Sécurité des Systèmes Informatiques

Politiques de sécurité administratives et logiques

TLS-SEC

Rodolphe Ortalo
CARSAT Midi-Pyrénées
rodolphe.ortalo@free.fr
(rodolphe.ortalo@carsat-mp.fr)
http://rodolphe.ortalo.free.fr/ssi.html

Politiques de sécurité

Politiques de sécurité du système d'information (PSSI)

Organisation dans une entreprise

- Un « responsable » (RSSI)
- Comité de sécurité informatique
- Groupes de travail
  - Mise en place de l'organisation SSI
  - Sensibilisation des utilisateurs
  - Audit et gestion des risques
  - Autorisation et actions de sécurité opérationnelle
  - Surveillance et contrôle
  - Veille technologique
  - *projet*
- Gestion de crise

Fonctions du RSSI

Cigref 2001

- Définition de la politique de sécurité
- Analyse de risques
- Sensibilisation et formation aux enjeux de la sécurité
- Étude des moyens et préconisations
- Audit et contrôle
- Veille technologique et prospective

Rôles de conseil, d'assistance, d'information, de formation et d'alerte.
Si possible indépendant de la direction informatique.

(Le point de vue d'un informaticien incompétent en matière de droit sur la) Législation

- La protection légale des informations nominatives est forte et obligatoire en France (CNIL/CIL) et en Europe
- L'utilisation du chiffrement est sujette à contrôle strict en France (ANSSI)
- Toutes les législations et conventions s'appliquent (au système d'information)
  - Lois, décrets, ordonnances, circulaires, …
  - Secret médical, secret bancaire, secret professionnel, …
  - Droit du travail, convention collectives, règlements intérieurs
  - Droit commercial, contrats, …
  - (Législation d'exception, antiterrorisme, interception, etc.)
- La jurisprudence arrive à son propre rythme
  - Signature et preuve numérique ne sont pas très éprouvés
  - Le rythme des défaillances de sécurité est différent
    - Défaillance MD5, autorités de certification, interceptions massives d'état... sans parler du spam bien sûr.
- La protection est d'abord sur le papier...

Les actions concrètes du RSSI

- www.cert.org, www.us-cert.gov, www.certa.ssi.gouv.fr
- Paramétrage du *firewall*
- Animation du comité de sécurité et des groupes de travail
- Documentation (PSSI, guides, etc.)
- Interaction avec les organismes extérieurs
- Sensibilisation à gogo

- Suivi des tests d'intrusion, gestion des autorisations

Traitement du risque ou simple gestion ?

Environnement de la SSI

- Internes ou associés
  - Direction
  - Service études
  - Service exploitation
  - Sous-traitants
  - Organismes nationaux
  - Tutelles
  - CE/DP
  - Service juridique
  - Maîtrise du risque
- Externes et indépendants
  - Justice
  - ANSSI (www.ssi.gouv.fr)
  - CNIL (www.cnil.fr)
  - CERT/CC (www.cert.org)
    US-CERT (www.us-cert.gov)
    CERTA (www.certa.ssi.gouv.fr)
    CERT-EU (cert.europa.eu)
  - CESTI
  - ENISA (www.enisa.europa.eu)
  - OCLCTIC (http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic)

L'Agence Nationale de la Sécurité des Systèmes d'Information

Des évolutions plus ou moins intéressantes:
http://www.ssi.gouv.fr/fr/anssi/publications/discours-de-patrick-pailloux-lors-de-la-conference-de-cloture-des-assises-de-la.html (lien local)

European Union Agency for Network and Information Security

enisa
European Network and Information Security Agency

http://www.enisa.europa.eu/

http://cybersecuritymonth.eu/

BE AWARE, BE SECURE.

Thank you for your interest in the European Cyber Security Month

This is an advocacy campaign taking place in October benefiting the citizens. It is supported by *ENISA* and *EC DG CONNECT* with the participation of many partners.

Surf, learn and get in touch!

October is CyberSecMonth!

- WEEK 1 Cyber Security Training for Employees
- WEEK 2 Creating a Culture of Cyber Security at Work
- WEEK 3 Code Week for All
- WEEK 4 Understanding Cloud Solutions for All
- WEEK 5 Digital Single Market for All

Cyber Security is a Shared Responsibility

242 Activities across 32 Countries

Building together a joint EU advocacy campaign on Cyber Security topics!

