



PREMIER MINISTRE

Secrétariat général
de la défense
nationale

Paris, le 30 novembre 2006

N° 2571/SGDN/DCSSI/SDS

*Direction centrale de la sécurité
des systèmes d'information*

RAPPORT PUBLIC

Orientation des travaux de recherche et de développement en matière de sécurité des systèmes d'information

Edition 2006

Le présent document est rendu obsolète par la publication de l'édition 2008 du rapport public d'orientation des travaux de recherche et de développement en matière de sécurité des systèmes d'information.

1 Introduction

La sécurité des systèmes d'information (SSI) devient chaque jour une nécessité plus essentielle, alors même que ces systèmes deviennent plus complexes et plus vulnérables aux menaces. Le présent rapport établit une liste des nouveaux enjeux de la sécurité des systèmes d'information, puis les confronte aux évolutions en cours ayant un impact sur la sécurité. Par rapport à ces enjeux et à ces évolutions, qui doivent guider le travail de recherche, est enfin présentée une analyse plus technique des domaines dont la maîtrise apparaît essentielle.

Le présent rapport constitue un document de référence, à caractère incitatif, pour l'orientation des choix stratégiques, y compris financiers, en matière de recherche et de développement dans le domaine de la SSI. Toutefois, ce type de choix résulte toujours d'une analyse de plusieurs facteurs, à laquelle le document ne prétend pas se substituer, se limitant à proposer des orientations scientifiques.

Par ailleurs, il convient de construire une vision prospective nationale à la fois ambitieuse, efficace et qui tienne compte des réalités actuelles au niveau mondial. Il est clair que les frontières numériques n'ont pas grand chose à voir avec les frontières géographiques. L'impact sur la sécurité comme sur la confiance qui en découle nécessitera des efforts de recherche croisés en économie, en sciences politiques et en sécurité des systèmes d'information, permettant de comprendre et d'anticiper les problèmes tant sur les plans technique et industriel que dans les aspects juridique et politique, et ce au niveau international.

Sommaire

1	INTRODUCTION.....	1
2	LES ENJEUX ACTUELS DE LA SECURITE DES SYSTEMES D'INFORMATION	3
2.1	LA SOUVERAINETE.....	3
2.2	LA PROTECTION DE LA VIE PRIVEE	3
2.3	LA DISPONIBILITE	4
2.4	L'IMPUTABILITE DES ACCES.....	4
3	ÉVOLUTIONS EN COURS AYANT UN IMPACT SUR LA SECURITE.....	5
3.1	ARCHIVAGE DE DONNEES.....	5
3.2	ADMINISTRATION ET SUPERVISION	5
3.3	IDENTITE NUMERIQUE ET NOMADISME	5
3.4	LES FLUX MULTIMEDIAS	5
3.5	LES DISPOSITIFS « SANS FIL » OU « SANS CONTACT ».....	6
4	L'ANALYSE DES DOMAINES TECHNIQUES A MAITRISER.....	6
4.1	FONDATIONS DE LA SECURITE DES SYSTEMES D'INFORMATION	6
4.1.1	<i>Système d'exploitation</i>	6
4.1.2	<i>Format des données – protocoles – interopérabilité de la sécurité</i>	6
4.1.3	<i>Cryptographie et architectures de gestion de clés</i>	7
4.2	ARCHITECTURE DES SYSTEMES.....	8
4.2.1	<i>Architecture des produits</i>	8
4.2.2	<i>Architectures diversifiées</i>	8
4.2.3	<i>Sécurité des systèmes auto-organisés</i>	8
4.2.4	<i>Évolution des paradigmes de sécurité</i>	8
4.2.5	<i>Fédération d'identités</i>	9
4.3	NOUVELLES TECHNOLOGIES	9
4.3.1	<i>Électronique et micro-électronique</i>	9
4.3.2	<i>Stéganographie</i>	9
4.3.3	<i>Biométrie</i>	10
4.4	OUTILS THEORIQUES	10
4.4.1	<i>Sûreté de fonctionnement</i>	10
4.4.2	<i>Ergonomie de la sécurité</i>	11
4.4.3	<i>Méthodes formelles et certification</i>	11
4.4.4	<i>Supervision</i>	11

- 0 -

Le présent document constitue le premier rapport public d'orientation des travaux de recherche et développement en matière de sécurité des systèmes d'information établi par la commission interministérielle de la sécurité des systèmes d'information (CISSI).

