Recherche et développement en sécurité des systèmes d'information : orientations et enjeux

Florent Chabaud

Sous-directeur scientifique et technique
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
51 boulevard de La Tour-Maubourg
75700 Paris cedex SP
florent.chabaud@sgdn.gouv.fr

Résumé À la croisée de la recherche, de l'industrie et des besoins opérationnels, la direction centrale de la sécurité des systèmes d'information (DCSSI) dispose d'un observatoire privilégié pour tenter de détecter les orientations que devraient suivre la recherche et le développement en matière de sécurité des systèmes d'information. Cet exposé s'attachera donc à présenter les orientations que préconise la DCSSI en la matière en cherchant à montrer sur quelques exemples en quoi ces orientations sont justifiées. Seront ainsi abordés la problématique des fonctions de hachage appliquée au cas de l'IGC/A, la modélisation d'une fonction cruciale de sécurité qu'est l'authentification distante, et les enjeux respectifs des développements matériel et logiciel en matière de sécurité des systèmes d'information.

1 Introduction

L'organisation de la sécurité des systèmes d'information (SSI) en France s'articule au niveau interministériel autour du secrétariat général de la défense nationale, organisme interministériel rattaché au Premier ministre. L'un des relais auprès des ministères est assuré par une commission interministérielle de la sécurité des systèmes d'information, qui peut organiser des groupes de travail pour traiter de problématiques particulières. C'est dans ce cadre, qu'un groupe de travail a élaboré pour la première fois un rapport public d'orientation des travaux de recherche et de développement en matière de SSI [1]. Ce rapport a été réactualisé début 2008 sans modification majeure [2]. Il se veut incitatif dans les domaines technologiques à étudier et à soutenir intéressant la sécurité des systèmes d'information. Il tente également de mettre en évidence les enjeux liés à la sécurité des systèmes d'information et les avancées technologiques qui peuvent présenter un fort impact sur ces enjeux.

L'objet de cet article n'est pas de paraphraser ce rapport, public et disponible en ligne, mais plutôt d'illustrer certains de ses aspects.

2 Enjeux et orientation en SSI

2.1 Le rôle de la recherche en SSI

Le premier enjeu cité par le rapport [2] est celui de la souveraineté. Cette notion est difficile à cerner. La définition du Larousse en est "*pouvoir suprême reconnu à l'État, qui implique l'exclusivité*

de sa compétence sur le territoire national et son indépendance internationale, où il n'est limité que par ses propres engagements" [3]. On comprend bien qu'il s'agit de protéger l'autonomie de décision de l'État, qui s'étend au delà des frontières, même lorsqu'elles sont numériques. Cette notion est également à rapprocher du rôle protecteur de l'État pour ses citoyens.

Or face à cet enjeu, que nous apprend l'histoire récente dans le domaine numérique ? On a vu un pays fortement numérisé, l'Estonie, souffrir pendant plusieurs jours d'attaques massives sur l'internet, attaques ayant conduit à perturber assez fortement le fonctionnement même de son économie et de ses institutions. Relever la fragilité des ordinateurs et des réseaux informatiques était depuis longtemps un lieu commun qui pouvait prendre place dans toute conversation de salon et déclencher ce petit rire crispé de celui qui parle d'une chose crainte sans vraiment croire qu'elle puisse arriver. Voir ce type de crainte se réaliser, qui plus est à l'échelle d'un pays, a eu ponctuellement un effet bénéfique dans la perception de l'enjeu de souveraineté correspondant. Mais d'autres évènements, moins médiatiques, révèlent aussi la portée de la révolution numérique que nous vivons.

Ainsi, en Grèce/Italie, on a vu se développer un marché noir de l'écoute téléphonique. Tel exploitant des infrastructures gouvernementales a ainsi vendu les services d'écoute normalement réservés au seul pouvoir judiciaire. De la même manière, les circuits décisionnels du gouvernement Grec ont été espionnés en exploitant des infrastructures existantes mal maîtrisées. On notera aussi les perturbations accidentelles des réseaux internet de pays entiers qu'ont pu occasionner la rupture de câbles sous-marins ou des erreurs de configuration de gros routeurs.

