Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Secrétariat général de la défense nationale

DIRECTION CENTRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

CENTRE DE FORMATION À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Catalogue 2004

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE
DCSSI / CFSSI
51, boulevard de La Tour-Maubourg
75700 PARIS 07 SP

Tél : 01 71 76 85 15
Fax : 01 71 76 85 10
cfssi@sgdn.pm.gouv.fr

www.formation.ssi.gouv.fr

2004

Avant-propos

Le Centre de formation à la sécurité des systèmes d'information est l'acteur central d'un réseau de sensibilisation aux problèmes liés à la sécurité des systèmes d'information (SSI) et l'organisme dédié à la formation d'experts hautement qualifiés dans les différents métiers de la discipline.

Dans le cadre de cette mission, le CFSSI poursuit un double objectif :

1. offrir, à partir d'une identification réaliste des besoins aux différents niveaux et sur la base d'un catalogue de formation rénové, une formation adaptée aux divers acteurs publics de la SSI (responsables, concepteurs et utilisateurs) ;

2. créer un réseau informel d'échanges d'expériences et d'enrichissement mutuel dans le domaine de la formation SSI avec des établissements d'enseignement supérieur et des centres de formation continue afin d'encourager la prise en compte de la SSI à tous les niveaux.

Sa mission s'inscrit donc tout naturellement dans les deux objectifs imbriqués que poursuit la DCSSI au sein du Secrétariat général de la défense nationale : assurer la sécurité des systèmes d'information de l'État (administrations et infrastructures vitales) et créer les conditions d'un environnement de confiance et de sécurité propice au développement de la société de l'information en France et en Europe.

L'installation du CFSSI au cœur de Paris, qui est effective depuis septembre 2003 dans des locaux plus vastes, lui permet de développer ses activités et d'accueillir dans les meilleures conditions ses stagiaires et ses étudiants du BESSSI, formation inscrite au Répertoire National des Certifications Professionnelles.

L'offre de formations 2004 consolide les stages renouvelés mis en place depuis 2002 pour toujours mieux s'adapter aux demandes des administrations. Ainsi, le stage sur les « Infrastructures de Gestion de Clés » est élargi à la problématique de l' «Administration Électronique et la Sécurité ». Un nouveau stage sur la « Sécurité du Sans-Fil » est créé. Vous en trouverez le détail dans ce catalogue qui propose des parcours cohérents, notamment pour un suivi efficace des stages de « Travaux Pratiques ».

Le développement des compétences en sécurité des systèmes d'information au sein des administrations passe, aujourd'hui, par la mise en place d'un plan interministériel de formation à la sécurité des systèmes d'information à caractère interdisciplinaire (scientifique, technique, juridique, économique) où le CFSSI aura un rôle moteur à jouer.

Henri SERRES
DIRECTEUR CENTRAL DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Table des matières

1 Le CFSSI

Le terme « système d'information » s'adresse aux moyens dont le fonctionnement fait appel, d'une façon ou d'une autre, à l'électricité, et qui sont destinés à élaborer, traiter, stocker, acheminer ou présenter l'information.

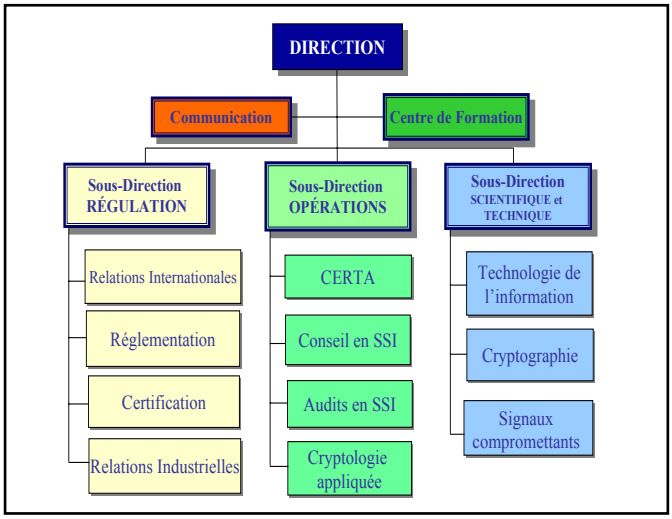
1.1 Mission du CFSSI

La mission du CFSSI est définie par l'article 1er du décret 87-354 du 25 mai 1987 :

- Sensibilisation à la sécurité des systèmes d'information
- Formation d'experts capables de concevoir, d'évaluer et de conseiller dans les domaines suivants de la sécurité des systèmes d'information:
  - sécurité des communications,
  - protection contre les signaux parasites compromettants,
  - sécurité informatique.

L'activité et l'enseignement du CFSSI sont dirigés et suivis par un Comité de perfectionnement présidé par le Secrétaire général de la défense nationale et composé de hauts fonctionnaires civils et militaires.

1.2 Organigramme de la DCSSI



1.3 Domaine d'intervention du CFSSI

Le CFSSI est particulièrement compétent en matière de formation et de sensibilisation dans le domaine de la sécurité des systèmes d'information (SSI).

Il peut être consulté par la Commission Interministérielle pour la Sécurité des Systèmes d'Information (CISSI).

La Sécurité repose sur les hommes :

- la sensibilisation des personnels à tous les niveaux,
- la formation des spécialistes,

sont une composante essentielle de la Sécurité des Systèmes d'Information.

1.4 Moyens pédagogiques du CFSSI

Le corps professoral est constitué :

- de professeurs de l'Enseignement Supérieur,
- de professeurs, d'ingénieurs et d'officiers de la DCSSI,
- de chargés de cours et de conférenciers de différents ministères ou du secteur privé.

Le CFSSI dispose de salles de cours équipées des matériels audiovisuels, vidéo et informatiques nécessaires à la conduite des cours théoriques et des travaux pratiques. De plus, les stagiaires ont la possibilité de consulter la documentation de la bibliothèque de la DCSSI.

1.5 Admission en stage

Tout renseignement concernant le programme des différents stages de formation et de sensibilisation, ainsi que les conditions d'admission peut être obtenu auprès de :

SGDN/DCSSI/CFSSI
51 boulevard de La Tour-Maubourg
75700 PARIS 07SP
tél : 01 71 76 85 15
fax : 01 71 76 85 10
cfssi@sgdn.pm.gouv.fr
www.formation.ssi.gouv.fr

Les candidatures aux journées de sensibilisation, aux stages ou séminaires de formation doivent être présentées au CFSSI :

- Pour le ministère de la Défense :
  - par l'État-major des Armées, division TEI,
  - par les organismes militaires chargés de l'enseignement militaire supérieur scientifique et technique (EMSST),
  - par les Directions ou les Délégations intéressées (CGA, DGGN, DGA,…) pour les personnels relevant de leur autorité.
- Pour les autres ministères, par les Hauts Fonctionnaires de Défense.

Des feuilles d'inscription sont jointes au présent catalogue. Les capacités d'admission étant limitées à 40 personnes par stage (moins pour les stages pratiques et méthodologiques), il est proposé aux stagiaires, quand le stage est programmé à plusieurs reprises, d'exprimer des ordres de priorité sur les dates proposées. Nous essaierons, dans la mesure du possible, de satisfaire leurs souhaits. Les stagiaires dont les candidatures sont retenues sont convoqués à travers la chaîne hiérarchique SSI, décrite ci-dessus.

Il est demandé aux stagiaires de respecter les niveaux d'admission à nos stages. Les stages plus techniques (stage n° 3b, 5b, 11) sont réservés à des informaticiens. Les stages de travaux pratiques n°7b et d'audit SSI nécessitent les connaissances du stage n° 5b. Le stage de travaux pratiques n°7a, ouvert à tous les praticiens de l'informatique, nécessite les connaissances du stage n°5a.

L'objectif de nos nouvelles formations est de présenter à nos stagiaires, issus de l'administration, les techniques de sécurisation des postes de travail et des architectures informatiques à travers l'exploration des fonctions indispensables à un travail partagé, de les sensibiliser aux menaces principales, de leur donner un certain nombre de réflexes

notamment dans la configuration des postes et des éléments actifs des réseaux. Par contre, il ne s'agit ni de les former à tel ou tel outil ou produit informatique particulier (cette formation est ou devrait être assurée par les fournisseurs de ces produits), ni de recommander tel ou tel outil particulier. Les produits utilisés pour illustrer les concepts de la sécurité sont choisis, dans la mesure du possible, soit dans les produits les plus répandus, soit dans le domaine du logiciel libre ou gratuit

1.6 Calendrier et horaires

Le calendrier 2004, joint avec ce fascicule, peut être modifié en fonction de nécessités de service. Les stagiaires concernés seront individuellement prévenus. Sauf mention contraire communiquée aux stagiaires, les cours se déroulent entre 9h30 et 17h00.

Par le métro : (M)

Lignes 4 12 : Arrêt Montparnasse-Bienvenue (environ 5 minutes)

Lignes 10 13 : Arrêt Duroc (environ 3 minutes)

Par le SNCF - réseau banlieue :

De la gare de montparnasse, prendre l'Avenue du Maine

Il faut 10 minutes pour effectuer le trajet à pied.

Par l'autobus :

28 82 92 Arrêt Maine-Vaugirard

Plan disponible sur le site

www.formation.ssi.gouv.fr

1.7 Détails pratiques

Voir site : www.formation.ssi.gouv.fr

Comment rejoindre le 120, rue du Cherche-Midi

En voiture

La rue du Cherche-Midi est en sens unique. Les possibilités de parking sont rares et payantes (parcmètres).

Le parking le plus proche est celui de la gare Montparnasse.

Conditions d'accès au CFSSI

A l'entrée du bâtiment, il vous sera remis un laissez-passer visiteur en échange d'une pièce d'identité (sont valables uniquement la carte nationale d'identité ou le passeport). Ce laissez-passer, que vous devrez rendre à votre départ, vous autorise à circuler dans les locaux (rez-de chaussée pour la plupart des stages, 2ème étage pour les travaux pratiques).

Le repas de midi n'est pas pris en charge par le CFSSI. Il est pris à l'extérieur du bâtiment dans l'un des nombreux restaurants du quartier.

2 Formations du CFSSI

La numérotation fait référence à la numérotation utilisée dans le calendrier

2 ans

1 à 5 semaines

1 à 5 jours

0 BESSSI : Brevet d'Études Supérieures de la Sécurité des Systèmes d'Information

Objectif : une formation scientifique de 10 mois (du 1er septembre au 30 juin) suivie d'un stage d'application de 6 mois (du 1er septembre au 31 décembre) ou d'un an (du 1er juillet au 30 juin). Ce stage est organisé en co-tutelle avec le ministère de rattachement du stagiaire
Périodicité : 1 promotion / an
Admission : sur dossier
Niveau d'admission : diplôme d'ingénieur ou équivalent (ou bien expérience professionnelle validante)

2a 2b Stage Signaux Compromettants

Durée : 1 semaine (**2a**)
2 semaines (**2b**)
Périodicité : 1 stage /an
Niveau d'admission : ingénieur ou technicien supérieur en électronique
Avec habilitation

3a 3b Stage Sécurité Informatique

Durée : 4 semaines + 1 semaine de «forums industriels»
Périodicité : 2 sessions / an (3a et 3b)
Participants :
3a : décideurs et responsables
3b : informaticiens

10 Stage Cryptologie

Durée : 4 semaines
+ 1 semaine optionnelle
Niveau d'admission : DEUG scientifique ou équivalent

Avec habilitation

1 Sensibilisation à la SSI

Durée : 1 jour
Périodicité : voir calendrier
Niveau d'admission : tous niveaux

4a 4b La méthode EBIOS

Durée : 2 jours (**4a**) ou 4 jours (**4b**)
Périodicité : voir calendrier
Niveau d'admission : tous niveaux

6 AES (Administration Électronique et Sécurité)

Durée : 3 jours
Périodicité : voir calendrier
Niveau d'admission : tous niveaux

5a 5b Internet et la Sécurité

Durée : 2 jours (**5a**) ou 4 jours (**5b**)
Périodicité : voir calendrier
Niveau d'admission :
5a : tous niveaux
5b : administrateur réseaux

7a 7b Travaux pratiques en SSI

Durée : 2 jours (**7a**) ou 5 jours (**7b**)
Périodicité : voir calendrier
Niveau d'admission :
7a : utilisateur avancé ou administrateur
7b : administrateur réseaux
Admission : **7b** sur dossieraprès stage 5b

8 Audits en SSI

Durée : 5 jours
Périodicité : 2 stages / an
Niveau d'admission : responsable ou administrateur sécurité
Admission : sur dossier après stage 5b

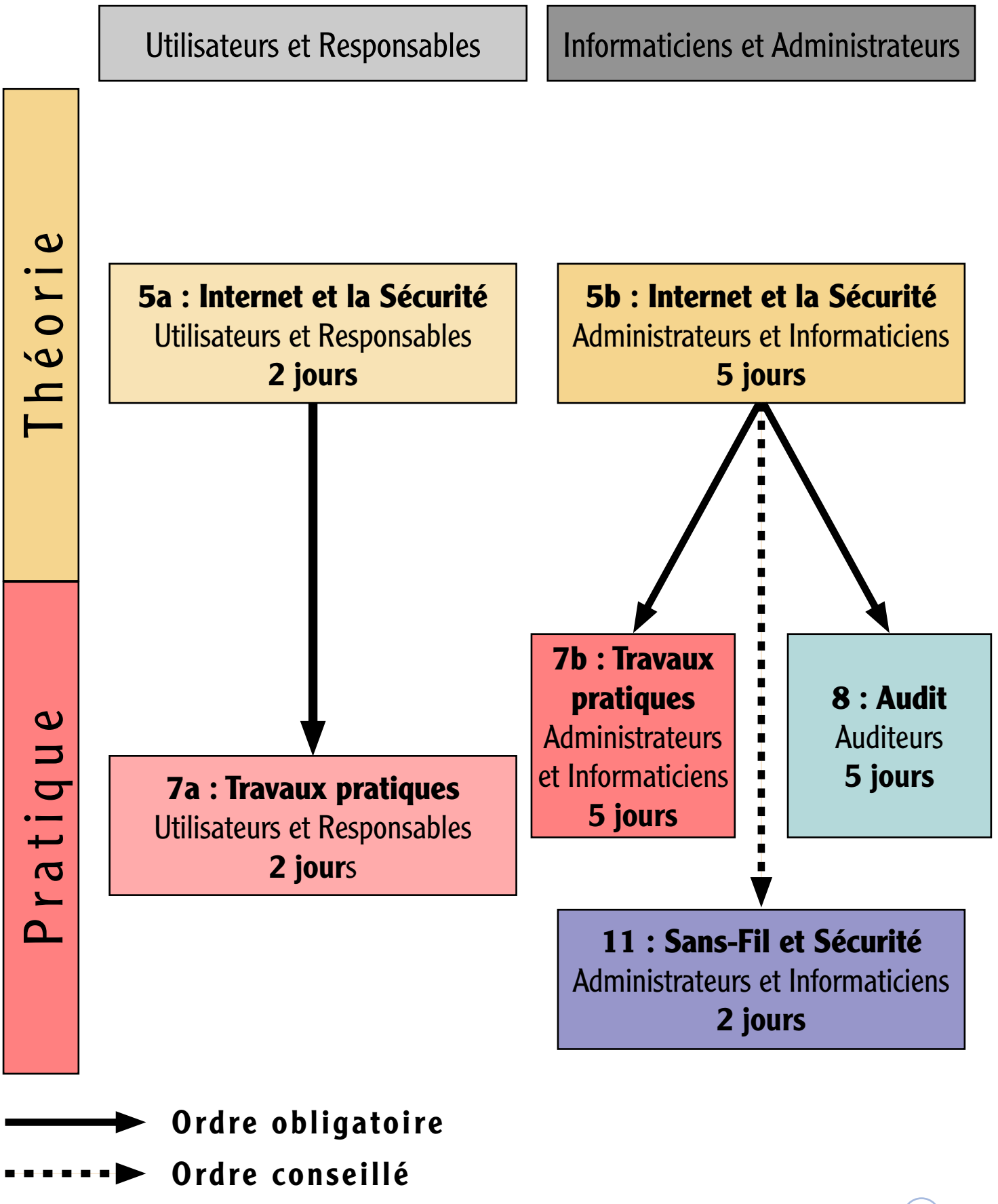
11 Sans-Fil et Sécurité

Durée : 2 jours
Périodicité : voir calendrier
Niveau d'admission :
administrateurs
informaticiens
Admission : sur dossier après stage 5b

9 Formations sur mesure

Le CFSSI peut également organiser des sessions spéciales d'une à plusieurs journées, adaptées aux besoins particuliers des différents ministères ou organismes publics qui en font la demande

Synopsis des stages



1

3 Sensibilisations à la SSI (n° 1)

Des sessions de sensibilisation à la sécurité des systèmes d 'information sont organisées périodiquement selon un calendrier diffusé chaque année au hauts fonctionnaires de défense et aux organismes concernés du ministère de la défense.