Selon les termes du décret n° 2001-694 du 31 juillet 2001 portant création de cette commission, la CISSI a en effet pour mission de participer à l'orientation des recherches, études et travaux lancés en France en vue de répondre aux besoins exprimés par les départements ministériels.

Ce rapport a été préparé par le groupe de travail « recherche et développement » constitué à cet effet au sein de la sous-commission « prospective et technologie » de la CISSI, qui regroupe des représentants des ministères, des organismes de recherche (CEA, INRIA) et des organismes de financement de la recherche (ANR, OSEO anvar).

- 0 -

2 Les enjeux actuels de la sécurité des systèmes d'information

2.1 La souveraineté

Les évolutions technologiques récentes confèrent aux systèmes d'information un rôle d'infrastructure chaque jour plus critique pour la société. Le fonctionnement même de l'État et de la nation s'avère tributaire de la disponibilité de ces infrastructures électroniques.

La confiance dans la société numérique passe par la confiance dans les systèmes d'information, et donc dans celle de leur sécurité.

Il ne fait aucun doute que la société de l'information est et restera vulnérable. De la même façon que le monde réel présente des risques, la civilisation numérique comportera toujours des vulnérabilités exploitables par des personnes mal intentionnées, avec comme facteur aggravant considérable l'effet multiplicateur de ces nouvelles technologies et de l'interconnexion des systèmes d'information. Les effets dévastateurs potentiels seront à la mesure des apports positifs indéniables de ce que ce qu'il est convenu d'appeler « l'ère de l'information ». L'objectif est donc bien de limiter les risques liés à l'utilisation de ces technologies, et non de les rendre parfaitement sûres, ce qui serait voué à l'échec.

Les dispositifs de sécurité sont essentiellement destinés à contrôler les systèmes d'information. Le risque existe qu'ils soient détournés de leur objectif initial pour obtenir un avantage significatif en matière d'intelligence économique, voire pour restreindre les prérogatives de l'État en lui interdisant d'exercer en totalité sa souveraineté dans le monde numérique. Par exemple, des contraintes techniques liées à des règles et normes étrangères ne doivent pas pouvoir s'imposer sans contrôle du pouvoir exécutif, et si nécessaire du pouvoir législatif.

Si l'on excepte le cas particulier des systèmes d'information classifiés, la confiance dans les dispositifs techniques de sécurité des systèmes d'information ne peut être établie que sur la base de spécifications ouvertes et sur le contrôle de leur bonne implantation dans les produits. Les réalisations doivent pouvoir être largement contrôlées, non seulement par des organismes agréés mais aussi, dans certains cas, par d'autres entités, notamment des laboratoires indépendants, voire des particuliers. Le mode de contrôle de la SSI ne doit pas être très différent de celui actuellement réalisé dans tous les domaines de la consommation, qui fait intervenir l'État, des organismes indépendants et des associations de consommateurs.

La capacité d'évaluation des produits de sécurité doit donc être assurée, et ce dans tous les domaines susceptibles de faire intervenir la sécurité. Ceci passe par le développement de méthodes formelles de conception et de contrôle qui soient disponibles pour l'ensemble des acteurs. Seule une conception des produits prenant systématiquement en compte la nécessité de l'évaluation est de nature à permettre la vérification des points clés en matière de SSI et l'atteinte du niveau de sécurité adéquat.

Cette capacité à maîtriser les différents aspects de conception et d'évaluation de la sécurité des échanges électroniques constitue un enjeu stratégique de souveraineté lié au développement de la société de l'information et aux moyens de la contrôler que confère la maîtrise des éléments de sa sécurité.

2.2 La protection de la vie privée

Le premier enjeu lié au développement de la société de l'information est celui de la protection de la vie privée. Il implique notamment la confidentialité des informations transmises. C'est aussi celui qui restera le plus important pour assurer la confiance de notre société dans le numérique.

La signature électronique implique une identité électronique, et « l'imputabilité », c'est-à-dire la garantie du lien entre cette identité et la donnée à laquelle s'attache la signature.

Mais elle présente d'autres obligations, comme la manifestation de la volonté du signataire et la non répudiation, c'est-à-dire la garantie dans le temps qu'un signataire de mauvaise foi ne pourra pas renier sa signature. Ce dernier point sera notamment particulièrement difficile à assurer sur une longue durée. L'équivalent numérique des actes notariés est un cas concret à étudier.