Ces derniers exemples sont bien compris des spécialistes réseaux. L'explication technique est simple et est liée entre autres à la spécification du protocole DNS qui organise de façon hiérarchique les serveurs de nommage de l'internet. Ne plus pouvoir accéder aux serveurs racines et, petit-à-petit, c'est le réseau qui s'arrête de lui-même, faute de savoir associer une adresse IP à un nom. Limiter les risques est possible, en gérant correctement des serveurs secondaires, en réglant les comportements de ces serveurs en mode dégradé, etc. Ces mesures nécessitent toutefois une bonne connaissance du protocole DNS pour ne pas perturber son fonctionnement nominal. Elles ne sont en outre qu'un pis-aller par rapport à des solutions plus drastiques comme de posséder un serveur racine. La question qu'on peut se poser alors est pourquoi ne pas l'avoir fait ? La réponse en est évidemment le manque de perception des enjeux correspondants au moment où cela aurait été possible.

Face à ce manque de perception lié à la difficulté de compréhension d'un domaine technique nouveau, la recherche a un rôle important à jouer. De la même façon que la protection de l'environnement a mis du temps à être prise en compte au niveau politique, la sécurité des systèmes d'information, en France, peine à "entrer dans les murs". C'est en partie dû à un manque de culture de sécurité. C'est aussi lié à un manque de formation ; la sécurité est en effet considérée comme une spécialisation de fin de cursus alors qu'elle concerne tous les métiers, à des degrés divers bien entendu.

2.2 Défense en profondeur en sécurité des systèmes d'information

Le concept de défense en profondeur appliqué à la sécurité des systèmes d'information peut se définir selon cinq axes complémentaires (voir figure 1).

Prévenir. Il s'agit d'éviter la présence de failles dans les constituants du système d'information. Cet axe de défense correspondra par exemple à l'emploi exclusif de produits évalués, certifiés, tenus à jour de leurs correctifs de sécurité. En termes de développement, des normes de qualité ou de

FIG. 1: Défense en profondeur en SSI

sûreté de fonctionnement pourront être employées. Au niveau de la conception enfin, la recherche de preuves de sécurité des choix réalisés contribuera à cet objectif de prévention.

Bloquer. Cet axe est celui qui a été le plus développé dans une réaction *a posteriori* aux vulnérabilités observées. Il s'agit d'empêcher les attaques qui en résultent de parvenir aux composants sensibles et potentiellement vulnérables du système d'information. Dans la pratique, on utilise donc des pare-feu, des serveurs mandataires, des filtres applicatifs, des ruptures protocolaires, mais aussi des équipements de chiffrement pour délimiter un périmètre de protection. À l'usage, ces techniques s'avèrent de moins en moins protectrices du fait de l'importance des canaux cachés potentiels qui subsistent et de la richesse sémantique des flux autorisés. Elles demeurent toutefois utiles pour réduire les chances de succès des attaques, offrir des potentiels de détection d'attaques en réduisant les degrés de liberté d'un attaquant potentiel.

Tolérer. C'est sans doute l'axe de défense qui reste le plus à développer dans les systèmes d'information actuels. Il s'agit de limiter les conséquences de la compromission de l'un ou l'autre des composants du système, sans pour autant savoir à l'avance lequel sera ciblé. Il s'agit aussi d'offrir des résistances successives à un attaquant potentiel pour qu'une attaque réussie ne puisse pas lui donner instantanément accès à toutes les informations dont il peut rêver. Les outils à envisager pour cet objectif sont par exemple les techniques de cloisonnement et de virtualisation utilisées dans certains systèmes d'exploitation (cages, *jail*, compartiments, etc.). L'idée est ici de limiter les degrés de liberté de l'attaquant qui a réussi à percer les défenses périmétriques en ne lui donnant pas immédiatement l'accès aux informations qu'il recherche.