3.1 Public visé

Le stage de sensibilisation à la SSI est destiné aux agents de l'État, informaticiens ou non, acteurs des Systèmes d'Information dans le cadre de leurs activités professionnelles.

3.2 Conditions d'admission

Voir 1.5. Nous essayons, dans la mesure du possible, de regrouper par catégorie (informaticiens, responsables et utilisateurs) les stagiaires pour une meilleure efficacité de la formation. C'est pour cela qu'il est demandé aux candidats à cette formation d'émettre plusieurs choix de dates (par ordre de priorité).

3.3 Objectifs du stage

Sensibiliser à la problématique de la SSI en illustrant le domaine par des démonstrations et des conseils pratiques.

3.4 Corps enseignant

L'enseignement est assuré par les ingénieurs et chercheurs de la DCSSI.

3.5 Durée

Une journée.

3.6 Enseignement

- Droit de la SSI
- Cryptographie
- Signaux Compromettants
- Sécurité Informatique
- Conseil en SSI
- Le CERTA

Des démonstrations accompagnent les diverses présentations.

4a : Formation d'utilisateurs de la méthode EBIOS

4a.1 Public visé

Agents d'État ayant des fonctions SSI.

4a.2 Conditions d'admission

Tous niveaux.

4a.3 Objectif du stage

A l'issue de la session, le participant sera capable de mettre en œuvre la méthode EBIOS ou d'en superviser des utilisateurs.

4a.4 Corps enseignant

L'enseignement est assuré par les membres du Bureau conseil de la DCSSI.

4a.5 Durée

2 jours.

4a.6 Enseignement

- Risques et gestion des risques SSI
- Étude du contexte
- Expression des besoins
- Étude des menaces
- Identification des objectifs de sécurité
- Détermination des exigences de sécurité

4b : Formation de formateurs occasionnels à la méthode EBIOS

4b.1 Public visé

Agents d'État ayant des fonctions SSI, amenés à dispenser occasionnellement des formations à la méthode EBIOS.

4b.2 Conditions d'admission

Avoir suivi la formation d'utilisateurs de la méthode EBIOS ou avoir acquis, par la voie de l'expérience, les compétences nécessaires à la mise en place de la méthode EBIOS.

4b.3 Objectif du stage

A l'issue de la session, le participant sera capable de dispenser occasionnellement des formations à la méthode EBIOS.

4b.4 Corps enseignant

L'enseignement est assuré par les membres du Bureau conseil de la DCSSI et par des formateurs spécialistes des problématiques de communication en situation de formation.

4b.5 Durée

5 jours.

4b.6 Enseignement

- Les règles de base de la communication
- La communication et la gestion d'un groupe
- Une situation de communication spécifique : la formation
- L'animation en formation
- Mises en situation d'animation de modules de la « formation d'utilisateurs de la méthode EBIOS » (4a)

5

5 Internet et la Sécurité (n° 5a et 5b)

5.1 Public visé

Le stage de base sur « Internet et la sécurité » (n° 5a) est destiné aux agents de l'État appelés à se servir d'Internet (utilisateurs et responsables) dans le cadre de leurs activités professionnelles.

Le stage avancé sur « Internet et la sécurité » (n° 5b) est destiné à des informaticiens ayant une bonne connaissance des mécanismes de l'Internet et une expérience de terrain sur ce sujet.

5.2 Conditions d'admission

Voir 1.5. Les candidats au stage avancé doivent avoir de bonnes connaissances informatiques sur les protocoles de l'Internet pour y participer utilement.

5.3 Objectifs du stage

L'objectif du stage de base est de faire connaître, à l'aide de démonstrations, les risques associés à la connexion Internet et les moyens de faire face à ces risques et de donner des conseils pratiques pour la mise en œuvre d'une connexion sur l'Internet. Ce stage n'abordera les détails techniques de réalisation que dans les aspects nécessaires à une bonne compréhension des conseils et des outils présentés.

L'objectif du stage avancé est, à partir des connaissances techniques préalables des stagiaires, de faire connaître, à l'aide de démonstrations, les principes de sécurisation de systèmes interconnectés à travers les techniques de l'Internet (autour du protocole central TCP/IP). Il décrit également les techniques et les savoir faire d'utilisation qui minimisent les risques associés à la connexion Internet. Enfin, il présente les moyens permettant de faire face à ces risques et des outils divers permettant de gérer la mise en œuvre sécurisée d'une connexion sur l'Internet.

Pour ces deux stages, l'enseignement s'applique aussi à des déploiement de réseaux internes (Intranet ou Extranet) utilisant les techniques de l'Internet.

5.4 Corps enseignant

L'enseignement est assuré par les ingénieurs et chercheurs de la DCSSI.

5.5 Durée

Deux journées pour le stage de base,

Quatre journées pour le stage avancé.

5.6 Enseignement

MODULE INTERNET ET LA SÉCURITÉ DE BASE (Stage 5a)

Architectures

- Personnelles
- Professionnelles : Internet, Intranet, Extranet
- Serveurs, DMZ, FW, accès distants
- Architecture simple de TCP/IP (notions) : Adresses IP, routage

Présentation d'Internet

- modes de communication
- Outils

Les principes pour la sécurisation des services Internet

- Le service de noms (DNS)
- Le transfert de fichiers (FTP)
- Le service de bavardage (IRC, IM)
- L'accès à distance (telnet)
- Le courrier électronique (SMTP)
  - Danger des pièces jointes
  - Problème de l'identification, manque de confidentialité
  - Messagerie sécurisée : S/MIME, PGP
- Le Web
  - les risque de la navigation
  - le Web sécurisé avec SSL
  - les riques liés aux cookies
  - les risques liés aux codes mobiles
  - les applets java et ActiveX
  - configurer les navigateurs, Internet Explorer

Les outils de sécurisation

- Garde-barrières personnels
- Anti-virus

MODULE INTERNET ET LA SÉCURITÉ AVANCÉ (Stage 5b)

Rappel complet sur le protocole TCP/IP

- Risques liés au protocole

Cryptologie

- Fonctions de hachage
- Chiffrement symétrique, asymétrique
- Algorithme Diffie-Hellman
- Les certificats X509 / IGCs
- Manipulation d'OpenSSL

IPSec

- Mode tunnel, Mode transport
- Les protocoles AH et ESP
- ISAKMP
- Implémentation dans Windows 2000 : les stratégies IPSEC
- Implémentation dans Linux : FreeSWan
- Implémentation dans OpenBSD

Services Internet et risques associés

- Telnet , SSH
- FTP : Mode passif
- DNS : transfert de Zone, Sécurité dans Bind, DNSSec

La messagerie : Les protocoles SMTP, POP

- Problème de l'identification, manque de confidentialité
- Messagerie sécurisée : S/MIME, PGP
- Danger des pièces jointes. Méthodes de sécurisation d'Outlook
- Bien configurer un serveur de messagerie

Le Web

- Présentation complet du protocole et risques liés
- Les cookies
- WebDav
- L'identification
- Le protocole SSL
- Distribuer IE : l'IEAK
- Bien configurer un serveur Web

Architecture

- principes, exemples, conseils

Outils

- supervision
- protection
- détection
- filtrage

Sécurité des systèmes d'exploitation

- Unix/Linux
- Windows

6

6 Administration Électronique et Sécurité (n° 6)

6.1 Public visé

Le stage sur l'Administration Électronique et la Sécurité est destiné aux agents de l'État appelés à utiliser ou mettre en œuvre ces techniques dans le cadre de leurs activités professionnelles.

Selon l'OCDE, l'administration électronique est "l'usage des technologies de l'information et de la communication et en particulier de l'Internet en tant qu'outil visant à mettre en place une administration de meilleure qualité". L'acceptation de ces nouveaux usages passe par la sécurisation des technologies mises en œuvre.

6.2 Conditions d'admission

Voir 1.5. Les candidats à ce stage doivent avoir des connaissances en Sécurité des Systèmes d'Information pour y participer utilement.

6.3 Objectifs du stage

L'objectif de ce stage est de faire connaître, après quelques rappels en cryptographie, les éléments constitutifs d'une sécurisation de l'administration électronique, notamment à travers le déploiement d'une Infrastructures de Gestions de Clés et la méthodologie de construction d'une telle Infrastructure.

6.4 Corps enseignant

L'enseignement est assuré par les ingénieurs et chercheurs de la DCSSI et de l'ADAE (Agence pour le Développement de l'Administration Électronique).

6.5 Durée

Trois jours.

6.6 Enseignement

MODULE IGC

Introduction

- Présentation de la cryptographie à clés publiques
- Modélisation d'une infrastructure
- Référentiel documentaire et état de l'art

Cryptographie

- Cryptographie à clé secrète
- Cryptographie à clé publique
- Courbes elliptiques

Définition des IGC

- Les différentes entités d'une IGC
- Exigences et objectifs de sécurité
- Politiques de certification et déclarations de procédures de certification

Démonstration d'un produit de signature et de chiffrement

Méthodologie de la SSI

- Méthodes et outils
- Expression de besoin

Méthodologie appliquée

- Profils de protection liés aux IGC

Les certificats X509

Démonstration du déploiement d'une IGC

Problèmes ouverts

- Croisement des politiques
- Interopérabilité des systèmes

Conseils

- Analyse des besoins
- Rédaction d'un cahier des charges

Certification

- Confiance dans les clés publiques et les produits sur étagère
- Exigences de sécurité portée sur les prestataires et opérateurs

Signature numérique

- Directive européenne
- Travaux de normalisation européens
- Accréditation

Retour d'expérience

« Outsourcing versus insourcing »

MODULE Administration Electronique

Projets en cours

- Téléservices
- Téléprocédures
- Carte d'identité numérique
- Référentiel documentaire et état de l'art

Référentiel général de sécurité

- Interopérabilité
- Exigences de sécurité
- Protection des données personnelles

Qualification de la sécurité

- Les prestataires de services
- Les produits
- Schéma français d'évaluation et de certification
- Référencement des dispositifs de sécurisation

7 Travaux Pratiques en SSI (n° 7)

7.1 Public visé

Deux types de stages différents seront organisés :

Stage n° 7a. Un premier stage destiné aux agents de l'État appelés à se servir de Windows et d'Internet (utilisateurs et responsables) dans le cadre de leurs activités professionnelles, comme indiqué dans le catalogue de formations 2001. Ce stage est en mesure d'accueillir efficacement une vingtaine de personnes.

Stage n° 7b. Un deuxième stage destiné aux administrateurs systèmes et réseaux qui sera dédié à la configuration complète d'un « Réseau sécurisé » : mise en place d'une zone démilitarisée (DMZ), configuration d'un pare-feu, configuration des services réseaux (DNS, FTP, Web avec SSL, ...), configuration de clients (machines nomades, ...). Ce stage, sous environnement mixte (LINUX et WINDOWS 2000) se déroulera sur une semaine et pourra accueillir huit à dix personnes. Le but de ce stage est de former les administrateurs système aux techniques récentes de sécurité. La connaissance des protocoles de l'Internet (enseignés durant le stage 5b) ainsi que des environnements Unix et Windows est nécessaire au suivi de ce stage. Ce stage est limité à 16 personnes travaillant en doublon.

Ces stages se déroulent sur des machines mises à disposition par la DCSSI.

7.2 Conditions d'admission

Voir 1.5. Les candidats au stage n° 7a doivent avoir de bonnes connaissances informatiques pour y participer utilement et avoir suivit .

Les participants doivent avoir suivi le stage 5a pour participer au 7a.

Voir 1.5. Le stage n° 7b est réservé aux administrateurs réseau ayant une expérience de déploiement d'une architecture de type Intranet, Extranet ou Internet. Un questionnaire d'évaluation est fourni aux candidats.

Les participants doivent avoir suivi le stage 5b pour participer au 7b.

7.3 Objectifs du stage

L'objectif de ces nouveaux stages est de présenter à nos stagiaires les techniques de sécurisation des postes de travail à travers l'exploration des fonctions indispensables à un travail partagé, de les sensibiliser aux menaces principales, de leur donner un certain nombre de réflexes notamment dans la configuration des postes.

Par contre, il ne s'agit ni de les former à tel ou tel outil ou produit informatique particulier (cette formation est ou devrait être assurée par les fournisseurs de ces produits), ni de recommander tel ou tel outil particulier. Les produits choisis pour illustrer les concepts de la sécurité seront choisis, dans la mesure du possible, soit dans les produits les plus répandus (par exemple : produits natifs Microsoft ou produits du pack Office, Internet Explorer, etc.), soit dans le domaine du logiciel libre ou gratuit.

7.4 Corps enseignant

L'enseignement est assuré par les ingénieurs et chercheurs de la DCSSI.

7.5 Durée

Deux journées pour le stage n° 7a.

Une semaine pour le stage n° 7b.

7.6 Enseignement

Stage n° 7a

Cours sur les clients de messagerie électronique

- Comprendre le fonctionnement global d'un système complet de messagerie électronique (structure du système, format des messages, protocoles …)
- Savoir bien utiliser son client de messagerie électronique (Outlook, Outlook Express, Netscape Messenger)
- Savoir installer et utiliser les outils nécessaires pour sécuriser son client de messagerie (PGP, S/MIME, …)
- Introduction à l'utilisation des certificats, quelques concepts sur les IGCs

Cours sur la navigation Web

- Les risques d'une connexion avec un navigateur
- Le rôle de la configuration d'un navigateur
- Vos traces
- Les certificats
- Où trouver les menus de configuration de sécurité
- Cookies, ActiveX, Java, Script
- Téléchargement
- Les Patchs

Administration sécurité d'un poste de travail sous Windows 2000

- Présentation des mécanismes de sécurité et des outils associés
- Comprendre les structures de fichiers, les bases de registres
- Les traces laissées sur les machine
- Démonstration d'outils d'analyse
- Administration sécurité des machines

Stage n° 7b

Jour 1

Présentation des architectures réseau sécurisée

Installation de linux sur le firewall

Configuration de linux : compilation du Kernel 2.4, modules, fichiers de configuration principaux de Linux

7

Jour 2

Cours sur iptables et création de scripts sur le firewall

Cours sur xinetd et configurations : exemple avec ftpd

Compilation et configuration de bind avec techniques de sécurisation (chroot, ...)