Différents documents

- Analyse des risques
- Politique de sécurité (PSSI)
- Spécifications de sécurité
- Guides de configuration ou de recette sécurité
- Synthèse/Suivi : alertes, filtrage, violations
- Tableau de bord ou audit/contrôle interne

Schéma directeur SSI

- Ensemble documentaire constitué par
  - PSSI (Politique de sécurité du syst. d'info.)
  - Spécifications ou règlements de sécurité par domaine
    - réseau, système, SGBD, développement, marchés, etc...
  - Guides pratiques et/ou points de validation
    - AIX 5.x, W2K Server SP4, IOS 12.x, Apache 1.2, etc.
  - Dossiers de sécurité des applications
    - paye, achats, compta., métier 1, métier 2, etc.
  - Gestion des risques (audit, suivi)
  - Tableau de bord
  - Plan d'action

PSSI

- Structure
  - Organisation et responsabilités
  - Intégration et interactions de la SSI
    - SSI et projets
    - SSI et exploitation
  - Objectifs de sécurité de l'organisme
  - Règles générales de sécurité
  - Gestion des risques

Modèle de PSSI diffusé par l'ANSSI

PSSIE « France » du 17/07/2014

- Domaines d'application
  - Communications
  - Violations
  - Vie privée
  - Achats de matériels
  - Messagerie
  - Maintenance
  - Audit
  - Communications
  - Identification
  - Authentification
  - Surveillance
  - Contrôle d'accès
  - Disponibilité
  - Réseau
  - …


Toulouse : Des Etoiles et d...
Yakovlev Yak-11 — Wikip...
Low Sec Lifestyle: CSM9 - ...
Bits of Bacon, Spaceships, ...
Le Premier ministre dote l'...
www.ssi.gouv.fr/fr/menu/actualites/le-premier-ministre-dote-l-etat-de-sa-premiere-politique-globale-de-securite.html
eve lego ship hurricane
English
ANSSI
Agence nationale de la sécurité des systèmes d'information
Que faire en cas d'incident ?
Le site du CERT-FR
Portail de la sécurité informatique/Documentation
L'ANSSI
La SSI
La défense des SI
Réglementation SSI
Guides et bonnes pratiques
Certification / Qualification
Produits et prestataires
Vous êtes ici : Accueil > menu > Actualités > Le Premier ministre dote l'Etat de sa première Politique globale de sécurité des systèmes d'information (PSSIE)
Le Premier ministre dote l'Etat de sa première Politique globale de sécurité des systèmes d'information (PSSIE)
29 août 2014
Portée par une circulaire du Premier ministre signée le 17 juillet 2014, la PSSIE fixe les règles de protection applicables aux systèmes d'information de l'État. Ce document est l'aboutissement de travaux pilotés par l'ANSSI qui s'appuient sur l'expérience des participants ministériels et de l'Agence en matière de prévention et de réaction aux attaques informatiques.
Essentiels à l'action publique, les systèmes d'information sont porteurs d'efficacité, mais aussi de risques : menaces d'exfiltration de données confidentielles, d'atteinte à la vie privée des usagers, voire de sabotage des systèmes d'information. Afin de prendre en compte ces risques, le Premier ministre a défini une politique volontariste, mais également pragmatique par laquelle l'État affiche sa volonté de se montrer exemplaire en matière de cybersécurité.
La PSSIE décline dix principes fondamentaux portant sur le choix d'éléments de confiance pour construire les systèmes d'information, sur la gouvernance de la sécurité et sur la sensibilisation des acteurs. Parmi ces principes, la circulaire met en exergue la nécessité pour les administrations de l'État de recourir à des produits et à des services qualifiés par l'ANSSI ainsi qu'à un hébergement sur le territoire national de leurs données les plus sensibles.
Chaque ministère est désormais responsable de l'application de la PSSIE qui entre en vigueur immédiatement. Celle-ci a également été conçue pour constituer une base méthodologique pour tout organisme ou institution, extérieur à l'État, ayant à élaborer un document de cette nature.
Plus d'information : La Politique de sécurité des systèmes d'information de l'Etat
Mise à jour du 29/08 : PSSIE au format PDF
Politique de Sécurité des Systèmes d'Information de L'état
PDF - 971.6 ko
REJOIGNEZ-NOUS
67 offres d'emploi
36 offres de stage
ALERTE
Attention escroquerie en ligne portant le logo de l'ANSSI !
Les alertes du CERT-FR
ANSSI © 2014
Flux RSS
Contacts
Informations éditeur
Aide et accessibilité
Presse
Actualités
Plan
www.legifrance.gouv.fr
Secrétariat général de la défense et de la sécurité nationale
Portail du gouvernement
Legifrance
Service public
France.fr