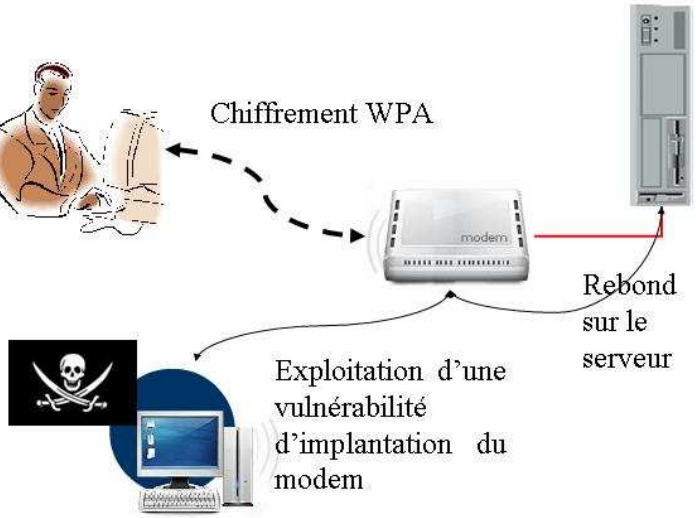

FIG. 2: Protection périmétrique d'un réseau sans-fil

Un exemple parlant peut être donné avec la connexion Wi-Fi d'un internaute à son domicile. La configuration conseillée la plupart du temps consiste à utiliser le protocole WPA ou WPA-2. En effet, le protocole initialement utilisé, le WEP, a subi des attaques sévères et son contournement est à la portée du premier venu à l'aide d'outils comme *aircrack-ng* [4]. Dans cette configuration on oppose donc à l'attaquant potentiel une barrière périmétrique supposée solide constituée par un chiffrement de bonne qualité (voir figure 2). Mais cette cryptographie constitue alors la seule défense. Si elle s'avère de mauvaise qualité, ce qui reste improbable, ou si son implantation s'avère comporter des faiblesses, ce qui est beaucoup plus probable, alors un attaquant potentiel pourra, une fois contournée cette défense périmétrique, accéder immédiatement aux informations importantes.

Pourtant, il existe une autre configuration à considérer dans un contexte de tolérance aux agressions. Il s'agit de ne sécuriser la connexion Wi-Fi qu'avec le protocole initial WEP et à compléter cette première ligne de défense par un chiffrement de couche basse comme IPsec [5]. On a ainsi (voir figure 3) une configuration typique de cet axe de défense, puisque l'attaquant potentiel, s'il parvient assez facilement à casser la première ligne de défense (le WEP) se retrouve ensuite face à une deuxième barrière (IPsec) pas forcément prévue et potentiellement aussi solide au plan cryptographique que WPA2. L'intérêt de cette approche est que la pénétration de la première ligne de défense constitue déjà un délit, puisqu'il y a cassage de la clé WEP, et que cet accès frauduleux peut être détecté dès lors qu'un trafic non autorisé (non IPsec) apparaît sur le réseau sans fil.

Bien entendu, il est encore plus sûr de mettre en place un chiffrement WPA de la liaison radio en complément du chiffrement IPsec interne, mais l'objet ici était de montrer l'intérêt que pouvait

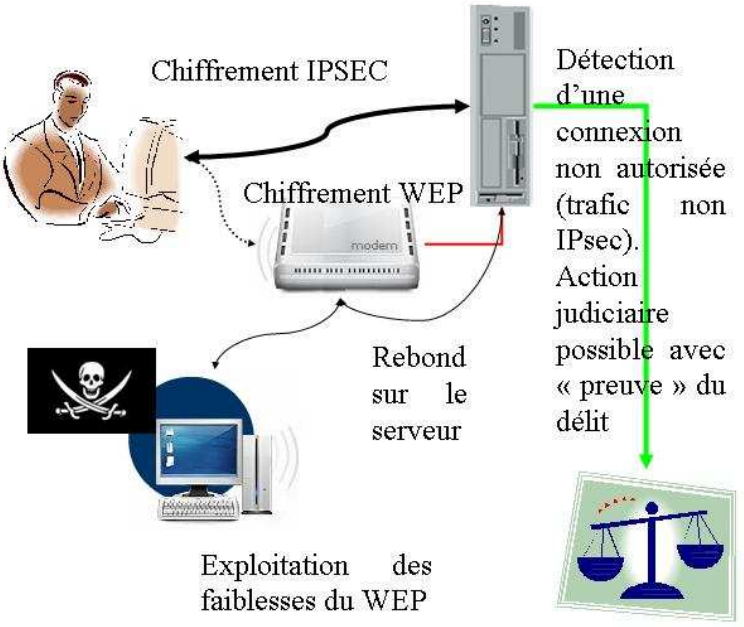

FIG. 3: Défense en profondeur d'un réseau sans-fil

avoir une démarche de défense en profondeur où la première ligne de défense n'est pas la seule ligne de défense d'une part, et où, d'autre part, elle ne constitue pas la ligne de défense la plus forte.

