

Voie d'Approfondissement  
**Sécurité des Systèmes et des Réseaux**  
( VAP SSR )

**Directeur de Programme :**

Hervé DEBAR

**Objectifs :**

Le développement de la sécurité dans les réseaux est aujourd'hui une véritable préoccupation pour les différents acteurs de l'économie : entreprises, collectivités locales, et opérateurs. En effet, les effets d'une intrusion sur un réseau peuvent parfois s'avérer dévastateurs pour la société concernée : atteinte à l'image de l'entreprise, perte de recettes, perte de confiance des clients, engagement de la responsabilité légale si le réseau attaqué est utilisé comme rebond pour attaquer un réseau tiers (pouvant donner lieu à des dommages et intérêts),...

*Un exemple de chiffres : l'étude 2011 Data Breach Investigations Report (DBIR – Verizon, US Secret Service, Dutch High Tech Crime Unit) a étudié 800 cas de pénétration en 2010 (900 entre 2004 et 2009), la moitié d'entre eux impliquant des codes malveillants et provenant de l'extérieur des organisations. En 2010, le US Secret Service a arrêté 1200 suspects pour des attaques informatiques, pour des pertes directes de 500 millions de dollars et a évité des pertes potentielles de 7 milliards de dollars.*

La diversité et la complexité des risques encourus et des failles d'un système ou d'un réseau sont telles que, la sécurité représente à elle seule un métier et un domaine de spécialisation à part entière, et en fait un marché en pleine expansion. *Le marché de la sécurité informatique, et plus particulièrement des éditeurs de solutions logicielles, retrouve un nouveau souffle avec une croissance de 12% en 2010, et un chiffre d'affaire global de 16,5 milliards de dollars (Gartner Mai 2011).* Cette expansion se fera à l'avenir dans le domaine bancaire (premier opérateur d'infrastructures réseau en France) et dans le domaine des opérateurs d'infrastructures vitales (OIV : énergie, eau, transport, sécurité globale, etc.)

Cette VAP se propose de former des ingénieurs aux techniques de sécurisation qui peuvent être utilisées dans les systèmes et les réseaux en vue d'assurer l'authentification des utilisateurs, protéger l'accès aux informations, préserver la confidentialité et l'intégrité des données.

Un point essentiel de ce cursus est d'être en adéquation avec les besoins du marché, c'est pourquoi l'implication des industriels est forte et une grande part du temps est consacrée aux aspects pratiques.

A l'issue de cette VAP, l'étudiant aura les compétences nécessaires pour :

- Evaluer les risques et les failles inhérentes aux systèmes et réseaux informatiques
- Auditer un réseau et préconiser des outils de prévention
- Concevoir et appliquer une politique de sécurité
- Préconiser et déployer des méthodes de protection des échanges de données basés

sur des méthodes d'authentification, de tunneling ou de chiffrement

- Définir et mettre en œuvre une politique de filtrage basée sur les contraintes et besoins de l'entreprise
- Concevoir et mettre en œuvre des architectures réseaux sécurisées globales

Outre le diplôme d'ingénieur de Télécom SudParis, cette VAP permettra aux étudiants (sous réserve de satisfaction des critères de validation spécifiques à la convention de collaboration signée entre Télécom SudParis et l'ANSSI) d'obtenir le titre d'expert en sécurité des systèmes d'information (ESSI) délivré par l'agence nationale pour la sécurité des systèmes d'information (ANSSI).

### **Organisation :**

Cette voie d'approfondissement s'inscrit dans le cycle d'approfondissement du cursus de Télécom SudParis. Elle se compose de six Unités de Valeur (UV) autonomes et cohérentes, programmées dans les semestres S8 et S9. Chaque UV représente une charge de travail total de 90 heures dont 45 heures au maximum sont réalisées en présentiel.

En complément de ces UVs, un projet d'approfondissement dans la thématique de la VAP sera réalisé en binôme ou en trinôme sur la période du semestre S10. Ce projet représente une charge de travail de 225 heures.

