Voie d'Approfondissement

Sécurité des Systèmes et des Réseaux

(VAP SSR)

Directeur de Programme :

Prof. 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. *(Selon des chiffres publiés à la Convention de la Sécurité en Juin 2005, le Cabinet britannique CANALYS a estimé que le marché européen de la sécurité a eu une croissance de 27 % en 2005.)* 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.). A l'heure actuelle, l'Europe ne forme que 25% des spécialistes en SSI dont elle aurait besoin dans les années à venir.

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 du 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 et de détection
- 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 et systèmes 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 S9. Ce projet représente une charge de travail de 225 heures.

Programme :

Semestre 8

- NET5038 : Introduction à la sécurité des réseaux
- NET5039 : Systèmes, virtualisation et sécurité

Semestre 9

- NET5531 : Evaluation des Risques et Détection des Attaques
- NET5532 : Authentification, VPN et Chiffrement
- NET5533 : Filtrage
- NET5534 : Sécurité des Applications et des Services
- NET5535 : Projet d'Approfondissement de la VAP SSR

Equipe pédagogique Télécom SudParis:

- Maryline LAURENT
- Christian BAC
- Hervé DEBAR
- Abdallah M'HAMED
- Patrick MAIGRON
- Olivier PAUL
- Grégory BLANC
- Vacataires industriels de la VAP

NET5038 Introduction à la sécurité des réseaux

Période : S8 / P3 **ECTS :** 4 **Langue :** Français

Organisation :

- Heures programmées / Charge Totale : 45/90
- Heures Cours/TD+TP/P/CF : 21/15/12/3

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 individuellement ou en binôme (voire exceptionnellement en trinôme).

Evaluation :

La validation de cette UV se fait grâce à une étude de cas notée (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 influe sur la note finale.

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

L'UV est validée si la note finale est ≥ 10 / 20

Objectifs :

- Consolider les connaissances de bases des mécanismes réseaux, indispensables à la compréhension des mécanismes de sécurité informatique
- Appréhender la sécurité des réseaux (entreprise, opérateur et domestique)
- Comprendre la règlementation et la stratégie de la sécurité en France
- Réaliser un projet bibliographique en anglais sur un sujet sécurité (1ère partie)

Compétences selon référentiel CDIO :

1.2 Connaissances des principes fondamentaux d'ingénierie
1.3 Connaissances avancées en ingénierie : méthodes et outils
2.1 Raisonnement analytique et résolution des problèmes
2.3 Pensée systémique
2.4 Attitudes et apprentissages

Mots clefs :

Menaces, vulnérabilités, cybersécurité, réseaux, réglementation

Prérequis :

Connaissance des réseaux TCP/IP et architectures associées (routage, nommage), Connaissance des architectures de service (Web, VoIP, DNS, LDAP)

Programme :

- Rappels TCP/IP : architecture, adressage, routage, services réseaux, etc.
- Initiation aux VPNs et à la sécurité réseaux
- Protection de la vie privée et Cybersurveillance
- Cybersécurité

- Traitement d'incidents de sécurité : cycle de vie des vulnérabilités et stratégie nationale de défense
- Sécurité des protocoles réseaux (HomeNetwork, FemtoCell, WPAN, etc.)
- Sécurité et LDAP
- Projet bibliographique (poursuivi et évalué en NET5039)

Supports de cours et bibliographie :

Supports de cours :

Polycopiés des interventions fournis par les intervenants

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 :

Abdallah M'HAMED (abdallah.mhamed@telecom-sudparis.eu)

Intervenants :

- Equipe pédagogique de la VAP SSR
- Intervenants extérieurs : ANSSI, Orange, etc.

NET5039 Systèmes, virtualisation et sécurité

Période : S8 / P4 **ECTS :** 4 **Langue :** Français

Organisation :

- Heures programmées / Charge Totale : 45/90
- Heures Cours/TD+TP/CF : 18/24/3

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.

Evaluation :

La validation de cette UV se fait grâce à un rapport de mini projet (R), une soutenance (S) et un contrôle final (CF) de 3h qui a lieu à la fin de l'UV.

La note de rapport de mini-projet (R) est commune au binôme ; la note de soutenance (S) peut être individualisée en fonction de la participation.

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

La présence aux heures programmées est obligatoire, et influe sur la note finale.

Note finale = Moy (¼ R, ¼ S, ½ CF)

L'UV est validée si la note finale est ≥ 10 / 20.