Détecter. Ce quatrième axe de défense en est encore à un stade peu avancé malgré les travaux menés dans le cadre de la détection d'intrusion. Plus exactement, l'exploitation opérationnelle de ces techniques est trop peu répandue. En effet, la détection consiste à identifier, **en vue d'y réagir**, les incidents ou compromissions qui surviennent sur le système d'exploitation. Or, trop souvent, les systèmes de détection d'intrusion, de même que les systèmes de protection périphérique qui peuvent remonter des alarmes sur des anomalies (pare-feu, chiffreur IP, etc.), ne donnent pas lieu à un traitement d'incident approfondi. Même si des outils de détection d'intrusion sont en place, leurs alertes sont souvent ignorées, faute de quelqu'un pour les surveiller. Or, en l'espèce, si une attaque réussit sur un système, l'attaquant va systématiquement chercher à cacher les traces de sa première agression car ce sont celles qui le mettent le plus en danger.

Réparer. Enfin, lorsque l'irréparable survient, il faut quand même pouvoir repartir sur des bases saines ! Et c'est souvent lorsqu'il est trop tard que l'on se rend compte que l'on ne dispose pas des moyens de remettre en fonctionnement nominal le système d'information, soit que les sauvegardes n'aient pas été effectuées correctement, soit que ces sauvegardes aient elles-mêmes été altérées par l'attaque, soit que le système d'information ne dispose pas de moyen de repartir d'un état sain.

2.3 Un constat : la SSI est intolérante !

Le constat que l'on peut dresser actuellement de la prise en compte de la sécurité des systèmes d'information est que seuls les deux premiers axes de la défense en profondeur sont réellement pris en compte. Historiquement, les défenses ont été édifiées dans une approche de blocage périphérique sous forme de pare-feu installés en segments d'interface (DMZ) et de dispositifs de contrôle d'accès distant. Depuis peu, le maintien à jour des systèmes opérationnels est devenu une réalité qui progresse grâce à la mise en place, par la quasi-totalité des éditeurs de systèmes d'exploitation et de logiciels, de systèmes de mises à jour automatiques et sécurisés. Cette approche constitue une mesure de prévention saine, surtout si elle est complétée par des outils d'audit indépendants permettant de vérifier la réalité des corrections apportées.

Historiquement toujours, des tentatives ont également vu le jour pour détecter et réparer les systèmes opérationnels. Il s'agit bien entendu des anti-virus et des systèmes de détection d'intrusion. Toutefois, ces outils s'avèrent de plus en plus impuissants face à l'explosion exponentielle du nombre d'attaques et aux techniques d'évasion mises en place par les codes malveillants. Cette évolution a en son temps été annoncée parcMarkus Ranum [6].

À ceci, nous proposons une explication provocatrice : la détection actuelle recherche les causes au lieu des effets ! En effet, deux grandes approches existent en matière de détection :

- la détection par signature vise à identifier une attaque connue en fonctions de caractéristiques précalculées ; les performances de ces outils sont directement liées aux algorithmes d'indexation et de recherche utilisés, mais il leur est difficile de s'écarter d'un modèle comportemental observé, c'est-à-dire que ces mécanismes de détection peuvent difficilement réagir à des attaques nouvelles inconnues ;
- la détection comportementale tente quant à elle de modéliser un comportement normal pour pouvoir distinguer des réaction anormales du système d'information ; dans les faits, il s'avère difficile d'obtenir un taux élevé de détection sans engendrer un nombre conséquent de faux positifs.

Bien entendu, cette seconde approche, qui cherche à détecter les effets d'une attaque, est intellectuellement plus satisfaisante car elle permet d'envisager de détecter les effets d'une attaque, même inconnue. Dans la pratique, la première approche reste toutefois celle qui donne rapidement des résultats.