Caractéristiques d'une bonne PSSI

- Réaliste
- Applicable
- Vision à long terme
- Clarté et concision
- Basée sur des rôles ou des profils
- Définition claire des domaines de responsabilité et d'autorité
- À jour (revue périodiquement)
- Communiquée à tout le personnel

➔ *Jamais très évident...*

« Spécifications »

- Spécifications de sécurité
  - Clauses contractuelles
  - Charte déontologique et utilisateurs (finaux, administrateurs, etc.)
  - Composants réseau
  - Systèmes
  - Collecte des traces et « cybersurveillance »
  - Systèmes d'authentification
  - Application (*X*, *Y*, *Y*, etc.)
  - Données (*A*, *B*, *C*, *D*, etc.)

➔ *Parfois, les risques changent...*

Documents opérationnels

- Guides de configuration / Points de contrôles
- Déclinés précisément par :
  - Système d'exploitation
    SunOS 4, AIX 4, 5, Solaris 2.6, 2.7, 2.9, RedHat 6, 7, Debian 2.2, 3.0, OpenBSD 3.3, 3.4, etc.
  - Logiciel
    iPlanet, Apache 1.3, 2, IIS 4, 5, 6, etc.
  - Equipement
    Routeurs Cisco 36xx, Nortell 2430, 5430
- Couvre des éléments de configuration ou de vérification concrets

```
echo "0" > /proc/sys/net/ipv4/ip_forward                    Linux procfs
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
net.inet.ip.forwarding=0                                    (Open)BSD sysctl(.conf)
vm.swapencrypt.enable=1
```

➔ *La pérennité est une difficulté...*

Positionnement par rapport aux différents projets des entreprises

- Projets SSI
  - Associés à l'infrastructure de sécurité elle-même
  - Jonction avec les autres projets d'infrastructure
- Assistance aux projets
  - Apporter des compétences
  - Intégrer la démarche sécurité aux projets
  - Clauses contractuelles
- Validation et contrôle des projets
  - Identifier des vulnérabilités et des risques résiduels
  - Accorder des autorisations d'ouverture

Face au cycle de vie d'un projet

- Besoin détaillé ? ⟷ Prendre en compte la PSSI
- Étude ? → Spécifications sécurité
- Appel d'offres → Spécifications sécurité
- Développement
- Intégration
- Validation
- Exploitation ⟷ Configuration / Contrôle sécurité
- Maintenance ⟷ Suivi / Surveillance
- Démantèlement ? → Quid ?

Petit tuyau: www.dban.org
(Darik's Boot And Nuke)

Veille vs. Suivi

- Veille technologique
  - Alertes CERT (cf ci-avant)
  - Alertes des constructeurs
  - Nouvelles vulnérabilités
  - Nouvelles techniques de protection
- Suivi de la sécurité
  - Contrôles réguliers des vulnérabilités
  - Suivi des préconisations
  - Validation de certaines configurations (e.g.: présence des antivirus)

Synthèse – Tableau de bord

- Rendre compte
  - de la mise en place des règles
  - de l'efficacité des mécanismes de sécurité (et de leur rentabilité)
  - du niveau de vulnérabilité et de risque
  - des agressions
- Évaluer le niveau de maturité

- *Se rendre visible. Plaire aux autorités...*

Politiques de sécurité

Politiques de sécurité logiques

Politiques et modèles de sécurité

- La politique de sécurité
  - « *est l'ensemble des lois, règles et pratiques qui régissent la façon dont l'information sensibles et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique*. » [ITSEC, 1991]
  - physique, administrative, ***logique***
- Modèle de sécurité
  - Formalisme ou représentation mathématique
- Partition entre entités
  - actives: sujets *s*
  - passives: objets *o*

