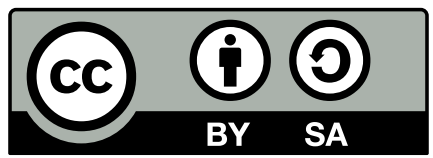
Présentation pour le CAPET externe dans la section sciences industrielles de l'ingénieur en option ingénierie informatique

Nicola Spanti

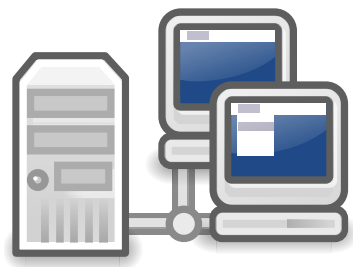
Juin 2017



Sommaire

Vue générale

- Le réseau Internet
- Les problématiques réseaux (disponibilité, rapidité, etc)
- Les proxys

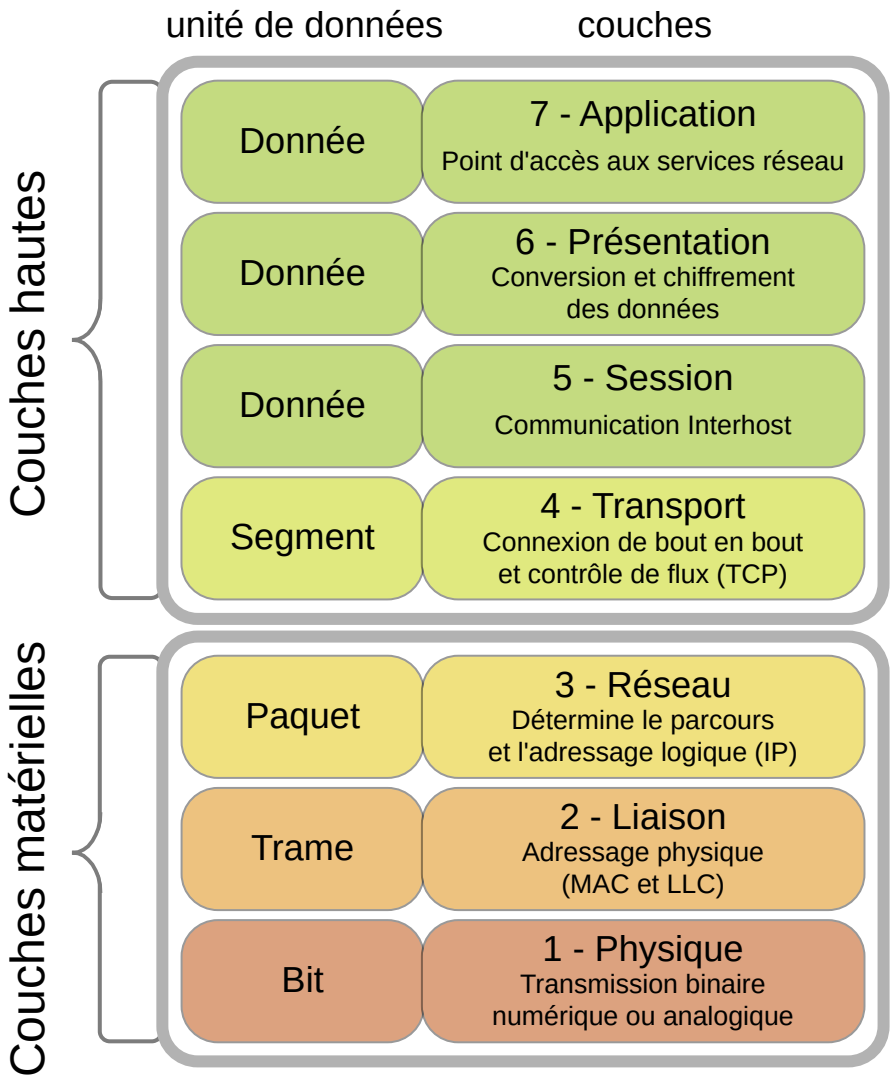


Proxy et chiffrement

- Le chiffrement
- L'importance du chiffrement pour l'usage d'Internet
- La problématique pour les proxys

Proxy filtrant

- Modèle OSI et Internet (applications et “métadonnées”)
- Filtrer avec :
  - les “métadonnées”
  - des statistiques
  - le DPI (*Deep Package Inspection*)