Avec l'introduction généralisée des équipements sans fil et l'arrivée prochaine massive de l'identification par radiofréquences (RFID), les possibilités de géo-localisation et de traçabilité deviennent chaque jour plus importantes et doivent être prises en compte, d'autant que beaucoup d'utilisateurs n'ont pas conscience des risques liés à cette possibilité de connaître leur identité et leur position géographique en temps réel.

Un manque de respect des règles de protection de la vie privée des individus pourrait entraîner une réaction de rejet de ces innovations et constituer un frein au développement des actes électroniques, notamment commerciaux.

2.3 La disponibilité

Le deuxième enjeu à venir est celui de la disponibilité, qu'il faut entendre au sens large, c'est-à-dire en y incluant l'objectif d'intégrité et d'authenticité des services disponibles. Les réseaux informatiques peuvent aujourd'hui être considérés comme une sorte de système nerveux des sociétés modernes, dont ils supportent les fonctions vitales (infrastructures critiques). Leur disponibilité est donc une question fondamentale, qui ne peut être résolue que par la mise en œuvre de moyens indépendants les uns des autres, à tous les niveaux physiques et logiques, dans une optique de redondance et de tolérance aux fautes et aux vulnérabilités. La recherche de ce qu'on pourrait appeler l'info-diversité est une condition indispensable à l'atteinte de cet objectif. Il faut cependant être convaincu dès à présent que des incidents, des accidents, voire des catastrophes, du point de vue de la disponibilité, interviendront sur des réseaux informatiques, et partant, sur les systèmes physiques qu'ils contrôlent. Des modes de secours doivent donc être prévus pour pallier ces dysfonctionnements.

Les bases théoriques de ces divers mécanismes bénéficieraient vraisemblablement d'une convergence des approches « sécurité des systèmes d'information » et « sûreté de fonctionnement », aujourd'hui trop nettement distinctes.

De nombreuses attaques observées ont porté atteinte à la disponibilité des systèmes en exploitant des vulnérabilités connues. Disposer d'outils performants du type « scanneur de vulnérabilités » permettrait de vérifier périodiquement ou en continu la bonne mise à niveau d'un système ou d'un réseau. De la même façon que les automobiles subissent des contrôles techniques, il faudrait pouvoir réaliser des audits réguliers ou circonstanciés des systèmes d'information. Comme pour les automobiles, ils ne garantiraient pas la sécurité absolue du système expertisé, mais permettraient d'éviter, ou au moins de connaître, les systèmes potentiellement dangereux pour eux-mêmes et pour les autres.

2.4 L'imputabilité des accès

Un troisième enjeu à privilégier est l'imputabilité des accès aux réseaux téléphoniques ou informatiques. En effet, la plupart des problèmes actuels d'utilisation du réseau internet proviennent de l'impunité ressentie par les utilisateurs mal intentionnés. Les moyens techniques disponibles ne permettent de remonter à un agresseur qu'au prix d'importants efforts. Le problème de l'imputabilité est malheureusement difficilement soluble au seul niveau national. Aucune solution réaliste ne semble envisageable à court terme compte tenu des protocoles de l'Internet actuel.

Chercher à obtenir l'imputabilité nécessite de définir une identité électronique. Cette identité sera utilisée notamment pour permettre la signature électronique et le contrôle de l'accès à des données personnelles.

Mais cette identité électronique ne peut être authentique et fondée sur la confiance sans garantir la confidentialité des données utilisées pour la caractériser (clé cryptographique notamment). Ce point met en évidence que toute la chaîne d'outils qui utilisera cette identité électronique doit susciter la confiance, sous peine de permettre l'usurpation d'identité, ou inversement, d'être inacceptable par la société du fait des conséquences indirectes, sur la vie privée, de la mise en place d'un tel outil.

3 Évolutions en cours ayant un impact sur la sécurité

3.1 Archivage de données

Les quantités phénoménales d'informations traitées par les systèmes ne permettent déjà plus de reposer sur les techniques d'archivage classiques du papier. La disponibilité de ces archives dans le temps, mais aussi la disponibilité de l'accès à ces données, tout en assurant le contrôle de cet accès, sont autant d'évolutions majeures à prendre en compte aux plans technique et juridique. Des exemples récents montrent que le contrôle des outils de recherche dans ces masses de données présente un caractère stratégique.

3.2 Administration et supervision

La complexité des systèmes d'information et la difficulté de leur administration, notamment au plan de la sécurité, rendent inévitables la spécialisation de ces tâches, la multiplication des acteurs et la mise en place d'outils de télé-administration. Ces outils, permettant la prise de contrôle à distance des systèmes d'information, revêtent, de par leur fonctionnalité même, un caractère stratégique. Ils devront susciter la confiance, tout comme leurs opérateurs.