Configuration de apache

Jour 3

Compilation, installation et configuration de postfix

Installation d'un serveur POP

Installation de Linux (RedHat) et de Windows 2000 Server avec MultiBoot

Configuration de Windows 2000, sécurisation et configuration du réseau

Jour 4

Installation de Freeswan sur un noyau Linux

Cours IPSec et configuration de freeswan

Mise en places de VPN entre les plates formes des étudiants

Configuration d'un proxy (Squid)

Jour 5

Installation de VPN avec postes nomades

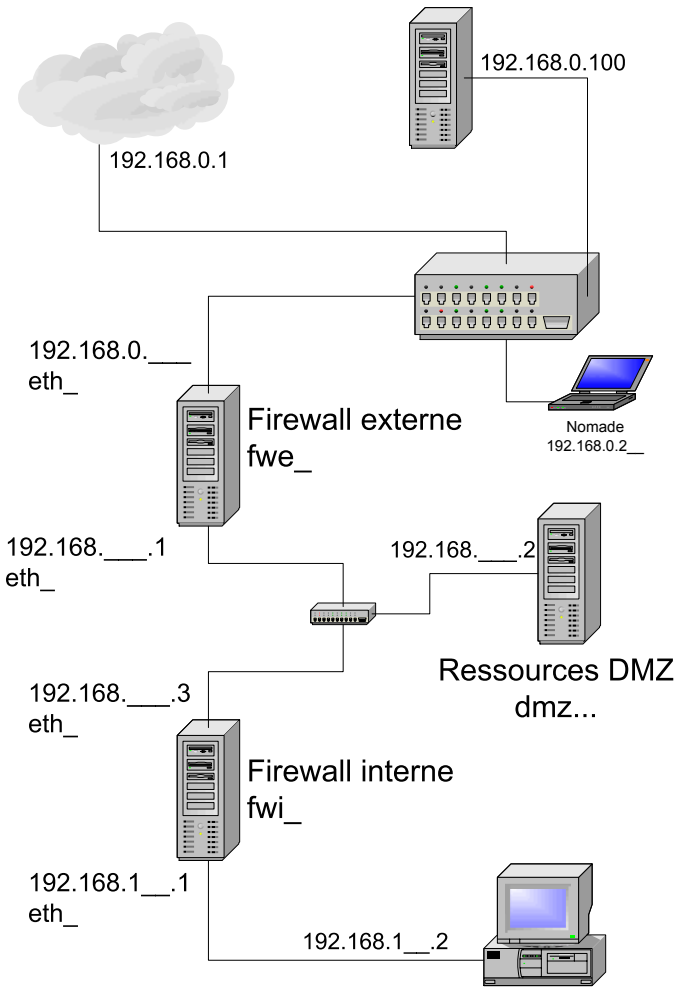
Installation de VPN avec interconnexion de passerelles sous Linux et Windows 2000

Présentation des IGC (certificats) et manipulation d'Openssl

Configuration d'un Web sécurisé via SSL (Apache , IIS)

Mise en place d'une messagerie sécurisée via S/MIME

Génération de certificats et implémentation dans la messagerie et dans Apache (SSL)



Exemple d'architecture réalisée

8 Audits en SSI (n° 8)

8.1 Public visé

Le stage de formation aux « Audits en SSI » est destiné aux agents de l'État appelés à réaliser ou superviser des audits de la sécurité des systèmes d'information dans le cadre de leurs activités professionnelles.

8.2 Conditions d'admission

Voir 1.5. Le stage sera réservé aux administrateurs réseau ayant une réelle expérience du déploiement d'une architecture de type Intranet, Extranet ou Internet. La connaissance et la capacité à administrer des systèmes d'exploitation Windows NT, 2000 et Linux est fortement souhaitable.

8.3 Objectifs du stage

L'objectif de ce stage est d'initier des agents de l'état aux techniques d'audit technique de la sécurité d'un système d'information (expertises sécurité). Cela permettra notamment de soutenir la mission d'audit des systèmes informatiques gouvernementaux de la DCSSI et de la démultiplier sur le terrain par les actions nécessaires de suivi des bonnes pratiques de sécurité indispensables au fonctionnement d'une administration électronique. Ce stage s'adressera à des correspondants sécurité, responsables sécurité, mais d'abord aux techniciens des chaînes fonctionnelles de sécurité (rattachés aux FSSI).

Les compétences méthodologiques et pratiques obtenues en fin de stage doivent permettre de superviser la réalisation d'un audit technique, voire de mener de façon autonome un audit technique élémentaire.

8.4 Corps enseignant

L'enseignement est assuré par les ingénieurs et chercheurs de la DCSSI, et en particulier du bureau audits en SSI.

8.5 Durée

Une semaine.

8.6 Enseignement

- Méthodologie générale des audits en SSI: approche organisationnelle, analyse de la sécurité physique et logique d'un système d'information.
- Techniques et procédures particulières: découverte d'un réseau, analyse de sécurisation de systèmes d'exploitation Windows NT, 2000 et Linux (Debian), d'applications (messagerie, serveur internet...) et d'un autocommutateur téléphonique. La bonne utilisation d'outils spécifiques sera également détaillée: scanner de vulnérabilités, outils de vérification de la force de mots de passe...

9

9 Formation sur mesure (n° 9)

9.1 Public visé

Le CFSSI peut également organiser des sessions spéciales d'une à plusieurs journées, adaptées aux besoins particuliers des différents ministères ou organismes publics qui en font la demande

9.2 Conditions d'admission

Voir 1.5.

9.3 Objectifs du stage

L'objectif des stages sur mesure est défini entre l'organisateur (DCSSI/CFSSI) et le demandeur.

9.4 Corps enseignant

L'enseignement est assuré par les ingénieurs et chercheurs de la DCSSI et/ou de l'organisme demandeur.

9.5 Durée

Selon la nature de la formation et la disponibilité des locaux.

9.6 Enseignement

Théorique ou pratique.

10 Sans-Fil et Sécurité (n° 11)

10.1 Public visé

Le stage de formation au « Sans-Fil et la Sécurité » est destiné aux agents de l'État appelés à réaliser ou superviser la mise en place de technologies sans-fil au sein de leurs systèmes d'information dans le cadre de leurs activités professionnelles.

10.2 Conditions d'admission

Voir 1.5. Le stage sera réservé aux administrateurs réseau et informaticiens ayant une réelle expérience du déploiement de réseaux. La connaissance du fonctionnement des réseaux de type Wifi est un préalable souhaitable.

10.3 Objectifs du stage

L'objectif de ce stage est de présenter les normes utilisées, les risques liés à l'usage des technologies sans-fil et de proposer des axes de sécurisation. Le stage sera agrémenté de démonstrations pratiques.

10.4 Corps enseignant

L'enseignement est assuré par les ingénieurs et chercheurs de la DCSSI.

10.5 Durée

Deux jours.

10.6 Enseignement

Wi-FI (IEEE 802.11)

- les diverses normes
- les évolutions
- vulnérabilités et parades
- architectures de réseaux

Sécurisation d'un réseau Wi-Fi

- organisation, déploiement, configurations
- les serveurs d'authentification : Radius
- les protocoles de sécurité : EAP, TLS, IPsec
- politique de sécurité

3

11 Sécurité informatique (n° 3a et 3b)

11.1 Public visé

Deux sessions de formation à la sécurité informatique sont organisés en 2002.

La première session du stage (n° 3a) est destinée aux cadres administratifs, agents et responsables de sécurité des systèmes d'information et ingénieurs qui veulent acquérir de solides connaissances dans le domaine de la sécurité informatique

Le deuxième session du stage (n° 3b) au contenu plus technique est destinée plus particulièrement à des stagiaires ayant une compétence professionnelle dans la mise en œuvre de systèmes informatiques opérationnels (administration, déploiement, expertise, etc.).

L'ensemble des stagiaires participera à une semaine commune (n° 3) consacrée à des « forums industriels ».

11.2 Conditions d'admission

Les candidatures sont transmises à la DCSSI par les Hauts fonctionnaires de défense ou les fonctionnaires de sécurité des systèmes d'information, et les admissions en stage sont prononcées par le directeur de la DCSSI.

11.3 Objectifs du stage

- Permettre aux stagiaires de compléter leurs connaissances en matière de sécurité informatique.
- Faire connaître les concepts, les méthodes et les techniques modernes de traitement de la sécurité.
- Faire le point de la recherche dans le domaine.
- Donner les moyens de se perfectionner ultérieurement et de se tenir informé des évolutions.
- Permettre aux stagiaires de devenir des formateurs en sécurité informatique.
- Faire connaître l'aide que le service est en mesure d'apporter dans le domaine du conseil et des formations complémentaires.

11.4 Corps enseignant

Le corps enseignant est constitué d'intervenants sélectionnés pour leur expérience et leurs compétences dans le domaine.

Ce sont :

- des professeurs de l'enseignement supérieur,
- des ingénieurs et des chercheurs de l'administration ou de l'industrie,
- des ingénieurs et personnels de la DCSSI.

11.5 Durée

Pour chaque stage : quatre semaines de cours étalées sur deux mois et une semaine de présentations d'offres industrielles.

11.6 Enseignement

Stage n° 3a :

- MODULE SI-0 : Module préparatoire
- MODULE SI-1 : Généralités - Méthodologie
- MODULE SI-2 : Aspects juridiques et internationaux de la SSI
- MODULE SI-3 : Méthodologies
- MODULE SI-6 : Témoignages et Critères d'Évaluation

Stage n° 3b :

- MODULE SI-1 : Généralités - Méthodologie
- MODULE SI-2 : Aspects juridiques et internationaux de la SSI
- MODULE SI-4 : Techniques de sécurisation et Forum
- MODULE SI-5 : Systèmes Particuliers
- MODULE SI-6 : Témoignages et Critères d'Évaluation

Les mêmes thématiques pourront être abordées de manière différente dans l'un ou l'autre des stages en prenant en compte les connaissances préalables des stagiaires. Les deux sessions couvriront l'ensemble de la problématique de la « sécurité informatique ».

MODULE SI-0 : MODULE PRÉPARATOIRE

Terminologie et définitions

Glossaire des principaux termes utilisés dans les domaines suivants : critères d'évaluation, cryptologie, cartes à puce, réseaux informatiques et Internet, informatique en général.

Réseaux

Connaissances de base sur le fonctionnement des réseaux d'ordinateurs (l'Internet est traité plus particulièrement dans les protocoles Internet) :

- Introduction (concepts, modèles de référence, les tendances)
- Couche physique
- Couche liaison de données (trames, détection et contrôle d'erreurs)
- Contrôle d'accès au canal (réseaux locaux)
- Couche réseau (réseaux, contrôle de flux, interconnexion)
- Couche transport
- Le réseau téléphonique, le RNIS
- Le réseau ATM
- Le multimédia

Présentation de Windows 2000

L'objectif de cet exposé et de présenter le système d'exploitation Windows 2000 destiné à remplacer Windows NT 4 et de décrire les nouvelles fonctionnalités de sécurité incluses dans Windows 2000.

Il comportera la présentation des différentes versions de ce système d'exploitation (professionnel, …), puis les nouveaux services et fonctionnalités de ces versions et finalement les nouveaux mécanismes de sécurité (Kerberos, IPSEC, …) inclus dans Windows 2000.

Des démonstrations seront effectuées pour illustrer les différentes fonctionnalités mises en œuvre.

Présentation d'UNIX

Connaissances de base sur les systèmes UNIX et leur utilisation :

- UNIX : généralité et architecture
- SHELL et commandes de base
- Processus
- Systèmes de fichiers et droits d'accès
- Services réseaux (NFS, NIS)

Protocoles de base sur Internet

Les protocoles de base sont présentés en détail : IP, ICMP,TCP/UDP, DNS, HTTP, FTP, SMTP,TELNET, …

MODULE SI-1 : GÉNÉRALITÉS - MÉTHODOLOGIE

Il s'agit de faire appréhender l'environnement dans lequel s'exerce aujourd'hui la sécurité informatique et de présenter les techniques sur lesquelles repose la sécurité des systèmes d'information.

Les concepts généraux de la sécurité informatique

- La société de l'information
- Le contexte actuel de la SSI
- Les tendances
- La réalité de la menace stratégique
- Les bases de la sécurité informatique

Fraudes et piratages informatiques

Il s'agit de présenter des exemples concrets et récents de fraudes et de piratages informatiques qui se sont produits en France

Menaces, vulnérabilité, parades

Après une revue de presse de différents incidents survenus sur des systèmes d'information, il s'agit de présenter chacune des menaces pesant sur ces systèmes, en soulignant les vulnérabilités exploitées et les parades possibles.

Les mesures opérationnelles : sécurité non technique

Les sécurités techniques ne permettent pas seules d'assurer la SSI, il faut que les locaux bénéficient d'une protection physique satisfaisante. Pour la protection des informations classifiées de défense, les normes de protection physique sont définies en fonction du niveau de classification ; pour la protection des informations sensibles, les normes ne sont pas définies mais il y a une obligation de résultats. La protection physique repose sur le contrôle des accès, sur des barrières, la détection des intrusions et des moyens d'intervention. Elle est à compléter par une protection et une sensibilisation des personnes qui requièrent une organisation adéquate.

La méthodologie de la DCSSI : EBIOS

La méthode EBIOS est une démarche de sécurisation de système d'information développée par la DCSSI et utilisée dans de nombreux organismes.

Elle permet l'expression des besoins de sécurité et l'identification des objectifs de sécurité. Elle participe à l'élaboration de la FEROS. Le but du module est de faire comprendre aux stagiaires les objectifs et principes de cette méthode, et de leur montrer les résultats.

L'articulation du module est la suivante :

- Présentation des concepts ;
- Présentation de la méthode ;
- Mise en œuvre d'un cas concret (étude par groupe avec restitution).

Politique de sécurité et schéma directeur

Il s'agit de donner un exemple pratique des facteurs à prendre en compte pour définir une politique de sécurité adaptée aux conditions particulières d'un organisme comme le CNRS dans le cadre d'un schéma directeur. A cette occasion, les multiples responsabilités et modes d'action d'un RSSI seront abordés.

La sécurité des systèmes d'information se pose au CNRS de façon contradictoire :

- D'une part le dynamisme de la recherche dépend de la capacité à communiquer ce qui rend nécessaire une plus grande ouverture des systèmes et des réseaux, dans un contexte où les individus sont de plus en plus rétifs aux règles, aux procédures et aux contraintes.
- D'autre part l'importance du nombre des attaques que nous subissons, leurs conséquences tant du point de vue économique que de celui de la préservation de notre patrimoine scientifique, la nécessité de protéger nos «circuits de décision», nous commandent d'assumer nos responsabilités.

Nous avons répondu à ce besoin contradictoire en mettant en place des structures originales, à la fois centralisées (fonctionnelles et opérationnelles) et décentralisées.

Le rôle de ces structures est d'abord de sensibiliser et de former les acteurs de nos systèmes d'information. Il est aussi de répondre, ponctuellement, à des appels «à l'aide». Il est enfin de mener une réflexion stratégique sur les problèmes auxquels nous sommes confrontés. La sécurité, comme dans tout système complexe, ne peut être appréhendée sans une méthode. Pour avoir méconnu cette évidence nous nous sommes parfois égarés dans des approches «techniques» (sécurité = firewall), au coup par coup (sans vision globale), victime d'effet de mode ou d'à priori. Il nous faut encourager une approche méthodologique, mais laquelle • Toutes les méthodes ne sont pas équivalentes car chacune induit implicitement un type d'organisation. Notre réflexion a permis de déboucher sur une approche plus concrète et mieux adaptée à nos structures décentralisées que les méthodes classiques.

