RECOMMANDATIONS RELATIVES À LA SÉCURITÉ DES (SYSTÈMES D') OBJETS CONNECTÉS

GUIDE ANSSI

ANSSI-PA-087
2021-08-27

PUBLIC VISÉ :

Développeur Administrateur RSSI DSI Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations relatives à la sécurité des (systèmes d') objets connectés »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`.
Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab [20].
Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.
Sauf disposition réglementaire contraire, ces recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	2021-08-27	publication initiale

Table des matières

1
Introduction

1.1 Objectif du guide

Le terme d'objet connecté recouvre aujourd'hui des matériels très divers,allant du *pacemaker* au système industriel en passant par des équipements de domotique grand public ou professionnels. De tels dispositifs présentent des risques qui peuvent être perçus comme nouveaux du fait de leur capacité à produire des effets "physiques" en dehors des systèmes d'information, ou des effets systémiques résultant de déploiements massifs ; mais ils sont également concernés par les menaces SSI classiques, pouvant être exacerbées par les faibles ressources disponibles pour assurer leur sécurité, ou par les difficultés de maintenance de systèmes non administrés.

Il est illusoire de vouloir proposer une lecture unique de la sécurité des objets connectés du fait de la diversité des situations rencontrées. Cet état de fait n'est cependant pas inhabituel : le point de départ de toute réflexion visant à assurer la sécurité d'un système consiste en une analyse de sécurité, qui permet d'identifier les scénarios d'attaque probables, les biens à protéger, les fonctions de sécurité et ce qui garantit leur bon fonctionnement. Une telle démarche permet d'accorder des recommandations générales à une situation particulière.

L'ambition de ce guide est donc double : d'une part, faciliter la réalisation d'une analyse de sécurité en listant des menaces potentielles pertinentes ; d'autre part, formuler des recommandations techniques permettant de répondre à ces menaces lorsque cela peut être fait de façon générique.

Le périmètre qui nous concerne est celui des objets connectés - que nous nommerons *dispositifs connectés* par la suite - et des systèmes mettant en œuvre des ensembles de dispositifs connectés dialoguant entre eux, que nous nommerons plus simplement *systèmes connectés*. Un dispositif est *connecté* s'il dispose d'une liaison numérique avec son environnement, généralement sous la forme d'un protocole qui n'est pas seulement point-à-point et qui supporte plusieurs rôles (transfert de données, mais aussi commande, mise à jour, etc.).

Les dispositifs connectés sont souvent en mesure d'interagir *physiquement* avec leur environnement, à travers des capteurs et/ou des actionneurs.

Enfin, les dispositifs connectés disposent le plus souvent d'un haut niveau d'autonomie, ce qui implique en général

- une capacité d'intervention auprès des dispositifs qui est réduite ou inexistante (pour dépannage, reconfiguration, etc.),
- des capacités de calcul, de stockage (volatil mais aussi non volatil) et de communication limitées, pour des raisons de coût ou de consommation énergétique. Ces capacités réduites peuvent restreindre les possibilités de mise à jour logicielles, ou empêcher l'emploi de protocoles réseau ou de standards cryptographiques non spécifiquement prévus pour ce cadre d'emploi.

1.2 Conventions de lecture

Pour certaines recommandations, il est proposé, au vu des menaces constatées lors de la rédaction de ce guide, plusieurs solutions qui se distinguent par le rapport entre le niveau de sécurité qu'elles permettent d'atteindre et leur difficulté d'implémentation. Le lecteur a ainsi la possibilité de choisir une solution offrant la meilleure protection en fonction du contexte et de ses objectifs de sécurité.

Ainsi, les recommandations sont présentées de la manière suivante :

R *

Recommandation à considérer en premier lieu

Cette recommandation est d'une difficulté de mise en œuvre minime au regard des garanties qu'elle offre.

R **

Recommandation à considérer en second lieu

Cette recommandation est d'une difficulté de mise en œuvre intermédiaire au regard des garanties qu'elle offre.

R ***

Recommandation adaptée à un besoin de sécurité élevé

Cette recommandation est d'une difficulté de mise en œuvre élevée, et doit être suivie lorsque les recommandations de mise en œuvre plus aisée ne permettent pas d'atteindre un niveau de risque résiduel acceptable.

R

Recommandation générale

L'effort requis pour mettre en œuvre cette recommandation, ou la protection qu'elle offre, ne peuvent être estimés indépendamment du contexte.

Dans une démarche permanente de gestion du risque numérique et d'amélioration continue de la sécurité des systèmes d'information [1], la pertinence de mise en œuvre des recommandations décrites dans ce document doit être périodiquement réévaluée.

La liste récapitulative des recommandations est disponible en page 36.

1. Se reporter au guide ANSSI relatif à la maîtrise du risque numérique [5].

2
Architecture d'un système connecté et propriétés de sécurité attendues

Objectif

Le présent chapitre expose la démarche visant à déterminer les mesures techniques pertinentes pour protéger un système connecté. Ces mesures visent à satisfaire des objectifs de sécurité dont une liste est proposée pour un système connecté générique.

