NUI Galway
OÉ Gaillimh

LA ROCHELLE

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

Soutenance de stage
Lavergne Clément

NUI Galway
OÉ Gaillimh

Introduction

- Présentation de la faculté

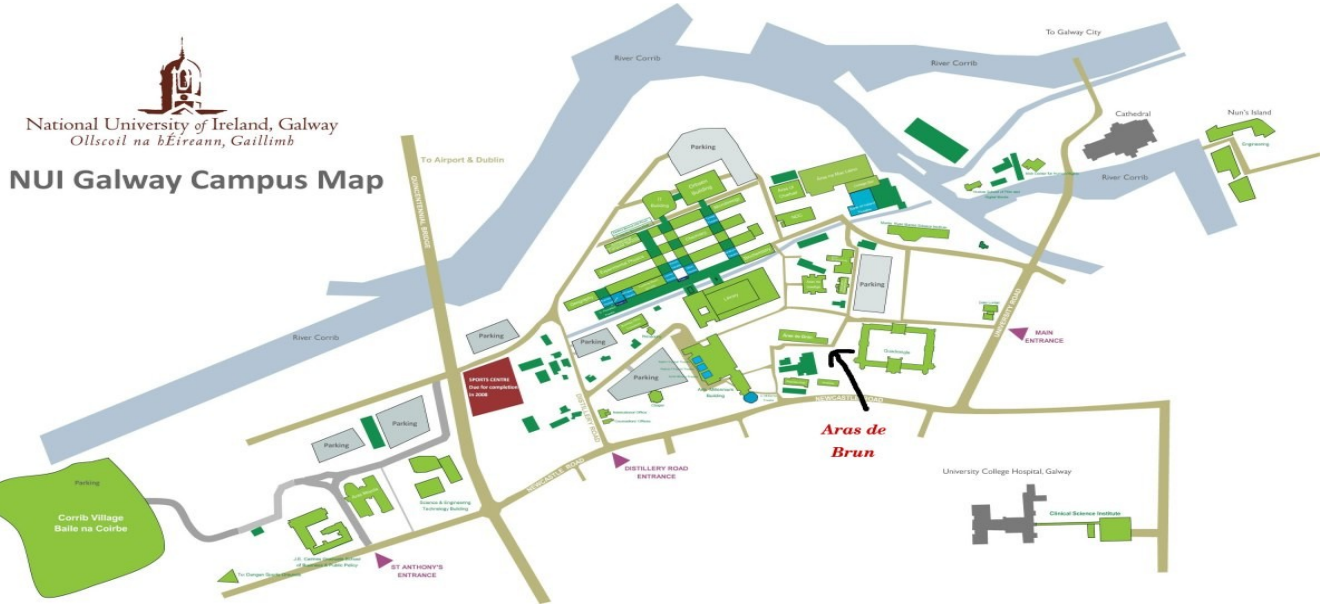
LA ROCHELLE

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

NUI Galway
OÉ Gaillimh

Introduction

- Présentation de la faculté



LA ROCHELLE

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

NUI Galway
OÉ Gaillimh

Introduction

- Présentation du groupe OSNA

  - Recherche en cybersécurité
  - Dirigé par Michael Schukat
  - Systèmes de contrôle

LA ROCHELLE

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

NUI Galway
OÉ Gaillimh

Introduction

- Présentation de système en place
  - Les outils

BeagleBones Back

Le serveur « rack »