La cryptologie et la sécurité informatique

- Présentation des principaux algorithmes de la cryptologie moderne (algorithmes de hachage, algorithmes à clés secrètes et algorithmes à clés publiques).
- Les différentes fonctions de sécurité de la cryptographie : l'intégrité et l'authentification, l'échange de clés et la confidentialité.

La cryptographie est le plus souvent l'unique moyen de sécuriser des informations sensibles conservées ou échangées à l'aide des systèmes d'information modernes. Nous verrons comment les outils de la cryptographie sécurisent le contrôle d'accès, comment les algorithmes à clés publiques offrent la possibilité de signer des documents numériques et comment l'utilisation de l'ensemble de ces outils protège la confidentialité. Naturellement ces nouvelles solutions posent de nouveaux problèmes, notamment la problématique des infrastructures de gestion des clés publiques.

- Législation française sur l'emploi de la cryptologie.
- Règles à respecter sur l'implantation de la cryptologie dans les systèmes d'information.

Les signaux parasites compromettants

- Présentation théorique
  - Définition
  - Modes de propagation
  - Rayonnement
  - Conduction

La protection contre les signaux parasites compromettants

- Généralités
- Les matériels ou systèmes agréés
- Le zonage TEMPEST
- Les enceintes faradisées
- Les règles d'installation
- Protection des matériels
- Contrôles des matériels
- Mesures sur site

Réglementation interministérielle

Présentation pratique

- Démonstration de capture d'une console vidéo par rayonnement, par conduction
- Démonstration de capture d'un clavier sans fil

Conclusion

MODULE SI-2 : LES ASPECTS JURIDIQUES ET INTERNATIONAUX DE LA SSI

La sécurité et le droit européen

- Le champ de compétences de la communauté européenne en matière de SSI.
- Fondement des compétences : marché unique, libre circulation des biens, des capitaux et des personnes.
- Exclusion du champ des compétences : exemple le droit pénal.
- Exclusion des compétences : exemple la cryptographie.
- Les organes de l'Union européenne
  - Le Conseil européen
  - Le Conseil
  - Le Parlement européen
  - La Commission
  - La Cour de justice des communautés européennes
  - La Cour de comptes
  - Le Conseil économique et social
  - Le Conseil des régions
- Les normes communautaires
  - Typologie : règlement, directives, décisions
  - Élaboration des normes
  - Supériorité de la norme européenne sur la norme nationale
  - Mise en application par les États
- Les relations avec l'administration française
  - L'approche interministérielle : le SGCI
  - L'application du droit européen par les ministères
  - Le travail de proposition
  - La consultation de la Commission européenne
- Les perspectives d'avenir
  - La société de l'information et le développement des moyens de communication
  - Les élargissements
  - L'UEM
  - L'Europe et les États-Unis
  - Les lois françaises en matière de SSI

Le droit français et la SSI

- Introduction : une conception étatique de la SSI
  - La problématique de la SSI : une nouvelle donne, les diverses formes de la menace
  - La réaction sociale : la connaissance des attaques contre la SSI, la prévention, la répression
- Notions utiles de droit
  - Introduction : le droit et les droits, les spécificités de la règle de droit, problématique du droit de la SSI
  - Le droit positif : les sources principales du droit, les sources secondaires du droit
  - Les principes généraux du droit : le contrôle de conformité, la force obligatoire de la règle de droit, le double degré de juridiction, l'efficacité de la règle de droit
  - L'organisation judiciaire : les juridictions judiciaires, les juridictions administratives, les mécanismes du procès judiciaire, les acteurs du droit
- Introduction au droit pénal
  - Qu'est-ce que le droit pénal •
  - L'entrée en vigueur du nouveau code pénal (NCP) : historique, les apports du NCP, présentation de la partie législative
  - Les principes spécifiques du droit pénal : la classification des infractions, les éléments constitutifs de l'infraction, l'application de la loi pénale dans l'espace, l'application de la loi pénale dans le temps
  - La procédure pénale : l'organisation judiciaire pénale, les phases de l'action pénale
- Aperçu des textes juridiques en matière de SSI
  - Le vocabulaire
  - La police de l'information
  - Les propriétés de l'information
  - Le domaine contractuel : textes juridiques concernant ce domaine
- Le piratage informatique
  - Les textes internationaux
  - Le dispositif pénal français : la loi «Godfrain» art. 323-1 à 7 du NCP
  - Les services spécialisés
  - Évolution du traitement judiciaire depuis 1994
  - Conclusions pratiques
- La protection juridique des secrets
  - Le secret professionnel
  - Le secret de défense
  - Les secrets économiques et industriels
  - Les secrets de la vie privée
  - Conclusions
- Le problème de la contrefaçon
  - problématique originale du logiciel, un vaste arsenal juridique international, les textes nationaux et leurs sanctions
  - la protection juridique des fichiers, la protection juridique des banques et bases de données : la directive 96/9
  - conclusions à tirer au plan pratique
- Les contrôles technologiques
  - Le contrôle de la cryptologie : l'arsenal juridique, les régimes institués (autorisation et TPC), le contrôle

- Le contrôle de destination finale : le dispositif européen, les dispositions nationales en cryptologie
- Normalisation
- L'évaluation et la certification

- Conclusion générale

Les difficultés liées à la preuve : une déstabilisation évidente.

La recherche de standards internationaux d'action : OCDE et surtout le G8, nouveau forum d'impulsion dans les NTIC (nouvelles technologies de l'information et de la communication).

Les problèmes juridiques soulevés par Internet et les réseaux numériques

- Résumé des propositions du Conseil d'État
  - Protéger les données personnelles et la vie privée
    - un besoin nouveau de protection
    - les exemples étrangers : autorégulation et liberté de circulation de l'information
    - une nécessaire combinaison du droit et des mesures autorégulation
  - Favoriser les échanges par une confiance accrue des acteurs
    - transactions électroniques et protection du consommateur : la sécurité juridique des transactions électroniques ; la mise en place d'un cadre juridique international adapté
    - la reconnaissance de la valeur juridique du document et de la signature électroniques : les problèmes posés par le droit civil traditionnel ; la valeur probatoire du message électronique et les offres de services de certification
    - les enjeux de la cryptologie sur Internet
    - l'adaptation de la fiscalité au commerce électronique : les problèmes posés par la dématérialisation des transactions
    - noms de domaine et droit des marques : des modalités d'attribution peu satisfaisantes ; état des propositions pour une amélioration
  - Valoriser les contenus par la protection de la propriété intellectuelle
    - l'adaptation du régime aux enjeux d'Internet et des nouveaux réseaux ; la lutte contre la contrefaçon
  - Lutter contre les contenus et comportements illicites
    - préciser la loi applicable et la compétence du juge français ; clarifier la responsabilité des acteurs ; faciliter l'action de la police et de la justice ; renforcer l'autorégulation des acteurs •
  - Adapter la réglementation de la communication à la convergence de l'informatique, de l'audiovisuel et des télécommunications
    - la distinction entre communication publique et correspondance privée reste d'actualité plus que jamais ; des adaptations rendues nécessaires par la convergence technologique et le développement de services en ligne

Éléments sur les principaux problèmes posés aujourd'hui par Internet

- Internet et les auteurs : Les conditions de la protection d'une œuvre créée ou diffusée en ligne. Les conditions d'exploitation d'une telle œuvre. La titularité des droits en cas de pluralité d'auteurs.
- L'internet et la fraude. Les infractions spécifiques du Code pénal. La procédure pénale appliquée à Internet. Le travail du G8.
- Internet et les données personnelles. La loi du 6 janvier 1978 à l'épreuve du réseau mondial. La transposition en droit français de la directive 95/46. Le dispositif international : OCDE, OMC et autorégulation.
- L'internet et les libertés. La liberté d'expression. La protection des libertés individuelles : diffamation et injure ; haine raciale, négationnisme et révisionnisme ; la protection des mineurs ; le terrorisme ; l'espionnage privé ; les jeux clandestins ; les sondages d'opinion ; l'emploi de la langue française.
- Internet et la responsabilité des fournisseurs. La voie judiciaire. La voie de la régulation. La voie de l'autorégulation.
- Internet et les consommateurs. Le commerce électronique : la directive 97/66. La charte de l'internet. Le consommateur et le FAI (fournisseur d'accès à l'internet). La TVA et Internet.
- Internet et la sécurité. La preuve sur Internet : recevabilité et force probatoire de la preuve électronique. Le régime légal de la cryptologie : de la conception sécuritaire de 1990 à la libéralisation totale de l'an 2000.
- L'internet et les noms de domaine. Le système actuel de nommage et son contentieux. La réforme des noms de domaine. Les propositions du CE.
- L'internet et la publicité. Les critères de la publicité sur Internet ; la réglementation applicable ; le cas spécifique de certains produits ; la réglementation applicable au support ; rôles et responsabilités.

Organisation de la sécurité informatique en international, la normalisation

- Les instances internationales concernées par la sécurité des systèmes d'information, leur influence sur la SSI en France
  - UE (SOGIS - G5)
  - OCDE
  - OTAN, UEO
  - Les relations bilatérales en la matière
  - Programmes d'armement internationaux
- La normalisation : définitions, enjeux, exemples, le processus international de normalisation ISO, IETF, etc…

La protection des libertés individuelles – La CNIL

- Présentation générale de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : historique (SAFARI), rappel de l'article 1er de la loi.
- Champ d'application : la notion de donnée nominative, la notion de traitement automatisé, l'application de certaines dispositions de la loi aux fichiers manuels.
- Les six principes clés de la protection des données (nb : illustrations par des cas concrets) : le principe de finalité, le principe de pertinence des données, le droit à l'oubli ou le principe d'une durée de conservation limitée des informations, l'obligation de ne communiquer les données qu'aux destinataires et tiers autorisés à en connaître, l'obligation de sécurité, le respect des droits des personnes : droit à l'information, droit d'accès, de rectification, droit d'opposition …
- La CNIL : statut, composition et fonctionnement, missions de la CNIL (contrôle à priori : les formalités préalables, explications pratiques, le contrôle à posteriori : plaintes, réclamations, autosaisines, vérifications sur place …), conseil et information (ex : site WEB de la CNIL).

- Conclusion : La transposition de la directive européenne du 24.10.1995, le rapport Braibant, les propositions de la CNIL.

MODULE SI-3 : MÉTHODOLOGIES

Principes et modèles de la sécurité informatique

L'objectif de ce cours est de mieux faire percevoir l'enjeu d'une représentation abstraite et éventuellement formelle (appelée modèle) de la sécurité d'un systèmes informatique. La construction d'un tel modèle oblige tout concepteur à se doter d'une bonne définition de la sécurité ainsi que des contrôles chargés de la mettre en œuvre.

Le cours, dans une première partie, est centré sur la problématique de la sécurité logique dans les systèmes informatiques. Sont ainsi examinés : définitions, problèmes, types de contrôles et adéquations de ces contrôles aux menaces.

La deuxième partie du cours cherche à montrer comment ces divers éléments de problématique sont capturés par différentes définitions de la sécurité informatique, introduites par différents modèles de sécurité dont certains s'attachent à décrire la gestion des droits d'accès dans un système, et d'autres le contrôle des accès ou des flux d'informations.

Audit de sécurité d'un site

En premier point, sont rappelés des principes de base orientés vers une gestion de risques :

- cycle de vie de l'information,
- gestion de la sécurité dans le temps et l'espace,
- approche globale (par entreprise ou organisme) de la sécurité de l'information.

Puis sont présentés comparativement les méthodes classiques d'analyses de vulnérabilité réglementaire des systèmes d'information : MARION, MELISA, MASSIA.

Enfin, une méthode de gestion des risques, basée sur la maîtrise des écarts sur objectif, est détaillée.

Des cas concrets illustrent les points exposés, avec un suivi constant de pragmatisme pour expliciter la conduite d'un audit de sécurité.

La journée se termine par une animation sur des exemples de moyens, de ressources et d'organisations dans le domaine de la guerre de l'information.

Les plans de secours

Trois grandes études complémentaires permettent d'obtenir des procédures complètes à l'épreuve de tout sinistre :

- l'étude de «secourabilité»,
- le plan de secours informatique
- le plan de secours utilisateurs.

L'étude de «secourabilité» est une analyse de l'existant qui détermine si un site informatique est «secourable», c'est-à-dire si le département informatique s'est doté des mesures et des moyens nécessaires pour assurer son redémarrage suite à un incident.

A la suite de cette étude de «secourabilité», les différentes procédures – techniques, logistiques et humaines – à activer lors des transitions entre les divers états que peut prendre un centre informatique, sont développées afin d'établir le plan de secours informatique adéquat. Il a pour principale mission d'éviter les erreurs et les omissions et de faire gagner un temps considérable.

En complément du plan de secours informatique, un plan de secours utilisateurs permet d'étendre les procédures à suivre en cas de sinistre aux utilisateurs, afin qu'ils puissent faire face efficacement à tout incident informatique.

Le génie logiciel

Nous présenterons les méthodes et outils utilisés pour industrialiser la production de logiciel, selon le plan suivant :

- Introduction et généralités
  - Les cycles de développement.
  - Les différentes notions de tests.
  - Les outils de suivi de la production.
- Tests et vérification
  - Le test de code.
  - La génération (semi-)automatique de tests.
  - La vérification (ou preuve) de code.
- Méthodes formelles
  - Différentes approches.
  - La notion de raffinement.
  - Une courte introduction à la méthode B.

Méthodes et moyens de la sûreté de fonctionnement

- Notions de sûreté de fonctionnement
  - Concepts de base et terminologie
  - Classification des fautes, des erreurs et des défaillances
  - Mesures de la sûreté de fonctionnement
  - Prévention des fautes accidentelles
- Techniques de tolérance aux fautes accidentelles
  - Traitement d'erreur et traitement de faute
  - Détection d'erreur
  - Recouvrement par reprise
  - Recouvrement par poursuite
  - Recouvrement par compensation
- Techniques de tolérance aux fautes intentionnelles
  - Tolérance aux fautes de conception intentionnelles
  - Tolérance aux intrusions

MODULE SI-4 : TECHNIQUES DE SÉCURISATION

La protection des systèmes répartis

- Introduction
  - Sécurité des réseaux et sécurité des systèmes répartis
- Applications réparties typiques
  - Annuaires, répertoires, certification
  - Courrier électronique
  - Notion de tiers de confiance
- Authentification
  - Définition
  - Authentification à chiffre symétrique (ex : Kerberos)
  - Serveur d'authentification à clé publique
  - Authentification sans apport de connaissance
- Autorisation
  - Définition, principe du moindre privilège,TCB
  - Architectures classiques : TCB centralisée, approche TNI, approche Kerberos-Sesame
- Commerce électronique
  - Protocoles existants (SSL, S_HTTP, ...)

- Ipv6
- SET et variantes
- Porte-monnaie électronique

Protection des stations de travail

Ce cours aborde la problématique des stations de travail, placées au regard de l'exigence de sécurité informatique. Principalement orienté sur l'architecture des systèmes, à travers des exemples, le cours s'intéresse dans une première partie aux stations centralisées. Il présente un premier choix d'architectures de systèmes opératoires fondé sur l'extension et la restructuration de systèmes préexistants. Il présente également d'autres choix d'architecture faisant coopérer le matériel à la mise en œuvre de la sécurité.

