SÉCURITÉS DE L'INFORMATION & ASPECTS ORGANISATIONNELS

Comment intégrer les différents aspects de la sécurité ?

Conférence de Gilles Trouessin - ACCESSS-IF
rapportée par Martine Otter

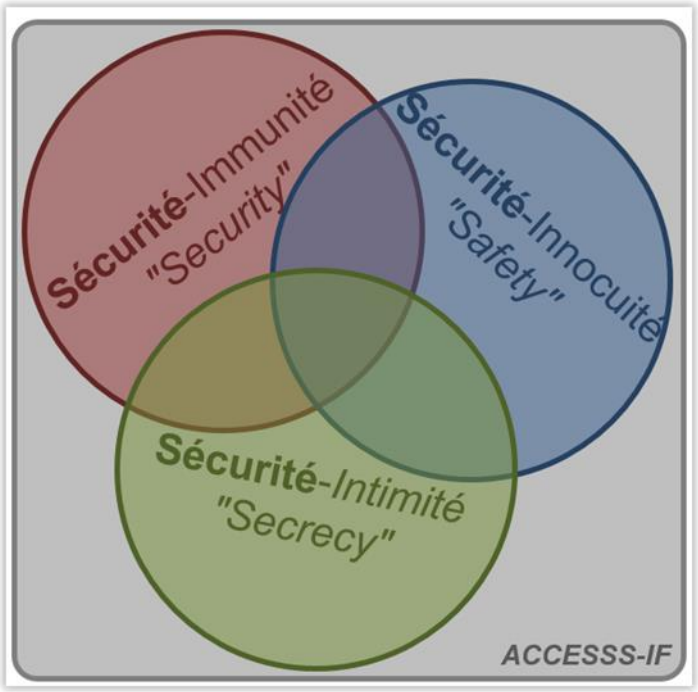
Gilles Trouessin conduit depuis plusieurs années une réflexion originale sur la sécurité de l'information, ou plutôt, comme il le précise ici, sur les 3 volets de la sécurité que sont l'immunité, l'innocuité et l'intimité. Dans un article paru en janvier 2001 dans la Lettre d'ADELI n°42, il nous brossait un panorama des différentes propriétés élémentaires que recouvre le terme de sécurité. Il nous a brillamment présenté une synthèse de ces travaux à l'occasion de l'assemblée générale 2014 d'ADELI qui s'est tenue le 12 janvier 2015.

L'objectif premier du travail présenté dans cet article est, avant tout, de contribuer à l'amélioration pragmatique de la prise en compte de l'ensemble des attentes potentielles pouvant relever des trois acceptions possibles de cette notion générique de « sécurité des systèmes » :

- ***la sécurité de systèmes d'information usuels (la sécurité-security), ici sécurité-immunité ;***
- ***la sûreté des systèmes informatiques critiques (la sécurité-safety), ici sécurité-innocuité ;***
- ***la protection des données à caractère personnel (la sécurité-secrecy), ici sécurité-intimité ; elle-même très étroitement liée au respect de la vie privée et intimité de la personne (la sécurité-privacy).***

L'objectif indirect de tout ce travail est, aussi et surtout, de chercher à comprendre les raisons de la prise en compte, manifestement trop compartimentée et très partielle, de ces trois acceptions possibles de la « sécurité des systèmes ».

Les 3 sécurités :



S-Immunité : Sécurité des Systèmes Informatiques / Systèmes d'Informations

Immunité [n.f.] : ensemble des mécanismes de défense d'un organisme contre les éléments étrangers à l'organisme, en particulier les agents infectieux (virus, bactéries ou parasites). [Larousse2014].

La première sécurité répond au besoin de protection des systèmes d'information. Elle a suscité l'élaboration de dispositifs normatifs de mieux en mieux adaptés à la maîtrise des risques :

- [TCSEC1983] & [TCSEC 1985], dans les années quatre-vingt, visant la « sécurité des systèmes d'exploitation » ;
- [ITSEC1991] & [ITSEM1993], des années quatre-vingt-dix, ciblant la « sécurité des technologies de l'information » ;
- [ISO15408], dans les années 2000, pour assurer la « sécurité des systèmes informatiques » ;
- et enfin la série des [ISO27***] des années 2010's, la plus récente, pour la « sécurité des systèmes de management d'informations ».

