Introduction à la sécurité
Cours 0 – Introduction générale

Julien Lavauzelle

Université Paris 8

Licence 3 Informatique et Vidéoludisme

11/09/2023

Plan

Présentation

Quelques informations personnelles :

- Julien Lavauzelle, maître de conférences à l'Université Paris 8
- email : `lavauzelle@up8.edu`
- Ma recherche : codes correcteurs, applications en cryptographie
- Enseigne surtout en mathématiques : Algèbre linéaire 1 (L1), Calcul Formel (L2), Tremplin Master (L3), Théorie de l'information (M1), Cryptographie à clef publique (M1), Algorithmes arithmétiques II (M2)

La **page web** de ce cours :

`https://lvzl.fr/teaching/2023-24/is.html`

Contiendra :

- informations générales,
- slides de cours,
- sujets de TP et fichiers utiles.

Évaluation

Modalités d'évaluation de l'UE :

1. **Première note : TPs à rendre**
   - 4 TPs à rendre, **avant le dimanche 24 septembre**.

Évaluation

Modalités d'évaluation de l'UE :

1. **Première note : TPs à rendre**
   - 4 TPs à rendre, **avant le dimanche 24 septembre**.

2. **Seconde note : projet**
   - travail **individuel**
   - m'envoyer par email une proposition de sujet **avant le jeudi 28 septembre** (c'est mieux encore avant, pour qu'on puisse en discuter)
   - les projets sont à rendre **avant le dimanche 05 novembre** (ensuite, vous aurez des projets dans d'autres matières)

Évaluation

Modalités d'évaluation de l'UE :

1. **Première note : TPs à rendre**
   - 4 TPs à rendre, **avant le dimanche 24 septembre**.

2. **Seconde note : projet**
   - travail **individuel**
   - m'envoyer par email une proposition de sujet **avant le jeudi 28 septembre** (c'est mieux encore avant, pour qu'on puisse en discuter)
   - les projets sont à rendre **avant le dimanche 05 novembre** (ensuite, vous aurez des projets dans d'autres matières)

Note finale : 50 % note 1 + 50 % note 2

Programme

Planning :

Cours « intensif » : du lundi au vendredi, 9h00-12h00 puis 13h30-17h30

Programme

Planning :

Cours « intensif » : du lundi au vendredi, 9h00-12h00 puis 13h30-17h30

Programme prévisionnel du cours :

1. Introduction générale à la sécurité
2. Cryptologie « historique »
3. Cryptologie « moderne » 1 : cryptographie symétrique + TP
4. Cryptologie « moderne » 2 : cryptanalyse (symétrique) + TP
5. Cryptologie « moderne » 3 : cryptographie asymétrique + TP
6. Simulation d'attaque par canaux auxiliaires + TP
7. (Ouverture : enjeux cryptographiques modernes)
8. (Notions de sécurité système et réseaux en semi-autonomie)

Plan

Temps d'échange

La **sécurité informatique**...

- ... c'est **quoi** ?

Temps d'échange

La **sécurité informatique**...

- ... c'est **quoi** ?
- ... ça protège **quoi** ?

Temps d'échange

La **sécurité informatique**...

- ... c'est **quoi** ?
- ... ça protège **quoi** ?
- ... contre **quoi** ?

Temps d'échange

La **sécurité informatique**...

- ... c'est **quoi** ?
- ... ça protège **quoi** ?
- ... contre **quoi** ?
- ... **qui** l'utilise ?

Temps d'échange

La **sécurité informatique**...

- ... c'est **quoi** ?
- ... ça protège **quoi** ?
- ... contre **quoi** ?
- ... **qui** l'utilise ?
- ... **quand** l'utilise-t-on ?

Définition

La **sécurité informatique** (ou sécurité des systèmes d'information – SSI) désigne **l'ensemble des moyens** à déployer dans le but d'**empêcher des pratiques non-désirées** sur un système d'information.

Définition

La **sécurité informatique** (ou sécurité des systèmes d'information – SSI) désigne **l'ensemble des moyens** à déployer dans le but d'**empêcher des pratiques non-désirées** sur un système d'information.

- c'est une définition **générique** → domaine très vaste
- **« moyens »** : techniques, organisationnels, juridiques, humains, ...
- **« pratiques non-désirées »** : à définir. Souvent : utilisation non-autorisée, mauvais usage, modification ou détournement de données.

Définition

La **sécurité informatique** (ou sécurité des systèmes d'information – SSI) désigne **l'ensemble des moyens** à déployer dans le but d'**empêcher des pratiques non-désirées** sur un système d'information.