L'interconnexion des stations autour d'un réseau de communication est étudiée dans une seconde partie. Divers choix d'architectures de systèmes, reposant sur différents types de contrôles, sont examinés. Le cours aborde à travers un exemple, l'implication de la sécurité dans l'architecture de nouvelles générations de systèmes opératoires répartis. Il situe également l'ensemble de ces techniques, reposant sur l'architecture interne des systèmes, par rapport à des approches reposant sur l'utilisation de dispositifs externes ou applicatifs, en particulier les firewalls et les machines virtuelles Java.

Protection des bases de données

Il s'agit de traiter le problème de la sécurité des informations gérées par un système de gestion de base de données (SGBD), d'examiner les aspects de la protection hors chiffrement, de voir le modèle relationnel.

Puis les solutions actuelles seront présentées : logiciel de SGBD supposé sûr, système d'exploitation sécurisé.

En conclusion, seront évoquées les orientation futures.

Architecture des réseaux sécurisés

- Les risques et menaces
- Services et mécanismes de sécurité
- Quelques exemples applicatifs (X400, EDIFACT, ETEBAC5, ECMA)

Forum sur les firewalls (gardes), la sécurité des bases de données, les audits et tests d'intrusion, la sécurité des systèmes d'exploitation

Sur ces différents thèmes, des fournisseurs d'équipements ou de service viendront présenter, sous forme de tables rondes, les prestations qu'ils sont susceptibles de fournir aux administrations pour sécuriser leurs systèmes d'information.

Sécurité des technologies sans-fil

MODULE SI-5 : SYSTÈMES PARTICULIERS

Sécurité des systèmes Windows NT

Cet exposé a pour principal objectif d'étudier les services de sécurité proposés sous Windows NT et ses compléments (Word, …). La présentation de certains mécanismes employés et celle des principaux éléments de l'architecture du système permettront à l'auditeur de mieux apprécier le niveau de sécurité offert par Windows NT. De manière complémentaire, une démonstration sera proposée. Elle servira à alimenter une réflexion sur les évolutions qu'il est possible d'envisager pour renforcer le niveau de protection de ce système.

Les virus informatiques

S'il est un sujet fréquemment défrayé par la chronique, c'est bien celui-ci. Pourtant, si le thème s'avère récurrent, rares sont les publications qui le traitent sérieusement. Aussi, dans l'intention de contribuer à démythifier et à démystifier le phénomène, une étude technique sera-t-elle proposée. A partir de la présentation de mécanismes systèmes, plusieurs types de virus seront analysés.

Les différentes méthodes de prévention et de protection seront présentées ; elles ne se limiteront pas à l'utilisation d'antivirus mais elles donneront un certain nombre de techniques à intégrer dans la politique de sécurité de l'organisme à protéger.

L'Unix sécurisé

L'objectif du cours est de donner un guide pratique concernant la sécurité des systèmes UNIX à l'attention des utilisateurs et des administrateurs. On montrera comment les principes de base de la sécurité informatique peuvent être mis en œuvre dans les systèmes UNIX.

Les aspects suivants seront abordés :

- les caractéristiques générales des OS UNIX,
- le système de protection des fichiers,
- les principales vulnérabilités,
- conseils pour une installation et configuration sûres.
- Des exemples seront donnés sur Unix Solaris (SUN) et sur Linux.

Internet et la sécurité

- Les bases de TCP/IP
- Présentation d'Internet
- Les services Internet
- Les Firewalls
  - l'architecture d'un firewall
  - les fonctions d'un firewall
  - le filtrage des paquets
  - les serveurs «proxies»
  - le filtrage adaptatif
  - le contrôle du contenu
  - la traduction d'adresse IP
  - le chiffrement
  - l'authentification
  - la journalisation
- Les principes pour la sécurisation des services Internet
- L'accès à distance (telnet)
- Le courrier électronique (SMTP)
- Le transfert de fichiers (FTP)
- Le service de noms (DNS)
- Le Web
  - le service entrant (serveur Web)
    - les risques
    - sécuriser un serveur Web
  - le service sortant (consultation du Web)
    - les risques liés aux cookies
    - les risques liés aux codes mobiles
    - les applets java
    - ActiveX
  - configurer le firewall

- configurer les navigateurs
  - Internet Explorer
  - Netscape Navigator

JAVA et la sécurité

L'objectif de cet exposé est de présenter le fonctionnement de Java et les problèmes de sécurité dus aux applets Java.

Après une présentation de l'architecture et du modèle de sécurité de Java, les failles présentes dans ce modèle de sécurité seront indiquées. Ensuite, plusieurs démonstrations feront apparaître les effets des applets «hostiles» sur les machines. D'autres types d'attaques (locales, applets malicieuses, …) seront présentées ainsi que les moyens de rendre Java plus sécurisé en se protégeant mieux.

La carte à puce

- Histoire de la carte à puce : les premiers brevets, les premières réalisations, l'explosion du marché, le problème des «terminaux tueurs», l'époque actuelle
- Physique de la carte à mémoire
  - Les trois types de mémoire : RAM, ROM, EEPROM et leur utilisation
  - Le microcalculateur : 8 bits, fréquence de l'horloge
  - Les normes (tailles, emplacements, etc …)
- La cryptographie dans la carte à puce
  - Les premiers algorithmes (TELEPASS), le DES et triple DES, les cartes avec coprocesseur à clé publique
  - Répartition actuelle des divers algorithmes dans les cartes
  - Comparaison des performances et des coûts des différents algorithmes
  - Voies de recherche actuelles
- Les attaques physiques des cartes
  - Les attaques par recherche brute, les défauts de fabrication, la «Peel-Back Attack», les «Timing Attack», les attaques de type «Micro-onde», les «Differental Power Attack»
  - Quelques idées sur les parades implémentées

MODULE SI-6 : TÉMOIGNAGES ET CRITÈRES D'ÉVALUATION

Les CERTS français (CERT A, CERT IST, CERT RENATER)

Il s'agit de présenter les CERTS, leur rôle, le fonctionnement du réseau des CERTS, quelques statistiques et des exemples d'incidents traités par ces organismes.

La sécurité informatique au CEA

La sécurité des systèmes d'information au ministère de l'Équipement, en insistant sur le rôle du FSSI

La sécurité des systèmes d'information dans l'armée de l'air en présentant les actions à mener par les différents acteurs de la SSI

Le schéma d'évaluation – Les critères d'évaluation et de certification – Les critères communs – Les profils de protection

- Le schéma d'évaluation

C'est le 1er septembre 1995 qu'a été publié au Journal Officiel de la République française l'avis du Premier ministre relatif à la délivrance des certificats pour la sécurité des produits informatiques contre la malveillance. Le schéma définit l'organisation nécessaire à la conduite des évaluations dans les meilleures conditions de coût, d'efficacité et d'impartialité.

Au cœur de cette structure, la Direction centrale de la sécurité des systèmes d'information (DCSSI), organisme de certification, agrée et contrôle les centres d'évaluation commerciaux et délivre les certificats à l'issue des évaluations.

L'évaluation est basée sur des critères objectifs et rigoureux. Les critères ITSEC publiés en 1991 par la Commission Européenne sont aujourd'hui largement utilisés en Europe et font l'objet d'une reconnaissance mutuelle entre pays membres. Les Critères Communs actuellement normalisés à l'ISO sont des critères reconnus à l'échelle internationale.

Les certificats émis dans le cadre du schéma sont valables pour des versions spécifiques des produits. Il est important de pouvoir certifier rapidement de nouvelles versions d'un produit, en évitant de reprendre entièrement toutes les étapes de l'évaluation initiale. Il existe pour cela des programmes de maintenance mis en place dans le cadre du schéma. Les aspects de la maintenance sont abordés. Un catalogue à jour des produits certifiés sera présenté.

- L'évaluation selon les critères communs

Les Critères communs représentent l'aboutissement des efforts consentis pour développer des critères d'évaluation de la sécurité des TI qui soient largement utilisables par la communauté internationale. Destinés à devenir une norme ISO, les Critères Communs ouvrent la voie de la reconnaissance des résultats dans le monde entier. La version 2.0 publiée en juin 1998 est en cours de normalisation ISO.

La structure des Critères Communs permet une grande flexibilité pour la spécification de produits de sécurité. Les utilisateurs et les développeurs peuvent spécifier les fonctionnalités de sécurité d'un produit et choisir indépendamment le niveau d'assurance de l'évaluation parmi sept niveaux d'assurance.

- Profils de protection

Un profil de protection définit un ensemble d'exigences de sécurité, indépendant de l'implémentation, pour une catégorie de produits qui couvre des besoins de sécurité communs à plusieurs utilisateurs. Un profil de protection est réutilisable et permet de définir des exigences connues comme étant utiles et efficaces pour satisfaire des objectifs identifiés.

Le concept de profil de protection permet le développement de standards fonctionnels et constitue une aide à la formulation du cahier des charges d'un produit. Plusieurs profils de protection sont déjà disponibles pour des cartes à puce, des firewall, des infrastructures de clés publiques …

12 Formation à la cryptologie (n° 10)

12.1 Public visé

Ingénieurs et cadres de l'administration destinés à occuper des postes de responsabilité dans le domaine de la sécurisation des réseaux.

12.2 Conditions d'admission

Les candidatures sont transmises à la DCSSI par les Hauts fonctionnaires de défense ou les fonctionnaires de sécurité des systèmes d'information, et les admissions en stage sont prononcées par le directeur de la DCSSI. Il est souhaitable que les candidats soient titulaires d'une habilitation CONFIDENTIEL DÉFENSE.

12.3 Objectifs du stage

Former au profit de tous les ministères des personnels ayant de bonnes connaissances en cryptologie pour assurer le déploiement des nouvelles technologies de sécurisation des réseaux qui reposent pour la plupart sur des systèmes cryptologiques.

12.4 Corps enseignant

Le corps enseignant est constitué d'intervenants sélectionnés pour leur expérience et leurs compétences dans le domaine.

Ce sont :

- des professeurs de l'enseignement supérieur,
- des ingénieurs et des chercheurs de l'administration ou de l'industrie,
- des ingénieurs spécialisés de la DCSSI

12.5 Durée

Quatre semaines étalées sur deux mois auxquelles s'ajoute une semaine en option. Un stage cryptologie est organisé au cours du dernier trimestre de l'année calendaire.

12.6 Enseignement

Enseignement commun

- Module CRYPT-1 : Rappels Mathématiques
- Module CRYPT-2 : Algorithmique
- Module CRYPT-3 : Architecture
- Module CRYPT-4 : Implantations
- Module CRYPT-5 : Culture Générale en sécurité

Enseignement optionnel

- Module CRYPT-6 : Clés secrètes et Clés publiques

MODULE CRYPT-1 : RAPPELS MATHÉMATIQUES

Algèbre

- Structures finies et applications à la théorie des registres à décalage.

Arithmétique

- Notions et pratiques d'arithmétique nécessaires au RSA.

MODULE CRYPT-2 : ALGORITHMIQUE

Histoire

- La cryptologie depuis la 2ème guerre mondiale.
- Notions de cryptologie manuelle.

Concept de base de la cryptologie

- Quelques repères historiques.
- Notion de protocole et de service cryptologique, authentification, signature, intégrité, disponibilité, horodatage, mise en gage, échange de clef, annuaire électronique.
- Analyse de la menace. Canaux cachés. Clés. Cryptopériode. Principes de sécurité. Évaluation cryptologique. Taxonomie des systèmes cryptologiques. Interface télécom d'un système cryptologique, gestion des erreurs en ligne, synchronisme chiffre. Entropie. Secret parfait. Clé une fois, pseudo-aléa. Éléments de théorie de la complexité. Fonction à sens unique avec/sans trappe. Fonction de hachage cryptologique.
- Contrôle légal de la cryptologie. Tierces parties de confiance, séquestre et récupération de clé.
- Références bibliographiques générales. Revues scientifiques. Sites Web.

Infrastructure de gestion de clé

L'utilisation de la cryptographie asymétrique et des certificats de clés publiques permet de garantir les services de sécurité que sont l'intégrité, la confidentialité, l'authentification et la non-répudiation. Pour cela, les éditeurs et prestataires offrent des moyens et services liés à la gestion des certificats de clés publiques et qui permettent d'assurer la confiance au sein d'un domaine de sécurité.

Après avoir défini la signature numérique, ainsi que les certificats de clés publiques, les différents acteurs intervenant dans une IGC seront présentés, en termes techniques et en terme de service rendu.

Le cours présentera également un profil normalisé de certificat de clé publique, un exemple de politique de certification ainsi qu'une démonstration de fonctionnement (à confirmer).

Ce cours a pour but de définir la plateforme technique et organisationnelle nécessaire au déploiement d'une infrastructure de gestion de clés afin de mettre en évidence les enjeux actuels des IGC.

Cryptologie non-symétrique

- Les systèmes basés sur le logarithme discret :
- Aspects mathématiques élémentaires du logarithme discret sur un groupe cyclique. Protocoles cryptologiques basés sur le log discret : échange public de clé de Diffie-Hellman, signature de EL_Gamal, de Schnorr, chiffrement EL_Gamal. Étude du DSS. Protocole du RHC, de VKT. Algorithmes de calcul du log discret. Courbe ellip-

tique et log elliptique. Précaution d'emploi du log discret.

- Les systèmes basés sur la factorisation d'entiers :
  - Aspects mathématiques élémentaires de la factorisation d'entiers. Protocoles cryptologiques basés sur RSA : signature, échange public de clé, Fiat-Shamir. Conditions nécessaires de sécurité cryptologique du RSA. Extensions du RSA. Failles dans certains protocoles basés sur RSA (exposant e petit, exposant d petit, clairs dépendants, PKCS, …). Tests de primalité : théorie et performances. Algorithmes de factorisation. Problèmes d'implémentation et d'accélération des calculs : utilisation du reste chinois, utilisation d'un coprocesseur public, vérification de la correction des calculs, … Attaque par mesure de la durée des calculs. Attaque par stress physique du processeur.
- Quelques autres systèmes (percés)
  - Système de Lu_Lee, de Mac Curley, du knapsack, de Matsumoto-Imai, de Zu-Hua, de Pieprzick, …
- Références : Bibliographie, revues, conférences périodiques, sites Web, normes ISO.

MODULE CRYPT-3 : ARCHITECTURE

Gestion de clés secrètes

- Généralités : qu'est-ce qu'une clé • Caractère sensible d'une clé. Caractéristiques des clés : usage (session, trafic, …), classification, crypto-période. Formats de clés (standard DS 100, …).
- Cycle de vie d'une clé : chaque stade du cycle de vie d'une clé sera précisé et détaillé avec ses caractéristiques, ses spécificités … (création, conditionnement, distribution, stockage, archivage, utilisation, destruction, …). Compromission d'une clé : conséquences, traitement.
- Protection des clés : identification des besoins en matière de protection des clés. Concepts de distribution noire de bout en bout. Impacts sur la classification des clés, sur les habilitations des opérateurs. Clés rouges / clés noires. Clés de base (appariement, distribution, …). Dispositifs physiques associés à la protection (CIK …). Impacts sur la crypto, sur les équipements …
- Distribution des clés : les filières. Distribution manuelle. Distribution électronique : le système SELTIC, distribution par voies radio (OTAD, OTAR, OTAT). Protocoles de distribution sécurisée.
- Transfert des clés : protocoles de transfert de clés (DS102, DS 101), injecteurs «mécaniques», injecteurs électroniques (DTD …).
- Aspects réglementaires : archivage, séquestre et recouvrement de clés, mécanismes et protocoles permettant de répondre à ces exigences réglementaires, le Royal Holloway Protocol.