Au sens de J.-C. LAPRIE [Laprie1992] & [GSdF1995], il s'agit de la Sécurité-Confidentialité, caractérisée par la prédominance de la perception de confidence ; puis, au sens où l'entend Y. DESWARTE [Deswarte1991], elle s'appelle Sécurité-Immunité* , axée sur la tolérance face à tout maliciel (ou «malware») : ver, virus, cheval de Troie, bombe logique, etc.) ; elle sera nommée ici, indifféremment : sécurité-security, sécurité-immunité ou S-Immunité.

S-Innocuité : Sécurité des Personnes, Biens et Lieux Physiques

La deuxième sécurité est la « sécurité des systèmes critiques », qu'ils soient ou non informatisés. Développée à partir des années soixante-dix dans les milieux industriels pour éviter et traiter les défaillances, elle est directement issue du domaine de la recherche en sûreté de fonctionnement (ou «dependability») [Laprie1985] et elle est devenue l'un des attributs perceptifs de la sûreté de fonctionnement, complémentaire de la fiabilité et de la maintenabilité.

Au sens de Jean-Claude LAPRIE [Laprie1985] [GSdF1995], il s'agit de la Sécurité-Innocuité, caractérisée par la prédominance des risques de défaillances catastrophiques vis-à-vis, d'abord, de l'environnement mais aussi des personnes physiques ; elle sera nommée ici, indifféremment : sécurité-safety, Sécurité-innocuité ou S-Innocuité.

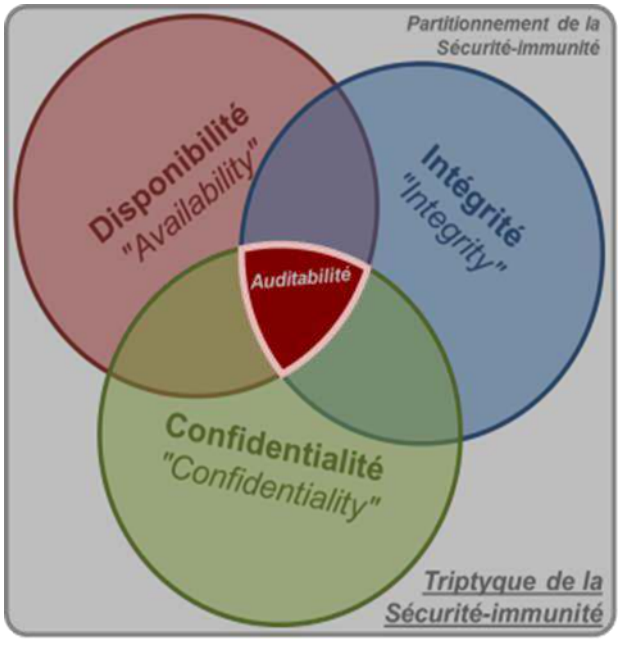
S-Intimité : Sécurité en Respect de l'Intimité et la Vie Privée de l'Individu

La troisième sécurité de la trilogie des « 3-Sécurités » est progressivement apparue depuis la fin des années soixante-dix, avec la publication de la loi relative à l'informatique, aux fichiers et aux libertés, dite « Loi Informatique & Libertés (LIL) » [L-IFL1978]. Elle est centrée sur le respect de l'intimité et de la vie privée des individus et se consacre donc exclusivement à la Protection des Données à Caractère Personnel (PDCP), à travers le respect absolu de la vie privée, tant dans sa réalité (exigence haute de respect de toute la confidentialité due à l'individu) que dans sa véracité (exigence forte d'intégrité vis-à-vis de toute exploitation).

Plus récemment, au plan européen depuis la Directive Européenne de 1995 [DPEC95/46/CE], et, surtout, au plan français avec son adoption en droit français par la révision de la LIL [L-PPP2004], il s'agit désormais de mettre en place des dispositifs visant à améliorer le respect de l'intimité « secrète » de l'individu tout au long de la chaîne collecte / traitement / exploitation / réutilisation / exportation /sauvegarde / archivage / publication de toute information relevant de la problématique de la PDCP. Elle sera nommée ici, indifféremment : sécurité-secrecy, Sécurité-inimité ou S-Intimité.

PROPRIÉTÉS DE LA « SÉCURITÉ-IMMUNITÉ »

Ces propriétés sont classiquement au nombre de trois : disponibilité, intégrité et confidentialité, auxquelles est venue s'adjoindre l'auditabilité qui permet la mise en place d'un système de preuves.