3.3 Identité numérique et nomadisme

La généralisation d'Internet modifie l'utilisation informatique, et permet notamment le « nomadisme ». Dans le domaine des technologies de l'information et de la communication (TIC), il n'y a plus de réelle différence entre le lieu de travail et le domicile. Le contrôle à distance de l'identité électronique revêt ainsi une importance grandissante. À plus long terme, devrait se développer pour l'identification une approche multimodale associant différentes techniques (cartes, biométrie, ...) renforçant l'identification. La multiplication des services en ligne et des terminaux d'identification/authentification va susciter un besoin de simplification pour l'utilisateur et pour les administrateurs. Les mécanismes de fédération d'identité, permettant à l'utilisateur de s'authentifier une fois pour toutes, sont appelés à se généraliser. La maîtrise de ces mécanismes est cruciale, car ils permettent de contrôler l'accès à tous les services utilisés.

3.4 Les flux multimédias

La généralisation des flux multimédias est également inévitable, comme par exemple la convergence entre les flux téléphoniques et les flux de données. Elle présente des risques accrus en termes de sécurité du fait du caractère « temps réel » de ces flux. Les problèmes vont concerner la protection de bout en bout, particulièrement dans des foyers où se multiplieront les terminaux interconnectés (TV, ordinateur, chaîne audio, lecteur MP3, ...). En effet, les équipements actuels de sécurité des systèmes d'information (pare-feu, routeurs chiffants, détecteurs d'intrusion, etc.) ne sont pas en mesure de gérer des flux de données en temps réel avec le même niveau de sécurité que des flux asynchrones.

La convergence de ces modes de transmission implique de repenser l'architecture de sécurité des réseaux, qui doit davantage reposer sur la sécurité des équipements terminaux que par le passé. Il est donc important que la France et plus largement l'Europe soient mieux positionnées pour les équipements terminaux.

3.5 Les dispositifs « sans fil » ou « sans contact »

L'évolution des menaces va être largement liée aux nouveaux objets communicants qui accompagnent le nomadisme. La multiplication des liaisons sans fil (modems wifi de série, bluetooth, ...) ouvrent autant de chemins d'attaques possibles, ce qui augmente le niveau de menace sur la confidentialité des données et la disponibilité des services. La situation est d'autant plus critique que les terminaux mobiles sont massivement utilisés par les cadres et dirigeants et véhiculent donc des données stratégiques.

Les principales menaces sont :

- l'interception des communications, plus aisée que celle des communications filaires, et qui menace la confidentialité ;
- le brouillage des communications ;
- l'intrusion dans le réseau via les connexions radio ouvertes, aisément accessibles de l'extérieur des bâtiments.

Les systèmes sans contact font ainsi leur apparition dans de nombreux domaines, y compris à haute sécurité (administration électronique, domaine bancaire, etc.). Ces systèmes permettent une lecture de données à travers des obstacles opaques aux ondes lumineuses et à une distance allant d'une dizaine de centimètres (carte sans contact) à plusieurs mètres (RFID).

4 L'analyse des domaines techniques à maîtriser

Tous les produits et systèmes de SSI reposent sur un certain nombre de briques fonctionnelles communes qui concourent à la sécurité globale. La maîtrise des différents domaines techniques est indispensable à la confiance finale dans le système d'information. Toutes ces technologies sont actuellement disponibles, même si elles ne sont pas forcément maîtrisées au niveau national. L'intégration maîtrisée de ces technologies est nécessaire à la confiance recherchée dans la SSI.

Ce paragraphe tente de faire le point sur les technologies importantes en matière de sécurité des systèmes d'information. Comme pour toute étude à valeur prospective, il convient de le lire avec la plus extrême prudence du fait de l'extraordinaire rapidité d'évolution du domaine.

4.1 Fondations de la sécurité des systèmes d'information

La sécurité des systèmes d'information repose sur un certain nombre de briques fondamentales qui, si elles ne sont pas comprises et maîtrisées, ne permettent pas de réaliser des systèmes d'information sûrs et de confiance.

4.1.1 *Système d'exploitation*

Tous les systèmes logiciels reposent sur un système d'exploitation qui gère les périphériques matériels. La confiance dans le système d'exploitation utilisé est donc indispensable à la confiance dans la sécurité des systèmes d'information.