Politique de sécurité = objectifs + règles

- Objectifs de sécurité : exemples
  - confidentialité : le dossier médical ne peut être consulté que par le patient ou son médecin traitant
  - intégrité : un chèque de plus de 1000 doit être validé par un ordonnateur et un comptable
  - disponibilité : si la carte et le PIN sont valides, le distributeur de billet doit fournir l'argent dans les 30 secondes
- Règles de sécurité : exemples
  - un fichier ne peut être lu que par les utilisateurs autorisés par le propriétaire du fichier
  - un message de type « chèque de + de 1000€ » n'est valide que s'il est signé par P1 et T2 et que les signatures sont valides
  - l'insertion d'une carte lance automatiquement l'action

Cohérence d'une politique

- La politique est cohérente si, partant d'un état quelconque où les objectifs sont satisfaits, il n'est pas possible d'atteindre, en respectant les règles, un état où ils ne sont plus satisfaits
- Intérêts d'un modèle formel
  - Décrire de manière précise les objectifs et les règles
  - Prouver des propriétés sur la politique (cohérence, complétude, ...) et sur son implémentation par le système informatique

Logique déontique
(une logique modale)
P, **O**, **F**
($\Box$, $\Diamond$)

Politique, protection et contrôle d'accès

- Les règles doivent être mises en oeuvre par des mécanismes (matériels, logiciels)

- Facile à imaginer pour les règles du type « il est permis de... » ou « il est interdit de... » – mécanismes de protection – instructions privilégiées, contrôle d'accès à la mémoire, contrôle à l'ouverture des fichiers, etc.
  ➞ autorisation : confidentialité, intégrité

- Difficile pour les règles du type « il est obligatoire de... » ou « il est recommandé de... »
  ➞ actions automatiques, gestion de ressources : intégrité, disponibilité

Matrice de contrôle d'accès

[Lampson 1971]

- Machine à états : état = (S,O,M)
  - O ensemble d'objets
  - S ensemble de sujets ($S \subseteq O$)
  - $M(s,o)$ est l'ensemble des droits que le sujet s possède sur l'objet o
  - les droits sont pris dans un ensemble fini A

Modèle HRU (1976)

- Commandes de modification

  command $\alpha(x_1, x_2, ...x_k)$

  if $a' \in M(s',o')$ and $a'' \in M(s'',o'')$ and ... and $a^{(m)} \in M(s^{(m)},o^{(m)})$

  then op_1; op_2; ...; op_n

  end

  $a^{(i)} \in A$

  op_i: *create a into M(s,o)* *delete a from M(s,o)*

  create subject s *destroy subject s*

  create object o *destroy object o*

- Problème de protection (Q_0 sûr pour *a*)
  - *indécidable* dans le cas général
  - *décidable* pour les systèmes à mono-opération (*n*=1)

Politiques discrétionnaires et obligatoires

- Politique discrétionnaire
  - chaque objet *o* est associé à un sujet *s* précis, son propriétaire qui manipule les droits d'accès à sa discrétion
  - le propriétaire peut librement définir et transmettre ces droits à lui-même ou un autre utilisateur

- Politique obligatoire
  - règles discrétionnaires (droit d'accès)
  - *plus* : règles incontournables (habilitation)

Exemple : protection des fichiers UNIX

- Règles :
  1) un utilisateur peut créer librement des fichiers dont il devient propriétaire
  2) les droits d'accès à un fichier sont définis librement par le propriétaire : par exemple, il peut décider quels utilisateurs sont autorisés à lire le fichier
- Objectif :
  - "un utilisateur non-autorisé à lire un fichier ne peut obtenir aucune information contenue dans le fichier (même avec la complicité d'un utilisateur autorisé)" : impossible à garantir

$(2) \Rightarrow (4)$: (s1,f1,propriétaire) $\rightarrow$ (s2,f1,lire)

$(1+2) \Rightarrow (5)$: (s2,f2,créer) $\rightarrow$ (s2,f2,écrire)$\wedge$(s3,f2,lire)

$(4+5) \Rightarrow (6)$: (s2,f1,lire)$\wedge$(s2,f2,écrire)$\wedge$(s3,f2,lire) $\rightarrow$ (s3,k(f1),lire)

Inconvénient des politiques DAC

- Possibilité d'abus de pouvoir
  (par malveillance ou par maladresse) :
  - s'il est possible pour un utilisateur légitime d'accéder à certains objets ou d'en modifier les droits d'accès, il est possible qu'un cheval de Troie en fasse de même.
  - si un utilisateur a le droit de lire une information, il a (en général) automatiquement le droit de la divulguer à n'importe qui.
  - il est difficile de corriger les effets d'une divulgation…