Capteur ADAM

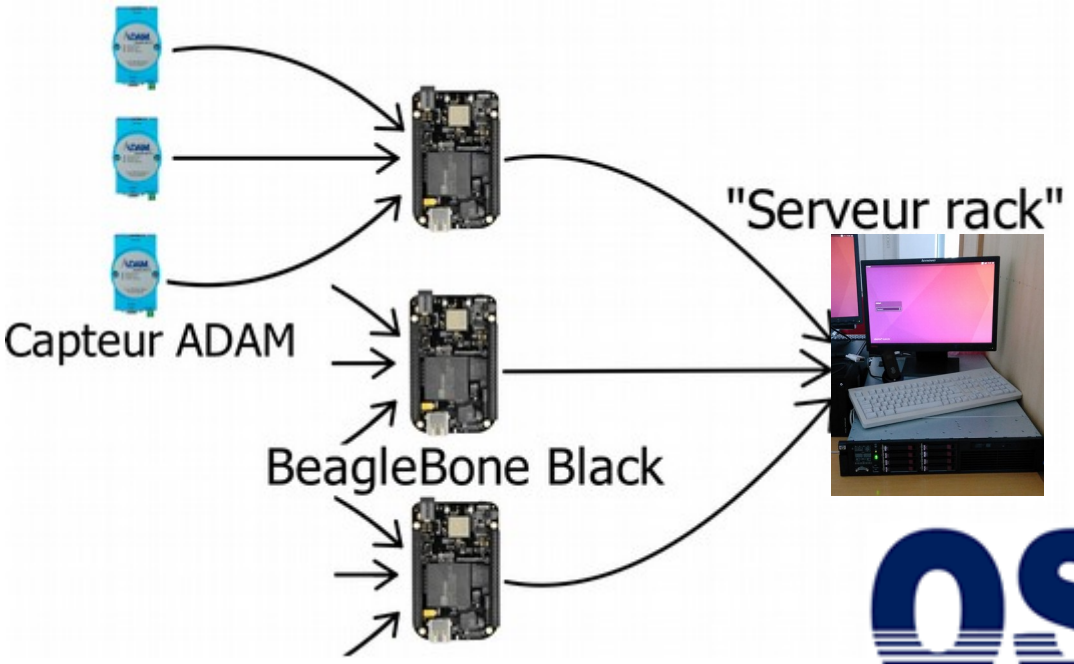
LA ROCHELLE

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

NUI Galway
OÉ Gaillimh

Introduction

- Présentation de système en place
  - Les communications



LA ROCHELLE

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

NUI Galway
OÉ Gaillimh

Problématiques

Quels sont les types de menaces pesant sur un réseau industriel ?

Comment immuniser un réseau soumis à des sources de menaces multiples ?

