R4B10 - Cryptographie et Sécurité

Introduction

Bruno BEAUFILS

2024/2025

1. Présentation

2. Prérequis

Bruno BEAUFILS

- Maître de conférences en informatique
- Université de Lille
  - IUT / Département informatique
    - Systèmes d'exploitation
    - Réseaux
  - CRIStAL (*Centre de Recherche en Informatique, Signal et Automatique de Lille*)
    - Systèmes Multi-Agents (Théorie des jeux, Finance computationnelle)
    - Intelligence artificielle distribuée / Vie artificielle
    - Réseaux de co-auteurs
    - Médiation scientifique
- Contacts
  - bureau : IUTA-4A49
  - email : `bruno.beaufils@univ-lille.fr`
  - matrix : `@beaufils:matrix.org`
  - web : `https://beaufils.u-lille.fr`
  - mastodon : `@beaufils@mastodon.social`
  - téléphone : `03 59 63 21 57`

Cours

- Objectifs
  - utiliser **pratiquement** les concepts de cryptographie
  - approcher les enjeux de sécurité
    - vus de l'administration des systèmes
- Logistique
  - 5 séances de TP (4 de 3h et 1 de 2h)
  - un peu de cours au début de chaque séance
- Évaluation
  - 4 QCMS (généralement en fin de séance)
- Ressources

`https://r4b10.iutinfo.fr`

1. Présentation

2. Prérequis

Bases d'Unix, informatique, cryptographie

- BUT
  - **programmation** de base — *R1.01, R1.02*
  - **système** d'exploitation et **shell** — *R1.03, R1.04*
  - infrastructure **TCP/IP** — *R2.05, R3.06*
  - adminsys et Debian — *S1.03, S3.03*
  - concepts de **cryptographie** — *R3.09*
- savoir programmer
  - **scripts** shell (plus tard python ou perl)
  - aimer et pratiquer le KISS et la philosophie UNIX :-)
- principes de base d'**UNIX** — *R3.05*
  - fichiers — `open(2)`, `read(2)`, `write(2)`, `close(2)`
  - dossiers — `opendir(3)`, `readdir(3)`, `closedir(3)`
  - modèle d'exécution — `fork(2)`, `execv(3)`, `pipe(2)`
- **shell** (bash)
  - interpréteur — `${...}`, `$(...)`, `*`, `?`
  - redirections — `>`, `<`
  - tubes — `|`
  - droits d'accès

Bases d'Unix, informatique, cryptographie (suite)

- commandes Unix standards
  - fichiers `ls(1)`, `stat(1)`, `nano(1)`, `od(1)`, `hexedit(1)`
  - processus `ps(1)`, `kill(1)`
  - **filtres**
    - indispensables `grep(1)`, `cut(1)`, `tr(1)`
    - essentiels `head(1)`, `tail(1)`, `sort(1)`, `uniq(1)`, `tee(1)`, `sed(1)`
  - réseaux `ping(1)`, `ip(8)`, `tcpdump(8)`, `wireshark(1)`
- expressions régulières
- distribution Debian
  - paquets logiciels `apt-get(8)`, `apt-cache(8)`

Documentation

- accès au manuel UNIX `man(1)`, `apropos(1)`, `whatis(1)`
- organisation du manuel UNIX
  - sections du manuel
  - nommage des pages
  - sections des pages
    - `NAME`, `SYNOPSIS`, `DESCRIPTION`, `SEE ALSO`
- conventions de synopsis
  - `EXP` : texte à remplacer par l'argument approprié
  - `[ EXP ]` : expression (arguments) facultatifs
  - `EXP1 | EXP2` : expression pas utilisables simultanément
  - `EXP ...` expression répétable
- lecture de page `less(1)`
  - recherche
  - déplacement
- accès au manuel GNU `info(1)`
- produire du texte proprement
  - Markdown