### **Programme :**

Semestre 8

- NET5038 : Evaluation des Risques et Détection des Attaques
- NET5039 : Authentification, VPN et Chiffrement

Semestre 9

- NET5533 : Les Fondements de la Sécurité
- NET5531 : Filtrage
- NET5532 : Sécurité des Applications et des Services
- NET5534 : Architectures Sécurisées
- NET5535 : Projet d'Approfondissement de la VAP SSR

## **NET5038      Evaluation des risques et détection des attaques**

**Période :** S8 / P3

**ECTS :** 4

**Langue :** Français

### **Organisation :**

- Heures programmées / Charge Totale : 45/90
- Heures Cours/TD/TP/CF1 : 31/2/9/3

La plupart des cours portant sur des sujets de pointe ou en constante évolution sont effectués par des industriels. Les travaux dirigés sont réalisés en petits groupes. Les travaux pratiques se font individuellement ou en binôme (voire exceptionnellement en trinôme).

### **Evaluation :**

La validation de cette UV se fait grâce à un TP noté (TP) et un contrôle final (CF) de 3h qui a lieu à la fin de l'UV.

Pour cette UV, il n'y a pas de possibilité de rattrapage.

La présence aux heures programmées est obligatoire, et peut influencer sur la pondération de la note finale.

Note finale = Moy (1/3 TP, 2/3 CF)

L'UV est validée si la note finale est  $\geq 10 / 20$

### **Objectifs :**

- Evaluer les risques et les failles inhérentes aux réseaux informatiques (grandes familles de risques, bases des attaques, et exemples concrets d'attaques possibles sur un réseau)
- Auditer un réseau
- Préconiser des outils de prévention et/ou détection
- Concevoir et appliquer une politique de sécurité grâce à des méthodologies et des modèles de sécurité
- Connaître la législation associée à la sécurité en France

### **Mots clefs :**

Attaques, audit, détection, intrusions

### **Prérequis :**

Bonnes connaissances en systèmes d'exploitation (UNIX, Windows, ...) et en réseaux (TCP/IP, routage,...)

### **Contenu :**

- Initiation aux VPNs et à la sécurité réseaux
- Sécurité des réseaux : risques et parades
- Méthodologie d'Analyse des Risques
- Droits et devoirs en matière de sécurité des systèmes d'informations
- Audit
- Détection d'intrusions

- Traitement d'Incidents de Sécurité et Honeypots

### **Supports de cours et bibliographie :**

Supports de cours :

- « VPN and Network Security » (Polycopié)
- « Risques et Parades » (Polycopié)
- « Audit » (Polycopié)
- « Détection d'intrusions » (Polycopié)
- « Méthodologie d'Analyse des Risques » (Polycopié)
- « Réglementation en matière de Cryptologie » (Polycopié)
- « Honeypots » (Polycopié)

Bibliographie :

- *Advances in Enterprise Information Technology Security*, IDEA Group Publishing, IRM Press, ISBN: 978-1-59904-090-5, Mars 2007.
- Solange Ghernaouti-Hélie, *Sécurité informatique et réseaux*, DUNOD , ISBN 978-2-10-052156-2

### **Responsable :**

Sophie GASTELLIER-PREVOST (Sophie.Gastellier@it-sudparis.eu)

### **Intervenants :**

- Sophie GASTELLIER-PREVOST : Ingénieur d'Etudes Télécom SudParis
- Dr Claudine GUERRIER : Maître de Conférences Télécom Ecole de Management
- Pr Abdallah M'HAMED : Maître de Conférences Télécom SudParis
- Pr. Hervé DEBAR : Professeur Télécom SudParis
- Intervenants industriels : Orange, ANSSI, consultant en environnement bancaire et opérateurs, ...

**NET5039      Authentification, VPN et chiffrement****Période : S8 / P4****ECTS : 4****Langue : Français****Organisation :**

- Heures programmées / Charge Totale : 45/90
- Heures Cours/TD/TP/CF : 24/6/12/3

La plupart des cours portant sur des sujets de pointe ou en constante évolution sont effectués par des industriels. Les travaux dirigés sont réalisés en petits groupes. Les travaux pratiques se font en binôme ou trinôme.

**Evaluation :**

La validation de cette UV se fait grâce à un contrôle final (CF) de 3h qui a lieu à la fin de l'UV, ainsi que par un TP noté en binôme ou trinôme (TP).

