Sécurité des réseaux SECRES (INF944)
Présentation et organisation du cours

Master 2, Sorbonne Université - Télécom Paris,

UE SECRES

Responsable : Rida Khatoun

Maître de conférences, Télécom-Paris

rida.khatoun@telecom-paris.fr

Plan

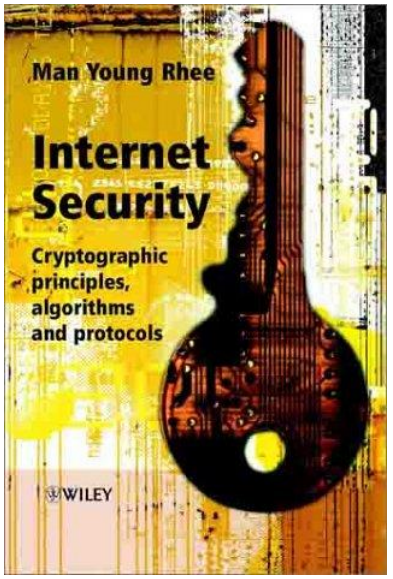
- Présentation
  - Responsable de l'UE :
    - Rida Khatoun, MCF, département INFRES
    - Bureau : 4C62 à Saclay !!
    - E-mail : rida.khatoun@telecom-paris.fr
  - Responsable de TD/TP :
    - Christophe Kiennert, Télécom Sud Paris
    - E-mail : christophe.kiennert@telecom-sudparis.eu
- Plan du cours
- Projets et organisation

Plan du cours

- INF944 (SECRES) : Sécurité des réseaux
- Contenu et objectif du cours
  - Services de sécurité
  - Architecture de sécurité et protocoles
  - Attaques/intrusions
  - Systèmes de détection/défense
  - Aspects recherche
- Projets : techniques / recherche
- Evaluation :
  - Examen final (70 %)
  - Projet avec soutenance (30%)

Plan détaillé du cours

- Introduction à la sécurité des réseaux
  - Architecture de sécurité
  - Services ou critères de sécurité
  - Algorithmes asymétriques/symétriques
  - Fonctions de hachage
  - Cryptographies à courbes elliptiques



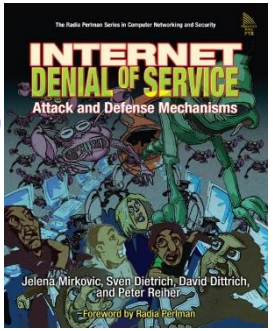
- Sécurité du support de communication SSL
  - Besoins
  - Architecture et protocoles SSL
  - Certificats de serveurs X.509
  - Faiblesses de SSL et attaques

Plan détaillé du cours

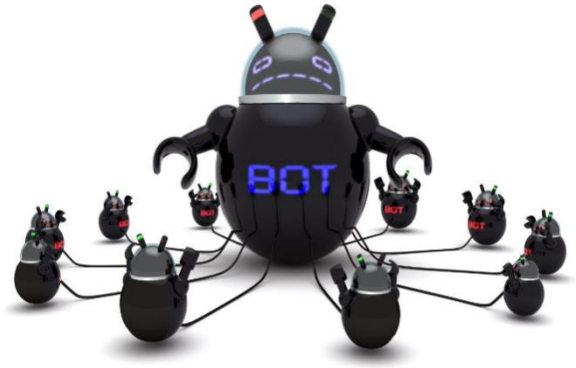
- Identité numérique et Authentification
  - Les modèles d'identités
    - Login / mot de passe : Déclinaisons et alternatives
  - Fédération des identités
  - Formalisation des protocoles d'authentification

- Public Key Infrastructure (PKI)
  - Présentation du standard X509 et X509v3
  - Autorités de certification
  - Délégation de confiance
  - Signature électronique et authentification

Plan détaillé du cours



- Attaques de déni de service distribuées (DDoS)
  - Contexte et historique
  - Types d'attaques
    - Spoofing
    - Smurfing
    - ICMP flooding
    - TCP flooding
  - Botnets et leurs architectures
  - Exemples de scénarios d'attaques
  - Mesures de prévention
  - Approches de détection
  - Approches de traçabilité
- *Cloud Computing* comme une plateforme d'attaques