- c'est une définition **générique** → domaine très vaste
- **« moyens »** : techniques, organisationnels, juridiques, humains, ...
- **« pratiques non-désirées »** : à définir. Souvent : utilisation non-autorisée, mauvais usage, modification ou détournement de données.

Attention : la sécurité est un ensemble de **moyens**, mais ce n'est pas une **fin**.

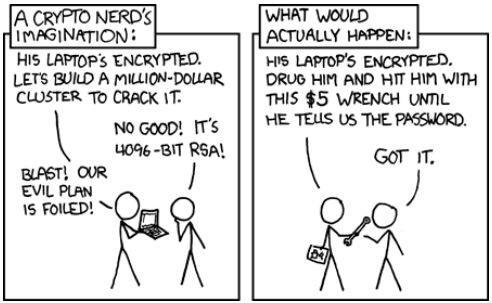
Ce qu'on étudiera

Dans ce cours d'**informatique**, on se concentre sur les **moyens techniques**.

Ce qu'on étudiera

Dans ce cours d'**informatique**, on se concentre sur les **moyens techniques**.

Ils sont **nécessaires**, mais **pas suffisants**.



Classification des moyens techniques

On peut classer les moyens techniques par ordre de dépendance :

1. **Cryptologie :** « science du secret ». Moyens et outils mathématiques, informatiques et électroniques qui permettent de construire et analyser des **primitives cryptographiques**. Sécurise principalement **les données**. Bloc de base de la sécurité.

Classification des moyens techniques

On peut classer les moyens techniques par ordre de dépendance :

1. **Cryptologie :** « science du secret ». Moyens et outils mathématiques, informatiques et électroniques qui permettent de construire et analyser des **primitives cryptographiques**. Sécurise principalement **les données**. Bloc de base de la sécurité.
2. **Sécurité des systèmes**. Moyens permettant de **sécuriser des infrastructures** de données (ex : réseaux, serveurs, etc.).

Classification des moyens techniques

On peut classer les moyens techniques par ordre de dépendance :

1. **Cryptologie :** « science du secret ». Moyens et outils mathématiques, informatiques et électroniques qui permettent de construire et analyser des **primitives cryptographiques**. Sécurise principalement **les données**. Bloc de base de la sécurité.
2. **Sécurité des systèmes**. Moyens permettant de **sécuriser des infrastructures** de données (ex : réseaux, serveurs, etc.).
3. **« Privacy »** (protection de la vie privée). Moyens permettant de sécuriser l'information relative à l'humain. Exemples : confidentialité, anonymat, droit à l'oubli, etc.

Classification des moyens techniques

On peut classer les moyens techniques par ordre de dépendance :

1. **Cryptologie :** « science du secret ». Moyens et outils mathématiques, informatiques et électroniques qui permettent de construire et analyser des **primitives cryptographiques**. Sécurise principalement **les données**. Bloc de base de la sécurité.
2. **Sécurité des systèmes**. Moyens permettant de **sécuriser des infrastructures** de données (ex : réseaux, serveurs, etc.).
3. **« Privacy »** (protection de la vie privée). Moyens permettant de sécuriser l'information relative à l'humain. Exemples : confidentialité, anonymat, droit à l'oubli, etc.

Par ailleurs, il existe des disciplines **transverses** :

- la sécurité système, la sécurité réseaux, la sécurité web, la sécurité matérielle

Classification des moyens techniques

On peut classer les moyens techniques par ordre de dépendance :

1. **Cryptologie :** « science du secret ». Moyens et outils mathématiques, informatiques et électroniques qui permettent de construire et analyser des **primitives cryptographiques**. Sécurise principalement **les données**. Bloc de base de la sécurité.
2. **Sécurité des systèmes**. Moyens permettant de **sécuriser des infrastructures** de données (ex : réseaux, serveurs, etc.).
3. **« Privacy »** (protection de la vie privée). Moyens permettant de sécuriser l'information relative à l'humain. Exemples : confidentialité, anonymat, droit à l'oubli, etc.

Par ailleurs, il existe des disciplines **transverses** :

- la sécurité système, la sécurité réseaux, la sécurité web, la sécurité matérielle
- virologie informatique, analyse de *malware*

Classification des moyens techniques

On peut classer les moyens techniques par ordre de dépendance :

1. **Cryptologie :** « science du secret ». Moyens et outils mathématiques, informatiques et électroniques qui permettent de construire et analyser des **primitives cryptographiques**. Sécurise principalement **les données**. Bloc de base de la sécurité.
2. **Sécurité des systèmes**. Moyens permettant de **sécuriser des infrastructures** de données (ex : réseaux, serveurs, etc.).
3. **« Privacy »** (protection de la vie privée). Moyens permettant de sécuriser l'information relative à l'humain. Exemples : confidentialité, anonymat, droit à l'oubli, etc.