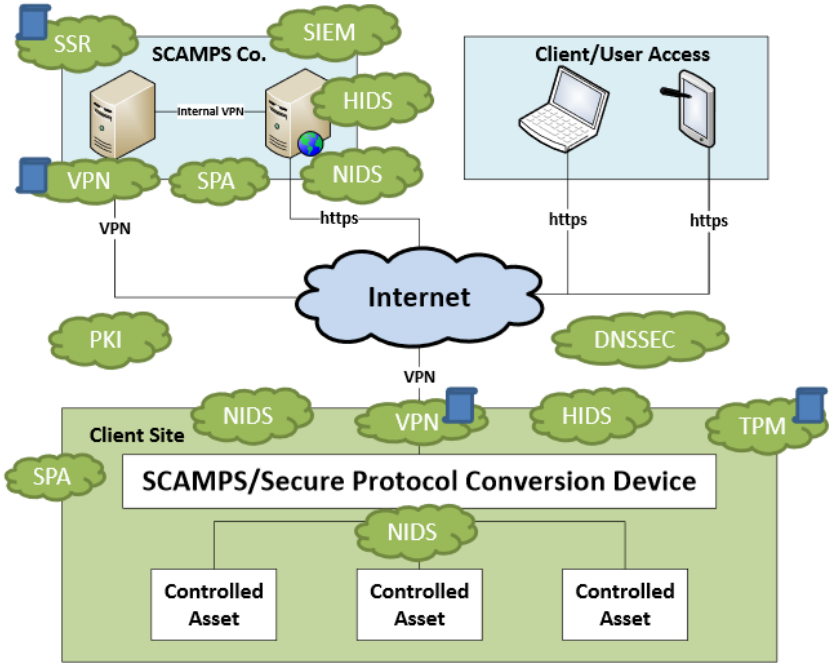
LA ROCHELLE

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

Objectifs

Security Features of SCAMPS

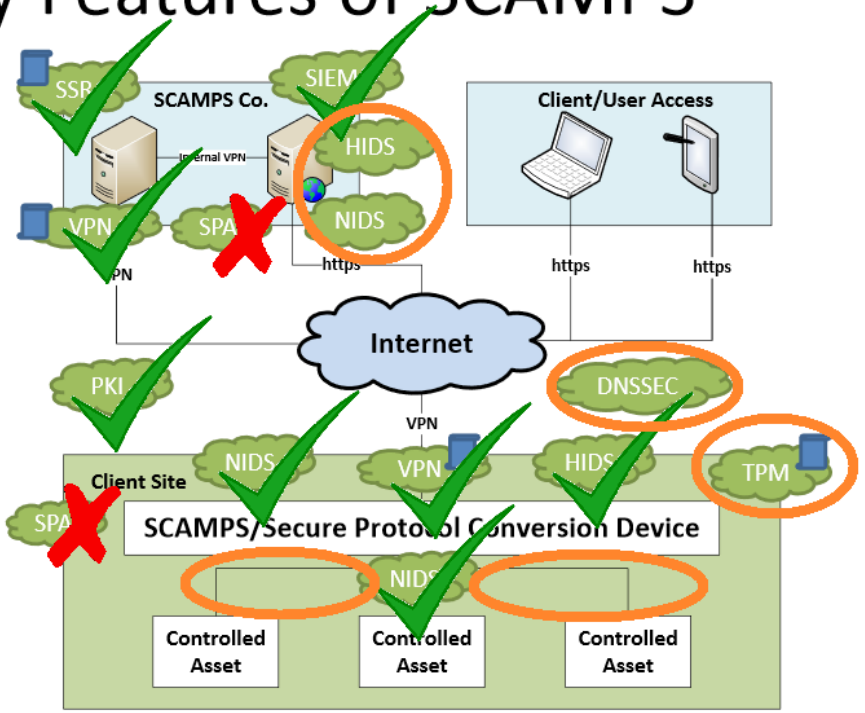
- TPM – Trusted Platform Module
- DNSSEC – Secure DNS
- SPA – Single Packet Authentication (port knocking) - optional
- VPN –OpenVPN tunnel
- PKI – Public Key Infrastructure
- NIDS / HIDS – Network / Host Intrusion Detection System
- SSR – Secure Software Repository
- SIEM - Security Information and Event Management



Résultats

Security Features of SCAMPS

- TPM – Trusted Platform Module
- DNSSEC – Secure DNS
- SPA – Single Packet Authentication (port knocking) - optional
- VPN –OpenVPN tunnel
- PKI – Public Key Infrastructure
- NIDS / HIDS – Network / Host Intrusion Detection System
- SSR – Secure Software Repository
- SIEM - Security Information and Event Management



NUI Galway
OÉ Gaillimh

Plan

- Plannings prévisionnel et réel
- VPN
  - Clé et certificat
  - Pourquoi un VPN
- NIDS
  - Règles
  - Pourquoi un NIDS
- Conclusion

