Choisir 1 sujet pour le Travail Personnel
à rendre sous forme électronique à riguidel@enst.fr avant le 23 - 11 - 2006

Sujet pour le Contrôle Continu

Numéro	Sujet	1er étudiant	2ème étudiant	3ème étudiant
S01	La sécurité de Windows (Vista)			
S02	La sécurité de Singularity (nouvel OS de Microsoft)			
S03	Les modèles formels de sécurité			
S04	Les modèles de la confiance			
S05	Les modèles de confiance inter-domaine (ebay, P2P)			
S06	Les modèles de réputation			
S07	Les modèles formels de contrôle d'accès			
S08	Les applications des modèles de sécurité multi-niveaux dans les Systèmes d'exploitation			
S09	Les applications des modèles de sécurité multi-niveaux dans les Bases de Données			
S10	La sécurité de l'administration électronique (gouvernementale)			
S11	La détection des attaques et des pannes dans les grands systèmes			
S12	Les techniques de protection des infrastructures critiques			
S13	Les techniques de DRM			
S14	Les techniques pour contrecarrer le piratage de téléchargement sur Internet			
S15	La protection des archives sur une longue période			
S16	L'acceptabilité de la sécurité (ergonomie, aspects éthiques)			
S17	Statistiques et typologie des attaques			
S18	L'économie de la sécurité et de la non-sécurité			
S19	La sécurité des solutions proposées pour la fédération d'identités ("Liberty Alliance", OpenID)			
S20	La gestion de l'identité, en général			
S21	Les cartes d'identité biométriques			
S22	Le management de l'identité (d'une personne)			
S23	La protection de l'identité (vie privée)			
S24	les techniques d'anonymisation			
S25	La gestion des problèmes de sécurité et de vie privée par les organisations gouvernementales			
S26	La sécurité de la sphère privée (modèles de privacy)			
S27	Les intrusions dans la vie privée avec GoogleEarth, le géoréférencement, la géolocalisation			
S28	La sécurité contre les malwares et les logiciels d'espionnage			
S29	La sécurité des mondes virtuels			
S30	Les attaques et la sécurité sur le Web 2 , Second Life, Facebook			
S31	Les attaques et la sécurité sur BitTorrent, eDonkey, eMule			
S32	La sécurité des structures et architectures virtuelles (organisations, grilles, communautés)			
S33	La sécurité de l'internet du futur			
S34	La confiance dans les logiciels et les preuves dans les calculs et les communications			
S35	Les méthodes d'authentification nouvelles (multimodale)			
S36	Comment implémenter l'imputabilité (accountability) et la non-répudiation			
S37	la sécurité du web sémantique			
S38	La protection des biens numériques (fichier, etc)			
S39	La sécurité du P2P			
S40	L'auditabilité (exploitation des journaux d'enregistrement .log)			
S41	Les attaques récentes sur le DNS, et sa sécurité			
S42	Les attaques de déni de service sur les serveurs gouvernementaux (Estonie, Géorgie, etc)			
S43	La sécurité de Skype			
S44	La sécurité des cartes sans contact			
S41	Protocoles Zero-Knowledge et identification			
S42	Utilisation de la mobilté pour plus de sécurité			
S43	Sécurité opportuniste: profiter de l'envrionnement multi-technologique pour la sécurité			
S44	Fouille de données et identification d'incident à une grande échelle			
S45	Techniques d'identification de déni de service distribué chez les opérateurs			
S47	Utiliser les arbres d'attaques pour quantifier la sécurité d'un système			
S49	IA et sécurité: filtrage bayesien, inférence, réseaux de neurones pour l'identification des incidents			
S50	Mécanismes utilisés en pratique contre le SPAM			