Infrastructure des clés publiques

- Position du problème : Approches principales : gestion classique à clé secrète, utilisation d'un serveur de clé, recours aux systèmes à clés publiques. Exemples de gestion de clés de messages par clé publique : type RSA par chiffrement de clé de message, type logarithme discret par échange de clé.
- Gestion des clés publiques : Propriétés souhaitables des clés : de chiffrement, de signature. Génération des clés. Certification des clés. Crytpo-période et renouvellement des clés.
- Exemples
- Failles classiques : Attaques par le milieu. Dilution de la confiance. Générateur aléatoire.
- Systèmes spéciaux : Systèmes basés sur l'identité.

Différents protocoles

- Introduction.
- Chaîne de hachage : Micro-paiement : PayWord, MicroMint, Millicent. Authentification : S/Key. Exercices.
- Authentification à clé secrète : Protocoles : 3 exemples de Token, Kerberos. Exercices.
- Authentification à clé publique : Protocoles 1-KP et 2-KP : DigiCash, Kleline, SSL v2 & v3. Exercices.
- Protocoles n-KP : PGP, PCT-S/MIME, SET, certification Inter-domaine, référentiel. Exercices.

MODULE CRYPT-4 : IMPLANTATIONS

Principe d'implantation

- Présentation de la problématique de l'implémentation des fonctions cryptographiques dans les équipements ; introduction : Ce que recouvre la sécurité dans un équipement de sécurité ; exigences de performance, exigences de pérennité. Place de l'évaluation dans l'assurance de sécurité, rôle de l'évaluation, conditions nécessaires pour que l'évaluation soit faisable (importance de l'implémentation des fonctions de sécurité).
- Solution technique : Domaine de confiance, domaine COMSEC. Importance de l'architecture de l'équipement. Cas particulier des fonctions cryptographiques.
- Prise en compte dans le cycle de vie d'un produit de sécurité : Principes généraux : Nécessité d'une prise en compte dès les phases amonts du développement. Nécessité d'une cohérence avec l'évaluation. Quelques exemples de démarches : Cas des administrations américaines pour le non classifié (guide de réalisation FIPS140-1). Cas du domaine civil : ce que prévoient les critères communs. Cas des matériels OTAN. Cas du poste radio américain MIDS, du module chiffre du GPS service précis. Démarche française.
- Conclusion

Cartes à puces

- Situation actuelle de l'industrie des cartes à puces.
- Implémentation des algorithmes cryptographiques dans les cartes.
- Législation.
- Attaques physiques et algorithmiques de certaines cartes.

Présentation des matériels crypto développés par Thalès, Sagem et Bull

- Présentations et démonstrations des offres des trois entreprises

MODULE CRYPT-5 : CULTURE GÉNÉRALE EN SÉCURITÉ

Méthodes FEROS, EBIOS et ROSCOF

Ces méthodes développées par le Service sont nécessaires en phase de conception des systèmes d'information pour exprimer, de façon rationnelle, les objectifs de sécurité.

Critères et schéma d'évaluation

- La situation en France et en particulier le rôle de la DCSSI dans l'évaluation et la certification.
- L'évaluation et la certification : Les centres d'évaluation (fonctions,

procédures d'agrément et contrôle, délivrance des certificats).
- Les critères d'évaluation : ITSEC, critères communs.
- Reconnaissance mutuelle des certificats ITSEC entre états.
- La documentation.

Les signaux parasites compromettants

- Présentation.
- Protection contre la menace SPC.
- Réglementation interministérielle relative à la protection contre les SPC.
- Démonstration pratique.

- **Principes du TRANSEC**

- Présentation générale du TRANSEC: Définition. Menaces prises en compte : brouillage, interception, écoute, détection, localisation, identification, intrusion. Fonctions de sécurité associées : étalement du spectre (par évasion de fréquence, par étalement en séquence directe), codage correcteur d'erreur, synchronisation variable, protection des messages techniques.
- Quelques caractéristiques des mécanismes de protection TRANSEC : Type de synchronisation temporelle. Caractéristiques des séquences pseudo-aléatoires. Cloisonnement TRANSEC/COMSEC.
- Conclusion.

Droit de la SSI

- Panorama des règles de protection des données à caractère personnel.
- Les missions de la CNIL.
- La position de la CNIL dans le domaine de la sécurité informatique.

Nouvelle loi sur la cryptologie

MODULE CRYPT-6 : SEMAINE SUPPLÉMENTAIRE (OPTIONNELLE)

CLÉS SECRÈTES

Algorithmes à clés secrètes

- Le DES : historique, l'algorithme, modes opératoires; réalisations.
- Cryptanalyse (exemples de DES) : clés faibles, clés complémentaires, attaque exhaustive, compromis temps-mémoire, attaque différentielle, attaque linéaire.
- Autres algorithmes : variantes du DES, IDEA, FEAL, RC2, RC5, AES.

Algorithmes de chiffrement en continu

- Générateur pseudo-aléatoire, autosynchronisation, RC4.

CLÉS PUBLIQUES

Éléments d'algorithmie

- Algorithmes classiques
- Analyse d'algorithmes
- Algorithmes de calcul élémentaire dans les corps finis

Courbes elliptiques

- Utilisation
- Génération de courbes, comptage de points

Factorisation

- Méthodes de calcul
  - Rho de Pollard
  - Méthode de courbes elliptiques
  - Pas de bébé / pas de géant
  - Crible quadratique
  - Crible algébrique

- **Faiblesse de choix de paramètres**

- **Clé publique et réduction de réseau**

- Algorithme LLL, ses améliorations
- Systèmes à base de sacs à dos
- Autres exemples

Systèmes divers

- Descriptions
- Éléments de sécurité
- Attaques connues

Fonctions de hachages et leurs faiblesses

Faiblesses de protocole

2

13 Signaux Compromettants (n° 2a et 2b)

13.1 Public visé

Ingénieurs ou techniciens appelés à assurer la protection des systèmes d'information en réduisant l'impact des émissions de signaux parasites compromettants (SPC).

Le stage 2a est destiné aux techniciens et praticiens du domaine.

Le stage 2b est destiné aux cadres administratifs, agents et responsables de sécurité des systèmes d'information et ingénieurs qui veulent acquérir des connaissances dans le domaine des rayonnements compromettants.

13.2 Conditions d'admission

Les candidatures sont transmises à la DCSSI par les Hauts fonctionnaires de défense ou les fonctionnaires de sécurité des systèmes d'information, et les admissions en stage sont prononcées par le directeur de la DCSSI. Les candidats doivent être titulaires d'une habilitation au CONFIDENTIEL DÉFENSE et au CONFIDENTIEL OTAN.

13.3 Objectifs du stage

Faire prendre conscience de la menace que font peser les SPC sur la sécurité des systèmes d'information. Former des personnes aptes à effectuer des mesures d'émission de SPC et à déterminer les mesures à prendre pour assurer la sauvegarde de la confidentialité des informations.

13.4 Corps enseignant

Le corps enseignant est constitué d'intervenants sélectionnés pour leur expérience et leurs compétences dans le domaine des SPC.

Ce sont :

- des cadres de la DCSSI,
- des ingénieurs et des chercheurs de l'industrie.

13.5 Durée

Deux semaines consécutives de quatre jours ; deux stages Signaux Compromettants sont organisés chaque année.

13.6 Enseignement

- Module TEMPEST-1 : Rappels sur la théorie (stage 2a)
- Module TEMPEST-2 : Réglementation
- Module TEMPEST-3 : Méthodes et moyens de mesures (stage 2a)
- Module TEMPEST-4 : Protection contre la menace TEMPEST (théorie)
- Module TEMPEST-5 : Protection contre la menace TEMPEST (pratique)

Module TEMPEST-6 : Démonstration de capture de Signaux Parasites Compromettants

MODULE SIGNAUX COMPROMETTANTS-1

Rappels sur la théorie

- Terminologie
- Les modulations
- Les lois de l'électromagnétisme
- L'étude de la génération des parasites
- La décomposition des perturbations
- Les signaux numériques
- Les décibels (dB)

MODULE SIGNAUX COMPROMETTANTS-2

Réglementation

- Rappels juridiques : Le droit de la SSI
- Présentation de la réglementation TEMPEST nationale
- Présentation de la réglementation TEMPEST OTAN
- Présentation détaillée de l'AMSG 720
- Présentation détaillée de l'AMSG 784
- Présentation détaillée de l'AMSG 788

MODULE SIGNAUX COMPROMETTANTS-3

Méthodes et moyens de mesures

- Les matériels de mesure
- Les méthodes de mesures de la Compatibilité ÉlectroMagnétique (CEM)
- Les méthodes de mesures TEMPEST

MODULE SIGNAUX COMPROMETTANTS-4

Protection contre la menace TEMPEST (théorie)

- Les moyens de protection
- La conception des matériels
- La conception des systèmes
- Le concept de zonage TEMPEST
- Les enceintes faradisées
- Les règles d'installation des équipements
- La maintenance TEMPEST
- L'élaboration d'un plan de tests
- L'élaboration d'un plan de tests réduit

MODULE SIGNAUX COMPROMETTANTS-5

Protection contre la menace TEMPEST (pratique)

- Le zonage TEMPEST de locaux
- La mesure d'une enceinte faradisée
- L'application pratique d'un plan de tests

MODULE SIGNAUX COMPROMETTANTS-6

Démonstration de capture de Signaux Parasites Compromettants

14 Le BESSSI

14.1 Public visé

Cadres de l'Administration destinés à devenir des experts de la sécurité des systèmes d'information.

14.2 Conditions d'admission

Diplôme d'ingénieur ou équivalent, ou bien avoir des connaissances d'un diplôme du premier cycle universitaire scientifique et une expérience de trois ans dans une des disciplines concernées par la sécurité des systèmes d'information.

Les candidatures sont transmises à la DCSSI par les Hauts fonctionnaires de défense ou les fonctionnaires de sécurité des systèmes d'information. Les admissions en stage sont prononcées par le Directeur central de la sécurité des systèmes d'information.

14.3 Objectifs du stage

Former des experts capables de concevoir des solutions, d'évaluer des produits et de conseiller les décideurs dans le domaine de la sécurité des systèmes d'information. Ce domaine comprend en particulier :

- la définition et la mise en place d'une politique de sécurité ;
- la conception et le déploiement d'architectures informatiques sécurisées ;
- la conception et la gestion d'une Infrastructure de Gestion de Clés ;
- la cryptologie ;
- la protection contre les signaux compromettants.

14.4 Corps enseignant

L'enseignement est assuré par :

- des professeurs de l'enseignement supérieur,
- des ingénieurs appartenant à la DCSSI et à des sociétés industrielles,
- des professeurs d'écoles d'ingénieurs,

sélectionnés pour leur expérience et leurs compétences dans les domaines traités.

14.5 Durée et sanction des études

Le stage comprend deux périodes :

- un enseignement scientifique d'une durée de neuf mois (du 1er septembre au 1er juin) sanctionné par un examen fin mai ;
- un stage d'application de 6 mois (du 1er juin au 31 décembre) ou d'un an (du 1er juin au 31 juin). Ce stage, réalisé en cotutelle avec l'organisme d'appartenance du stagiaire, est effectué au sein de cet organisme ou au sein des laboratoires de la DCSSI. À l'issue de ce stage, les étudiants produisent un mémoire et soutiennent leurs travaux devant un jury composé de représentants du monde académique et de spécialistes de la SSI.

Le jury est présidé par le Directeur central de la sécurité des systèmes d'information. Il délivre, à l'issue de ses délibérations, le Brevet d'Études Supérieures de la Sécurité des Systèmes d'Information (BESSSI), homologué au niveau I dans le groupe 45 de l'enseignement technologique (voir arrêté du 31 juillet 2000 complétant l'arrêté du 17 juin 1980 portant homologation de titres et de diplômes de l'enseignement technologique, journal officiel de la République française, 11 août 2000, page12453). Cette formation vient d'intégrer le nouveau dispositif d'enregistrement au Répertoire National des Certifications Professionnelles (arrêté d'homologation au Journal Officiel du 12 octobre 2002). Elle est enregistrée au niveau 1, code NSF326m.

14.6 Enseignement

La première période de la formation comprend les modules obligatoires suivants :

- Trois modules d'enseignement scientifique général
  - Module BESSSI-MATHÉMATIQUES
  - Module BESSSI-INFORMATIQUE
  - Module BESSSI-RÉSEAUX
- Cinq modules d'enseignement scientifique et technique spécialisés
  - Module BESSSI-CRYPTOLOGIE THÉORIQUE
  - Module BESSSI-CRYPTOLOGIE APPLIQUÉE
  - Module BESSSI-CRYPTOLOGIE MANUELLE
  - Module BESSSI-SÉCURITE INFORMATIQUE
  - Module BESSSI-TEMPEST
- Trois modules d'enseignement général
  - Module BESSSI-ÉCONOMIE GESTION
  - Module BESSSI-DROIT
  - Module BESSSI-ANGLAIS

Le détail de ces modules est donné ci-après.

Au cours de la deuxième période de la formation, l'étudiant réalise un travail personnel approfondi mené sous la direction d'un tuteur de la DCSSI en cotutelle avec l'organisme d'origine du stagiaire. Il recherche et analyse la littérature sur le sujet choisi et produit une réalisation informatique opérationnelle. Cette période a pour objectif de démontrer sa capacité à maîtriser les techniques et les méthodes de la SSI qu'il a acquises durant la première période d'enseignement.

Ces travaux couvrent des aspects techniques et scientifiques très divers. Voici quelques sujets récents:

- contrôle d'intégrité sur machine commerciale ;
- cryptanalyse des fonctions de sécurité de produits bureautiques grand public ;
- cryptanalyse opérationnelle du DECT (norme ETSI de réseaux local sans fil) ;
- gestion des clés pour une logique de chiffrement IP sous Windows NT ;
- analyse post-mortem de machines compromises (Unix, NT) ;
- module d'apprentissage à distance sur la signature électronique ;
- mise en évidence de faille sur des systèmes d'exploitation ;
- réalisation d'un logiciel sécurisé de téléphonie sur Internet ;
- étude d'un générateur de pseudo-aléa à synchronisation initiale ;
- analyse par une méthode formelle du sous-protocole IKE de l'IPSEC (standard de la sécurité des communications véhiculées par l'Internet) ;
- détection d'intrusion : deux logiciels libres pour la couche transport ipchains et TCP-wrapper ;
- comptage de points sur courbe elliptique ;
- application de méthodes formelles à la preuve de protocoles de sécurité ;

- cryptanalyse opérationnelle du Digital Audio Broadcasting ;
- méthodes d'évaluation des Infrastructures de Gestions de Clés ;
- les attaques rapides par corrélation ;
- contrôle d'intégrité d'un poste informatique ;
- génération de données aléatoires sans dispositif dédié ;
- la sécurité embarquée de Windows 2000 ;
- auto-formation en ligne pour adultes dans le domaine de la signature numérique ;
- comptage de points sur courbe elliptique : implémentation de l'algorithme de SATOH-FGH-AGM ;
- analyse de fichiers Office : recherche de macros.