Politiques d'autorisation obligatoires

MAC : "Mandatory Access Control"

- Des règles incontournables sont imposées, en plus des règles discrétionnaires

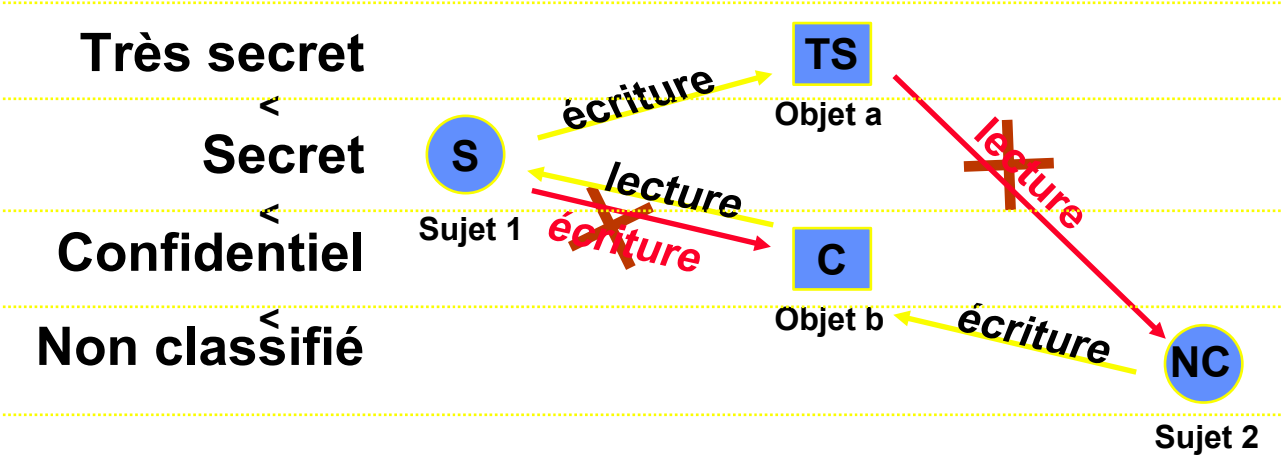
- Exemple : politique de confidentialité multi-niveau "militaire"
  des classes sont assignées aux utilisateurs (habilitation) et aux objets (classification). Une classe est définie par :

  un niveau (ordonné) :
  - non-classifié
  - confidentiel
  - secret
  - très secret

  et un compartiment = {catégories} :
  - crypto
  - nucléaire
  - OTAN
  - Bordurie / Syldavie
  - …

Politique multiniveau de Bell-LaPadula (1975)

- niveau (d'habilitation) des sujets *h(s)*
- niveau (de classification) des objets *c(o)*
- interdire les fuites d'information d'un objet vers un objet de niveau inférieur
- interdire à tout sujet d'obtenir des information d'un objet de niveau supérieur à son habilitation



Modèle de Bell-LaPadula

- classification *cl* : ensemble totalement ordonné
- compartiment *C* : ensemble de catégories
- $n=(cl,C)$, $n'=(cl',C')$: $n \preccurlyeq n' \Leftrightarrow cl \leq cl'$ et $C \subseteq C'$ (treillis)
- propriété simple

  $\forall s \in S,\ \forall o \in O,\ \text{read} \in M(s,o) \Rightarrow c(o) \preccurlyeq h(s)$
- propriété $\star$

  $\forall s \in S,\ \forall (o,o') \in O^2,\ \text{read} \in M(s,o) \wedge \text{write} \in M(s,o') \Rightarrow c(o) \preccurlyeq c(o')$

Inconvénients de Bell-LaPadula

- Surclassification : au fur et à mesure que l'information est traitée, sa classification augmente