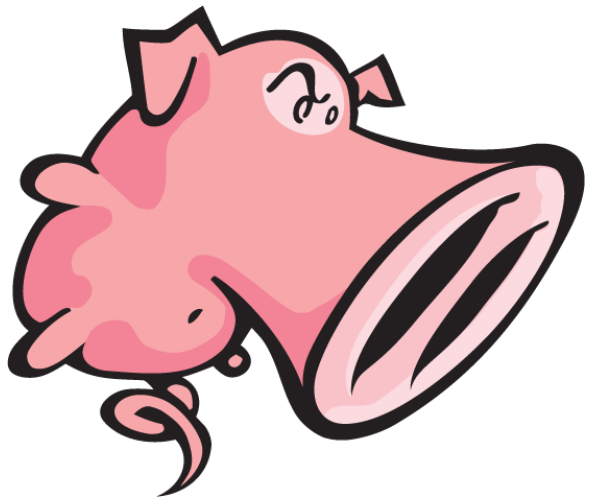
Proxy tampon

- Le cache
- L'anonymat
- Le déni de service

Le logo de Varnish

Proxy enregistreur

- Analyser le trafic (en temps réel ou a posteriori)
- Rejouer une session (pour tester une application ou un service)



Le logo de Snort

Restriction au Web

- Connu de tous et toutes (ou presque)
- Très courant et amené à rester
- Fait partie des programmes (IP, TCP, HTTP, HTML, codage de l'information)
- Technologies libres et gratuites
- Facile de faire de petits exercices autour de la thématique

Programmes scolaires

- Classe terminale au lycée
- Baccalauréats visés :
  - STI2D (sciences et technologies de l'industrie et du développement durable) en spécialité systèmes d'information et numérique
  - S (scientifique) de spécialité d'informatique et sciences du numérique

La situation professionnelle

Le service informatique a subi une attaque ! Vous en faites partie et on vous demande de faire un rapport sur le sujet (origine, ce qui a failli, et une solution pour réduire le risque).

1. Quelles pourraient en être les causes et pourquoi ?
2. Quelle(s) hypothèse(s) semble(nt) l'emporter vis-à-vis des données fournies ?
3. Comment limiter l'impact d'une telle attaque avec l'hypothèse retenue ?
4. Mise en place concrète d'une contre-mesure
5. Ce genre d'outil peut il être détourné et si oui comment ?

Objectifs généraux de formation

Développer les compétences suivantes et les savoirs associés.

- Appréhension d'un système complexe
- Élaboration et explication d'hypothèses
- Création d'une solution technique adéquate
- Réflexion sur l'impact sociétal de la technique et son usage

Matériel à prévoir

- Un ordinateur par groupe d'élèves
- Le logiciel Wireshark sur chaque ordinateur
- Un vidéo-projecteur pour certaines explications et les corrections

Tableau des séances

№	Description de la séance	Ordinateur	Temps
1	Quelles causes et pourquoi ?	Potentiellement	2,0h
2	Quel(s) est/sont les hypothèses réalistes ?	Oui	3,0h
3	Comment prévenir le risque ?	Potentiellement	1,5h
4	Mise en place d'une contre-mesure	Oui	2,5h
5	Détournement d'un outil	Non	1,0h

Durée totale : 9 heures ou 10 heures

Quelles causes et pourquoi ?

Production :

1. Proposition de causes
2. Estimation argumentée de leurs pertinences
3. Tri des causes potentielles identifiées par probabilité estimée

Compétences et savoirs :

- Fonctionnement matériel et logiciel d'un ordinateur
- Fonctionnement d'un réseau informatique
- Arithmétique
- Analyse d'un système multi-factoriel aboutissant à des hypothèses expliquées

Quel(s) est/sont les hypothèses réalistes ?

Préalable : Des données issues de l'attaque sont fournies.
Production :

1. Énumération des éléments qui semblent lier à l'attaque en justifiant
2. Proposition d'hypothèses issues des éléments de l'étape précédente
3. Tri argumenté des hypothèses

Compétences et savoirs :

1. Analyse de données
2. Sélection de la/les hypothèse(s) semblant réaliste(s)
3. Présentation et argumentations sur celle(s)-ci

Comment prévenir le risque ?

Préalable : Une hypothèse a été retenue.