Par ailleurs, il existe des disciplines **transverses** :

- la sécurité système, la sécurité réseaux, la sécurité web, la sécurité matérielle
- virologie informatique, analyse de *malware*
- contrôle d'accès, contrôle d'usage

Classification des moyens techniques

On peut classer les moyens techniques par ordre de dépendance :

1. **Cryptologie :** « science du secret ». Moyens et outils mathématiques, informatiques et électroniques qui permettent de construire et analyser des **primitives cryptographiques**. Sécurise principalement **les données**. Bloc de base de la sécurité.
2. **Sécurité des systèmes**. Moyens permettant de **sécuriser des infrastructures** de données (ex : réseaux, serveurs, etc.).
3. **« Privacy »** (protection de la vie privée). Moyens permettant de sécuriser l'information relative à l'humain. Exemples : confidentialité, anonymat, droit à l'oubli, etc.

Par ailleurs, il existe des disciplines **transverses** :

- la sécurité système, la sécurité réseaux, la sécurité web, la sécurité matérielle
- virologie informatique, analyse de *malware*
- contrôle d'accès, contrôle d'usage
- biométrie

Classification des moyens techniques

On peut classer les moyens techniques par ordre de dépendance :

1. **Cryptologie :** « science du secret ». Moyens et outils mathématiques, informatiques et électroniques qui permettent de construire et analyser des **primitives cryptographiques**. Sécurise principalement **les données**. Bloc de base de la sécurité.
2. **Sécurité des systèmes**. Moyens permettant de **sécuriser des infrastructures** de données (ex : réseaux, serveurs, etc.).
3. **« Privacy »** (protection de la vie privée). Moyens permettant de sécuriser l'information relative à l'humain. Exemples : confidentialité, anonymat, droit à l'oubli, etc.

Par ailleurs, il existe des disciplines **transverses** :

- la sécurité système, la sécurité réseaux, la sécurité web, la sécurité matérielle
- virologie informatique, analyse de *malware*
- contrôle d'accès, contrôle d'usage
- biométrie
- ingénierie sociale

Programme

Planning :

Cours « intensif » : du lundi au vendredi, 9h00-12h00 puis 13h30-17h30

Programme

Planning :

Cours « intensif » : du lundi au vendredi, 9h00-12h00 puis 13h30-17h30

Programme prévisionnel du cours :

1. Introduction générale à la sécurité
2. Cryptologie « historique »
3. Cryptologie « moderne » 1 : cryptographie symétrique + TP
4. Cryptologie « moderne » 2 : cryptanalyse (symétrique) + TP
5. Cryptologie « moderne » 3 : cryptographie asymétrique + TP
6. Simulation d'attaque par canaux auxiliaires + TP
7. (Ouverture : enjeux cryptographiques modernes)
8. (Notions de sécurité système et réseaux en semi-autonomie)

[Pour les projets tuteurés]

[Pour les projets tuteurés]

Planning à respecter :

1. **Premier semestre** : état de l'art :
   - comprendre où en est la science sur le sujet,
   - s'approprier la problématique,
   - commencer à esquisser une solution,
   - produire un rapport intermédiaire.

[Pour les projets tuteurés]

Planning à respecter :

1. **Premier semestre** : état de l'art :
   - comprendre où en est la science sur le sujet,
   - s'approprier la problématique,
   - commencer à esquisser une solution,
   - produire un rapport intermédiaire.
2. **Second semestre** : implémentation :
   - proposer une solution,
   - mettre en œuvre celle-ci par la programmation,
   - faire une démonstration à la fin de l'année,
   - mettre à jour le rapport avec les résultats obtenus.

[Pour les projets tuteurés]

Planning à respecter :

1. **Premier semestre** : état de l'art :
   - comprendre où en est la science sur le sujet,
   - s'approprier la problématique,
   - commencer à esquisser une solution,
   - produire un rapport intermédiaire.
2. **Second semestre** : implémentation :
   - proposer une solution,
   - mettre en œuvre celle-ci par la programmation,
   - faire une démonstration à la fin de l'année,
   - mettre à jour le rapport avec les résultats obtenus.

Informations complémentaires :

- Les projets tuteurés se font en **binôme**.
- Si le domaine de la **cryptologie**, des **codes correcteurs**, ou généralement de l'informatique appliquée aux **mathématiques** vous intéresse : contactez-moi !