

Sécurité des systèmes d'exploitation

Introduction

Plan

- Informations pratiques
- Sécurité des systèmes d'exploitation
- Approche normalisée : les critères communs

Informations pratiques

- Page Moodle SSE (Sécurité des Systèmes d'Exploitation)
 - <https://foad.univ-rennes1.fr/course/view.php?id=1006874>
- 8 séances de cours magistral
 - Salle B12D i-51
- 8 séances de TP/TD
 - Animées par Josselin Mariette
 - Salles B12D i-204 et i-205
 - Nombre de machines restreint (18)
 - Machines virtuelles Virtual Box mises en ligne avant les TP (lien sur la page Moodle)

Informations pratiques

- Évaluation en 3 parties
 - 1er examen (4 points) le 4/12 (30 minutes)
 - Examen final (20 points) le 25/01 (2h)
 - TP/TD (6 points)
- Les examens portent sur le contenu des cours et des TP/TD

Sécurité des systèmes d'exploitation

- Système d'exploitation ?
 - Définition (selon Andrew Tanenbaum) : couche logicielle dont le rôle est de gérer tous les périphériques et de fournir aux programmes utilisateur une interface simplifiée du matériel
- Le cours cible
 - les systèmes basés sur un noyau Linux
 - Sauf Android et systèmes embarqués
 - les systèmes Windows

Sécurité des systèmes d'exploitation

- Sécurité et système d'exploitation ?



Sécurité des systèmes d'exploitation

- Concept de « Trusted Computing Base »
 - Ensemble des composants matériels et logiciels qui sont responsables de l'application de la politique de sécurité (i.e. critiques pour la sécurité d'un système).
 - Tout défaut ou vulnérabilité au sein de la TCB peut compromettre la sécurité du système
 - La conception et l'implémentation doivent faire l'objet d'une attention particulière
 - Limitation/réduction de la taille de la TCB pour faciliter l'audit, l'utilisation de méthodes (semi-)formelles ...

Sécurité des systèmes d'exploitation

- Quelle TCB sur les systèmes courants ?
 - Idéalement le matériel, un sous-ensemble du noyau et le moniteur de référence
- En pratique :
 - tout ce qui est dans l'espace noyau (y compris les pilotes tiers)
 - des services en espace utilisateur, notamment
 - Pour Windows, le service LSASS
 - Pour Linux, login et les binaires associés à l'authentification
 - Cf. article *Reflections on Trusting Trust*, Ken Thompson, 1984

Approche normalisée : les critères communs

- Critères communs (CC)
 - <https://www.commoncriteriaportal.org/>
- Processus d'évaluation CC ayant pour but d'éditer un rapport impartial
 - rédigé par un centre d'évaluation (ITSEF, *IT Security Evaluation Facilities*),
 - indiquant si la cible d'évaluation (TOE, *Target of Evaluation*) satisfait à la cible de sécurité (ST, *Security Target*),
 - avec un degré de confiance préalablement défini lors de la déclaration du niveau d'évaluation (EAL, *Evaluation Assurance Level*).
 - 7 niveaux : EAL1 à EAL7

Approche normalisée : les critères communs

- *Common Criteria – Mutual Recognition Arrangement (CC-MRA)*
 - 1ère version : mai 2000
 - version en vigueur : juillet 2014
 - Un arrangement, pas un traité
 - son application dépend de la bonne volonté des États
- Finalité de l'accord CC-MRA
 - s'assurer que les évaluations des produits sont effectuées à des niveaux élevés de qualité
 - augmenter la confiance de ces produits
 - éliminer les multiples évaluations
- Reconnaissance mutuelle jusqu'à EAL 4 (*)

Approche normalisée : les critères communs

- Pays émetteurs de certificats
 - En Amérique
 - Canada, États-Unis
 - En Asie
 - Corée du sud, Inde, Japon, Malaisie, Turquie
 - En Europe
 - Allemagne, Espagne, France, Italie, Norvège, Pays-Bas, Royaume Uni, Suède
 - En Océanie
 - Australie, Nouvelle-Zélande
- Pays reconnaissant les certificats
 - Autriche, Danemark, Éthiopie, Finlande, Grèce, Hongrie, Israël, Pakistan, Qatar, République tchèque, Singapour

Approche normalisée : les critères communs

- En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est chargée de mettre en œuvre l'arrangement CC-MRA.
 - Désignée autorité de certification « Critères Communs » par le décret n°2002-535 du 18 avril 2002.
 - <http://www.ssi.gouv.fr/administration/produits-certifies/cc/>
- Centres d'Évaluation de la Sécurité des Technologies de l'Information (CESTI)
 - Laboratoires agréés par le Premier ministre et accrédités par le Comité français d'accréditation (COFRAC) selon la norme NF EN ISO/CEI 1702

Approche normalisée : les critères communs

- Corpus documentaire :
 - CC
 - *Part 1 Introduction and general model*
 - *Part 2 Security functional components*
 - *Part 3 Security assurance components*
 - CEM (*Common Evaluation Methodology*)
 - Dernière mise à jour : version 3.1 révision 5 (avril 2017)
 - <http://www.commoncriteriaportal.org/cc/>

Approche normalisée : les critères communs

- Cible de sécurité (CC Part 1, annexe A)
 - regroupe les exigences de sécurité et de spécifications qui seront utilisées comme base pour l'évaluation :
 - description de la TOE et de son environnement de fonctionnement, y compris les menaces auxquelles elle devra faire face ;
 - description des objectifs de sécurité accompagnés des exigences de sécurité fonctionnelles et exigences d'assurance ;
 - description des fonctions de sécurité et des mesures d'assurances ;
 - description de la façon dont le TOE répond aux objectifs de sécurité.

