle: https://www.techtarget.com/searchsecurity/definition/side-channel-attack)

Q.2 Quelques précisions supplémentaires :

- **Les attaques par canaux auxiliaires peuvent-elles être classées en différentes catégories ?**
- **Trouvez quelques exemples de plateformes/devices à l'égard desquelles des attaques par canaux auxiliaires ont déjà été menées.**
- **En quoi les attaques par canaux auxiliaires représentent-elles une menace pour la sécurité des systèmes?**
- **Comment peuvent-elles contourner les mesures de sécurité conventionnelles?**

a. Attaque simple par analyse de courant (Simple Power Analysis)

Une première attaque par canaux auxiliaires possible, parmi les plus simples, est l'attaque nommée *Simple Power Analysis* (SPA).

Q3. Quel est le principe des attaques SPA ?

Pour répondre à cette question, vous pourrez utiliser les informations présentées dans : https://docs.google.com/presentation/d/1oDPkvdy-NmP3_QjOjONSJRikCFUHAeI5vn8LLvKnRG0/edit?usp=sharing

L'objectif de cette attaque (ainsi que des autres attaques présentées dans cette partie) est de deviner la clé privée utilisée par un équipement terminal (device IoT par exemple). Pour comprendre le fonctionnement de cette attaque, nous allons nous focaliser ici sur l'algorithme à clé publique RSA (Rivest–Shamir–Adleman), couramment utilisé dans l'environnement IoT.

Avec cet algorithme, la fonction utilisée pour le déchiffrement d'un message est la suivante :

$$M=C^d \ mod(N)$$

où M correspond au message déchiffré, C au message chiffré, d à la clé privée de l'objet IoT et N à la multiplication de deux entiers premiers. Ainsi, l'objectif d'un attaquant serait ici de déterminer la valeur de d.

Or, avec RSA, la méthode la plus efficace pour calculer l'exponentiation d'un entier par un autre est la méthode dite d'exponentiation rapide :

****

Objectif, calculer d :

$d=d_n d_{n-1}...d_1 d_0$ #Calculer la décomposition binaire de d

T <- C #Définir la valeur du résultat T

Pour i allant de n-1 à 0: # Calculer l'exponentiation

si di=0:

T <- T x T # Carré

si di=1:

T <- T x T # Carré

T <- T x C # Multiplication

4. *renvoyer T*

****

Q.4 Si vous étiez un attaquant, en considérant l'algorithme ci-dessus, comment pourriez-vous être en capacité de deviner la clé de l'objet IoT ?

Pour répondre à cette question **(et à celles dans les sections suivante de cette partie Side Channel)**, vous pourrez utiliser les informations présentées dans : https://docs.google.com/presentation/d/1oDPkvdy-NmP3_QjOjONSJRikCFUHAeI5vn8LLvKnRG0/edit?usp=sharing

Q.5 Pour éviter ce problème et offrir une solution "à consommation constante", que le bit traité soit un 0 ou un 1, quelle contremesure pourriez vous proposer ?

b. Attaque par injection de fautes

Une contremesure que vous pourriez avoir introduit dans la partie précédente pourrait consister à introduire une opération factice lorsque le bit est à 0 :

****

si di=0:

T <- T x T (carré)

U <- T x C (multiplication)

si di=1:

T <- T x T (carré)

T <- T x C (multiplication)

****

Ainsi, grâce à cette approche, la solution garantit une consommation énergétique constante (que le bit soit à 1 ou 0) sans impacter le résultat final, rendant l'attaque SPA impossible.

Toutefois, cette solution est imparfaite. En effet, elle pourrait être sensible aux attaques dites d'injection de fautes.

Q.6 En quoi consiste dans ce contexte une attaque par injection de fautes ? Qu'est ce que l'attaquant pourrait être en mesure de faire en réalisant ce type d'attaque ? Quel serait l'impact sur le résultat ? Vous pourrez notamment expliquer ce qui se passerait si le système est perturbé au moment d'une opération non factice VS au moment d'une opération factice.

Vous venez normalement de conclure qu'une attaque par injection de fautes permet d'attaquer un système protégé uniquement contre les attaques SPA et de déterminer la valeur de la clé privée de l'objet IoT.

Q.7 Quelle contremesure pourrait être proposée pour résoudre ce problème ?

c. Ouverture : Attaque différentielle par analyse de courant (Differential Power Analysis)

Alors que les attaques SPA et par injection de fautes font partie des attaques "simples", pouvant être exécutées dans un environnement peu protégé (ce qui correspond à bon nombre d'objets IoT), les attaques DPA font partie d'attaques plus complexes pouvant être exécutées contre des systèmes mieux protégés.