Pour cette UV, il n'y a pas de possibilité de rattrapage.

La présence aux heures programmées est obligatoire, et peut influencer sur la pondération de la note finale.

Note finale = Moy (  $\frac{3}{4}$  CF,  $\frac{1}{4}$  TP)

L'UV est validée si la note finale est  $\geq 10 / 20$

**Objectifs :**

- Savoir mettre en œuvre les services d'authentification et de chiffrement
- Connaître les mécanismes d'authentification à base de cartes à puces, données biométriques et SSO (Single Sign On)
- Connaître les mécanismes utilisés dans les VPNs (Virtual Private networks)
- Etre capable de mettre en œuvre des VPNs basés sur IPsec
- Comprendre la cryptographie et connaître les algorithmes de chiffrement les plus couramment utilisés
- Etudier quelques applications possibles de la cryptographie : commerce électronique, sécurisation des emails, ...

**Mots clefs :**

Authentification, cryptographie, VPN

**Prérequis :**

Bonnes connaissances des attaques systèmes et réseaux, des méthodes d'audits, de la détection d'intrusions, et des aspects légaux liés au domaine de la sécurité

**Contenu :**

- Cartes à puce (architecture, applications, ...)
- Biométrie (techniques, usages, contrôle d'accès, ...)
- Architecture et protocoles d'authentification (EAP, AAA)
- Solution SSO (Single Sign On)

- Vérification des protocoles d'authentification
- Cryptographie
- VPN (Réseaux privés virtuels) et IPsec
- Mise en œuvre d'un VPN et du NAT
- Protocoles de Sécurité
- Sécurité des réseaux ad hoc
- Les signatures : une application de la cryptographie
- PKI et implémentations réelles de la cryptographie
- Sécurité des emails : PGP, S/MIME

### **Supports de cours et bibliographie :**

Supports de cours :

- Polycopiés des cours fournis par les intervenants

Bibliographie :

- Cheswick W., Bellovin S., et Rubin A. : *Firewalls and Internet Security, Repelling the Wily Hacker*, Second Edition. Addison-Wesley Professional, 2003.
- Gupta, M. : *Building a Virtual Private Network*, Premier Press
- Rescorla E. : *SSL and TLS : Designing and Building Secure Systems*, Addison-Wesley, 2nd Edition, March 2001.
- Schneier B : *Cryptographie Appliquée*, Second Edition. 1996

### **Responsable :**

Pr Maryline MAKNAVICIUS (Maryline.Maknavicius@it-sudparis.eu)

### **Intervenants :**

- Pr Bernadette DORIZZI : Professeur Télécom SudParis
- Sophie GASTELLIER-PREVOST : Ingénieur d'Etudes Télécom SudParis
- Patrick MAIGRON : Ingénieur d'Etudes Télécom SudParis
- Dr Hakima CHAOUCHI : Maître de conférences Télécom SudParis
- Pr Maryline MAKNAVICIUS : Professeur Télécom SudParis
- Intervenants industriels : SOLUCOM, Thalès, FTR&D

**NET5533 Les fondements de la sécurité**

Période : S9 / P1

ECTS : 4

Langue : Français

**Organisation :**

- Heures programmées / Charge Totale : 24/90
- Heures Cours/TD/TP/CF : 9/0/9/0

L'objectif de cette UV est de préparer les enseignements sur le filtrage et la sécurité système et web en étudiant de manière détaillée et pratique certains aspects du fonctionnement des réseaux TCP/IP et des systèmes d'exploitation. En parallèle des cours, des travaux de recherche sont à réaliser en binôme durant l'UV. Chaque binôme présente ses résultats aux autres étudiants de l'UV. L'ensemble de ces soutenances correspond à une durée totale de 6 heures de face-à-face environ.

**Evaluation :**

La validation de cette UV se fait individuellement grâce à un TP noté (TP) et par binôme grâce à un rapport (R) et une soutenance en anglais (S) portant sur le travail réalisé. Bien que la soutenance s'effectue par binôme, la note attribuée (S) est individualisée, fonction de la maîtrise et de la contribution apportée par chacun.

