ENSEIRB-MATMECA

Introduction à la sécurité de l'information et des réseaux

École / Prépa
ENSEIRB-MATMECA

Présentation

Code interne : ET8RE200

Description

En premier lieu, ce module débute par une introduction à la cybersécurité en l'illustrant par des exemples concrets et en introduisant les critères de sécurités communément utilisés pour définir et évaluer les propriétés des éléments d'un système d'information ou de l'intégralité d'un tel système. Ensuite, les spécificités des réseaux de données sont plus particulièrement étudiées afin de déterminer les techniques les plus appropriées pour protéger les flux d'informations. Parmi ces techniques de protection, l'accent est plus particulièrement mis sur les techniques et outils cryptographiques qui sont largement étudiés et dont la portée dépasse largement le contexte des réseaux. L'intérêt de la cryptographie est alors mis en évidence dans de multiples contextes : authentification d'utilisateurs vis à vis d'un système d'information, protection des informations, protection des flux réseaux, protocoles de communication sécurisés, tels que IPSec et TLS (ex-SSL), etc. Ce module se conclut par des travaux pratiques permettant de construire un VPN (Virtuel Private Network - réseau privé virtuel) faisant appel à la plupart des notions étudiées auparavant.

Objectifs

- En les comprenant, être conscient de la plupart des risques de cybersécurité auxquels les systèmes d'information sont exposés.
- Être capable, en tant que futur professionnel, d'éviter des risques de cybersécurité relativement simples auxquels les systèmes d'informations sont exposés en adoptant de bonnes pratiques tout aussi simples et, en tant qu'utilisateur, d'éviter les comportements à risque.
- En les comprenant, être conscient des limitations de quelques protocoles réseaux courants en termes de cybersécurité.
- Être capable, dans des cas relativement simples, d'envisager des solutions pour parer aux risques de cybersécurité auxquels les réseaux courants sont exposés.
- Connaître et comprendre les principes de base de la cryptographie appliquée.
- Être capable d'utiliser judicieusement la cryptographie afin de protéger des informations quelconques ou des flux réseaux.
- En les comprenant, être capable d'utiliser des protocoles réseaux sécurisés afin de protéger les flux d'informations.

Heures d'enseignement

CM	Cours Magistraux	32h
TDM	Travaux Dirigés sur Machine	4h

Pré-requis obligatoires

- Notions générales en informatique.
- Principes et architectures des réseaux, en particulier IPv4 et IPv6.

Syllabus

- Notion de sécurité de l'information : sensibilisation et initiation à la cybersécurité
  - Enjeux de la sécurité des systèmes d'information
  - Besoins fondamentaux de sécurité
    Introduction des critères DICP : Disponibilité, Intégrité, Confidentialité et Preuve.
  - Notions de vulnérabilité, menace et attaque
    Illustrations et conséquences potentielles pour les entités victimes d'attaques.
  - Quelques aspects règlementaires et légaux
- Notion de sécurité des réseaux
  - Exemples de faiblesses de protocole courants simples
  - Sécurité de l'information et protection des flux réseaux
  - Nécessité de l'utilisation des techniques et outils cryptographiques
- Techniques et outils cryptographiques appliqués aux critères de sécurité DICP
  - Fonctions de calcul d'empreinte (hachage)
    - Applications à la génération de MAC (Message Authentication Code - code de vérification d'authenticité de message) et de MIC (Message Integrity Code - code de vérification d'intégrité de message).
    - Notions de sel et de poivre.
    - Applications au stockage irréversible de secrets et à l'anonymisation de données.
  - Cryptographie symétrique à clé secrète partagée
    Propriétés et utilisation pour la protection des flux réseaux (entre autres).
  - Cryptographie asymétrique à clés publique et privée
    - Propriétés et utilisation pour la protection des flux réseaux (entre autres).
    - Notions de certification et d'autorité de certification.
- Applications
  - Authentification d'utilisateurs vis à vis d'un système d'information
  - Protocoles réseaux sécurisés : IPSec et TLS (ex-SSL)
    Notion de VPN (Virtual Private Network - réseau privé virtuel).
- Travaux pratiques
  Illustration de la plupart des notions vues auparavant par la construction d'un VPN.

N.B. : volontairement, ce module n'aborde pas le « test de pénétration », ou « pentesting », ni l'attaque de systèmes réels ; seuls quelques exemples sont évoqués, sans moyens concrets de les exploiter, à des fins d'illustration et de justification des notions étudiées.

Bibliographie

- Documentation officielle du DoD Internet : https://www.rfc-editor.org.
- Documents édités par l'ANSSI : https://www.ssi.gouv.fr.
- W. Stallings, "Cryptography and Network Security: Principles and Practice" - 7th Edition, Pearson, 2017.
- Polycopié de cours non exhaustif (prise de notes obligatoire) et textes de travaux pratiques.

Modalités de contrôle des connaissances

Évaluation initiale / Session principale

Type d'évaluation	Nature de l'évaluation	Durée (en minutes)	Nombre d'épreuves	Coefficient de l'évaluation	Note éliminatoire de l'évaluation	Remarques
Contrôle Continu Intégral	Contrôle Continu					Détails du contrôle continu : 0.25 * Participation Active + 0.75 * Écrit de synthèse (1h30, documents interdits, calculatrice en mode examen autorisée, tout autre moyen informatique et tout moyen de communication interdits).

Infos pratiques

Contacts

Responsable module

Xavier Delord
Xavier.Delord@bordeaux-inp.fr