Pour que cette seconde approche puisse être efficace, il faut que le comportement "normal" soit facilement identifiable et que les écarts à ce comportement soient caractéristiques d'une transgression. Or c'est exactement ce que l'on observe sur un système d'information "tolérant" aux agressions. En effet, si le système d'information a été conçu avec des hypothèses d'agression, il est possible d'en limiter *a priori* les effets en réduisant les privilèges des applications au strict minimum de leurs besoins. Par exemple, si un logiciel de messagerie a été, par un cloisonnement, isolé des applications de banque en ligne, le fait de chercher à accéder depuis ce logiciel à un service de banque en ligne est sans doute le révélateur d'une attaque par hameçonnage (*phishing*). De même, dans l'exemple ci-dessus (cf. § 2.2), une intrusion sur le réseau sans-fil pourra être facilement révélée parce que le comportement normal du réseau sera de n'autoriser qu'un trafic IPsec.

Ce qui est d'ailleurs étonnant en la matière est que les techniques de pot de miel reviennent justement à réaliser des systèmes d'information tolérants aux agressions pour être en mesure de les détecter et de les analyser. Le paradoxe est qu'on en vient ainsi à réaliser des configurations particulièrement sécurisées et à les appliquer sur des systèmes qui ne contiennent aucune information intéressante, alors que les systèmes intéressants, quant à eux, ne bénéficient pas des mêmes efforts de sécurisation !

3 Axes d'effort techniques

Le rapport [2] identifie un certain nombre d'axes d'effort techniques. Nous allons maintenant illustrer certains d'entre eux.

3.1 Systèmes d'exploitation et évolution des paradigmes de sécurité

L'une des technologies de tout premier plan dont la maîtrise au plan de la sécurité reste à améliorer est celle des systèmes d'exploitation. En effet, bien que présent sur tout équipement informatique, depuis le serveur jusqu'au téléphone, dans la majorité des cas le système d'exploitation reste vulnérable à des attaques. Nuançons toutefois le propos, les systèmes d'exploitation des serveurs exploitent désormais des fonctionnalités de cloisonnement qui les rendent plus robustes. C'est là une des conséquences de leur exposition permanente aux attaques de l'internet. Mais, sauf dans de très rares cas, les terminaux des utilisateurs n'exploitent pas ces possibilités, principalement pour des problèmes d'ergonomie. Or l'évolution des applications fait que ces terminaux vont devoir très prochainement renforcer de façon drastique leur sécurité. En effet, de nombreuses applications temps réel (jeux, téléphonie, visiophonie, etc.) sont en train de se déployer sur les postes terminaux. Or ces applications ne peuvent pas être sécurisées correctement au niveau périphérique car leur caractère temps réel interdit de les faire passer par une passerelle de vérification. Tout au plus peut-on contrôler le flux initial de signalisation.

Mais si les différentes solutions de sécurité existent depuis longtemps, il s'avère difficile de les mettre en place pour des raisons d'ergonomie. C'est la raison pour laquelle a été lancée en 2008, en liaison avec l'agence nationale de la recherche, un appel à projets de type "défi", consacré à une configuration sécurisée pour l'internaute [7]. L'idée est de regrouper sur une même configuration plusieurs fonctionnalités distinctes qui restent cloisonnées les unes des autres, par exemple la télédéclaration des impôts, la banque en ligne, la messagerie, etc. et de permettre ainsi d'utiliser ces fonctionnalités indépendantes les unes des autres sans risque de voir une vulnérabilité de l'une mettre en cause une autre fonction. On retrouve là une démarche de défense en profondeur classique. Si cette initiative permet d'aboutir à un résultat intéressant, il sera possible de l'étendre à d'autres fonctionnalités comme les réseaux pair-à-pair ou la téléphonie sur IP.