La présence aux heures programmées est obligatoire, et peut influencer sur la pondération de la note finale.

Pour cette UV, il n'y a pas de possibilité de rattrapage.

Note finale = Moy (2/5 TP, 1/5 R, 2/5 S)

L'UV est validée si la note finale est  $\geq 10 / 20$

**Objectifs :**

- Appréhender des thématiques d'actualité liées au domaine de la sécurité dans le domaine des réseaux IP et des systèmes d'exploitation
- Être capable de faire une recherche bibliographique sur un sujet donné, d'en faire une synthèse tant écrite qu'orale.

**Mots clefs :**

Actualité, sécurité, métier

**Prérequis :**

Bonnes connaissances des communications réseaux, attaques systèmes et réseaux, des méthodes d'audits, de la détection d'intrusions, des honeypots, des méthodes d'authentification, des VPNs et de la cryptographie

**Contenu :**

- Conférences d'industriels sur des thématiques d'actualité du domaine de la sécurité (éditeurs, intégrateurs, ...). Les conférences peuvent porter sur des problématiques métiers, des solutions logicielles et/ou matérielles, des méthodologies, ...
- Attaque et défense d'un système
- Fonctionnement et défaillances d'un réseau IP

- Fonctionnement et défaillances d'un système d'exploitation

**Responsable :**

Prof. Hervé DEBAR (herve.debar@it-sudparis.eu)

**Intervenants :**

- Equipe pédagogique de la voie d'approfondissement SSR

**NET5531 Filtrage****Période : S9 / P2****ECTS : 4****Langue : Français****Organisation :**

- Heures programmées / Charge Totale : 40,5/90
- Heures Cours/TD/TP/CF : 18/3/16,5/3

La plupart des cours portant sur des sujets de pointe ou en constante évolution sont effectués par des industriels. Les travaux dirigés sont réalisés en petits groupes. Les travaux pratiques se font en binôme ou trinôme.

**Evaluation :**

La validation de cette UV se fait grâce à un contrôle final (CF) de 3h qui a lieu à la fin de l'UV, par un TP noté en binôme ou trinôme (TP) et par une présentation réalisée en TD (TD).

Pour cette UV, il n'y a pas de possibilité de rattrapage.

La présence aux heures programmées est obligatoire, et peut influencer sur la pondération de la note finale.

Note finale = Moy (1/2 CF, 1/4TP, 1/4TD)

L'UV est validée si la note finale est  $\geq 10 / 20$

**Objectifs :**

- Comprendre les problèmes que les systèmes de filtrage visent à résoudre
- Comprendre et maîtriser les différents mécanismes de filtrage qui peuvent être déployés dans un réseau.
- Etre capable de mettre en œuvre les mécanismes de filtrage (à base de routeurs, firewalls) en tenant compte d'une politique de sécurité.

**Mots clefs :**

Filtrage, firewall

**Prérequis :**

Bonnes connaissances des architectures systèmes UNIX, TCP/IP, attaques, détection intrusions

**Contenu :**

- Problématique de filtrage (origine, exemples, vocabulaire).
- Architectures des modules de filtrage (contrôle d'accès, traitement des attaques de niveau réseau et circuit).
- Architectures pour le filtrage applicatif (contrôle d'accès, traitement des attaques de niveau circuit et application).
- Filtrage des applications multimédia (impact du filtrage/translation d'adresses et applications multimédia, solutions existantes).
- Deni de Service (classification, prévention, détection, traçage, suppression).
- Etude d'une politique de filtrage, avec recherche bibliographique préalable.

- Mise en œuvre de filtrage à base de routeurs.
- Mise en œuvre de filtrage avancé à base de firewalls.

### **Supports de cours et bibliographie :**

Supports de cours :

- Polycopiés fournis par les enseignants

Bibliographie :

- *Building Internet Firewalls*, (2nd Edition), Elizabeth D. Zwicky, S. Cooper, and D.B. Chapman, 2000.
- *Firewalls and Internet Security: Repelling the Wily Hacker*, Second Edition, W. R. Cheswick, S. M. Bellovin, A.D. Rubin, 2003.