Dans le cas le plus général, une analyse de risques permet de déterminer au cas par cas quelles sont les menaces à considérer sur un système, et permet de caractériser la couverture de ces menaces par les fonctions de sécurité. L'analyse de risques, et certaines spécificités des systèmes connectés, sont développées au paragraphe 2.1.

En vue de faciliter l'analyse de risques d'un système connecté et l'élaboration des mesures de sécurité à employer , un système connecté type, et un ensemble d'objectifs de sécurité pertinents pour celui-ci, sont exposés respectivement aux paragraphes 2.2 et 2.3. Ces objectifs sont mis en relation avec les éléments et les interactions qu'ils concernent dans le système. Cette correspondance permet de déterminer l'ensemble des propriétés applicables à une situation réelle ne comportant qu'une partie des éléments du système type. Dans la section 2.4, ces objectifs sont associés aux recommandations techniques qui permettent de les atteindre et qui sont détaillées au chapitre 3. Pour approfondir le sujet, de nombreuses références externes qui ont été employées lors de la rédaction de ce guide sont référencées dans l'annexe A.

Une liste de recommandations techniques applicables à une situation particulière peut être obtenue

- en identifiant, via la section 2.2, les éléments à protéger ;
- en compilant la liste des objectifs de sécurité à considérer à cette fin avec la section 2.3,
- en traduisant enfin ces objectifs abstraits en recommandations techniques à l'aide de la matrice du paragraphe 2.4.

Lors de l'application de cette démarche à un système réel, une attention particulière doit être portée à ce qui n'est pas couvert par le système type et qui nécessite une analyse et des réponses *ad hoc*.

2.1 Analyse de risques, objectifs et fonctions de sécurité

L'analyse de risques vise à identifier en toute généralité les éléments à protéger, les propriétés à garantir, les scénarios d'attaque probables étant donné le déploiement envisagé, et permet de choisir les mesures de protection à mettre en œuvre.

Le périmètre de cette analyse ne doit pas se limiter aux dispositifs déployés, mais doit inclure le système connecté dans son intégralité. En effet, les éléments déportés de cette infrastructure et les dispositifs déployés forment un ensemble cohérent d'hypothèses et de propriétés de sécurité qui doivent se correspondre.

Les éléments du système, leurs interactions, ainsi que les interactions entre les dispositifs connectés et leur environnement, déterminent les biens sensibles du système. Ceux-ci sont à identifier parmi

- les données manipulées : on veut généralement garantir la confidentialité et/ou l'intégrité des données sensibles. L'intégrité des données peut être nécessaire pour garantir des prises de décision correctes, notamment lorsqu'elles sont issues de capteurs physiques ;
- l'état des dispositifs et de l'infrastructure : de leur intégrité et leur disponibilité peuvent dépendre les biens et les personnes présents dans leur environnement, et également des tiers susceptibles de subir des attaques auxquelles les dispositifs prendraient part.

Face aux éléments à protéger, l'analyse des vecteurs d'attaque potentiels s'appuie sur le scénario de déploiement envisagé par le concepteur, ou, dans le cas de produits grand public, sur un scénario probable de déploiement du produit. Dans tous les cas, ce scénario doit être *explicite* et *réaliste*.

Exemple

Dans le cas de dispositifs grand public exposant des fonctionnalités sur Internet, il n'est en général pas crédible de supposer que l'environnement assure la protection des dispositifs vis-à-vis de malveillances provenant du réseau.

L'analyse des éléments à protéger et des scénarios d'attaque en rapport avec l'environnement, dans un contexte d'emploi donné, peut être effectuée à travers une méthodologie normalisée comme EBIOS Risk Manager [10]. Cette analyse permet également d'expliciter les recommandations d'emploi du système et les risques résiduels que son opérateur doit accepter.

L'expérience relative aux systèmes connectés fait apparaître des spécificités dans leur analyse de sécurité.

- Les dispositifs connectés manipulent souvent des données d'apparence anodine mais dont des usages détournés peuvent avoir des implications sécuritaires. Par exemple, l'accumulation des positions instantanées d'un téléphone permet de déduire le domicile de son propriétaire et les moments où il en est absent ; le croisement de données de position de plusieurs téléphones permet de construire des graphes sociaux. De même, des données de consommation électrique ou de fonctionnement d'ampoules connectées renseignent sur la présence de personnes physiques. Plus généralement, des dispositifs n'ayant pas eux-mêmes de rôle sécuritaire peuvent poser des problèmes de sécurité à leurs utilisateurs dès lors que leur emploi nécessite la création d'un compte utilisateur comportant des données personnelles et que celles-ci sont mal protégées.
- L'altération de données issues de capteurs ou obtenues d'une source en dehors du périmètre analysé peut avoir des conséquences sécuritaires. Le contrôle de la fiabilité de signaux issus de capteurs physiques en présence d'un attaquant et avant la traduction de ces signaux en valeurs numériques ne relève de pas de la SSI et par conséquent, ce guide ne propose pas de mesure pour s'en prémunir [2] ; la probabilité et l'impact de mesures faussées doivent toutefois être évalués dans le cadre d'une analyse de risque.