Le niveau de performance atteint aujourd'hui par les ordinateurs et la maturité des logiciels de machine virtuelle permettent désormais d'envisager sérieusement l'utilisation de ce type d'outil dans un environnement de production. Cette approche permet notamment de confiner un service dans une machine virtuelle dédiée, ce qui permet un cloisonnement profitable à la sécurité.

4.1.2 *Format des données – protocoles – interopérabilité de la sécurité*

Les débuts de l'informatique ont été marqués par des organisations client – serveur, qui ont été privilégiées du fait du coût d'investissement élevé des calculateurs.

Ce coût baissant, les ordinateurs se sont rendus autonomes en réalisant eux-mêmes les opérations qu'ils demandaient auparavant à un serveur, seules les données restant centralisées sur des serveurs. La montée en puissance des réseaux informatiques permet d'envisager une nouvelle approche client – serveur pour l'utilisation de bases de données, ces bases s'organisant vraisemblablement autour de grappes d'ordinateurs, comme le sont déjà les services de recherche sur Internet. Les problématiques de base en matière de sécurité (confidentialité, intégrité, authenticité, disponibilité et contrôle d'accès) seront donc à appliquer à des échelles différentes. Dans ce domaine, l'émergence du standard XML¹ offre des perspectives de standardisation dans la structuration du stockage de données.

D'un autre côté, l'évolution actuelle des réseaux informatiques est une convergence vers les standards de l'Internet, à savoir l'utilisation généralisée du protocole IP.² Ce protocole permet l'envoi de paquets de données d'une machine à une autre par un système d'adressage numérique. Ces adresses numériques sont associées à des adresses normalisées par l'intermédiaire du service DNS.³

Sur la base du protocole IP et du service DNS, d'autres protocoles sont utilisés pour proposer un certain nombre de services. On notera ainsi le développement d'IPsec, qui permet l'établissement de réseaux privés virtuels par l'utilisation de chiffrement. Mais c'est aussi sur IP que se développent de nouveaux services temps réel (voix, visioconférence, flux « *streamés* »), alors même que le protocole IP n'a pas été prévu pour acheminer ce type de données puisqu'aucune qualité de service n'est garantie. Des services nouveaux (« *peer-to-peer* »), aussi véhiculés par IP, visent à une mise en commun de ressources par l'intermédiaire du réseau. Ceci n'est pas sans rappeler l'émergence des grappes d'ordinateurs.

De façon générale, tous ces protocoles sont des structurations de l'information numérique, et leur bonne interprétation est cruciale en matière de sécurité informatique, tout autant que d'interopérabilité. La réalisation d'implantations de référence validées formellement est un facteur de sécurité et de confiance à développer.

4.1.3 Cryptographie et architectures de gestion de clés

La quasi-totalité des équipements de sécurité informatique utilisent de façon incontournable des fonctions cryptographiques. Celles-ci ne peuvent être efficaces que si les infrastructures de gestion des clés cryptographiques sont maîtrisées. Ceci ne se limite pas à la notion d'infrastructure de clés publiques, mais va jusqu'à la fourniture sécurisée à l'utilisateur des moyens de stockage et d'utilisation de ses clés.

La cryptographie fournit les primitives de base de nombreuses fonctions de sécurité, dans le cadre de techniques bien connues reposant sur la difficulté de résolution de problèmes mathématiques. Ces primitives sont en constante amélioration, mais il faut souligner que ce domaine n'est pas à l'abri, un jour, d'une percée majeure – mathématique ou technologique – susceptible de réduire à néant du jour au lendemain la sécurité de nos systèmes. Une veille très active est donc indispensable, ainsi que l'analyse d'éventuelles solutions alternatives.

Une activité de recherche soutenue dans ce domaine est donc indispensable pour anticiper les évolutions algorithmiques et les impacts sur les architectures de gestion de clés.

¹ Extensible markup language

² Internet Protocol

³ Domain Name Service

4.2 Architecture des systèmes

La sécurité des systèmes d'information résulte autant de celle des briques fondamentales utilisées que de l'architecture générale retenue.

De la même façon que les progrès dans le secteur du bâtiment et des travaux publics s'appuient sur l'amélioration des matériaux et des théories architecturales, la sécurité des systèmes d'information doit améliorer ses briques fondamentales évoquées ci-dessus et s'investir de façon significative dans la compréhension théorique des apports de telle ou telle technique architecturale.

4.2.1 *Architecture des produits*

La plupart des solutions de sécurité s'appuyant sur des technologies logicielles sont susceptibles d'être détournées ou contournées par le fait même qu'elles sont liées à du code logiciel, chargé et exécuté sans contrôle par le système.