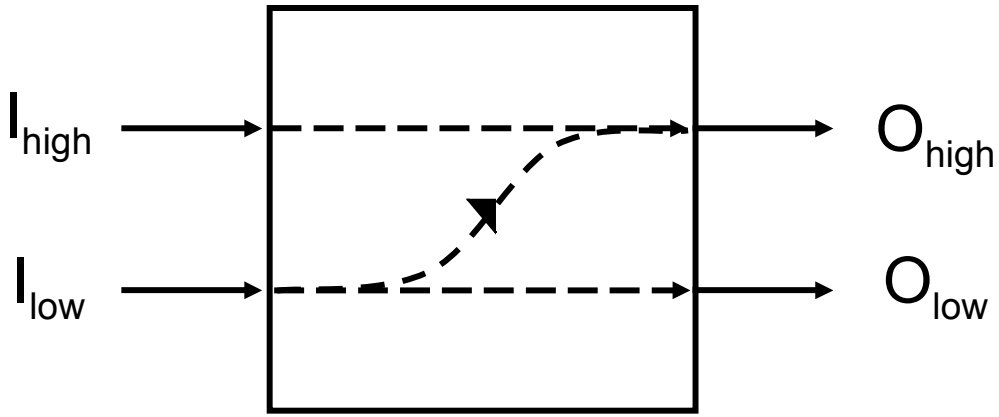
  $\Rightarrow$ "*trusted process*" pour déclassifier
- Variantes :
  - Habilitation flottante pour les *sujets* (à partir du login), mais habilitation fixe pour chaque utilisateur
  - Classification flottante pour les *objets*

- Le modèle ne représente pas tous les flux d'information et ne prend pas en compte les *canaux cachés*
  - Echanges d'information sur conventions implicites associées à l'utilisation de ressources partagées

Autres politiques de confidentialité

- “Muraille de Chine” :
  chez les agents de change (conflits d’intérêt)

- Modèle de non-interférence : O_{low} ne dépend pas d’I_{high}



Politiques de contrôle d'interface – Modèle

- ensemble *S* de sujets, ensemble Γ de commandes ou opérations, ensemble d'états Σ du système, σ_0 état initial
- un ensemble Out dont les éléments sont les sorties visibles par un utilisateur
- out : $\Sigma \times S \rightarrow$ Out do : $\Sigma \times S \times \Gamma \rightarrow \Sigma$
- **trace**, suite ordonnée de commandes
  $w \in traces = (S \times \Gamma)^*$
- [*w*] $\in \Sigma$ état atteint en partant de σ_0
- $\langle\ \rangle$, $\nu \cdot \gamma_1(u_1) \cdot \gamma_2(u_2) \cdot \ldots \cdot \gamma_n(u_n)$, $(\gamma_i)_{1 \le i \le n}$, $(u_i)_{1 \le i \le n}(u_i)$
- Γ_{out}, read(*u*), highin(*u*), lowout(*u*), lowin(*u*)

Non-interférence

[Goguen&Meseguer 1982]

- purge : S × traces → S

$$purge(u, \langle\rangle) = \langle\rangle$$

$$purge(u, hist \cdot command(u')) = \left\{ \begin{array}{l} purge(u, hist) \cdot command(u') \quad si\ h(u) \geqslant h(u') \\ purge(u, hist) \quad si\ h(u) < h(u') \end{array} \right\}$$

- propriété

$$\forall u \in S, \forall w \in traces, \forall c \in \Gamma_{out}$$

$$out(u, w \cdot c(u)) = out(u, purge(u, w) \cdot c(u))$$

- assez proche de l'intuition mais aussi très forte

Non-interférence & co.

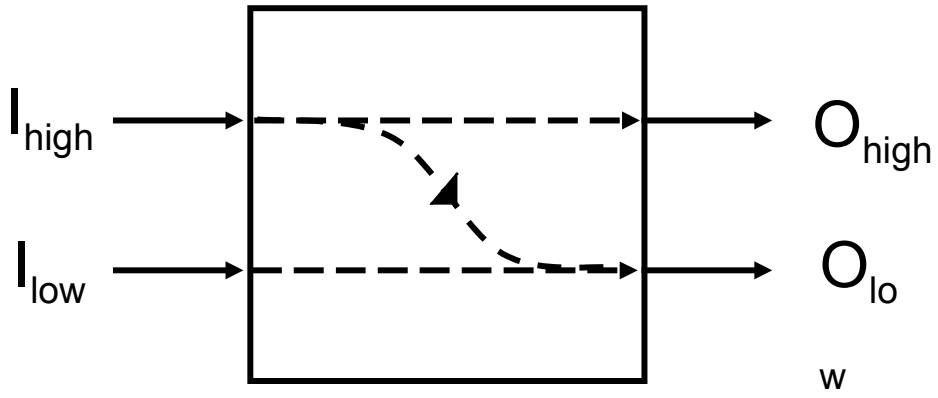
- Proche de l'intuition (vs. BLP)
  - interdit les canaux cachés
  - autorise des opérations (sans interférence)
- Limitations
  - interdit l'utilisation de canaux cryptographiques (même parfaits)
  - applicable seulement aux systèmes déterministes
- ***Non-déductibilité*** [Sutherland 1986] puis ***Non-interférence généralisée*** [McCullough 1987] visent les systèmes non-déterministes
- La ***restriction*** [McCullough 1990] vise à préserver la propriété en cas de composition de deux systèmes