3.2 Cryptographie et architectures de gestion de clés

Le domaine de la cryptographie est l'un de ceux qui est identifié dans le rapport comme devant être maîtrisé. Il pourrait sembler curieux de continuer à faire porter l'effort sur un domaine où les résultats semblent acquis. Mais la recherche en cryptographie a souvent vu des avancées surprises remettant en cause des résultats apparemment consolidés. Ainsi, les attaques de 2005 [8] dans le domaine des fonctions de hachage ont profondément remis en cause celui-ci. Les fonctions de hachage largement employées dans les systèmes opérationnels doivent maintenant être remplacées par de nouvelles, qui restent encore à définir. En effet, même si les attaques en question, qui visent à construire des collisions, ne remettent pas en cause toutes les applications des fonctions de hachage, ces attaques démontrent des faiblesses qui doivent être considérées comme des signaux d'alarme vis-à-vis d'attaques plus efficaces encore.

Or, ce qu'il faut prendre en compte en matière de cryptographie c'est l'extraordinaire inertie des systèmes d'information. Changer un algorithme cryptographique dans un système d'information peut sembler simple en théorie. Dans la pratique, dès lors que le système est un peu complexe, met

en jeu plusieurs acteurs et est disséminé physiquement, le changement d'algorithme cryptographique s'avère pénible, plus exactement il est souvent très long de pouvoir retirer un algorithme faible du service opérationnel, alors que tant qu'il est pris en compte au titre de la compatibilité ascendante, c'est une possible vulnérabilité pour le système tout entier.

À titre d'illustration, prenons le cas de l'infrastructure de gestion de la confiance de l'administration (IGC/A), dont l'autorité de certification racine est gérée par la DCSSI [9]. La clé de certification utilisée a été générée le 13 décembre 2002. À cette date, pour que le certificat puisse être utilisable par la majorité des navigateurs employés effectivement, le dimensionnement de ce dernier a été limité à RSA 2048 bits et la fonction de hachage utilisée était SHA-1. Par ailleurs, pour disposer de deux clés publiques possibles, au cas où un problème surviendrait sur RSA, une seconde clé publique conforme au standard DSA a été générée. À l'époque cette clé était de 1024 bits et utilisait là encore SHA-1. Cinq ans plus tard, et après l'édification des textes réglementaires qui assurent la légitimité de cette racine, c'est toujours cette même clé publique RSA qui vient d'être incorporée dans les magasins de certificats par défaut, par exemple ceux gérés par Microsoft. Entre temps, outre les évolutions sur les fonctions de hachage déjà évoquées, la DCSSI a également formalisé des règles et recommandations sur les dimensionnements des mécanismes cryptographiques [10], qui font que ces dimensionnements sont d'ores et déjà obsolètes.

Face à ces évolutions, la DCSSI va devoir générer de nouvelles clés publiques. La clé DSA va tout d'abord être détruite sans avoir jamais été utilisée, ce qui évite le problème de sa révocation. Une clé EC-DSA va la remplacer pour rétablir une redondance algorithmique. À terme, une nouvelle clé RSA, de taille renforcée (4096 bits) sera générée et utilisée avec une nouvelle fonction de hachage, vraisemblablement SHA256.

Pour autant, il est peu vraisemblable que la clé actuelle soit révoquée car elle a été utilisée pour certifier des autorités de certification racine ministérielles et la retirer du service pourrait poser des problèmes opérationnels. Il y a donc fort à parier que cette clé survive jusqu'à la date prévue de son expiration, en 2020, même si elle n'est plus utilisée pour certifier de nouvelles autorités racines.

Cet exemple montre l'extraordinaire difficulté qu'il y a à modifier des algorithmes cryptographiques lorsqu'ils sont enfouis profondément dans un système d'information. Il convient donc, le plus tôt possible, et c'est la raison d'être d'une recherche active en cryptographie, d'anticiper les évolutions pour ne pas se retrouver dans des situations dangereuses où des algorithmes obsolètes continuent d'être employés.