Un niveau supérieur de confiance peut être obtenu en intégrant des mécanismes de sécurité dans l'architecture même des ordinateurs ou des systèmes. On peut limiter les vulnérabilités en intégrant des solutions cryptographiques sous forme de composants matériels. L'intégration de solutions de diagnostic intégré et de tests de cohérence dans les processeurs eux-mêmes est également importante.

4.2.2 *Architectures diversifiées*

La haute disponibilité des infrastructures critiques ne peut être atteinte que par des architectures appliquant les techniques de sûreté, qui visent à pallier les pannes probables d'un composant par sa redondance. Mais dans le domaine de la sécurité des systèmes d'information, cette redondance est d'autant plus difficile à assurer que la menace d'attaque simultanée des deux composants doit être envisagée.

Plus encore que par des architectures redondantes des systèmes d'information, c'est donc bien en recherchant des architectures diversifiées sur les plans matériel et logiciel qu'il sera possible de maîtriser le risque de propagation d'attaques de grande ampleur.

4.2.3 *Sécurité des systèmes auto-organisés*

La disponibilité des données est pour le moment encore majoritairement garantie par des configurations matérielles coûteuses et de lourds processus de maintenance et de sauvegarde. L'amélioration des performances des réseaux et des ordinateurs laisse toutefois entrevoir des évolutions possibles du modèle classique client – serveur où le réseau en lui-même et les données qu'il contient seraient robustes à la panne d'un ou plusieurs de ses éléments. Ces technologies d'auto-organisation issues du pair-à-pair (« peer-to-peer ») et des grappes d'ordinateurs doivent encore être perfectionnées pour véritablement remplir l'objectif de disponibilité attendu, mais couplées aux mécanismes cryptographiques, elles pourraient conduire à des architectures robustes, interopérables, hétérogènes et supportant les changements d'échelle.

Les pistes qui semblent à privilégier à court terme pour ces développements concernent les serveurs de fichiers et ceux de bases de données.

4.2.4 *Évolution des paradigmes de sécurité*

La plupart des concepts mis en œuvre pour sécuriser un système reposent à un moment donné sur la définition d'une forme d'enceinte protégeant les données ou les services utilisés, dont l'accès et l'utilisation doivent être contrôlés. Les systèmes évoluent lentement mais sûrement, pour des raisons d'efficacité, du paradigme de la forteresse vers celui de l'être vivant, où cette notion de frontière est en grande partie abolie.

Cette mutation, de l'approche classique, périmétrique, de la SSI, de ses mécanismes, de ses standards et de ses protocoles, vers un futur encore à perfectionner de défense en profondeur,

nécessite un effort de recherche et de développement considérable, déjà engagé dans certaines initiatives comme le Forum Jericho.

4.2.5 *Fédération d'identités*

L'intégration des nouvelles techniques de fédération d'identité dans les systèmes d'information est un processus en cours de standardisation, sous l'impulsion de structures comme le « trusted computing group » ou « liberty alliance ». Le suivi de ces travaux de normalisation par nos industriels et le monde académique est aujourd'hui largement insuffisant, alors même que l'utilisation de ces techniques s'avère incontournable pour les systèmes d'information futurs (télé-procédures, titres d'identité électronique, etc.).

La bonne compréhension des protocoles utilisés et l'identification des briques fondamentales à maîtriser dans ces systèmes de fédération d'identité restent à acquérir pour permettre d'orienter la stratégie sur ce point.

4.3 Nouvelles technologies

La sécurité des systèmes d'information est indissociable des technologies qui l'utilisent et qu'elle utilise. Une bonne connaissance des évolutions des nouvelles technologies est indispensable pour comprendre les nouvelles menaces qui peuvent apparaître, mais aussi les apports pour la sécurité qui peuvent en résulter.

4.3.1 *Électronique et micro-électronique*

Tous les équipements d'un système d'information, y compris ceux qui contribuent à sa sécurité, sont réalisés à partir de briques physiques. Ces briques sont électroniques, micro-électroniques et prochainement nano-technologiques. Elles peuvent être le talon d'Achille d'équipements de sécurité, notamment par l'émission de signaux compromettants, mais aussi par les possibilités de piégeage qu'offre la maîtrise de leur conception, celle des micro-processeurs par exemple.

La maîtrise et l'autonomie d'approvisionnement des composants électroniques stratégiques dans ce domaine sont donc des objectifs à moyen terme. Ils nécessitent toutefois des efforts majeurs.