Politique de Biba (intégrité)

- Multiple niveaux d'intégrité (crédibilité, vérification…)
  - à chaque sujet s_i correspond un niveau $is(s_i)$
  - à chaque objet o_j correspond un niveau $io(o_j)$
- Règles :
  - $(s_i, o_j, observer) \Rightarrow is(s_i) \leq io(o_j)$
  - $(s_i, o_j, modifier) \Rightarrow io(o_j) \leq is(s_i)$
  - $(s_i, s_j, invoquer) \Rightarrow is(s_j) \leq is(s_i)$
- Propriété : empêcher la *contamination* des niveaux élevés : diffusion de fausses informations, propagation d'erreur, …
- Inconvénient : dégradation progressive des niveaux d'intégrité
- Variantes : niveaux flottants, soit pour les sujets, soit pour les objets
- Modèle Totel : remonter le niveau par tolérance aux fautes

Autres politiques d'intégrité

- Politique de Clark-Wilson : (transactions financières)
  - Deux niveaux d'intégrité
    - UDI (données non contraintes)
    - CDI (données contraintes), vérifiables par des IVP (*Integrity Verification Procedures*), ne pouvant être manipulées que par des TP (*Transformation Procedures*) certifiées
  - Règles : listes de relations autorisées
    - CDI ↔ TP, Utilisateurs ↔ TP (avec éventuellement "*separation of duty*"), UDI ⟶ CDI par (TP+IVP)
- Modèle de non-interférence : O_{high} ne dépend pas d'I_{low}



Politiques de contrôle de flux

[Bieber&Cuppens 1992, d'Ausbourg 1994]

- *(o,t)* : entrées, sorties ou points internes (et temps)
- dépendance causale : $(o',t') \rightarrow (o,t)$ avec $t' < t$
- cône de causalité: $cone(o,t) = \{ (o',t') / (o',t') \rightarrow^* (o,t) \}$
- cône de dépendance: $dep(o,t) = \{ (o',t') / (o,t) \rightarrow^* (o',t') \}$
  - si *s* connait une sortie x_o il peut inférer $cone(x_o)$
  - si *s* connait une entrée x_i il peut inférer $dep(x_i)$

- confidentialité
- intégrité

$$\bigcup_{x_o \in O_s} cone(x_o) = Obs_s \subseteq R_s$$

$$\bigcup_{x_i \in A_s} cone(x_i) = Alt_s \subseteq W_s$$

Politiques basées sur les rôles

RBAC : *Role-Based Access Control*

- On définit des rôles, pour représenter des fonctions dans l'organisation
- On associe à chaque rôle les privilèges (ensemble de droits) nécessaires pour remplir la fonction
- On associe à chaque utilisateur le(s) rôle(s) qu'il peut jouer dans l'organisation

- Administration facilitée :
  - Les rôles et leurs privilèges changent rarement
  - Il suffit d'identifier les rôles que peut jouer un utilisateur

OrBAC : Organization-based AC

- Modèle conçu dans MP6 (Modèles et politiques de sécurité des systèmes d'information et de communication en santé et social) :
  Ernst & Young, IRIT, LAAS-CNRS, ONERA, ENST-Bretagne,…
- Abstractions :
  - User -> rôle
  - Objet -> vue
  - Action -> activité
- Liaisons entre niveaux abstrait (*politique*) & concret (*mécanismes de contrôle d'accès*) : définies par l'organisation
- Règles :
  - Définies au niveau abstrait
  - Permissions/interdictions + obligations
  - Validées par le contexte (concret)

Remerciements

- Yves Deswarte† (LAAS-CNRS)