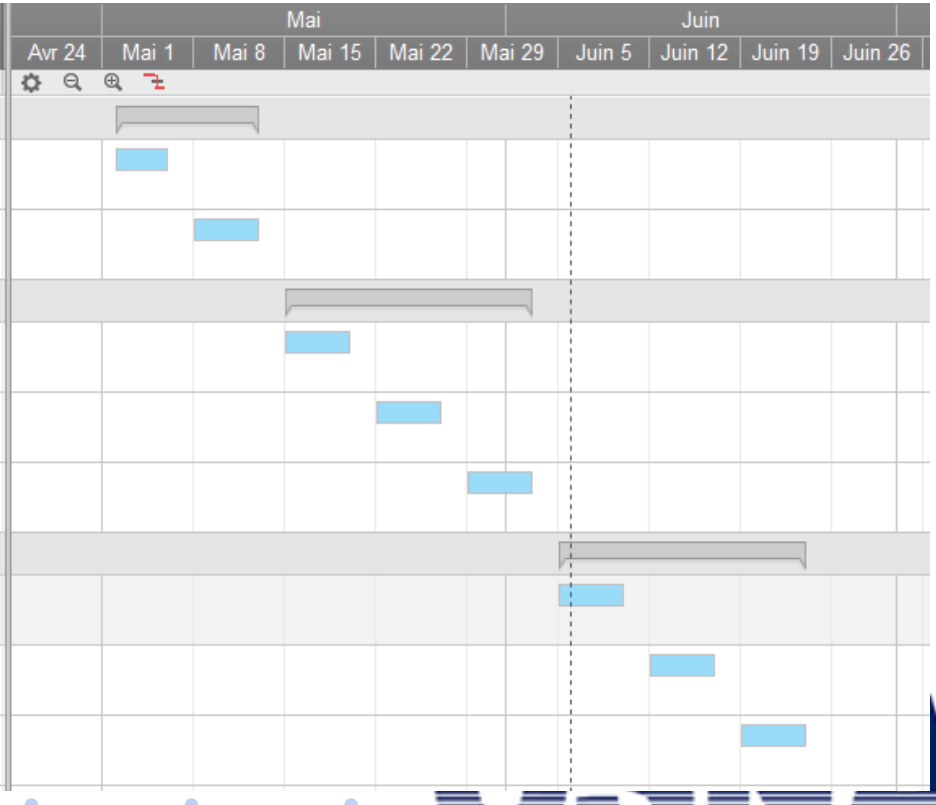
LA ROCHELLE

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

Plannings prévisionnel et réel

- Planning prévisionnel

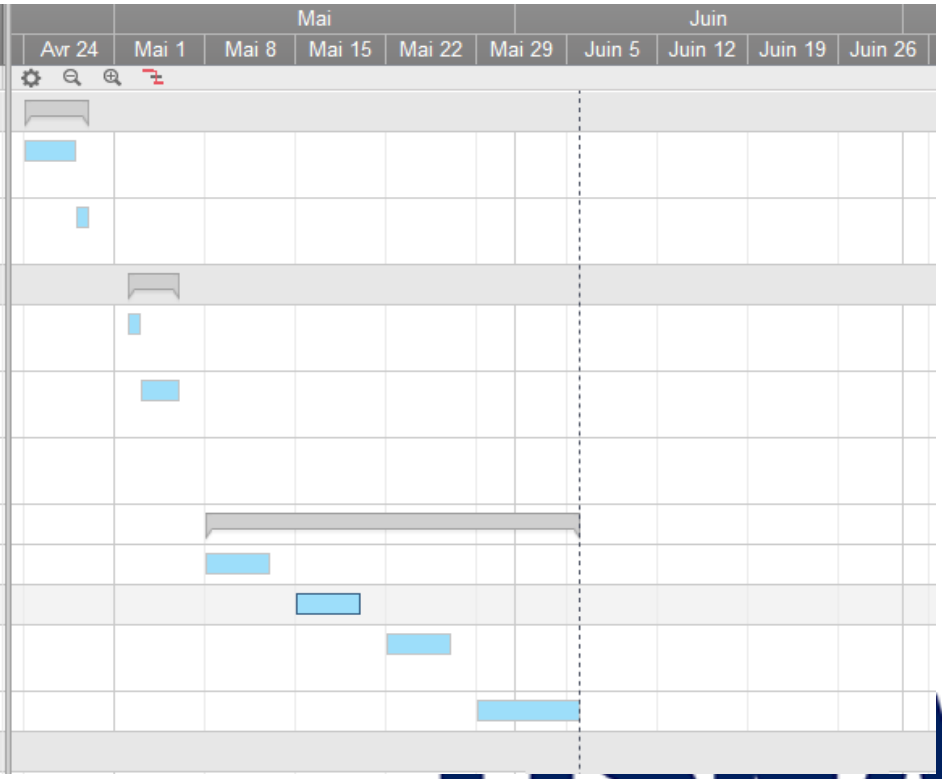
Nom de la Tâche	Date de Début	Date de Fin	Durée
Section 1 - Connexion VPN	**02/05/17**	**12/05/17**	**9j**
Sous-tâche 1 - Créer une connexion VPN	02/05/17	05/05/17	4j
Sous-tâche 2 - Sécuriser la connexion à l'aide de clés et de certificats	08/05/17	12/05/17	5j
Section 2 - Mise à jour	**15/05/17**	**02/06/17**	**15j**
Sous-tâche 1 - Mettre à jour le BBB en local	15/05/17	19/05/17	5j
Sous-tâche 2 - Mettre à jour depuis le serveur	22/05/17	26/05/17	5j
Sous-tâche 3 - Mettre à jour de manière sécurisée	29/05/17	02/06/17	5j
Section 3 - Gestion des données	**05/06/17**	**23/06/17**	**15j**
Sous-tâche 1 - Récupérer les données en provenance des capteurs	05/06/17	09/06/17	5j
Sous-tâche 2 - Envoyer les données au serveur	12/06/17	16/06/17	5j
Sous-tâche 3 - Sécuriser l'envoie des données	19/06/17	23/06/17	5j