L'existant national en micro-électronique dans le domaine de la SSI est principalement axé sur la carte à puce et les composants cryptographiques. Or la micro-électronique intervient aussi dans le domaine des microprocesseurs généralistes utilisés dans les ordinateurs. On observe une convergence de ces domaines avec les cartes à puce, qui embarquent désormais des systèmes d'exploitation multi-applicatifs. Il faut donc bien identifier les fonctions de sécurité physique nécessaires jusqu'au niveau du composant pour asseoir la sécurité globale du produit.

Afin d'améliorer la sécurité des systèmes d'information au niveau des composants physiques, il est nécessaire de développer des techniques pour d'une part lutter contre la rétro-conception et le piégeage, d'autre part contrer les attaques par canaux auxiliaires. Ces techniques, bien connues dans le domaine des cartes à puce, mériteraient d'être étendues aux autres types de composants électroniques afin de poursuivre l'amélioration du savoir-faire en ces domaines.

4.3.2 *Stéganographie*

Les techniques de stéganographie sont au moins aussi anciennes que celles de cryptographie. Elles visent à protéger l'information sensible en la dissimulant au milieu d'informations anodines. Ces techniques s'appuient sur des outils théoriques voisins de ceux de la cryptographie. Leur emploi a longtemps été réservé à des contextes très particuliers où l'emploi de la cryptographie était en soi révélateur de l'activité que l'on souhaitait dissimuler (recherche de renseignement en territoire hostile, action de forces spéciales ou terrorisme, par exemple).

Savoir détecter de tels procédés de stéganographie ou inversement les rendre difficilement détectables sont donc les deux aspects complémentaires du glaive et de la cuirasse. Développer

les connaissances dans ce domaine paraît d'autant plus important qu'il offre également des outils pour améliorer la traçabilité des informations.

Le « water-marking » utilise en effet des outils proches de la stéganographie pour marquer une information de façon indélébile, permettant *a posteriori* de détecter une copie illégale, voire de remonter à la source de diffusion de cette copie.

4.3.3 Biométrie

Les techniques biométriques se développent actuellement sur un marché porteur. Deux grands domaines d'application semblent se dégager.

D'une part l'aide à l'identification, par la capacité des technologies biométriques à sélectionner rapidement dans des bases de données les personnes enregistrées se rapprochant le plus de mesures biométriques réalisées sur le terrain. Ces techniques intéressent le contrôle aux frontières et les enquêtes judiciaires.

D'autre part l'authentification, pour laquelle elles peuvent apporter des solutions là où les techniques classiques s'avèrent inapplicables pour des raisons pratiques (ergonomie, coût, etc.).

L'amélioration de ces techniques doit se poursuivre, notamment par le développement d'outils multi-modaux, qui utilisent plusieurs critères biométriques pour améliorer leurs performances. Le recours à ces techniques ne doit pas être systématique, mais au contraire résulter d'une connaissance précise de leurs apports et de leurs limitations, permettant de décider au cas par cas s'ils sont adaptés au besoin ressenti pour telle ou telle application.

Des solutions nouvelles permettant l'identification de l'être humain par d'autres caractéristiques que son image photographique, son empreinte digitale ou l'analyse de l'iris sont en gestation.

L'évaluation des méthodes pour leurrer ces dispositifs et la mesure objective de la fiabilité de ces techniques constituent un axe d'effort pour permettre de comparer ces différentes techniques entre elles.

4.4 Outils théoriques

4.4.1 Sûreté de fonctionnement

Les systèmes informatiques et matériels sur lesquels reposent de plus en plus nos activités deviennent extrêmement complexes tant dans leur conception que dans leur réalisation.

Le domaine sécurité se caractérise aujourd'hui par une assez bonne maîtrise, théorique et pratique, des composantes et mécanismes utilisés pourvu que ceux-ci restent à un niveau de complexité relativement faible. Le passage à des systèmes sensiblement plus complexes pose des problèmes encore mal résolus, si ce n'est de manière partielle ou artisanale (cas particuliers ou savoir-faire d'experts). Un effort important semble donc nécessaire en matière de modélisation et de simulation dans le domaine de la sécurité, pour être capable de développer de manière rigoureuse des architectures garantissant les propriétés souhaitées et de passer des comportements microscopiques au comportement global.

Les liens sont extrêmement forts entre les aspects sécurité, qui visent à résister à des actions délibérées, et les aspects sûreté, qui visent à maintenir un fonctionnement nominal malgré des fautes ou des actions non délibérées, comme l'effet de particules atmosphériques ou d'autres perturbations liées à l'environnement opérationnel.