MODULE BESSSI-MATHÉMATIQUES

ALGÈBRE GÉNÉRALE

Structures algébriques

- Groupes et sous-groupes
  - Définitions
  - Groupes monogènes
  - Groupes quotients
  - Groupes de permutations
- Anneaux
  - Définitions
  - Anneaux quotients
- Corps
  - Définitions
  - Utilisation d'un logiciel de calcul formel

ANNEAUX DE POLYNÔMES

- Définitions
- Propriétés
- Utilisation d'un logiciel de calcul formel

Extensions de corps

- Définitions
- Propriétés
- Utilisation d'un logiciel de calcul formel

Corps finis

- Propriétés
- Période d'un polynôme
- Polynômes primitifs
- Utilisation d'un logiciel de calcul formel

ARITHMÉTIQUE

- Propriétés élémentaires
- Résidus quadratiques
- Applications à la cryptologie
- Utilisation d'un logiciel de calcul formel

ALGÈBRE DE BOOLE

Treillis

- Définitions
- Propriétés algébriques

Algèbre de Boole

- Définitions
- Algèbres de Boole atomiques
- Différentes méthodes de réduction
- Résolution d'équations booléennes
- Matrices booléennes
- Utilisation d'un logiciel de calcul formel

THÉORIE DES GRAPHES

Définitions

Applications des propriétés des matrices booléennes

REGISTRE À DÉCALAGES

Définitions

Propriétés

Combinaisons non linéaires de sorties

Exemples d'attaques

ANALYSE NUMÉRIQUE

Analyses d'algorithmes

Exemples

ANALYSE COMBINATOIRE

Fonction gamma

Fonction combinatoire avec paramètres non entiers

Formule de STIRLING

Formules du binôme et du multinôme généralisées

Polynômes factoriels et opérateurs aux différences finies

Fonctions génératrices

LOGIQUE

Notions préliminaires

Les paradoxes

Formalisation systèmes formels langue et métalangue

Le calcul propositionnel

Le calcul des prédicats du premier ordre

Les théories axiomatiques

Calculabilité effective notions d'algorithmes machines de TURING thèse de CHURCH

Les problèmes métathéoriques complétude consistance Décidabilité théorème de GODEL

Automates théorie des automates finis

Théorie de la complexité

COMPLÉMENTS DE PROBABILITÉS

Fonctions génératrices

- Définition
- Exemples pour les principales lois discrètes
- Application à la recherche de loi de probabilités dans le cas de processus aléatoires discret

Fonctions caractéristiques

- Définition
- Exemples pour les principales lois continues
- Théorèmes de la limite centrale unidimensionnel et multidimensionnel
- Loi multinomiale et loi du Chi –deux
- Théorèmes limites

STATISTIQUES

Estimation ponctuelle et par intervalle

Tests

- Définition selon Von Neyman
- Test sans biais
- Puissance d'un test

Test associé à un échantillon asymptotiquement normal

Test du Chi-deux

Test d'adéquation de deux lois

Exemples de tests appliqués à la cryptologie

- Tests classiques d'aléa : fréquences, délais d'attente
- Test des figures fondamentales
- Tests de record : plus longue suite

THÉORIE DE LA COMPLEXITÉ

Définition d'un problème intrinsèquement difficile

Existence de preuves que certains problèmes sont difficiles

Moyens de construire des algorithmes cryptographiques reposant sur des problèmes intrinsèquement difficiles

MODULE BESSSI-INFORMATIQUE

Le programme d'informatique de la première année est divisé en quatre parties :

- Langages
- Programmation
- Architecture des ordinateurs
- Systèmes d'exploitations

Le but de ces quatre parties est double :

- permettre l'acquisition d'une culture informatique couvrant de nombreux domaines. Une telle culture élargie est indispensable pour l'adaptation à de nouvelles situations ainsi qu'à l'évolution rapide de l'informatique.
- Permettre l'acquisition d'une spécialité dans la sécurité informatique, que ce soit dans l'administration d'un serveur ou dans l'élaboration ou le test d'un logiciel.

I - LANGAGES

Cette partie a deux buts :

- rendre les élèves capables de produire du code de qualité en les rendant maître d'un langage (le langage C),
- donner aux élèves une culture sur d'autres langages qu'ils pourraient être amenés à utiliser : le C++ pour l'objet, Java pour l'Internet, l'assembleur pour le test de logiciel.

Notion de compilation

- compilation, code objet, compilation séparée, édition de liens, librairie statique, librairie dynamique, table des symboles, utilisation de la mémoire, pile, tas, passage des arguments et des valeurs de retour en mémoire

Le langage C

- révision du langage
- main, variables, affectations, for, while, if, switch
- les fonctions
- utilisation des fonctions, passage d'arguments par valeur, valeur de retour, minimisation de l'utilisation des variables globales
- les pointeurs et les tableaux
- utilisation des pointeurs, passage par valeur, correspondance pointeur-tableau, tableau à plusieurs dimensions, tableau de pointeurs, passage de tableaux à plusieurs dimensions
- éléments utiles du C
- struct et enum, comment les utiliser pour modulariser le code C, le préprocesseur C et son utilisation intelligente

Codage défensif

- Utilisation des fonctions pour modulariser le code, gestion d'erreur intelligente, utilisation propre de const, règles de codage, erreurs fréquentes

Optimisation d'un programme

- Débuggage d'un programme, désassemblage d'un programme, options d'optimisation des compilateurs, mélange d'assembleur dans du code C

Initiation à la programmation Objet

- Introduction du concept objet à partir des fonctions, des librairies et des structures, schématisation de l'objet, classes et objet, concepts liés à l'objet (héritage de type et héritage de comportement), apport de l'objet à la programmation, différences entre vrais langages objets (Effeil, SmallTalk) et langages orientés objet (C++)

Initiation au langage C++

- Présentation du C++, rapport avec le C, les classes et l'instanciation dans le C++, les nouveaux opérateurs, l'héritage en C++, la surcharge de méthode et d'opérateur en C++, la librairie standard C++

Initiation au langage Java

- Présentation du langage Java, rapport au C++, la machine virtuelle Java, différence entre application et applet, les classes et l'instanciation, l'absence de pointeurs en Java, les interfaces et l'héritage, les librairies Java

II - PROGRAMMATION

Cette partie a pour but de former les élèves à différents domaines de programmation, afin qu'ils puissent écrire ou étudier des applications professionnelles. Cette partie est la directe prolongation de la partie précédente. Une fois le langage maîtrisé, les élèves apprennent à l'utiliser pour réaliser des applications ayant de véritables fonctionnalités.

Programmation Internet

- Le Web, HTML et HTTP, le futur avec XML, les formulaires, l'interactivité serveur avec CGI, l'interactivité client avec JavaScript et Java

Programmation TCP/IP

- le client : ouverture et fermeture d'une socket, bind, connect, les structures d'adresses, envoie de commande et réception de réponse
- le serveur : listen, accept, select, ouverture d'une socket pour la connexion et d'une socket pour le client, traitement des commandes et envoi de réponse

Programmation Win32

- Les threads, le graphisme, le réseau Microsoft

Programmation avec les MFC

- Programmation d'interface graphique avec les MFC et l'AppWizard de Visual C++, concept d'une librairie de classe, hiérarchie et concepts des MFC

Étude d'un virus DOS

- Étude d'un virus simple, affectant un fichier .com présent dans le même répertoire, reproduction d'un virus, charge utile, code relogeable, infection, détection

III - ARCHITECTURE DES ORDINATEURS

Le but de cette partie est de doter les élèves d'un modèle mental du fonctionnement d'un ordinateur, en partant des composants physiques pour arriver au lancement du système d'exploitation. Un tel modèle permet de comprendre le fonctionnement de l'ordinateur depuis l'intérieur, ce qui assure une grande adaptabilité, et développe le sens critique des élèves vis-à-vis des annonces publicitaires.

Composants physiques

Le CPU, les registres, le microcode, la RAM, les différents caches, les bus données, adresses, la ROM, les bus périphériques, PCI, ISA, SCSI, IDE, ATAPI, les cartes périphériques, le disque dur, les chipsets

Montage d'un ordinateur

- Carte mère, cartes périphériques, les différents bus, interruptions, chipsets, vitesses d'horloges, le BIOS

Installation des systèmes d'exploitations

- DOS, Windows NT, Linux sur le même ordinateur, conflit de MBR, loadeur et partitions

Démarrage d'un ordinateur

- Le BIOS, les tests de démarrage, la table des partitions, le MBR, le secteur de boot, le noyau système

IV - SYSTÈMES D'EXPLOITATIONS

Cette partie a pour vocation de familiariser les élèves avec la plus complexe et la plus utilisée des couches de l'informatique : le système d'exploitation. Après un cours général sur les systèmes d'exploitations, trois systèmes sont étudiés de manière quasi-égale : Windows NT, Linux et Novel Netware. Le but est de donner aux élèves une formation d'utilisateur, d'administrateur système et d'administrateur sécurité dans chacun des trois systèmes.

Principes généraux des systèmes d'exploitations

- Mode kernel et mode utilisateur du CPU, abstraction de la machine virtuelle, partage des ressources mémoires et processus, multitâches et multithread, les droits et le multi-utilisateurs, le lancement des programmes
  - Chaque système d'exploitation est étudié suivant le schéma suivant :
    - Utilisation : utilisation générique du système, interface graphique et shell, astuce d'utilisation et power user, spécificité de chaque système
    - Programmation système : accès aux API systèmes, gestion propre au système des fichiers, des processus, de la mémoire, des droits et de la sécurité, accès aux spécificités du système
    - Architecture et administration : modèle et architecture du système, accès au système, paramétrisation du système, tâches courantes de l'administrateur système
    - Sécurisation du système : droits et mécanismes de sécurité du système, erreurs classiques et failles

connues, gestion d'une politique de sécurité et gestion des logs

Windows NT 4

Linux

Novel Netware

MODULE BESSSI-RÉSEAUX

BUT DE LA FORMATION : Acquérir une connaissance des réseaux permettant de comprendre la sécurisation de ceux-ci.

PRÉSENTATION PRATIQUE

Travail pratique

- Démonstrations :
  - Un analyseur de réseau durant une session de connexion sur un serveur (réseau IPX)
  - Un analyseur de réseau durant une session de connexion sur un réseau Novell ou Windows NT
  - Un sniffer sur une connexion PPP, durant une connexion sur Internet

Présentation des différents réseaux publics

- RTC
- RNIS
- TRANSPAC
- Services d'un réseau, présentation des différents services qu'apporte un réseau (vision d'un concepteur de systèmes)

ASPECTS THÉORIQUES

Architecture

- Architecture OSI de l'ISO
- Notion de système en couches
- Les instances de normalisation
- Les couches du modèle OSI

Couche physique

- Transmission
- Supports : paire torsadée, câble coaxial, fibre optique, ondes (radio, hertziennes)
- Topologie des réseaux : anneaux, étoile, bus, réseau maillé
- Protocoles
- Examens des données du tp

Couche liaison

- Méthodes d'accès centralisée : commutation de circuit
- Méthodes d'accès compétitive : CSMA/CD
- Méthode d'accès distribuée : jeton CSMA/CA

Couche réseau

- Types de réseaux : commutation de circuits, commutation de paquets
- Prococoles
- Examen des données du tp

Couche transport

- Architecture des différents réseaux
- Adressage
- Protocoles
- Examen des données du tp

Couche session

- Services
- Protocoles
- Examen des données du tp

Couche présentation

- Protocoles
- examen des données du tp

Couche application

- Protocoles
- Examen des données du tp

TECHNIQUES PARTICULIÈRES

Administration des réseaux

- Fonctions de l'administration
- Protocoles
- Outils d'observation et d'audit

Interconnexion des réseaux

- Équipements associés : répéteur, pont, routeur, passerelle
- Encapsulation des protocoles

Réseaux propriétaires

- BULL DSA
- IBM SNA

Réseau haut débit

- ATM
- FDDI

- **Réseau Internet**

- **Technologies sans-fil**

MODULE BESSSI-CRYPTOLOGIE THÉORIQUE

I - CONCEPTS DE BASE DE LA CRYPTOLOGIE

Quelques repères historiques

Services cryptologiques

- confidentialité, authentification, signature, intégrité, disponibilité, échange de clef, horodatage, mise en gage, enchéres électroniques, filigrane digital, commerce électronique... Analyse de la menace. Sûreté / Sécurité. Protocole cryptologique et menace: acteurs, canaux, primitives cryptologiques, logique du protocole, implémentations (FIPS140), exploitation. Propriétés formelles de protocoles. Sources de failles. Exemples, classification.
- Transec et comsec. Analyse de trafic. Canal subliminal. Canal caché. Stéganographie.

Clefs et gestion des clefs

- Clef de confidentialité, de signature, de chiffrement de clef.
- Création, certification, formatage, distribution.
- Protection: clef rouge/clef noire.
- Cryptopériode.
- Clef de réseau, clef de session, dérivation de clef, mise à la clef, révocation des clefs, séquestre et récupération de clef, partage de secret.
- Compromission des clefs.
- Réseau cryptologique ouvert / réseau fermé.
- Infrastructure de gestion de clefs.

Interface télécom d'un système cryptologique

- Gestion des erreurs en ligne, synchronisme chiffre.

Taxonomie des systèmes cryptologiques

- Systèmes symétriques, non-symétriques et quantiques.

Principes de sécurité

- Cryptanalyse d'attaque/cryptanalyse d'évaluation.
- Sécurité logique/sécurité physique.
- Principes de Kerckhoff, cloisonnement
- Formalisation et preuves de protocoles cryptologiques.

Références bibliographiques générales

- Revues scientifiques.
- Sites Web.

II - ALGORITHMIQUE ET THÉORIE DE L'INFORMATION

Algorithmes classiques de traitement numérique ou algébrique

- Performance, complexité.
- Calcul formel.

Sources d'information : Entropie

- Théorème du codage sans bruit.
- Compression.
- Statistique des langues humaines.

Canal d'information : Transinformation

- Capacité.
- Théorème du codage avec bruit.

Codes correcteurs d'erreur

- Étude de quelques codes, et de leur décodage.
- Transformée de Mac-Williams.
- Reconnaissance de codes dans un train binaire.

Équivocation

- Secret parfait.
- Diffusion/confusion.
- Distance d'unicité.
- 3ème théorème de Shannon.

III - LES SYSTÈMES SYMÉTRIQUES

Introduction

- Classification des systèmes selon le synchronisme. Autoclave. Messages parallèles.
- Décryptement de messages parallèles.
- Clef, marquant, clé de message, valeur initiale. Générateur d'aléa vrai/ pseudo-aléa.
- Choix et dimensionnement des clefs et des marquants. Mise à jour des clefs.

Les systèmes synchrones

- Système à clé une fois.
- Machine à pseudo-aléa. Critère d'aléa. Contrôle statistique de l'aléa. Test des motifs.
- Automates. Périodicité. Recherche de cycles. Diffusion/confusion. Critères de conception.
- Étude des registres à décalage. Cas linéaire. Période. Autocorrélation. Polynômes primitifs. Algorithme de Berlekamp-Massey et ses généralisations. Théorèmes de Herlestam. Complexité de suites : linéaire, d'ordre maximal, algébrique, de Kolmogorov. Suites de De Bruijn. Autocorrélation. Suites de synchronisation parfaites ou presque parfaites.
- Attaque par force brute. Contraintes de mise en œuvre opérationnelle.
- Étude des fonctions booléennes scalaires. Transformées de Fourier. Table des différences. Fonction booléenne faiblement résiliente. Théorème de Xiao-Massey. Fonction courbe, extrémale, symétrique, dégénérée, asymétrique. Dualité. Décompositions et approximations de fonctions booléennes en divers sens. Transformation non-linéaire. Résilience forte.
- Attaque de Siegenthaler. Mise en œuvre algorithmique.
- Méthodes de filtrage. Mise en œuvre algorithmique.
- Étude et évaluation de systèmes synchrones obtenus par combinaison non-linéaire de registres. Étude cryptanalytique de machines à rotor.
- Étude cryptanalytique de systèmes à horloge contrôlée : Stop-and-go, Shrinking generator, gsm, dect,….