Objectifs :

- Consolider les bases informatiques nécessaires à la compréhension des attaques (architecture système, architecture web, systèmes d'exploitation, virtualisation)
- Comprendre la sécurité du poste de travail et des différents outils et logiciels associés : messagerie, navigateur
- Comprendre les mécanismes d'attaque des systèmes en ligne (injection SQL, Cross-Site Scripting, etc.) sur des applications réelles et les mettre en œuvre.
- Réaliser un projet bibliographique en anglais sur un sujet SSI (2eme partie)

Compétences selon référentiel CDIO :

1.2 Connaissances des principes fondamentaux d'ingénierie
1.3 Connaissances avancées en ingénierie : méthodes et outils
2.1 Raisonnement analytique et résolution des problèmes
2.3 Pensée systémique
2.4 Attitudes et apprentissages

Mots clefs :

Système, Internet, architecture, poste client, attaques

Prérequis :

Connaissance des environnements web et des architectures associées (Apache, MySQL), des ordinateurs et des systèmes d'exploitation (Unix, Windows)

Programme :

- Architecture matérielle et logicielle des ordinateurs : sécurité du poste de travail
- Architecture des services et applications web : sécurité des services en réseau
- Architecture des systèmes d'information
- Sécurité des navigateurs
- Attaques web et « Capture the Flag »
- Sécurité des emails : PGP, S/MIME
- Projet bibliographique

Supports de cours et bibliographie :

Supports de cours :
- Polycopiés des cours fournis par les intervenants

Bibliographie :
- Dave Wreski, *Linux Security HOW TO*, http://tldp.org/HOWTO/html_single/Security-HOWTO/, 2004
- Linux Security HOWTOs, http://www.linuxsecurity.com/
- Linux Security for Beginners, http://www.linuxtopia.org/LinuxSecurity/, 2010
- Solange Ghernaouti-Hélie, *Sécurité informatique et réseaux*, DUNOD , ISBN 978-2-10-052156-2

Responsable :

Joaquin GARCIA-ALFARO (joaquin.garcia-alfaro@telecom-sudparis.eu)

Intervenants :

- Equipe pédagogique de la VAP SSR
- Intervenants extérieurs : ANSSI, Cassidian, Orange, Solucom, Technicolor, etc.

NET5531 Evaluation des risques et détection des attaques

Période : S9 / P1 **ECTS :** 4 **Langue :** Français

Organisation :

- Heures programmées / Charge Totale : 45/90
- Heures Cours/TD+TP/P/CF : 24/18/0/3

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 influe sur la note finale.

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

L'UV est validée si la note finale est ≥ 10 / 20

Objectifs :

- Évaluer 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)
- Appréhender la démarche et les outils d'audit d'un réseau
- Comprendre les attaques web et utiliser des outils de prévention et/ou détection
- Concevoir et appliquer une politique de sécurité grâce à des méthodologies et des modèles de sécurité

Compétences selon référentiel CDIO :

1.2 Connaissances des principes fondamentaux d'ingénierie
1.3 Connaissances avancées en ingénierie : méthodes et outils
2.1 Raisonnement analytique et résolution des problèmes
2.3 Pensée systémique
2.4 Attitudes et apprentissages

Mots clefs :

Attaques, menaces, audit, intrusions, détection, modèle, méthodologie

Prérequis :

Bonnes connaissances des réseaux TCP/IP et des architectures associées (routage, nommage), des environnements web et des architectures associées (Apache, MySQL), des ordinateurs et des systèmes d'exploitation (Unix, Windows, virtualisation).

Programme :

- Sécurité des réseaux : menaces et parades
- Méthodologies d'Analyse des Risques
- Modèles de Sécurité
- Audit
- Détection d'intrusions

Supports de cours et bibliographie :

Supports de cours :
- Polycopiés des cours fournis par les intervenants

Bibliographie :
- Solange Ghernaouti-Hélie, *Sécurité informatique et réseaux*, DUNOD , ISBN 978-2-10-052156-2

Responsable :

Grégory BLANC (gregory.blanc@telecom-sudparis.eu)

Intervenants :

- Équipe pédagogique de la VAP SSR
- Intervenants extérieurs : BNP Paribas, Bull, Société Générale, Orange, etc.

NET5532 Authentification, VPN et chiffrement

Période : S9 / P2 **ECTS :** 4 **Langue :** Français

Organisation :

- Heures programmées / Charge Totale : 45/90
- Heures Cours/TD+TP/CF : 30/12/3

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 influe sur la note finale.