### **Responsable :**

Dr Olivier PAUL (Olivier.Paul@it-sudparis.eu)

### **Intervenants :**

- Dr. Olivier PAUL : Maître de conférences, Télécom SudParis
- Dr. Sophie GASTELLIER-PREVOST : Ingénieur d'Etudes, Télécom SudParis

**NET5532      Sécurité des applications et des services****Période : S9 / P3****ECTS : 4****Langue : Français****Organisation :**

- Heures programmées / Charge Totale : 41/90
- Heures Cours/TD/TP/CF : 21/3/15/2

La plupart des cours portant sur des sujets de pointe ou en constante évolution sont effectués par des industriels. Les travaux pratiques se font individuellement.

**Evaluation :**

La validation de cette UV se fait grâce à un contrôle final (CF) de 2h qui a lieu à la fin de l'UV, ainsi que par un TP noté individuel (TP).

Pour cette UV, il n'y a pas de possibilité de rattrapage.

La présence aux heures programmées est obligatoire, et peut influencer sur la pondération de la note finale.

Note finale = Moy (CF, TP)

L'UV est validée si la note finale est  $\geq 10 / 20$

**Objectifs :**

- Comprendre les problématiques de sécurité des systèmes informatiques et appréhender les principales stratégies de prévention et de résolution de ces problèmes
- Connaître les principes du contrôle d'accès des systèmes
- Avoir expérimenté les méthodes d'injection de code dans les applications et les techniques permettant d'y résister
- Comprendre les relations entre la sécurité des applications et l'établissement de réseaux de confiance en particulier pour les applications Java, et les distributions linux.
- Connaître la sécurité des systèmes d'exploitation Linux, et Windows, et les outils permettant de la gérer
- Comprendre le fonctionnement des virus
- Appréhender la sécurisation des infrastructures réseaux sans fil

**Mots clefs :**

Contrôle des droits, sécurité système d'exploitation, sécurité applications, sécurité Web, sécurité réseaux sans fil, politique de sécurité d'un site

**Prérequis :**

Connaissances sur les systèmes d'exploitation multitâches, les méthodes d'authentification, la programmation procédurale et objet. La maîtrise d'installations de systèmes d'exploitation facilite la compréhension de l'UV.

## **Contenu :**

- Contrôle d'accès
- Sécurité Système d'Exploitation et Linux
- Sécurité Windows
- Sécurité des applications Web et Java
- Virus et anti-virus
- Sécurité et réseaux sans fils
- Gestion d'une politique de sécurité globale à un site

## **Supports de cours et bibliographie :**

Supports de cours :

- Polycopiés fournis par les enseignants

Bibliographie :

- Wreski D.: *Linux Security HOW TO*, [http://tldp.org/HOWTO/html\\_single/Security-HOWTO/](http://tldp.org/HOWTO/html_single/Security-HOWTO/)
- Skoudis E. and Liston T.: *Counter Hack Reloaded*, Prentice Hall, dec. 2005, pp. 784,
- McClure S., Scambray J. and Kurtz G. : *Hacking Exposed*, Sixth Edition, McGraw-Hill, jan. 2009, pp. 720
- Hatch B., Lee J.: *Hacking Linux Exposed*, McGraw-Hill, apr. 2005, pp. 692 pages,
- Filiol E.: *Les virus informatiques : théorie, pratique et applications*, SPRINGER, pp. 384, 2004
- Cannings R., Dwivedi H., and Lackey Z.: *Hacking Exposed Web 2.0 : Web 2.0 Security Secrets and Solutions*, McGraw-Hill, dec. 2007, pp 258 (traduit en français Hacking sur le Web 2.0)
- *La sécurité dans les réseaux sans fil et mobiles*, traité IC2, Hermès, mars 2007

## **Responsable :**

Dr Christian BAC (Christian.Bac@it-sudparis.eu)

## **Intervenants :**

- Pr Hossam AFFIFI : Professeur Télécom SudParis
- Dr Christian BAC : Directeur d'Études Télécom SudParis
- Dr Sébastien LERICHE : Maître de Conférences Télécom SudParis
- Dr Abdallah M'HAMED : Maître de Conférences Télécom SudParis
- Intervenants industriels : SOLUCOM, ...