Plannings prévisionnel et réel

- Planning réel

Nom de la Tâche	Date de Début	Date de Fin	Durée
Section 1 - Connexion VPN	**24/04/17**	**28/04/17**	**5j**
Sous-tâche 1 - Créer une connexion VPN	24/04/17	27/04/17	4j
Sous-tâche 2 - Sécuriser la connexion à l'aide de clés et de certificats	28/04/17	28/04/17	1j
Section 2 - Mise à jour	**02/05/17**	**05/05/17**	**4j**
Sous-tâche 1 - Mettre à jour le BBB en local	02/05/17	02/05/17	1j
Sous-tâche 2 - Mettre à jour depuis le serveur	03/05/17	05/05/17	3j
Sous-tâche 3 - Mettre à jour de manière sécurisée			
Section 4 - NIDS	**08/05/17**	**05/06/17**	**21j**
Sous-tâche 1 - Premières installations	08/05/17	12/05/17	5j
Sous-tâche 2 - Configuration et tests	15/05/17	19/05/17	5j
Sous-tâche 3 - Nouveau NIDS, installation et configuration	22/05/17	26/05/17	5j
Sous-tâche 4 - Lien avec le serveur	29/05/17	05/06/17	6j
Section 4 - Gestion des données			

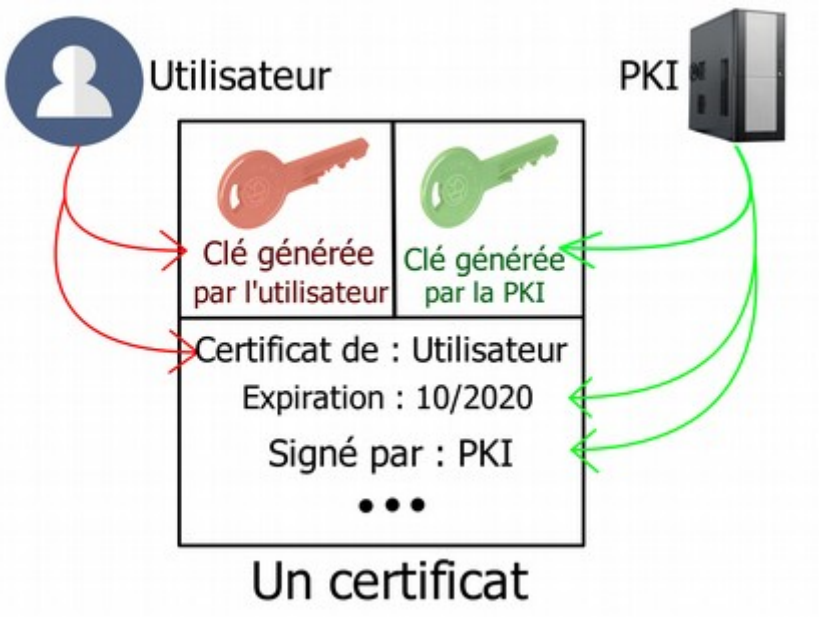


VPN

- OpenVPN
  - Application pour la création de tunnels
  - Adaptée aux systèmes embarqués
  - Utilisation de clés