Typiquement, une politique de sécurité dont l'implantation ne serait pas sûre n'apporterait évidemment aucune garantie.

Des erreurs d'un programme non sûr pourront être exploitées pour créer des failles de sécurité, de la même manière qu'une erreur dans la conception informatique du système de freinage d'un véhicule peut entraîner des conséquences dramatiques sur la sécurité physique des passagers.

Par ailleurs, les méthodes, outils et techniques utilisés pour la sécurité et ceux destinés à la sûreté, par prévention et/ou par tolérance, ainsi que l'évaluation de mesures de la sûreté (fiabilité, disponibilité, etc.) ont des points communs qu'il est possible d'exploiter dans les systèmes ayant les deux types d'exigences.

Il faut se donner les moyens de prouver la correction et la robustesse de la sécurité mise en œuvre et adapter pour cela les méthodes mises au point dans le domaine de la sûreté et de la fiabilité.

4.4.2 Ergonomie de la sécurité

De nombreux problèmes de sécurité résultent d'erreurs ou d'approximations dans la conception de l'interface homme-machine des systèmes. Ce point particulier, qui a reçu dans d'autres domaines plus sensibles aux incidents (aviation, énergie, etc) l'attention qu'il méritait, devrait être traité plus sérieusement qu'il ne l'est habituellement. Un effort s'impose sur l'ergonomie de la sécurité, de manière à garantir qu'un apprentissage ou qu'un mode d'emploi suffisamment faciles des fonctions externes d'un système se traduisent à l'intérieur de celui-ci par les comportements souhaités au niveau de ses mécanismes élémentaires.

4.4.3 Méthodes formelles et certification

Les différentes approches de sécurité doivent se donner les moyens de certifier formellement leur niveau de sécurité. Ce besoin est partiellement pris en compte dans les « critères communs⁴ », qui offrent une certaine mesure de la confiance par rapport à des niveaux de sécurité ou de sûreté.

On voudra pouvoir prouver formellement, *i.e.* dans un système logique formel, que telle propriété de sécurité est vérifiée et sous quelles hypothèses précises. Cette preuve devra pouvoir être communiquée et être vérifiée par des tiers, indépendamment du système qui a participé à la construire. Cela permettra en particulier de développer les notions de « cryptographie prouvée », qui permet d'assurer formellement qu'un algorithme de cryptographie a les propriétés voulues, pour garantir l'implantation d'un algorithme de chiffrement est effectivement conforme à sa spécification.

De la même manière, l'analyse formelle de programmes devra être développée avec deux objectifs. D'abord être capable de comprendre, dans les développements logiciels réalisés pour la sécurité, la qualité des programmes de manière à en améliorer significativement la sûreté. Ensuite, être capable de conduire sur du code étranger, des analyses permettant de reconnaître s'il réalise effectivement ses fonctions et ses fonctions seulement. Les méthodes de typage, d'analyse statique et d'interprétation abstraite pourront utilement être développées dans ce cadre.

Avec pour objectif de certifier les propriétés de sûreté et de sécurité, il faudra développer les moyens de certifier formellement l'ensemble des éléments intervenant dans la construction de la sécurité d'un système :

- les architectures, y compris matérielles, sur lesquelles sont exécutés les programmes ;
- la sémantique des langages de programmation utilisés ;
- les codes machines générés, soit en utilisant des compilateurs certifiés et en se basant sur des programmes de haut niveau dont les propriétés sont elles-mêmes prouvées, soit en prouvant directement les codes générés.

4.4.4 Supervision

La supervision des systèmes d'information doit devenir un outil de sécurité majeur des systèmes futurs. En effet, la technicité de plus en plus grande des attaques comme des moyens de

⁴ Norme ISO/IEC 15408

protection milite pour des gestions centralisées de la sécurité, assurées par des équipes spécialisées. Mais pour que cette supervision soit possible, il convient de disposer d'outils sécurisés et de confiance, ce qui est loin d'être le cas aujourd'hui.

Le développement de tels outils ne pourra que tirer bénéfice de l'effort dans le domaine des méthodes formelles et des techniques liées à la sûreté de fonctionnement et impactera l'architecture même des systèmes d'information. Ce développement devra également s'intéresser aux outils d'aide à la décision nécessaires à la supervision pour traiter les quantités très importantes d'informations remontées au niveau central, par exemple par les outils de détection d'intrusion.