3.3 Fédération d'identités

L'authentification est l'un des domaines d'amélioration importants de la sécurité des systèmes d'information. On constate en effet, par exemple, que des attaques par hameçonnage (*phishing*) exploitent des faiblesses structurelles des systèmes d'authentification actuellement employés, largement basés sur le diptyque identifiant/mot de passe. Des propositions de solution à ces problèmes sont développées depuis de nombreuses années dans le domaine de la fédération d'identité, sans que la mise en place de ces solutions soit réellement effective. Il y a en effet un travail important à réaliser, à la fois au plan technique et juridique, pour harmoniser les différents systèmes d'authentification et permettre de répondre à des questions comme : "si je m'authentifie par un mot de passe à usage unique (*OTP*), l'implication légale quant à l'engagement de ma responsabilité est-il de même niveau que si je m'authentifie à l'aide d'une empreinte digitale ?" En effet, dans cet exemple, la diversité des réalisations techniques dans ces deux domaines rend toute réponse systématique impossible. Or, c'est justement en répondant à ce type de question que la problématique cruciale de l'imputabilité des actions d'une personne dans le monde numérique pourra être résolue.

Dans ce domaine, la DCSSI a proposé une nouvelle modélisation de l'authentification distante au travers d'un référentiel technique [11] et d'une communication [12]. Cette modélisation a pour but de clarifier la distinction entre mécanismes cryptographiques et mécanismes de déverrouillage dans un processus d'authentification. Les seconds se caractérisent par le fait qu'ils sont rejoués par l'utilisateur à chaque authentification, alors que les premiers doivent être insensibles au rejeu. Un mot de passe est ainsi clairement un mécanisme de déverrouillage et non un mécanisme d'authentification cryptographique.

À titre d'exemple, un protocole d'authentification basé sur un système de mot de passe à usage unique pourra être représenté (voir fig. 4) entre trois acteurs qui disposent respectivement :

- pour l'utilisateur, qui emploie des mécanismes de déverrouillage :
  - d'un identifiant id,
  - d'un éventuel mot de passe statique $smdp$,
  - d'un environnement de confiance local, qui peut également mettre en oeuvre un mécanisme de déverrouillage propre (pin-code, empreinte digitale, etc.).
- pour l'environnement de confiance, qui emploie des mécanismes cryptographiques :
  - d'une clé $K_\pi^{(id)}$ dépendant de l'identifiant et permettant de "prouver" cette identité,
  - éventuellement d'un compteur interne t.
- pour le SI distant :
  - éventuellement de la valeur $H^{(id)}(smdp)$,
  - d'une clé $K_\nu^{(id)}$ dépendant de l'identifiant et permettant de "vérifier" cette identité,
  - éventuellement d'un compteur interne t',
  - éventuellement d'un générateur de défi aléatoire $chall$.

La fédération d'identité, si elle permet de développer des solutions d'authentification, porte également en germe l'apparition de nouveaux acteurs de la sécurité des systèmes d'information, qui pourraient cherche à tirer profit de leur positionnement central dans les processus d'authentification. La confiance dans ces acteurs doit donc se construire progressivement et il est donc important que la recherche dans ce domaine progresse pour stimuler l'amélioration de la sécurité globale des solutions proposées et assurer un contrôle extérieur de leur qualité.

4 Conclusion

La recherche dans son ensemble peut contribuer à développer les compétences au niveau national et européen sur les technologies critiques pour la sécurité des systèmes d'information. Mais, inversement, son rôle est aussi de mettre en évidence le caractère critique de certaines technologies afin que des décisions d'ordre politique puissent être prises à bon escient. Il est important aussi de noter que des intérêts apparemment divergents peuvent exister entre sécurité et apport économique. C'est toutefois souvent une vision de court terme, car le besoin de sécurité, s'il est réel, finit toujours par s'imposer et le coût de la sécurité est toujours beaucoup plus élevé si elle n'a pas été prise en compte dès le début de la mise en place d'une technologie.

Il importe enfin de ne pas ignorer des initiatives sous des prétextes idéologiques. Toute technologie de sécurité apporte plus ou moins de bons et de mauvais côtés. Il est donc, au contraire, indispensable de participer à ces évolutions pour éventuellement pouvoir alerter sur leurs dangers et donner au politique des arguments objectifs permettant d'en corriger d'éventuels travers. Dans ce domaine, la recherche a un rôle capital à jouer, un rôle citoyen, qu'elle se doit d'assumer à la manière de ce qu'elle a pu faire dans la prise de conscience sur les questions environnementales.

