Sécurité des Systèmes Informatiques (SSI)

Ce Master vise à répondre au besoin croissant de sécurisation des environnements de travail numériques, cruciale pour maintenir la productivité et la fiabilité des services, cette formation prépare les étudiants à maîtriser les aspects organisationnels, applicatifs et réseaux de la sécurité informatique, les diplômés de ce master peuvent trouver des débouchées professionnels comme : responsables sécurité, concepteurs d'applications et évaluateurs, experts en ingénierie logicielle capables d'intégrer la sécurité dès le développement, les experts techniques, spécialistes des vulnérabilités et de leur exploitation dans des domaines spécifiques, aptes à identifier et à résoudre les failles critiques.

S1 :

- Architectures des réseaux informatiques (ARIN)
- Veille technologique et Bases de données avancées (VTBD)
- Complexité algorithmique (CALG)
- Systèmes d’exploitation (SYEX)
- Arithmétique modulaire (ARMO)
- Introduction à la sécurité informatique (INSI)
- Anglais pour l’informatique (ANIN)
- Aspects juridiques dans la sécurité informatique (AJSI)

• **Architectures des réseaux informatiques (ARIN) :**

Rappel des bases de réseaux**,** algorithmes de routage statique et dynamique, IPV6, les principales architectures des réseaux téléinformatiques et télécommunications

• **Veille technologique et Bases de données avancées (VTBD) :**

Méthodologie de veille et de recherche, méthodes de conception de schéma, développement pratique, gestion d'une base de données

• **Complexité algorithmique (CALG) :**

Complexité, outils mathématiques, notions nécessaires pour analyser et classer les problèmes de différents domaines, algorithmes de tri, structures de données

• **Systèmes d'exploitation (SYEX) :**

Méthodes de conception d'un système d'exploitation, gestion de processus et processeur, gestion de la mémoire, gestion de fichier, communications inter-processeurs, les moniteurs

• **Arithmétique modulaire (ARMO) :**

Les bases des mathématiques et algorithmiques nécessaires à la bonne compréhension des cours de cryptographie

• **Introduction à la sécurité informatique (INSI) :**

Introduction, survol sur les différents aspects reliés à la sécurité informatique, les phases de la sécurité de l'étape de reconnaissance jusqu'à l'accès au système, langage de script

• **Anglais pour l'informatique (ANIN) :**

Les bases de l'anglais nécessaires à la bonne compréhension de la documentation en anglais

• **Aspects juridiques dans la sécurité informatique (AJSI) :**

Les aspects juridiques (action menant à des amendes ou des peines de prison) et les risques liés à la confidentialité et l'intégrité des informations issues d'Internet et des informations contenues dans son propre ordinateur, code pénal algérien

S2 :

- Cryptographie et sécurité (CRYS)
- Politiques de Contrôle d’accès (PCAC)
- Administration et tuning de bases de données (ATBD)
- Sécurité réseaux (SERE)
- Sécurité système (SESY)
- Sécurité des Réseaux sans fil (SERF)
- Algorithmique répartie (ALRE)
- Sûreté de fonctionnement et fiabilité du logiciel (SFFL)

- **Cryptographie et sécurité (CRYS) :**

Algorithmes de chiffrement, authentifications, signatures électroniques, cryptographie moderne

- **Politiques de Contrôle d’accès (PCAC) :**

Politiques d’accès logique et physique modélisation des mécanismes de contrôle d’accès

- **Administration et tuning de bases de données (ATBD) :**

Principes de tuning de BDD en restant indépendant du SGBD, du système d'exploitation ou du matériel, sécurité des BDD, création de rôle, distribuer des rôles

- **Sécurité réseaux (SERE) :**

Sécurité de toutes les couches OSI, voir les grandes idées qui sous-tendent tous les différents modules en sécurité informatique

• **Sécurité système (SESY) :**

Les principaux problèmes de sécurité dans les systèmes d'exploitation et les méthodes pour y remédier, politique d’accès, Projet TP gestion de la sécurité de Kubernetes

• **Sécurité des Réseaux sans fil (SERF) :**

Mécanismes de sécurisation des réseaux sans fil, Bluetooth, sécurité des Wi-Fi

• **Algorithmique répartie (ALRE) :**

Algorithmes distribués, les principaux concepts de l’algorithmique répartie

• **Sûreté de fonctionnement et fiabilité du logiciel (SFFL) :**

Méthodes garantissant qu'un logiciel a atteint un niveau de fiabilité suffisant, probabilité

S3 :

- Sécurité système avancée (SYSA)
- Méthodes pratiques et outils de détection d'intrusions (MPOD)
- Audit de sécurité (AUSE)
- Programmation et sûreté des systèmes répartis (PSSR)
- Modélisation des systèmes communicants (MOSC)
- Sécurité applicative (SEAP)
- Sécurité et contrôle du trafic réseau (SCTR)
- Méthodes d'optimisation (MEOP)

• Sécurité système avancée (SYSA) :

Fonctionnement et administration des systèmes d'exploitation de la famille Windows NT, gestion des certificats numériques

• Méthodes pratiques et outils de détection d'intrusion (MPOD) :

Analyse des failles de sécurité et des possibilités de pénétration de système dans un projet complexe, types de protocole

• Audit de sécurité (AUSE) :

Mettre en place une procédure d'audit d'un système informatique càd trouver toutes les vulnérabilités du système

• Programmation et sûreté des systèmes répartis (PSSR) :

Bases de la programmation parallèle et répartie, programmation multi-agent, solutions aux problèmes de coût et de fiabilité des systèmes repartis

• **Modélisation des systèmes communicants (MOSC) :**

Module théorique, algèbre, réseaux de Petri, les méthodes classiques de modélisation de systèmes communicants à travers les applications à différents problèmes de sécurité

• **Sécurité applicative (SEAP) :**

Maitriser la sécurisation globale d'une application, que ce soit dans ses aspects système ou réseau, investigation numérique, Buffer Overflow, SQL injection

• **Sécurité et contrôle du trafic réseau (SCTR) :**

Gestion du trafic réseau, Acces List, administration et sécurité des routeurs

• **Méthodes d'optimisation (MEOP) :**

Outils mathématiques et expérimentaux pour optimiser les systèmes informatiques

Avantages :

• Modules très intéressent et utiles dans le monde du travail

Inconvénients :

• Programme trop chargé

• Quelques modules inutiles

Opportunités de travail :

• Responsables de la sécurité des systèmes d’informations

• Auditeur de Sécurité

• Pentester

• Analyste en sécurité des Systèmes d'Information

• Consultant en cybersécurité pour les entreprises

• Ingénieur sécurité réseaux

• Concepteurs et évaluateurs d’applications