Plan détaillé du cours

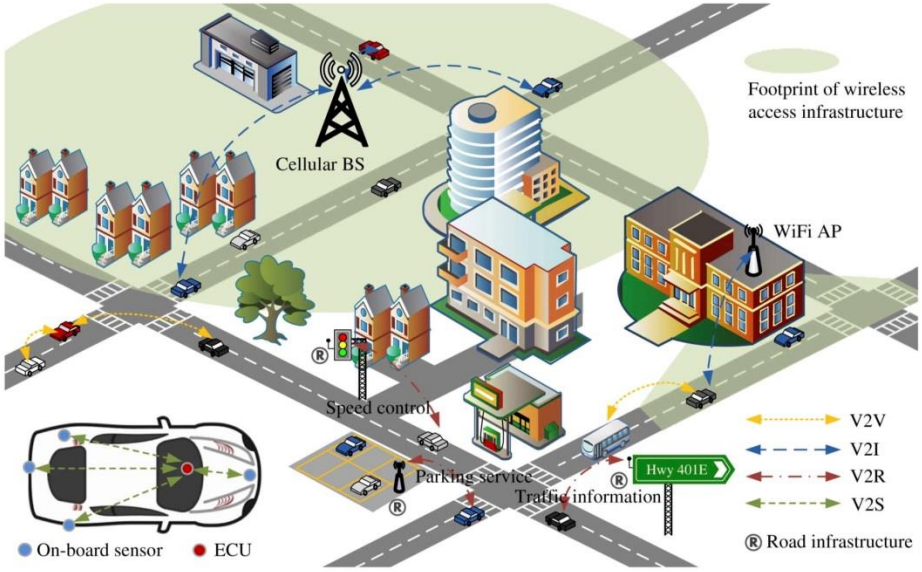
- Systèmes de détection d'intrusion
  - Types majeurs de l'IDS
    - Détection par signature
    - Détection d'anomalies
  - Pourquoi a-t-on besoin de l'IDS?
  - Source des informations
    - HIDS
    - NIDS
    - Hybride
  - Exemple : Snort, Bro, Prelude
  - Placement d'IDS

Plan détaillé du cours

- Sécurité des réseaux Wi-Fi
  - Utilisation du Wi-Fi
  - Sécurité des points d'accès
  - Sécurité des protocoles
- Sécurité des réseaux cellulaires
  - Mobilité
  - Authentification des utilisateurs
  - Confidentialité des données
  - Confidentialité des info de signalisation

Plan détaillé du cours

- Réseaux Véhiculaires
  - Architecture V2V, V2I et standards
  - Dépoilement
  - Attaques et vulnérabilités



Projets de recherche

- Objectif :
  - Comprendre une problématique, étudier l'état de l'art, analyser, proposer une solution
  - Rédiger un rapport/article de recherche
- Références
  - Articles publiés, revues, thèses
  - Ex :
    - http://ieeexplore.ieee.org/Xplore/dynhome.jsp
    - http://www.sciencedirect.com/
    - RFC

Projets techniques

- Objectif :
  - Comprendre : enjeux, solution technique
  - Implémentation, test et analyse
  - Savoir rédiger un rapport technique
- Références
  - Articles
  - Blogs spécialisés
  - Etc.

Structure du rapport

- Résumé : condensé du contenu
- Introduction : objectifs, cadre du sujet et plan
- Etat de l'art
  - Définitions, hypothèses, ...
  - Illustrations techniques
  - Comparaison
- Conclusion : rappel des résultats, point de vue critique, nouvelles pistes proposées
- Références bibliographiques
- Volume minimal : 5 pages par personne

Citations

- Citations littérales autorisées mais :
  - Courtes (quelques lignes au plus)
  - Clairement identifiées comme telles (guillemets, source indiquée juste après la citation)
  - En nombre assez restreint
- Rappel : une citation présentée comme une partie de votre texte est assimilable à du plagiat

Projets

- Projet par groupe de **5 ou 4** étudiants
- Désigner un animateur de groupe
- Attribution de projets
  - Sur place ou….
  - Par mail en choisissant **3** sujets avec l'ordre de priorité (l'e-mail doit être envoyé par l'animateur du groupe) au responsable de l'UE
- Suivi des projets
  - Voir le correspondant de votre projet **3** fois dans le semestre selon un planning défini ultérieurement

Projets techniques

- Projet 1 : Développer un module OTP dans TLS1.3
- Projet 2 : Développer un protocole de consensus de couche physique en utilisant la technique de codage Lattice (sur Matlab)
- Projet 3 : Développement d'un script en python pour la Factorisation de Lenstra et benchmarking
- Projet 4 : Etude et simulation des algorithmes quantiques
- Projet 5 : Pegasus : étude, implémentation, scénario
- Projet 6 : Cryptolightweight : études et benchmarking des algorithmes
- Projet 7 : Etude, analyse et implémentation des oracles dans la blockchain (oracle=serveur inter-blockchain)
- Projet 8 : Etude et analyse des protocoles de communication entre les blockchains
- Projet 9 : Ransom0? Byob? raanET ransomwares: analyse et implémentation
- Projet 10 : BUSMASTER CAN bus Simulator (DoS, spoofing simulation)
  - Analyser les messages sur le bus CAN
  - Injection des faux messages

Projets de recherche

- Projet 11 : Développement des scenarios d'attaques VANET's sur Matlab
  - Automated Driving Toolbox

- Possibilité de proposer d'autres projets.

Remarques

- Réunion tous les mois
- Sans plagiat
  - *Antiplagiat tool* « https://www.compilatio.net »
- Rôle de l'animateur
  - Porte parole du groupe
  - Organisation des réunions
  - Envoi des mails
- Mail:
  - Sujet : Groupe X [Objectif du mail]
  - Signature : Membres du groupe