Systèmes auto-synchronisants

- Propriétés et évaluation d'exemples.

Étude des systèmes par blocs

- Modes normalisés.
- Attaque par le milieu.
- Recherche de collisions par points distingués.
- Compromis temps-mémoire. Précalcul. Technique de hachage informatique. Études des fonctions booléennes vectorielles.
- Cryptanalyse linéaire, et variantes.

- Cryptanalyse différentielle, et variantes.
- Étude détaillée du DES,Triple DES, FEAL, IDEA, SAFER, et RC5.

Étude des fonctions de hachage

- Multipermutation
- Étude de MD4, MD5 et SHA

IV - LES SYSTÈMES NON-SYMÉTRIQUES

- **Introduction.**

- Éléments de théorie de la complexité. Fonction à sens unique avec/sans trappe. Fonction de hachage cryptologique.
- Protocoles dans les réseaux ouverts : authentification zéro-connaissance, transfert aveugle, monnaie électronique, traçabilité, anomymat.
- Annuaire électronique.

Algorithmique algébrique et de théorie des nombres

- Calculs sur les entiers, polynômes, matrices, réseaux, extension de corps, courbes elliptiques, ...Démonstrations de calcul formel. Draft IEEE P1363.

Les systèmes basés sur le log discret

- Logarithme discret sur un groupe cyclique.
- Protocoles cryptologiques basés sur le log discret: Diffie-Hellman, El_Gamal, Schnorr, DSS,…
- Protocoles de tierces parties de confiance : RHC,VKT.
- Algorithmes de calcul du log discret. Conditions de sécurité.

Les systèmes basés sur la factorisation

- Le RSA et ses extensions. Signatures, échange public de clef, authentification zéro-connaissance. Failles dans certains protocoles basés sur RSA.
- Tests de primalité : théorie et performances.
- Algorithmes de factorisation . Problèmes d'implémentation et d'accélération des calculs : reste chinois, coprocesseur public, vérification des calculs. Conditions de sécurité.
- Timing attack. Attaque par stress physique. DPA.

Autres systèmes.

- Cryptanalyse du knapsack, de Matsumoto-Imai, de Zu-Hua, de Pieprzick, …

V - LA CRYPTOLOGIE DANS LA SOCIÉTÉ DE L'INFORMATION

- Les institutions cryptologiques en France, en Europe et à l'étranger.
- Le contrôle légal de la cryptologie. Les tiers de confiance.
- Infrastructure de gestion de clef. Annuaire électronique. Certification de clef publique. Séquestre de clés. Recouvrement de clés. Signature numérique.
- Normes.

Annexe : CRYPTOLOGIE QUANTIQUE

- Les principes physique de base. Stéganographie quantique. Ordinateur quantique. Algorithme de Chor.

MODULE BESSSI-CRYPTOLOGIE APPLIQUÉE

INTRODUCTION - GÉNÉRALITÉS

Historique

Réglementation

Cryptologie gouvernementale et commerciale

CRYPTOLOGIE ET SÉCURITÉ DES SI

Les besoins de sécurité dans les systèmes d'information

Les fonctionnalités cryptologiques

Notions d'algorithme et d'éléments secrets

ALGORITHMES CRYPTOLOGIQUES

Algorithmes réversibles

- symétriques (par blocs, générateurs de pseudo-aléa)
- asymétriques (clés publiques)

Algorithmes non réversibles

- fonction de hachage

Différentes formes de réalisations des algorithmes

Études de quelques algorithmes

- générateur de pseudo-aléa (Défense)
- DES, IDEA
- MD5, SHA

GESTION DES ÉLÉMENTS SECRETS

Buts de la gestion des éléments secrets

- Caractéristiques des éléments secrets
- Caractéristiques de la gestion des éléments secrets
- Les différentes méthodes de gestion des éléments secrets

CRYPTOLOGIE GOUVERNEMENTALE

Les acteurs

Les algorithmes gouvernementaux

Les matériels gouvernementaux

- nationaux
- Otan

Étude de quelques systèmes gouvernementaux

CRYPTOLOGIE NON GOUVERNEMENTALE

Les acteurs

Les algorithmes

Étude de quelques systèmes

- authentification
- PGP
- GSM

Cryptologie sur Internet

- infrastructure de clés publiques (PKI)
- réseau privé virtuel (VPN)
- SSL
- SET

ANALYSE CRYPTOLOGIQUE

- **Méthode Siegenthaler**
- **Méthode Olive**
- **Tests de suites aléatoires**
- **Analyse d'un système de cryptophonie**

PROJETS

P0 : étude des messages parallèles

P1 : réalisation d'un logiciel de chiffrement (générateur de pseudo-aléa)

P2 :mise en œuvre de la méthode Siegenthaler

P3 : réalisation d'un logiciel de chiffrement (algorithme par blocs)

P4 : mise en œuvre des différents modes de fonctionnement d'un algorithme par blocs et étude de leurs effets en cas d'erreur de transmission

P5 : mise en œuvre de tests de suites pseudo-aléatoires

MODULE BESSSI-CRYPTOLOGIE MANUELLE

SUBSTITUTION SIMPLE À REPRÉSENTATION UNIQUE (SSRU)

L'analyse cryptologique s'appuie sur les caractéristiques statistiques de la langue, sur l'approche intuitive (mot probable) et sur la reconstitution des alphabets cryptographiques. On se limite aux procédés lettre à lettre et les procédés de chiffrement par bigrammes ne sont que brièvement décrits (Playfair).

SUBSTITUTION SIMPLE À REPRÉSENTATION MULTIPLE (SSRM)

L'analyse vise à se ramener à celle d'une substitution simple en s'appuyant sur les isologues du cryptogramme.

L'évolution historique du SSRM débouche sur les nomenclateurs, les répertoire codes et dictionnaires de chiffrement encore utilisés dans les années 70 ; la cryptanalyse des codes et dictionnaires ne saurait entrer dans le cadre restreint imparti, elle est très brièvement évoquée.

TRANPOSITIONS

Il n'y a que deux principes de chiffrement : la Substitution et la Transposition.

Par les exercices proposés, on montre que l'analyse des transpositions est facilitée par les erreurs des chiffreurs : exploitation de plusieurs cryptogrammes de même longueur permettant la reconstitution au moins partielle de la suite de l'anagramme, répétition de cryptogrammes mal chiffrés, etc … Une double transposition ou une transposition améliorée bien utilisée offre une sécurité cryptographique élevée.

SUBSTITUTION POLYALPHABÉTIQUE (À ALPHABETS NORMALEMENT ORDONNÉS ET À ALPHABETS INCOHÉRENTS)

Les quatre procédés classiques sont étudiés (Vigenère, Beaufort, Allemande 1ère et 2nde).

On recherche la longueur du mot clé par étude des répétitions de polygrammes du crypto (un commentaire est fait sur les méthodes modernes d'autocorrélation statistique du cryptogramme).

Le danger des recouvrements est mis en évidence par l'analyse de huit messages chiffrés avec la même clé.

Un autoclave (clair comme clé) et un cryptoclave (crypto comme clé) sont analysés ainsi qu'un très court message chiffré par clé texte ce qui conduit les élèves à découvrir de façon pragmatique et par eux-mêmes la clé aléatoire une fois.

HISTORIQUE DU CHIFFRE

Les origines : l'antiquité et le moyen-âge

L'éveil

La maturité : le XVII siècle

Le déclin

Le réveil

La Grande Guerre

L'entre deux guerres

La seconde guerre mondiale

L'après-guerre jusqu'à nos jours

MODULE BESSSI-SÉCURITÉ INFORMATIQUE

GÉNÉRALITES - MÉTHODOLOGIE

La sécurité informatique – Les concepts

- La société de l'information
- Les bases de la sécurité informatique

Fraudes et piratages informatiques, exemples vécus

Menaces, vulnérabilités, exploitation des vulnérabilités, parades possibles

Mesures de protection opérationnelles et organisationnelles, bases sur lesquelles repose la protection physique, sensibilisation des personnes

Méthodologie de la DCSSI : expression des besoins et identification des objectifs de sécurité (EBIOS), application de la méthode à un cas concret

Politique de sécurité et schéma directeur, facteurs à prendre en compte, modes d'action

ORGANISATION DE LA SÉCURITÉ INFORMATIQUE ET NORMALISATION

Organisation de la SSI au plan national

Responsabilités aux différents niveaux dans les administrations : haut fonctionnaire de défense, fonctionnaires de sécurité des systèmes d'information, responsables de sécurité des systèmes d'information, agents de sécurité des systèmes d'information

SSI au niveau international, les instances européennes (UE, OCDE, UEO)

Normalisation : définitions, enjeux, exemples, processus international de normalisation

LÉGISLATION ET RÉGLEMENTATION

Sécurité et droit européen

- champ de compétence de l'UE
- organes de l'UE
- normes communautaires
- relations avec l'administration française
- perspectives d'avenir

Problème juridiques soulevés par Internet et les réseaux numériques

- résumé des propositions du Conseil d'État
- Principaux problèmes posés aujourd'hui par Internet : Internet et la fraude, et les données personnelles, et les libertés, et la responsabilité des fournisseurs, et les consommateurs, et la publicité
- Réglementation interministérielle

MÉTHODOLOGIE

Génie logiciel

- méthodes et outils utilisés pour industrialiser la production de logiciels
- aide apportée par les méthodes formelles

Principes et modèles de la sécurité informatique

- enjeu d'une représentation abstraite de la sécurité informatique
- problématique de la sécurité logique dans les systèmes d'information
- différentes définitions de la sécurité informatique

Audit de sécurité d'un site

- méthodes classiques d'analyse de vulnérabilité : MARION, MELISA, MASSIA
- méthode de gestion de risques basée sur la maîtrise des écarts sur objectif

Plans de secours

- étude de «secourabilité»
- plan de secours informatique
- plan de secours utilisateurs

Méthodes et moyens de la sûreté de fonctionnement

- notions de sûreté de fonctionnement
- techniques de tolérance aux fautes accidentelles
- techniques de tolérance aux fautes intentionnelles

TECHNIQUES DE SÉCURISATION

Protection des systèmes répartis

- introduction
- applications réparties typiques
- authentification
- autorisation
- Commerce électronique

Protection des stations de travail

- stations centralisées
  - choix d'architectures de systèmes opératoires et de matériels
  - interconnexion de stations
  - choix d'architectures de systèmes et différents types de contrôles

Protection des bases de données

- sécurité des informations gérées par un système de gestion de base de données (SGBD), logiciel supposé sûr

Architecture des réseaux sécurisés

- risques et menaces
- services et mécanismes de sécurité
- quelques exemples applicatifs

Présentation de produits de sécurité

- sécurité des réseaux bureautiques et applications coopératives
- firewalls (gardes)
- sécurisation des bases de données
- outils existants pour faire audits et tests d'intrusion
- outils de sécurisation des systèmes d'exploitation

SYSTÈMES PARTICULIERS

Sécurité des systèmes WINDOWS NT

- éléments d'appréciation du niveau de sécurité offert par Windows NT
- réflexion sur les évolutions pour renforcer le niveau de protection

Virus informatiques

- différents types
- méthodes de prévention et de protection à inclure dans la politique de sécurité de l'organisme

Unix sécurisé

- caractéristiques des OS Unix
- système de protection des fichiers
- principales vulnérabilités
- conseils pour une installation et une configuration sûres

Internet et la sécurité

- bases de TCP/IP
- firewalls
- principes pour la sécurisation des différents services Internet
- actions à mener

Java et la sécurité

- architecture et modèle de sécurité de Java
- failles présentes dans ce modèle de sécurité
- moyens de renforcer la protection de Java

La carte à puce

- histoire
- physique de la carte à mémoire
- cryptographie dans la carte à puce
- attaques physiques des cartes
- idées sur les parades implantées

Les CERTS

- rôles, fonctionnement

TÉMOIGNAGES ET CRITÈRES

Sécurité informatique au sein d'organismes et de départements ministériels : ministère de l'Industrie - ministère de l'Équipement, des Transports et du Logement – ministère de la Défense

Schéma français d'évaluation des produits de sécurité

- schéma d'évaluation
- évaluation selon les critères communs
- profils de protection

MODULE BESSSI-TEMPEST

RAPPELS D'ÉLECTRONIQUE

Les modulations

Lois de l'électromagnétisme

Générations de parasites

Signaux numériques

CONCEPT TEMPEST

MOYENS DE PROTECTION

Blindage

Filtrage

Cages de Faraday

MÉTHODES ET MOYENS DE MESURE

NORMES DE PROTECTION

ÉLABORATION DES PLANS DE TESTS

RÈGLES D'INSTALLATION ZONAGE «TEMPEST»

CONCEPTION DE MATÉRIEL ET DE SYSTÈMES

MODULE BESSSI-DROIT

DROIT DE LA CRYPTOLOGIE, DE L'INFORMATION ET DES TÉLÉCOMMUNICATIONS

Introduction générale au droit

L'organisation de l'Union Européenne

Présentation du droit communautaire

Le droit de la cryptologie

Le droit et l'informatique

La protection des bases de données

La CNIL

Le droit des télécommunications (avec notamment les problèmes juridiques posés par Internet et le commerce électronique)

La réglementation sur la protection du secret

FORMATION PROFESSIONNELLE

La responsabilité pénale des fonctionnaires

Les marchés publics

CONTRÔLE

MODULE BESSSI-ÉCONOMIE ET GESTION

ÉCONOMIE : COURANTS ET CONCEPTS

Historique

La fonction d'utilité du consommateur, l'offre et la demande

Les néoclassiques (marché libre) : hypothèses et critiques

Introduction à la comptabilité nationale (les agrégats)

LES MARCHÉS FINANCIERS

Les acteurs

Les hypothèses

La notion de risque

Évaluation (VAN, EVA, MVA)

Introduction à la gestion financière (budgétisation, analyse financière)

MARKETING

Introduction

Concepts fondamentaux

La vente

DROIT

Les sources du droit

Introduction au droit des sociétés

Notions de fiscalité

STRATÉGIE ET TECHNOLOGIES DE L'INFORMATION

Concepts fondamentaux

Les ressources de l'entreprise

Notions d'organisation

Systèmes d'information en entreprise

Le commerce électronique

MODULE BESSSI-ANGLAIS

EXPRESSION ORALE

Mise en situation

Débats

Jeux de rôles

Jeux linguistiques

Échanges d'opinions

Commentaires oraux à partir de documents authentiques (écrits, audio, audiovisuels)

Présentation sur des sujets techniques

COMPRÉHENSION ORALE

Documentaires grand public et techniques

Nouvelles radio et télévision

COMPRÉHENSION ÉCRITE

Articles et dossiers

Littérature (nouvelles)

Documents techniques

GRAMMAIRE

Remise à niveau générale

Acquisition de structures nouvelles, notamment : temps et aspects, modalité, prépositions, adverbes, articles et déterminants …

VOCABULAIRE

Acquisition de vocabulaire général et technique

TRADUCTION

Préparation aux examens militaires selon la demande