Disponibilité des données & services

La première propriété constitutive de la sécurité-security est la disponibilité ou « mise à disposition d'informations / données et/ou fonctions / services, excluant toute rétention non autorisée » [TCSEC1983] [TCSEC1985] [ITSEC1991] [FC-ITS1992-I] [FC-ITS1992-II] [CTCPEC1993] [ISO15408].
La totalité des secteurs d'activité utilisant des systèmes pour le traitement informatisé ou la manipulation d'informations (défense, militaire, bancaire, finance, marketing, industrie, énergie,

nucléaire, ferroviaire, aérien, spatial, médical, hospitalier, sanitaire, socio-sanitaire, médico-social, etc.) ont inévitablement de forts besoins de disponibilité, avec des niveaux d'exigences variables : notamment dans la sphère Santé/Social et tout particulièrement dans le secteur hospitalier [Cartau2012].

Intégrité des données & fonctions

La deuxième propriété constitutive de la sécurité-security est l'intégrité ou « non modification / altération d'information / données et/ou de fonctions / services, de façon non autorisée » [TCSEC1983] [TCSEC1985] [ITSEC1991] [FC-ITS1992-I] [FC-ITS1992-II] [CTCPEC1993] [ISO15408].
La quasi-totalité des secteurs d'activités traitant ou manipulant des informations, avec ou sans aide de systèmes de traitements informatisés ou de manipulation d'information font aussi appel au besoin d'intégrité à divers niveaux : notamment la sphère Santé/Social et ainsi que le secteur hospitalier [Cartau2012].

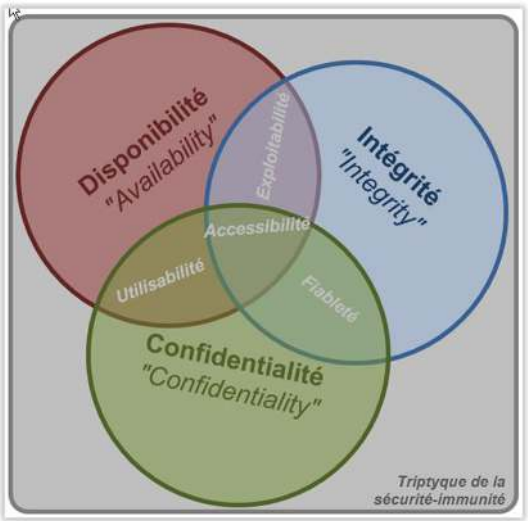
Confidentialité des données & traitements

La troisième propriété constitutive de la sécurité-security est la confidentialité ou « non divulgation / diffusion d'informations / données (voire des fonctions / services), de façon non autorisée » [TCSEC1983] [TCSEC1985] [ITSEC1991] [FC-ITS1992-I] [FC-ITS1992-II] [CTCPEC1993] [ISO15408].
Une grande majorité des secteurs d'activités traitant des données / informations, avec ou sans utilisation de systèmes de traitement informatisés ou de manipulation d'informations font aussi appel au besoin d'intégrité, à divers niveaux : tout particulièrement dans les domaines du médical ou du social [Cartau2012].

Auditabilité des Systèmes d'Information et de la Sécurité des Systèmes

Une quatrième propriété constitutive de la sécurité-security est l'auditabilité ou « capacité à auditer les systèmes d'information mis œuvre, ainsi que les mesures de sécurité de ces systèmes » [TCSEC1983] [TCSEC1985] [ITSEC1991] [FC-ITS1992-I] [FC-ITS1992-II] [CTCPEC1993] [ISO15408].
Une petite majorité des systèmes de traitement informatisés ou de manipulation d'informations intègrent peu ou prou, sinon déclarent plus ou moins, des besoins en matière d'auditabilité intrinsèque (traçabilité interne des activités intérieures au système), voire d'auditabilité extrinsèque (imputabilité de tout événement relevant de la sécurité-immunité). Au fil des deux dernières décennies, cette propriété d'auditabilité, qui n'est pas applicable aux données primaires (données-utilisateur, données-métier, données applicatives) mais plutôt réservée aux méta-informations (données de contrôle d'accès, données de supervision des systèmes, événement et d'incidents de sécurité), s'est ajoutée naturellement aux trois propriétés historiquement fondatrices de la propriété de (ou triptyque en ~) sécurité-immunité, pour composer l'acronyme désormais bien connu et reconnu suivant : D + I + C & A = Disponibilité + Intégrité + Confidentialité & Auditablité