Approche normalisée : les critères communs

- Niveaux d'évaluation (CC Part 3)
 - EAL1 - functionally tested
 - EAL2 - structurally tested
 - EAL3 - methodically tested and checked
 - EAL4 - methodically designed, tested, and reviewed
 - EAL5 - semiformally designed and tested
 - EAL6 - semiformally verified design and tested
 - EAL7 - formally verified design and tested

Approche normalisée : les critères communs

- EAL 1

- EAL4

Assurance Class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

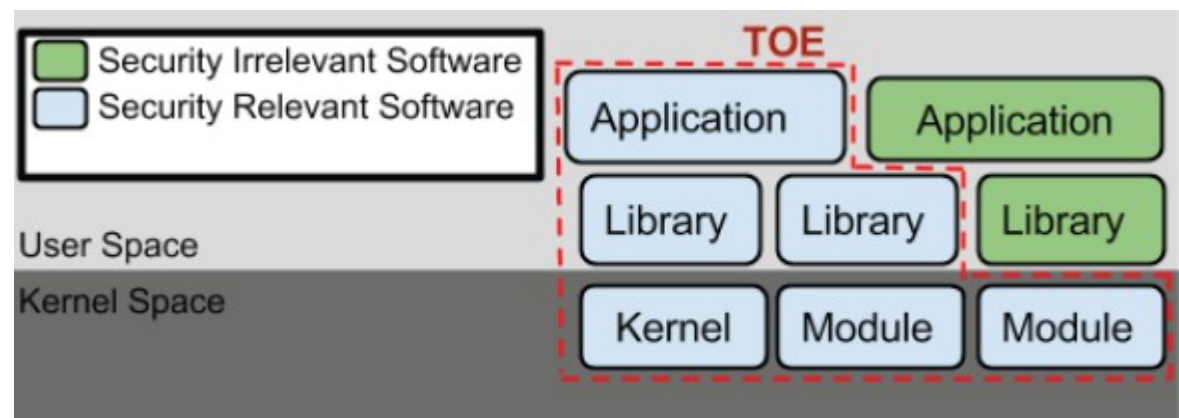
Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Approche normalisée : les critères communs

- Valeur des certificats délivrés
 - Ciblent une version précise de produit
 - Validité limitée dans le temps :
 - Maximum 5 ans
- **Approche ANSSI**
 - Version identique
 - Surveillance : revue régulière de l'analyse de vulnérabilité réalisée lors de l'évaluation initiale
 - Nouvelles versions :
 - Continuité de l'assurance : justifier que les évolutions du produit n'ont pas d'impact sur la sécurité du produit
 - Nouvelle certification : l'évaluation peut se faire en réutilisant certains résultats précédents

Approche normalisée : les critères communs

- Profil de protection : cible de sécurité générique ciblant une catégorie de produits
- *General Purpose Operating Systems*
 - Cible les postes utilisateurs, les serveurs et les systèmes de Cloud (hors couche de virtualisation)
 - Version 4.1 (mars 2016)
 - Le matériel sous-jacent est exclu du profil



Source : NIAP

Approche normalisée : les critères communs

- Menaces identifiées
 - Attaque réseau
 - L'attaquant peut initier des communications avec les applications et les services qui s'exécutent sur l'OS
 - Il peut également modifier des communications légitimes
 - Écoute réseau
 - L'attaquant peut surveiller et accéder aux données échangées par les applications et les services qui s'exécutent sur l'OS
 - Attaque local
 - Un attaquant peut compromettre des applications s'exécutant sur l'OS
 - Accès physique limité

Approche normalisée : les critères communs

- Objectifs de sécurité
 - Traçabilité
 - Intégrité
 - Gestion
 - Fourniture d'interfaces permettant d'administrer la sécurité
 - Stockage sécurisé
 - Communications sécurisées

Approche normalisée : les critères communs

- Exigences de sécurité fonctionnelles
 - Cryptographic Support (FCS)
 - Cryptographic Key Generation, Establishment & Destruction
 - Cryptographic Operation : Encryption/Decryption, Hashing, Signing, Keyed-Hash Message Authentication
 - Random Bit Generation
 - Storage of Sensitive Data
 - TLS Client Protocol
 - User Data Protection (FDP)
 - Access Controls for Protecting User Data
 - Information flow control

Approche normalisée : les critères communs

- Exigences de sécurité fonctionnelles (suite)
 - Security Management (FMT)
 - Management of security functions behavior
 - Protection of the TOE Security Functionality (FPT)
 - Access controls
 - Address Space Layout Randomization
 - Stack Buffer Overflow Protection
 - Boot Integrity
 - Trusted Update
 - Trusted Update for Application Software
 - Audit Data Generation (FAU)
 - Audit Data Generation

Approche normalisée : les critères communs

- Exigences de sécurité fonctionnelles (suite)
 - Identification and Authentication (FIA)
 - Authentication failure handling
 - Multiple Authentication Mechanisms
 - X.509 Certificate Validation & Authentication
 - Trusted Path/Channels (FTP)
 - Trusted channel communication
 - Trusted Path
- Exigences optionnelles
 - Default TOE access banners
 - Software Restriction Policies
 - Write XOR Execute Memory Pages

Questions ?