Note finale = Moy (¾ CF, ¼ TP)

L'UV est validée si la note finale est ≥ 10 / 20

Objectifs :

- Savoir mettre en œuvre les services d'authentification et de chiffrement
- Connaître les mécanismes de gestion d'identité (SSO - Single Sign On) et d'infrastructures de clefs publiques (PKI)
- Connaître les mécanismes utilisés dans les VPNs (Virtual Private networks)
- Etre capable de configurer des VPNs basés sur IPsec
- Comprendre la cryptographie, connaître les algorithmes de chiffrement les plus couramment utilisés et comprendre les mécanismes avancés
- Comprendre les bases et les enjeux de sécurité des protocoles associés aux nouveaux services

Compétences selon référentiel CDIO :

1.2 Connaissances des principes fondamentaux d'ingénierie
1.3 Connaissances avancées en ingénierie : méthodes et outils
2.1 Raisonnement analytique et résolution des problèmes
2.3 Pensée systémique
2.4 Attitudes et apprentissages

Mots clefs :

Authentification, cryptographie, VPN, PKI, SSO, IAM

Prérequis :

Bonnes connaissances des réseaux TCP/IP et des architectures associées (routage, nommage), des environnements web et des architectures associées (Apache, MySQL), des ordinateurs et des systèmes d'exploitation (Unix, Windows,

virtualisation), des vulnérabilités et des mécanismes d'attaque, des mécanismes d'audit et d'analyse des risques.

Programme :

- Architecture et protocoles d'authentification (EAP, AAA)
- Solutions PKI et SSO (Single Sign On), protocoles d'authentification
- Cryptographie : mécanismes mathématiques et algorithmes de base, algorithmes avancés, protocoles et applications
- VPN (Réseaux privés virtuels) et IPsec
- Mise en œuvre d'un VPN et du NAT
- Protocoles de Sécurité

Supports de cours et bibliographie :

Supports de cours :
- Polycopiés des cours fournis par les intervenants

Bibliographie :
- H. Chaouchi, M. Laurent, Ed. : *La sécurité dans les réseaux sans fil et mobiles* , Traité IC2, série Réseaux et télécoms, 3 volumes, Éd. Lavoisier, ISBN 978-2-7462-1697-6, ISBN 2 978-2-7462-1698-3, ISBN 3 978-2-7462-1699-0, mai 2007.
- W. Cheswick, S. Bellovin et A. Rubin : *Firewalls and Internet Security, Repelling the Wily Hacker*, Second Edition. Addison-Wesley Professional, 2003. M. Laurent : *Introduction à la Sécurité des Systèmes d'Information*, Techniques de l'Ingénieur, Sécurité des systèmes d'information, H5000, oct. 2011.
- M. Laurent : *La suite de protocoles IPsec au service des VPN et de la mobilité*, Technique de l 'ingénieur, Sécurité des systèmes d'information, TE7545v2, 2007.
- E. Rescorla : *SSL and TLS : Designing and Building Secure Systems*, Addison-Wesley, 2nd Edition, March 2001.
- Schneier B : *Cryptographie Appliquée*, Second Edition. 1996
- S. Ghernaouti-Hélie : *Sécurité informatique et réseaux*, DUNOD, ISBN 978-2-10-052156-2, 2011.
- C. Tessereau : *La sécurité des transactions par les protocoles SSL/TLS*, Technique de l 'Ingénieur, Traité SSI H5230, 2005.
- P. Thoniel : *Méthodes d'authentification*, Techniques de l'ingénieur, Traité SSI, H5535, 2009.

Responsable :

Maryline LAURENT (maryline.laurent@telecom-sudparis.eu)

Intervenants :

- Equipe pédagogique de la VAP SSR
- Intervenants extérieurs : ANSSI, Cassidian, Orange, Solucom, Technicolor, etc.

NET5533 Filtrage

Période : S9 / P3 **ECTS :** 4 **Langue :** Français

Organisation :

- Heures programmées / Charge Totale : 45/90
- Heures Cours/TD+TP/CF : 15/27/3

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 rapport noté en binôme (TP) et par une étude de cas réalisée par binôme en TD, incluant une présentation orale (TD).

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

La présence aux heures programmées est obligatoire, et influe sur la note finale.

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

L'UV est validée si la note finale est ≥ 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.

Compétences selon référentiel CDIO :

1.2 Connaissances des principes fondamentaux d'ingénierie
1.3 Connaissances avancées en ingénierie : méthodes et outils
2.1 Raisonnement analytique et résolution des problèmes
2.3 Pensée systémique
2.4 Attitudes et apprentissages

Mots clefs :

Filtrage, firewall

Prérequis :

Bonnes connaissances des réseaux TCP/IP et des architectures associées (routage, nommage), des environnements web et des architectures associées (Apache, MySQL), des ordinateurs et des systèmes d'exploitation (Unix, Windows, virtualisation), des vulnérabilités et des mécanismes d'attaque, des mécanismes d'audit et d'analyse des risques, des mécanismes de gestion d'identité et de chiffrement, des mécanismes de détection d'intrusions.