Combinaisons des propriétés de sécurité-immunité

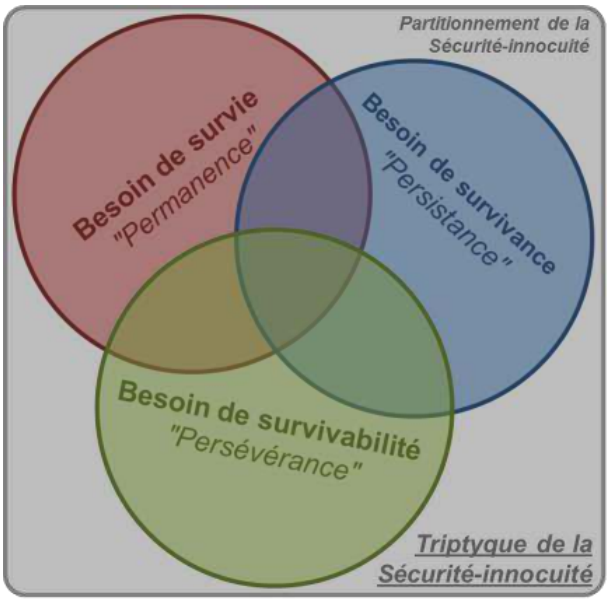


Les intersections des 3 critères présentés ci-dessus permettent de définir les propriétés combinées d'exploitabilité, « fiableté », utilisabilité, accessibilité.

- L'information n'est exploitable que si elle est disponible et intègre.
- Elle n'est fidèlement fiable que si elle est intègre et confidentielle.
- Elle n'est utilisable que si elle est disponible dans le respect de son niveau de confidentialité.
- L'information n'est accessible que si elle est intègre et disponible dans le respect de son niveau de confidentialité.

PROPRIÉTÉS DE LA « SÉCURITÉ-INNOCUITÉ »

Deuxième volet, celui de la Sécurité-innocuité, qui s'intéresse plus spécialement aux défaillances des systèmes, à leur prévention et à leur traitement. Là encore, une approche triptyque des propriétés est envisageable.



Garanties de survie (permanence de la Sécurité-innocuité)

Première exigence pour un système critique : ne pas subir de défaillance catastrophique pour l'environnement et les personnes physiques.
La première propriété de la « sécurité-innocuité » porte sur cette garantie de permanence :
Un système sûr de fonctionnement se doit de fonctionner tel que prévu… en permanence. Il s'agit ici de la garantie de survie de la Sécurité-innocuité, car il n'est pas envisageable et encore moins acceptable qu'un système dit « safe » (de « safety »), tel qu'un système de command-and-control d'une centrale nucléaire, d'un transport automatisé sans chauffeur ou de transport d'énergie ou d'opérateur de réseau de communication ou encore par exemple un système IRM hospitalier, puisse s'arrêter de fonctionner sans garantir une permanence minimale.

Garanties de survivance (persistance de la Sécurité-innocuité)

Deuxième exigence pour les systèmes critiques : pouvoir continuer de travailler sans interruption, même en mode dégradé, à la suite d'un sinistre, quelle que soit sa cause : panne, destruction, sabotage ou malveillance.
La deuxième propriété de la « sécurité-innocuité » concerne cette garantie de persistance :
Dans n'importe quelle circonstance, un système sûr de fonctionnement (au sens Sécurité-innocuité) se doit ainsi de continuer à fonctionner avant de passer dans un état sûr dit « sauf » (au sens de « survivant

»). Il s'agit ici de garantir la survivance de la Sécurité-innocuité, car il n'est pas envisageable et encore moins acceptable qu'un système dit « safe », tel que les systèmes critiques (nucléaires, transports, énergies, communications, hospitaliers, etc.) puisse se mettre à dysfonctionner sans garantir une persistance minimale.

Garanties de « survivabilité » (persévérance de la Sécurité-innocuité)

Troisième exigence, celle du retour au fonctionnement normal à la suite du sinistre. Le système défaillant peut être reconstruit.
La troisième propriété de la « sécurité-innocuité » concerne cette garantie dite de « survivabilité" :
Dans la durée, un système sûr de fonctionnement (au sens Sécurité-innocuité) se doit d'avoir la capacité de reprendre son activité considérée comme vitale pour revenir dans un état sûr dit « sûr » (pour « sécurisé » au sens de « sûreté »). Il s'agit ici de garantir la « survivabilité » de la Sécurité-innocuité ; car il n'est ni envisageable ni acceptable que tout système dit « safe » du nucléaire / transport / énergie / communication / hospitalier, ne puisse se remettre en ordre de marche sans garantie de persévérance minimale.