Q.8 Expliquez en quoi consiste une attaque de type DPA ? Pour ce faire, entrez dans les détails en expliquant comment on pourrait être en mesure de retrouver la clé d'un utilisateur.

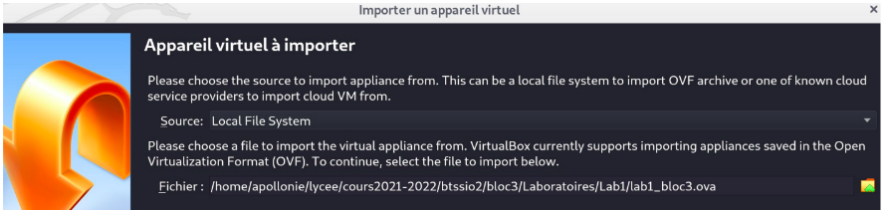
Cette attaque, basée sur des variations très petites, et non liée à une erreur dans l'implémentation de l'algorithme de chiffrement, est bien plus puissante que les attaques SPA et d'injections de fautes. Toutefois, des contremesures sont possibles.

Q.9 Quelles contremesures pourraient être proposées contre ce genre d'attaques ?

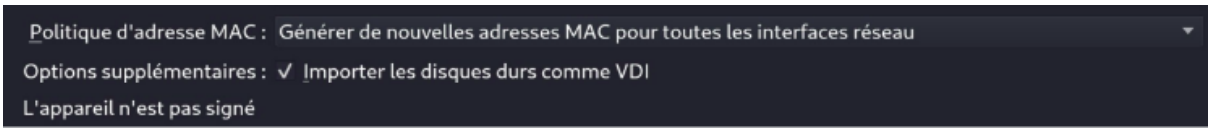
C. Mise en oeuvre du Lab

Une fois que vous avez téléchargé l'archive du Lab, ainsi que VirtualBox, commencez par l'extraire puis réalisez les étapes suivantes :

1. Récupérez le fichier lab1_bloc3.ova et importez-le sur le logiciel VirtualBox (Fichier>Importer un appareil virtuel).



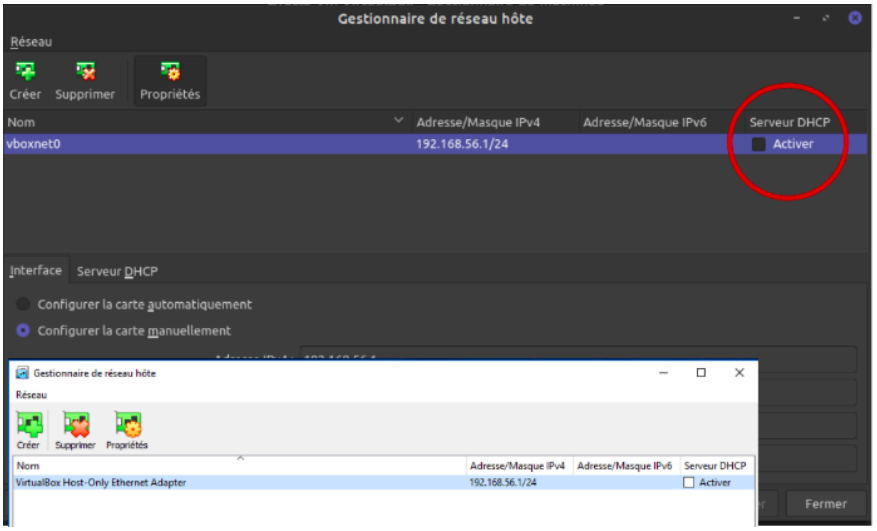
2. Cliquez sur suivant ; les quatre machines virtuelles vont venir se ranger dans le groupe « Lab1 bloc3 ».
3. Modifiez à ce moment là la politique d'adresse MAC : Générez de nouvelles adresses MAC pour toutes les interfaces réseaux.