Programme :

- 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).
- Déni de Service (classification, prévention, détection, traçage, suppression).
- Mise en œuvre de filtrage à base de routeurs.
- Mise en œuvre de filtrage avancé à base de firewalls.
- Etude de cas sur la mise en œuvre d'architectures réseaux sécurisées (opérateur et entreprise)

Supports de cours et bibliographie :

Supports de cours :
- Polycopiés des cours fournis par les intervenants

Bibliographie :
- Elizabeth D. Zwicky, S. Cooper, and D.B. Chapman,*Building Internet Firewalls*, (2nd Edition), 2000.
- W. R. Cheswick, S. M. Bellovin and A.D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker*, Second Edition, 2003.
- Solange Ghernaouti-Hélie, *Sécurité informatique et réseaux*, DUNOD, ISBN 978-2-10-052156-2

Responsable :

Olivier PAUL (olivier.paul@telecom-sudparis.eu)

Intervenants :

- Equipe pédagogique de la VAP SSR
- Intervenants industriels (Checkpoint, etc.)

NET5534 Sécurité des applications et des services

Période : S9 / P4 **ECTS :** 4 **Langue :** Français

Organisation :

- Heures programmées / Charge Totale : 45/90
- Heures Cours/TD+TP/CF : 21/21/2

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 influe sur la note finale.

Note finale = Moy (CF, TP)

L'UV est validée si la note finale est ≥ 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.
- Connaitre la sécurité des systèmes d'exploitation Linux, et Windows, et les outils permettant de la gérer
- Comprendre le fonctionnement des virus

Compétences selon référentiel CDIO :

1.2 Connaissances des principes fondamentaux d'ingénierie
1.3 Connaissances avancées en ingénierie : méthodes et outils
2.1 Raisonnement analytique et résolution des problèmes
2.3 Pensée systémique
2.4 Attitudes et apprentissages

Mots clefs :

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

Prérequis :

Bonnes 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.

Programme :

- 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 des cours fournis par les intervenants

Bibliographie :
- Wreski D.: *Linux Security HOW TO*, http://tldp.org/HOWTO/html_single/Security-HOWTO/
- E. Skoudis and T. Liston : *Counter Hack Reloaded*, Prentice Hall, dec. 2005, pp. 784,
- S. McClure, J. Scambray and G. Kurtz : *Hacking Exposed*, Sixth Edition,McGraw-Hill, jan. 2009, pp. 720
- B. Hatch and J. Lee : *Hacking Linux Exposed*, McGraw-Hill, apr. 2005, pp. 692 pages,
- E. Filiol : *Les virus informatiques : théorie, pratique et applications*, SPRINGER, pp. 384, 2004
- R. Cannings, H. Dwivedi and Z. Lackey : *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)
- Solange Ghernaouti-Hélie, *Sécurité informatique et réseaux*, DUNOD, ISBN 978-2-10-052156-2

Responsable :

Christian BAC (christian.bac@telecom-sudparis.eu)

Intervenants :

- Equipe pédagogique de la VAP SSR
- Intervenants extérieurs : ANSSI, Cassidian, Orange, Solucom, Technicolor, etc.

NET5535	**Projet de la voie d'approfondissement SSR**	
Période : S9	**ECTS :** 8	**Langue :** Français

Organisation :

- Heures programmées / Charge Totale : 20/225

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

Chaque étudiant doit réaliser un projet en monôme ou binôme.

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.

Compétences selon référentiel CDIO :

- 1.3 Connaissances avancées en ingénierie : Méthodes et outils
- 2.1 Raisonnement Analytique et résolution de problèmes
- 2.4 Attitude et apprentissages
- 3.2.3 Communication écrite
- 3.2.6 Présentations orales

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).

Note finale = Moy (E, S))

L'UV est validée si la note finale est ≥ 10 / 20

Exemples de sujets :

- Mise en œuvre d'authentification EAP-TTLS pour les réseaux IEEE 802.xx
- Elaboration d'une méthode de comparaison de contenus web pour la détection des attaques de phishing/pharmingCloud storage et chiffrementConfidentialité des informations de géolocalisation pour les smartphonesMise 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
- Validation formelle de protocoles de sécurité.
- Cryptographie « ID-based ».
- Conception d'une architecture ToIP sécurisée

Responsable :

Olivier PAUL (olivier.paul@telecom-sudparis.eu)

Encadrants :

- Equipe pédagogique de la VAP SSR
- Encadrants extérieurs : ANSSI, Cassidian, Orange, Solucom, Technicolor, etc.