Combinaisons des propriétés de sécurité-innocuité

Les intersections des 3 critères présentés ci-dessus permettent de définir les propriétés combinées de rémanence, réminiscence, résurgence et immanence, que l'on pourrait également qualifier de résilience.

PROPRIÉTÉS DE LA « SÉCURITÉ-INTIMITÉ »

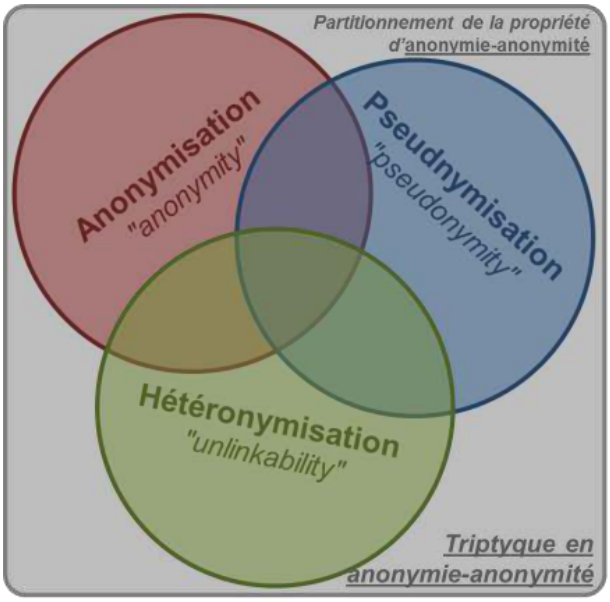
Nous abordons ici le volet de la protection des données personnelles, couvert par différents régimes juridiques :

- régime « exempt de toute formalité » ;
- régime « de formalité simplifiée », pourvu qu'il y ait conformité à une/des normes simplifiées définie et publiée par la Commission Nationale de l'Informatique et Libertés (CNIL) issue de la [L-IFL1978] ;
- régime dit « soumis à déclaration », obligeant à une déclaration formelle auprès de la CNIL, sinon à une auto-déclaration portée dans son registre par le C.I.L. – Correspondant Informatique et Libertés ou Correspondant à la Protection des Données à Caractère Personnel (CPDCP) au sens de [L-PPP2004] ;
- régime dit « soumis à demande d'autorisation », obligeant à une demande d'autorisation formelle auprès des services d'instruction des instances délibératives de la CNIL, surtout pour toute collecte, traitement, utilisation, ré-utilisation, exploitation, exportation, etc. de données dites « sensibles » au sens de la CNIL.

Il faut également rappeler que les lois protectrices de l'intimité (en mode « électronique ») des personnes et du respect de la vie privée de l'individu (en version « informatisée »), telles que [L-IFL1978] & [L-PPP2004], se doivent de respecter les obligations et droits fondamentaux suivants :

- obligation d'informer, lors de la collecte en direct (en face-à-face), comme en indirect (par téléphone, par internet, etc.), la personne concernée par la collecte, des utilisations prévues pour toutes les données personnelles collectées, au travers des "finalités des traitements" obligatoirement préalablement déclarées et autorisées auprès de la CNIL ;
- obligation d'informer la personne concernée par les traitements de ces données personnelles, de ces trois droits fondamentaux actuels que sont :
  - le droit d'accès (applicable à toute information à caractère personnel le concernant directement ou indirectement), ainsi que les modalités de l'exercice de ce droit d'accès fondamental,
  - le droit de rectification (applicable à toute information à caractère personnel le concernant directement ou indirectement ; et traitée, manipulée, archivée de façon non conforme à la réalité ou erronée ou obsolète), ainsi que les modalités de l'exercice de ce droit de rectification fondamental,
  - le droit de suppression de toute information à caractère personnel le concernant directement ou indirectement ; et traitée, manipulée, archivée de façon abusive (ou disproportionnée par rapport aux finalités des traitements obligatoirement préalablement déclarées / autorisées auprès de / par la CNIL), ainsi que les modalités de l'exercice de ce droit de suppression fondamental.

Un domaine particulièrement sensible et riche de la thématique Sécurité-intimité concerne la thématique de l'anonymie ou l'anonymité ; à travers les processus, protocoles, procédures, les méthodologies, méthodes, approches, démarches, les solutions techniques et outils permettant d'anonymiser toute donnée personnelle bien trop intime pour les traitements et manipulations envisagées (statistiques, études épidémiologiques).
Pour ce qui est de cette propriété d'anonymie-anonymité, à nouveau, une approche triptyque est inéluctable.