Production :

1. Proposition d'algorithmes pour prévenir l'hypothèse retenue
2. Évaluation de l'efficacité de ceux-ci (temps de calcul, usage de la mémoire, etc)
3. Estimation de l'investissement nécessaire pour chacun
4. Classement des algorithmes en se basant sur le travail fait aux précédentes étapes

Compétences et savoirs :

- Efficacité d'un algorithme
- Proportionnalité de la méthode, par rapport à :
  - la technique
  - la force de travail nécessaire
  - la pertinence économique

Mise en place d'une contre-mesure

Préalable : Une algorithme a été défini.
Production :

- Implémentation d'un algorithme de filtrage
- Explication de cet algorithme

Compétences et savoirs :

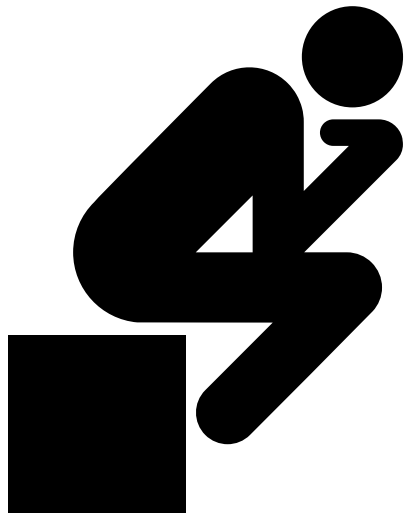
- Programmation
- Efficacité d'un algorithme
- Simplicité de la mise en œuvre
- Compte rendu de la production informatique

Détournement d'un outil

- Cette séance est optionnelle.
- Elle peut être faite en relation avec un·e professeur·e de philosophie, qui peut s'en servir pour engager ou prolonger une réflexion sur l'éthique.

Compétences et savoirs :

- Caractère supranational des réseaux
- Conséquences sociales, économiques et politiques de la technique
- Philosophie



Recherche du moment d'arrêt du fonctionnement et ce qui l'a engendré

Comment pourrions nous envisager cette séance ?

Fiche de déroulement

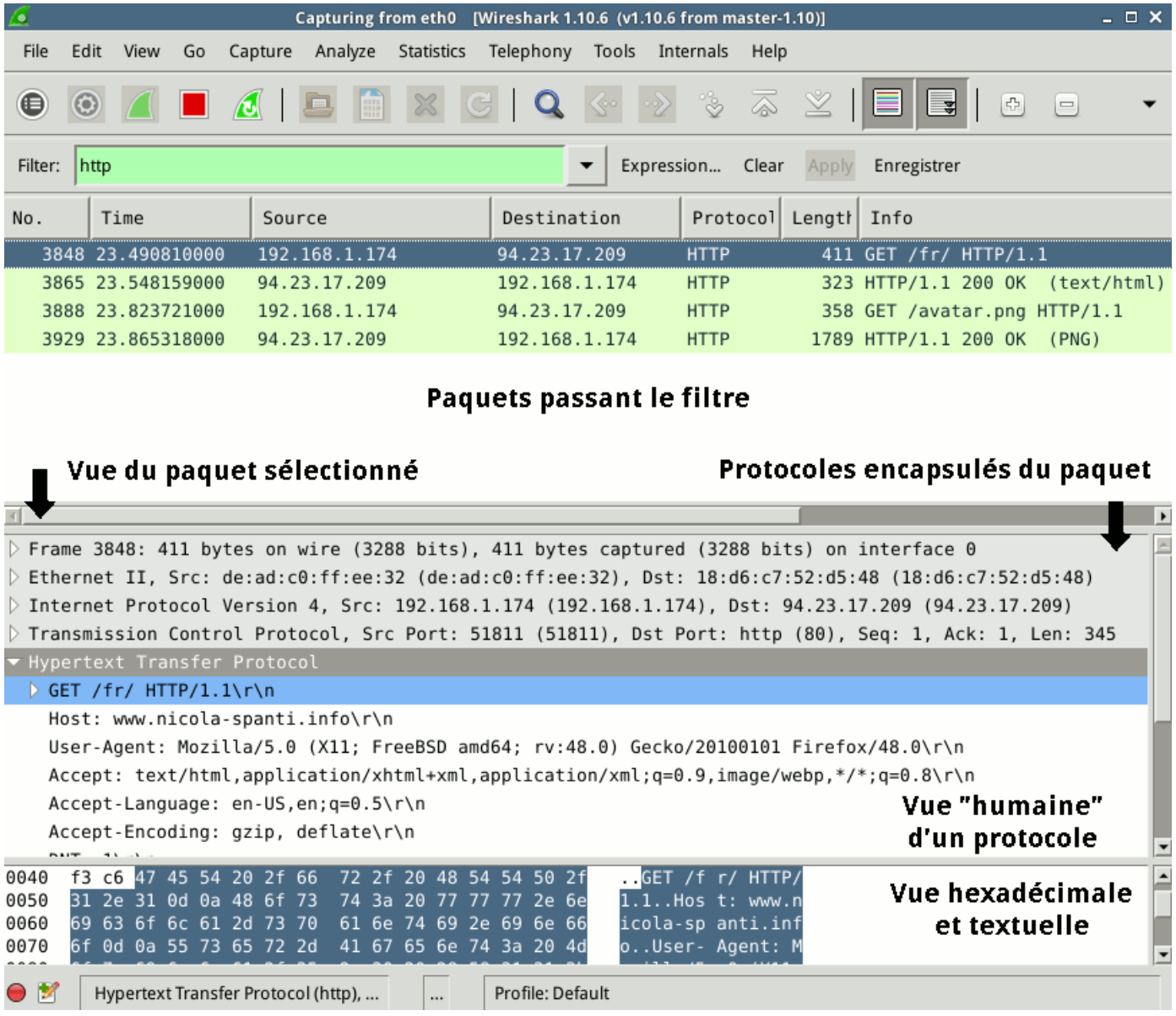
№	Description de l'étape	Temps
1	Présentation du contexte	5 min
2	Présentation de Wireshark	10 min
3	Prise en main de Wireshark	30 min
4	Identification du premier paquet sans réponse	30 min
5	Élaboration d'hypothèses	45 min
6	Débat sur les hypothèses	40 min
7	Correction	20 min