VPN

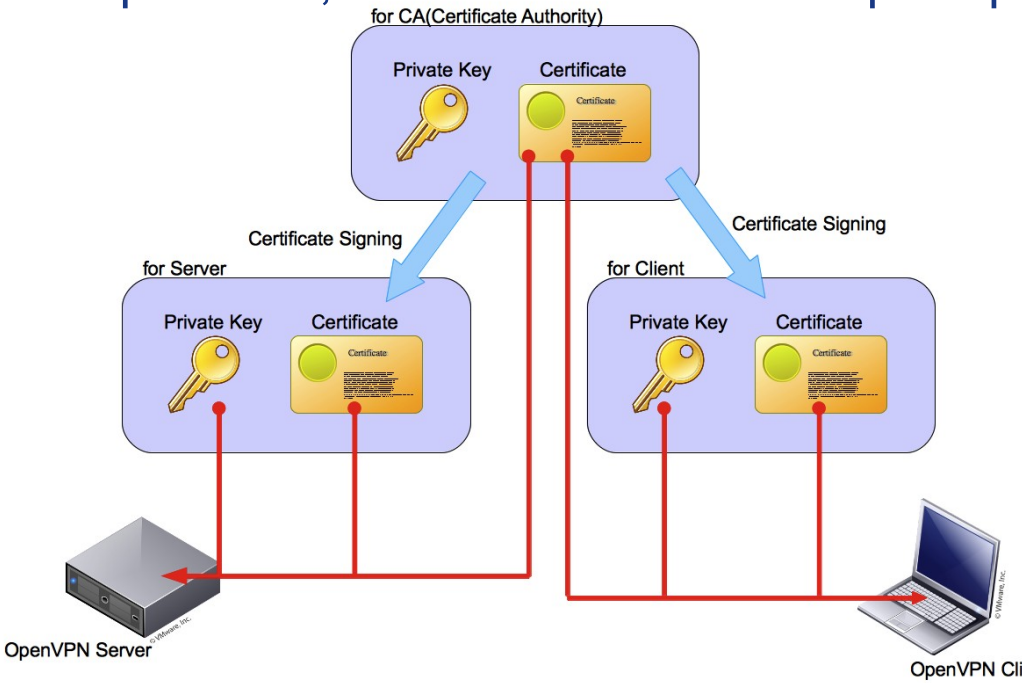
- OpenVPN, clés et certificats : Principe



Principe de clé et de certificat

VPN

- OpenVPN, clés et certificats : En pratique



Distribution des clés et des certificats avec OpenVPN

NUI Galway
OÉ Gaillimh

VPN

- Pourquoi
  - Répondre à un premier type de menace
  - Communication privilégiée, privée et cryptée
  - Ouvre la porte à la suite du projet

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

NIDS

- SNORT

- Détecter des connexions suspectes

- Alerter l'administrateur

NIDS

- SNORT

- Outil Pulledpork

- Ajout manuelle des règles

NIDS

- SNORT Règles

Description générale

action proto src_ip src_port direction dst_ip dst_port (options)

Exemple d'options

(msg:"FIN Scan"; flags: F; sid:1000001; rev:001; classtpe:network-scan;)

NUI Galway
OÉ Gaillimh

NIDS

- SNORT Règles

Cas d'utilisation couverts :

- Scan
- DDOS
- Attaque par MODBUS

LA ROCHELLE

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

NUI Galway
OÉ Gaillimh

NIDS

- SNORT Lien avec OSSIM

FAIRE SI LE BESOIN DE TEMPS DE PAROLE EN

LA ROCHELLE

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

NIDS

- Premier choix : psad
  - Mauvais choix car :
    - Règles peu adaptées
    - Lien avec OSSIM non documenté
    - Incapacité à faire fonctionner