Anonymisation

L'anonymisation est le remplacement des données plus ou moins directement ou indirectement nominatives par des informations plus ou moins totalement muettes, vis-à-vis de l'identité de la personne concernée.
Les données personnelles anonymisées ne peuvent plus être affectées ou rattachées à une personne en particulier, à un individu. L'anonymisation parfaite est irréversible.

Pseudonymatisation

La pseudonymisation est le remplacement toujours-et-partout, des données plus ou moins directement ou indirectement nominatives, par des informations plus ou moins toujours les mêmes (pseudonymes), permettant ainsi d'accorder une identité anonymisée (pseudonymisée) pour suivre et relier toute donnée et/ou événement concernant individuellement la personne concernée. Les données personnelles pseudonymisées perdent leur caractère nominatif sans pour autant être anonymes. Elles ne pourront être affectées ou rattachées à une personne en particulier, à un individu que dans des conditions bien particulières.

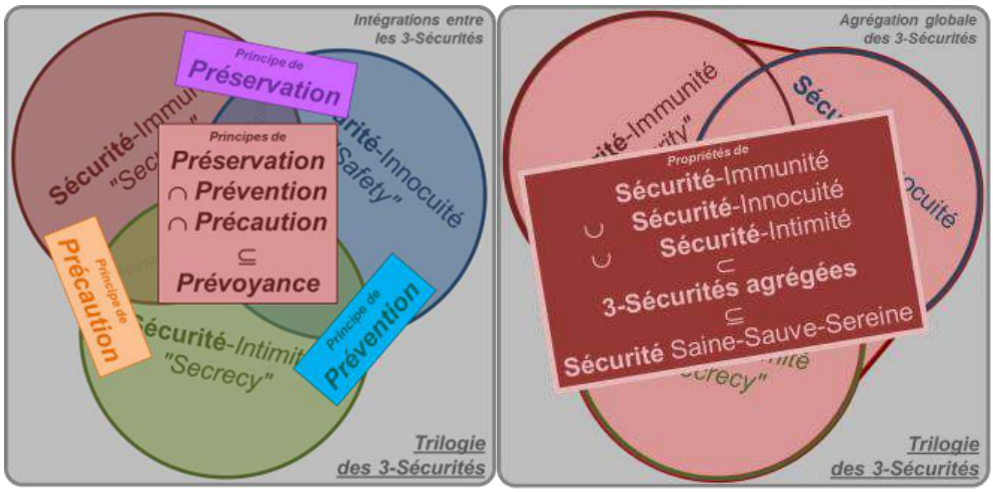
Hétéronymisation

L'hétéronymisation est le remplacement « presque-toujours_et_presque-partout », des données plus ou moins directement ou indirectement nominatives, par des informations « pas-toujours_et_pas-partout » les mêmes (hétéronymes), permettant ainsi d'accorder des identités anonymisées différenciées (hétéronymisées) pour suivre et relier toute donnée et/ou événement concernant individuellement la personne concernée, sans risque des levées d'anonymat indésirées (désanonymisations) dues à l'application de logiques et/ou techniques d'inférences, telles que les logiques de déduction / induction / abduction / adduction [SFdS2001] [SFdS2003] [SFdS2007] [SFdS2008] [Trouessin2008] [REE2009]. Il s'agit d'une anonymisation irréversible ou dépersonnalisation qui utilise des pseudonymes diversifiés, rendant les identificateurs impossibles à corréler.

INTÉGRATION / AGRÉGATION EN MATIÈRE DE « 3-SÉCURITÉS »

Les 3 sécurités présentées ici sont en réalité fortement imbriquées dans la vie réelle, du fait de l'omniprésence de l'informatique dans la vie quotidienne de chacun d'entre nous. Gilles illustre ce phénomène, particulièrement présent dans la sphère santé, avec l'exemple d'une personne âgée porteuse d'un système de téléalarme.

Un tel système doit reposer sur un réseau informatique sûr, ne subir aucune défaillance qui pourrait mettre en danger la vie des utilisateurs, tout en respectant la protection des données personnelles. Les 3-sécurités sont ici complètement intégrées. Des exemples identiques pourraient être pris dans bien d'autres domaines dont celui des transports, pour n'en citer qu'un.