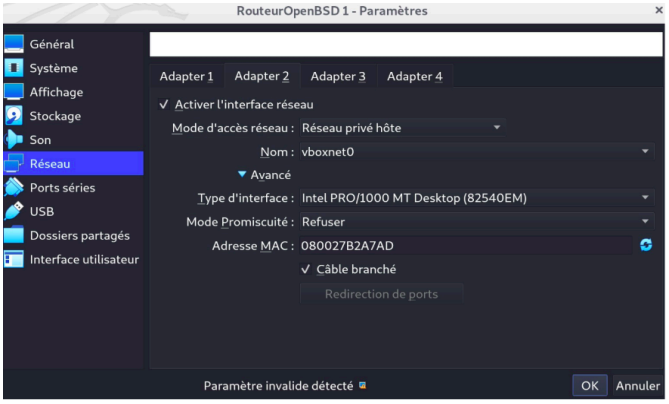
4. Cliquez sur "Importer"

Une fois les différentes machines virtuelles importées, il faut s'assurer qu'une carte réseau (vboxnet0 ou VirtualBox Host-Only Ethernet Adapter) a bien été créée dans le gestionnaire de réseau hôte :

1. Vous devriez voir apparaître une nouvelle carte réseau virtuelle nommée **vboxnet0** ou VirtualBox Host- Only Ethernet Adapter (suivi éventuellement d'un # et numéro si des cartes virtuelles ont déjà été créées auparavant) sous Windows avec comme adresse IP **192.168.56.1/24 (PENSEZ A CHANGER l'IP SI CE N'EST PAS LE CAS)**.
2. Décochez l'activation du serveur DHCP. Si aucune carte réseau n'apparaît, cliquez sur Créer puis indiquer les paramètres présents dans la capture d'écran ci-dessous.



3. Enfin, assurez vous dans les paramètres réseaux des machines virtuelles que les cartes réseaux définies en mode réseau privé hôte sont correctement liées à vboxnet0 ou VirtualBox Host-Only Ethernet Adapter. Par exemple, ci-dessous pour le routeur OpenBSD et l'adaptateur 2 :



A ce moment là il ne vous reste plus qu'à lancer l'ensemble des machines pour vérifier le bon fonctionnement de votre installation.

Note : Les identifiants à utiliser pour l'ensemble des machines virtuelles sont les suivantes : etusio Fghijkl1234*

Quelques erreurs que vous pourriez rencontrer au lancement/au déploiement du Lab :

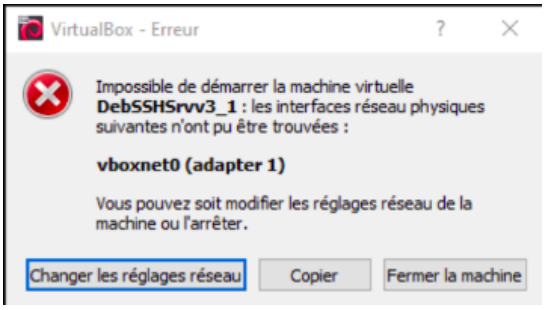
1. **Modification de la plage d'IP utilisée**

Sur les dernières versions de VirtualBox, il peut être nécessaire de réaliser une étape de configuration pour que l'ensemble des adresses IP puissent être utilisées (et vboxnet0 créé).

L'étape en question consiste à créer un fichier "/etc/vbox/networks.conf" contenant "* 0.0.0.0/0 ::/0" et à relancer VirtualBox.

Pour en savoir plus : https://www.virtualbox.org/manual/ch06.html#network_hostonly

2. **Message d'erreur concernant la carte réseau au démarrage des machines**



Sur une plateforme Windows, si vous n'avez pas accédé à la configuration réseau pour valider le nom de l'interface réseau avant de démarrer la machine, vous aurez probablement le message d'erreur suivant : Il suffira de cliquer sur « Changer les réglages réseau » et de valider la prise en compte du « VirtualBox Host-Only Ethernet Adapter » à la place de « vboxnet0 » pour régler le problème.

Sur une plateforme Linux, il suffit de :

- Cliquer sur changer les réglages réseau ;

- Enregistrer en cliquant sur « OK ».

Si cette simple manipulation ne fonctionne pas :

- « Fermez la machine » ;
- Reconfigurez les paramètres réseaux des machines virtuelles en décochant et réactivant la case « Activer l'interface réseau » ;
- Enregistrez en cliquant sur « OK ».

D. <u>Prise en main du Lab</u>

La dernière étape du jour va consister à comprendre la composition du Lab mis en œuvre et le rôle des différents éléments qu'il inclut.

Q.10 Pour ce faire, vous devrez répondre aux questions suivantes :

- **Combien y a-t-il de machines virtuelles ? Quel est à votre avis le rôle de chacune d'entre elles ? Quelle est leur adresse IP ? Quels types de services peut-on imaginer comme fonctionnant sur chacune de ces VMs ?**
- **Qu'est ce que Kali Linux ? Quelles actions pourrait-on imaginer dans ce contexte en utilisant cet outil ?**
- **Proposez une représentation simple de l'architecture (machines + IP + services)**

Note : 'ip a' ou 'ifconfig' peuvent-être utilisé pour récupérer l'IP d'une machine donnée