NUI Galway
OÉ Gaillimh

NIDS

- Choix de SNORT

- Communauté SNORT large et active

- Application déjà testée par le groupe de recherche

- Flexibilité d'utilisation

LA ROCHELLE

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

NUI Galway
OÉ Gaillimh

Conclusion

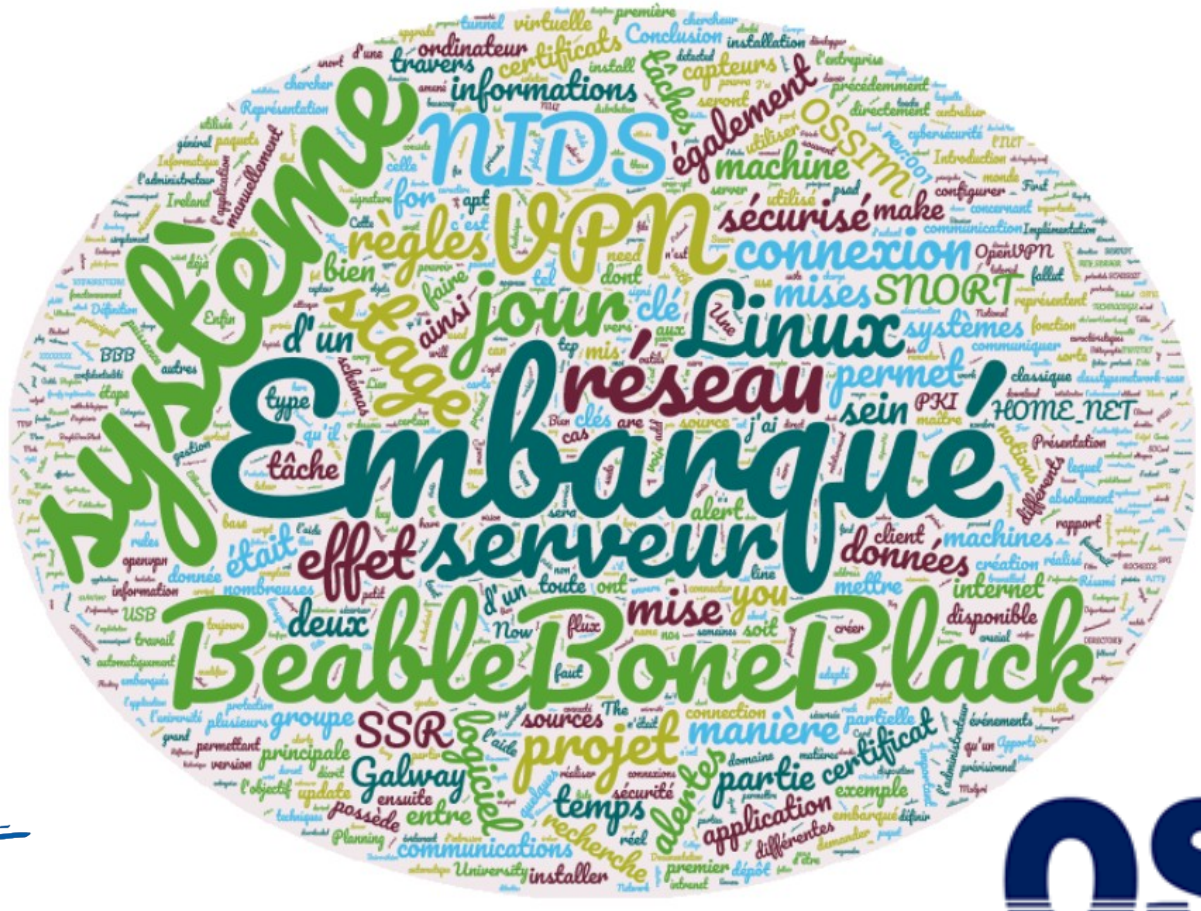
- Choix de ce stage
- Le projet
- Apports personnel

LA ROCHELLE

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

NUI Galway
OÉ Gaillimh

Merci de votre attention



LA ROCHELLE

OSNA
OPEN SENSOR NETWORK AUTHENTICATION