Temps total : 2 heures
L'outil utilisé est Wireshark sur un ordinateur sous GNU/Linux, macOS, ou Windows. Pendant les étapes 3 à 5, l'enseignant·e accompagne les élèves, notamment les plus en difficultés.

Présentation du contexte

1. Vous faites partie du service informatique de l'organisation.
2. L'infrastructure informatique a subi une attaque via le réseau.
3. Vous avez les paquets réseaux enregistrés par un proxy enregistreur.
4. Vous devez produire un rapport sur le sujet :
   - 4.1 Origine de l'attaque
   - 4.2 Ce qui a failli dans le système
   - 4.3 Une solution concrète et proportionnée pour réduire le risque

Présentation de Wireshark



Prise en main de Wireshark

Production et enregistrement d'un jeu de données par l'enseignant · e en utilisant Internet et Wireshark.

Exercices possibles :

- Quelle est l'adresse IP source de l'enseignant·e ?
- Quelle est l'adresse IP du serveur de www.education.gouv.fr (visité en HTTP 1 sans chiffrement pendant la session enregistrée) ?
- Quelle est la valeur hexadécimale pour la chaine de caractères "GET" (sans les guillemets) en HTTP ?
- Quel est le code de retour HTTP pour une réponse valide (comme la réponse pour www.education.gouv.fr) ?
- Dans quels protocoles est encapsulé le protocole HTTP dans l'exemple ?

Identification du premier paquet sans réponse

1. Parcours des trames réseaux
2. Identification d'un paquet sans réponse
3. Recherche du premier sans réponse
4. Rédaction sur le dit paquet (nature, etc) et indication de son numéro pour Wireshark

Élaboration d'hypothèses sur l'attaque

1. Énumération d'hypothèses
2. Réflexion sur les pertinences
3. Classement des hypothèses en fonction de leurs pertinences supposées
4. Écriture au propre des points précédents

Débat sur les hypothèses

1. Un 1er débat avec un autre groupe (10 minutes)
2. Un 2^{e} débat avec un autre groupe (10 minutes)
3. Un 3^{e} débat avec un autre groupe (10 minutes)
4. Explication écrite des changements sur les hypothèses que les débats ont pu amener (10 minutes)

Correction

Pour chaque étape, l'enseignant·e donne la réponse ou les réponses. Entre chaque étape, les élèves sont invités à poser des questions en cas d'incompréhension ou pour en savoir plus. La correction est remise aux élèves ou il leur est demandé de la recopier pour qu'il en garde une trace.