Gilles poursuit sa démonstration en continuant à appliquer le modèle de la « trilogie des triptyques » :

- l'agrégation entre Sécurité-immunité et Sécurité-innocuité est désignée sur le schéma comme le principe de Préservation (le système informatique est sûr et résistera aux défaillances potentielles) ;
- l'agrégation Sécurité-innocuité et Sécurité-intimité est désignée par le terme de « principe de Prévention » (système résistant aux défaillances et aux menaces sur l'individu) ;
- l'agrégation entre Sécurité-intimité et Sécurité-immunité est désignée par le terme de « principe de Précaution » (informatique sûre et données protégées).

Le terme de Prévoyance est utilisé pour l'intégration globale entre Sécurité-immunité et Sécurité-innocuité et Sécurité-intimité, et celui de Protection pour leur agrégation globale.
La terminologie utilisée pour ces combinaisons de propriétés est certes discutable, la distinction entre certains termes n'étant pas toujours évidente en français. L'important n'est donc pas ici le choix des mots mais plutôt l'identification des propriétés élémentaires et de leurs possibilités de combinaison multiples.

CONCLUSION

Vous l'aurez compris, la perspective ouverte par ces réflexions est de pouvoir améliorer et faire améliorer l'ensemble des propriétés, si souvent exprimées et traitées si rarement, en globalité pour la plupart des systèmes pouvant bénéficier d'une 3-Sécurité fiable, fidèle, efficace et efficiente, à la fois, c'est-à-dire de pouvoir bénéficier d'une 3-Sécurité à la fois Saine (« Secure »), Sauve (« Safe ») et Sereine (« Serene »).

Merci à Gilles pour cette belle démonstration.

RÉFÉRENCES

- [Cartau2012] C. Cartau, La sécurité du système d'information des établissements de santé, Ed. PRESSSES de l'EHESP, ISBN 978-2-8109-0083-1, mai 2012.
- [CTCPEC1993] Critères d'évaluation de la sécurité des produits informatiques Canadians [The Canadian Trusted Computer Product Evaluation Criteria (CTPSEC)], Canadian System Security Centre, Communications Security Establishment Government of Canada, janvier 1993.
- [Deswarte1991] Y. Deswarte, Chapitre 9 : tolérance aux fautes, sécurité et protection, pp. 9.1—9.50, in Construction des systèmes d'exploitation répartis, INRIA (Eds. : R.Balter, J.-P. Banâtre, S. Krakowiak), Collection Didactique, ISSN 0299-0733, ISBN 2-7261-0691-9, 1991, 388 p.).
- [DPEC95/46/CE] DIRECTIVE 95/46/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, 1995.
- [FC-ITS1992-I] Critères fédéraux d'évaluation pour la sécurité des technologies de l'information [Federal Critera for Information Technology Security (FC)], Draft, Vol. I, National Institute of Standards & Technology (NIST) and National Security Agency (NSA), 1992.
- [FC-ITS1992-II] Critères fédéraux d'évaluation pour la sécurité des technologies de l'information [Federal Critera for Information Technology Security (FC)], Draft, Vol. II, National Institute of Standards & Technology (NIST) and National Security Agency (NSA), 1992.
- [GSdF-LIS1995] J. Arlat, J.-P. Blanquart, A. Costes, Y. Crouzet, Y.Deswarte, J.-C. Fabre, H. Guillermain, M. Kaâiche, K. Kanoun, J.-C. Laprie, C. Mazet, D. Powel, C. Rabejac, P. Thévenod, Guide de la sûreté de fonctionnement du Laboratoire d'Ingénierie de la Sûreté de fonctionnement (LIS), sous la direction de J.-C. Laprie, CEPADUES Éditions (ISBN 2-85428-382-1, 1995, 369 p), 1995.
- [ISO15408] Common Criteria, Common Criteria Editorial Board (CCEB), norme ISO-IEC 15408.
  [ISO27~~~] Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information, Normes ISO-IEC 27001 / 27002 (accompagnées des ISO-IEC 27003 / 2004 / 2005).
- [ITSEC1991] Critères d'évaluation en sécurité des technologies de l'information [Information Technology Security Evaluation Critera (ITSEC)], v 1.2, Commission des Communautés Européennes, DG XIII, juin 1991.
- [ITSEM1993] Manuel d'évaluation en sécurité des technologies de l'information [Information Technology Security Evaluation Manuel (ITSEM)], v 1.0, Commission Communautés Européennes, DG XIII, sept. 1993.
- [Laprie1985] J.-C. Laprie, Sûreté de fonctionnement des systèmes informatique et tolérance aux fautes : concepts de base, in Techniques et Sciences Informatiques (TSI), vol. 4, n° 5, sept.-oct. 1985, pp. 419--429.
- [Laprie1992] J.-C. Laprie (Ed.), Dependability : Basic Concepts and Terminology in English, French, German, Italien and Japanese, Dependable Computing and Fault-Tolerant Systems, vol. 5, Vienna – Austria, Springer-Verlag, 1992.
- [L-IFL1978] Loi Informatique & Libertés – Loi du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, janvier 1978.
- [L-PPP2004] Loi Informatique & Libertés modifiée – Loi du 06 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, aux fichiers et aux libertés (en tant Loi modificative de la Loi du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés), août 2004.
- [REE2009] Revue de l'Électricité et de l'Électronique (REE), cahier central Les systèmes d'information hospitaliers, Edito. Les technologies de l'information et de la communication au service de la santé par Mme Roselyne Bachelot-Narquin (Ministre de la Santé et des Sport), Préambule au cahier central Les technologies de l'information et de la communication au service de la santé par M. Jean-Yves Robin (Directeur du GIP-DMP (2009)), article du cahier central Anonymisation, pseudonymisation et pseudo-anonymisation dans la sphère Santé-Social" par G.Trouessin, mars 2009.