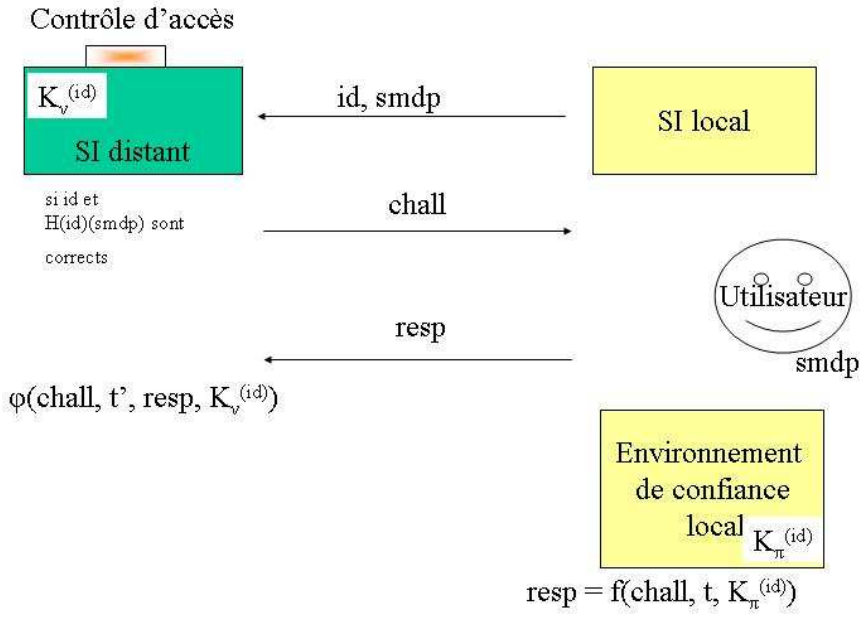

FIG. 4: Modélisation d'un mot de passe à usage unique

Références

1. *Orientation des travaux de recherche et de développement en matière de sécurité des systèmes d'information*, rapport public n°2571/SGDN/DCSSI/SDS du 30 novembre 2006, `http://www.ssi.gouv.fr/fr/sciences/fichiers/rapports/rapport_orientation_ssi_2006.pdf`.
2. *Orientation des travaux de recherche et de développement en matière de sécurité des systèmes d'information*, édition 2008, à paraître.
3. Le petit Larousse illustré, 2005, 100ième édition.
4. *Aircrack-ng, a 802.11 WEP and WPA-PSK keys cracking program*, `http://www.aircrack-ng.org/`.
5. S. Kent and K. Seo, *Security Architecture for the Internet Protocol*, RFC 4301, Déc. 2005, `http://tools.ietf.org/html/rfc4301`.
6. M. Ranum, *The Six Dumbest Ideas in Computer Security*, Sept. 2005, `http://www.ranum.com/security/computer_security/editorials/dumb/`.
7. *Défi Sécurité Système d'Exploitation Cloisonné et Sécurisé pour l'Internaute*, agence nationale de la recherche, appel à projet 2008, `http://www.agence-nationale-recherche.fr/AAPProjetsClos?NodId=18&lngAAPId=180`.
8. X. Wang, Y. L. Yin and H. Yu, *Finding Collisions in the Full SHA-1*, pp. 17-36, LLNCS 3621,CRYPTO 2005.

9. *Avis relatif aux certificats électroniques de l'autorité de certification racine de l'administration française, dits "certificats IGC/A"*, JORF n°41 du 17 février 2007, page 2946, texte n° 126, NOR : PRMX0710016V, `http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000646696`.
10. *Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard*, n°2741/SGDN/DCSSI/SDS/LCR version 1.10 du 19/12/2006 `http://www.ssi.gouv.fr/site_documents/politiqueproduit/Mecanismes_cryptographique_v1_10_standard.pdf`.
11. *Authentification - Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard*, n°729/SGDN/DCSSI/SDS du 12/04/2007, `http://www.ssi.gouv.fr/fr/politique_produit/catalogue/pdf/authentification_robustesse_standard_v0-13.pdf`.
12. F. Chabaud and O. Grumelard, *Authentication - a model of human - machine authentication, A common European language to identify security levels of authentication methods* ENISA, Novembre 2006 `http://www.ssi.gouv.fr/fr/sciences/fichiers/astec/authentication_enisa.pdf`.