**NET5534 Architectures sécurisées****Période** : S9 / P4**ECTS** : 4**Langue** : Français**Organisation :**

- Heures programmées / Charge Totale : 24/90
- Heures Cours/TD/TP/CF : 18/0/0/0

Les 18 heures de cours se font sous forme de conférences animées par des industriels du domaine de la sécurité. Des travaux de recherche sont à réaliser en binôme durant l'UV. Chaque binôme présente ses résultats aux autres étudiants de l'UV. L'ensemble de ces soutenances correspond à une durée totale de 6 heures de face-à-face environ.

**Evaluation :**

La validation de cette UV se fait d'une part par un contrôle individuel portant sur l'ensemble du programme des UV NET5038, NET5039, NET5531 et NET5532 (C), et d'autre part grâce à un rapport (R) et une soutenance (S) portant sur une étude de cas réalisée par binôme

La présence aux heures programmées est obligatoire, et peut influencer sur la pondération de la note finale.

Pour cette UV, il n'y a pas de possibilité de rattrapage.

Note finale = Moy (1/2C, 1/4 R, 1/4 S)

L'UV est validée si la note finale est  $\geq 10 / 20$

**Objectifs :**

- Etre capable de mettre en œuvre tout ou partie d'une architecture sécurisée, fonction des contraintes données, et d'en faire une synthèse tant écrite qu'orale.

**Mots clefs :**

- Architecture, sécurité, réseaux, systèmes

**Prérequis :**

Bonnes connaissances des communications réseaux, attaques systèmes et réseaux, des méthodes d'audits, de la détection d'intrusions, des honeypots, des méthodes d'authentification, des VPNs, de la cryptographie, du filtrage, de la sécurité des OS et de la sécurité des réseaux

**Contenu :**

- Conférences d'industriels sur des thématiques et/ou étude de cas d'architectures sécurisées du domaine de la sécurité (éditeurs, intégrateurs, ...).
- *Exemple de thème de conférence* : Problématiques de sécurité chez un opérateur mobile, Etude de cas d'architectures sécurisées, Etude de cas autour d'une problématique de télédéclaration ...

**Responsable :**

Sophie GASTELLIER-PREVOST (Sophie.Gastellier@it-sudparis.eu)

**Intervenants :**

- Equipe pédagogique de la voie d'approfondissement SSR
- Intervenants industriels : intégrateurs, éditeurs, constructeurs, opérateurs, ...

<b>NET5535</b>	<b>Projet de la voie d'approfondissement SSR</b>	
<b>Période : S9</b>	<b>ECTS : 8</b>	<b>Langue : Français</b>

### **Organisation :**

- Heures programmées / Charge Totale : 20/225

Le projet de la voie d'approfondissement CSI est réalisé sur la totalité du semestre 9.

Chaque étudiant doit réaliser un projet en binôme ou trinôme.

Des plages sont programmées dans l'emploi du temps afin d'être dédiées à ce projet.

La majorité des projets proposés dans la VAP SSR sont des projets industriels.

### **Evaluation :**

La validation du projet de voie d'approfondissement est basée sur la réalisation d'un rapport écrit (E) et d'une soutenance orale (S). L'évaluation de ces deux éléments est réalisée de manière individuelle.

Note finale = Moy (E, S))

L'UV est validée si la note finale est  $\geq 10 / 20$

### **Exemples de sujets :**

- Mise en œuvre d'authentification EAP-TTLS pour les réseaux IEEE 802.xx
- Conception et développement d'une architecture HoneyPot 802.11
- Publication anonyme et échanges sur Internet (P2P anonyme, Créations de communautés privées, ...)
- Expérimentation de Sécurité et Téléphonie sur IP
- Mise en œuvre et test d'un outil IDS/IPS dans un environnement P2P pour l'identification de comportements malveillants
- Etude et synthèse des failles de sécurité créées lors du développement d'une application
- Sécurisation d'un système d'exploitation Linux

### **Responsable :**

Dr Olivier PAUL (Olivier.Paul@it-sudparis.eu)

### **Encadrants :**

Equipe pédagogique de la voie d'approfondissement SSR