- [SFdS2001 Société Française de Statistique, conférence : Chaînage des informations et conception de systèmes sécurisés, in Séminaire sur Les appariements de données, conférencier : G. Trouessin, 28 février 2001.
- [SFdS2003] Société Française de Statistique, Intervention Présentation de l'expérience et l'état des travaux du Centre d'Études des Sécurités du Système d'Information (CESSI) de la Caisse Nationale de l'Assurance Maladie des Travailleurs Salariés (CNAMTS), in Formation 20 & 21 janvier 2003 sur la Pratiques des appariements sécurisé, présentée par : G. Trouessin, 2003.
- [SFdS2007 Société Française de Statistique, Intervention à la table ronde Applications actuelles par recours à un tiers de confiance, in séminaire Appariements sécurisés, intervention par : G. Trouessin, 16 novembre 2007.
- [SFdS2008] Société Française de Statistique, Risques d'identification et rappels sur les techniques d'appariements sécurisés, in séminaire Appariements sécurisés, intervention par : G. Trouessin, 16 novembre 2008.
- [TCSEC1983] Critères d'évaluation des systèmes d'ordinateur de confiance du département de la défense américain (Department of Defense Trusted Computer Security Evaluation Criteria), Department of Defense, Technical Report, CSC-STD-001-83, 1983.
- [TCSEC1985] Critères d'évaluation des systèmes d'ordinateur de confiance du département de la défense américain (Department of Defense Trusted Computer Security Evaluation Criteria), Department of Defense, Technical Report, DoD 5200.28-STD, 1985.
- [Trouessin1991a] G. Trouessin, Reliable Processing f Confiential Information, in Proc. 7th International Conference on Information Security (IFIP/Sec'1991) – Creating Confidence in Information Processing, Brighton – UK, 15—17 mai 1991 ; paru dans Information Security, North-Holland 1991 (Eds. : D.T. Lindsay, W.L. Price, ISBN 0-444-89219-2, pp. 210--221.
- [Trouessin1991b] G. Trouessin, Quantitative Evaluation of Confidentiality by Entropy Calculation, in Proc. The Computer Security Foundations Workshop IV (CSFW'IV), Franconia (NH) – U.S.A., 18—20 juin 1991, pp. 12--21.
- [Trouessin1991c] G. Trouessin, Y.Deswarte, J.-C.Fabre, B. Randell, Improvement of Data Processing Security by means of Fault-Tolerance, in Proc. 14th NIST-NCSC National Computer Security Conference (NCSC-14), Washington (DC) – U.S.A., 01—04 oct. 1991.
- [Trouessin1991d] G. Trouessin, Trait.ments fiables de données confid.tielles par frag.tion-red.dance-dis.tion, Thèse de Doct., 1991.
- [Trouessin1999]G. Trouessin, Dependability Requirements and Security Architectures for the Healthcare/Medical Sector, in Safety Computing Symposium (Safecomp'1999), Toulouse – France, 27—29 sept. 1999.
- [Trouessin2008]G. Trouessin, Quelle confidentialité pour quelle confidence et avec quelle confiance ?, in Computer & Electronics Security Application