2. Des techniques utilisées en sûreté de fonctionnement peuvent contribuer a maîtriser ce problème, comme la redondance de capteurs.

2.2 Système type

Un système connecté type, ici un système domotique, est représenté figure 2.1. Il est composé d'une infrastructure centralisée (1) à laquelle sont adossés les dispositifs connectés déployés (2). Cette infrastructure est accessible depuis Internet (3) ; elle peut être complémentée des ressources nuagiques externes (4) qui font alors partie du système pour ce qui concerne son analyse de sécurité. Les utilisateurs interagissement directement avec les dispositifs déployés, mais également indirectement avec ceux-ci *via* les fonctions accessibles depuis Internet.

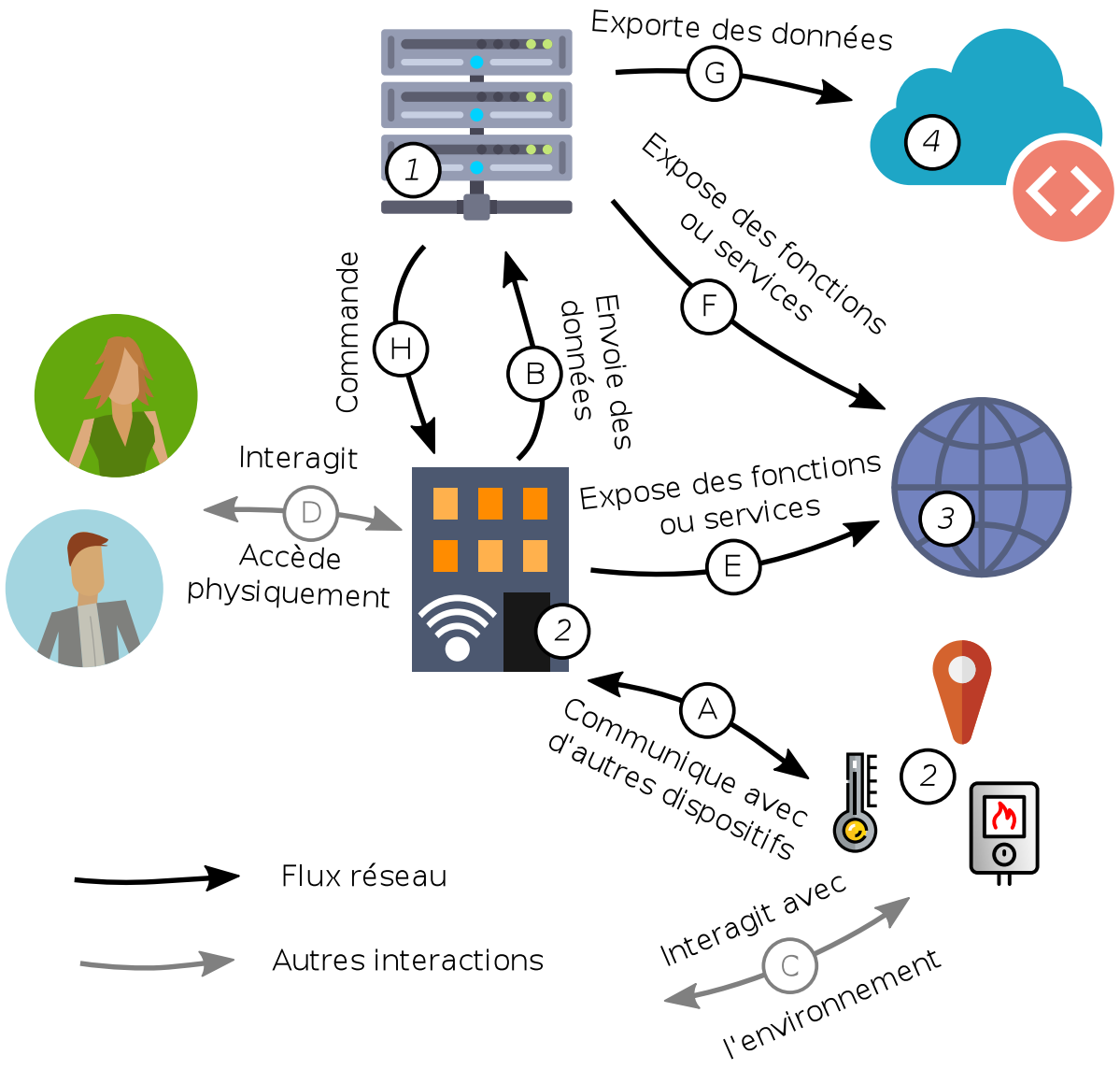


FIGURE 2.1 – Système connecté type

2.3 Objectifs de sécurité pour un système connecté

Ce paragraphe détaille différents objectifs de sécurité pouvant s'appliquer à un système connecté. Ces objectifs sont énoncés indépendamment des mesures techniques et/ou organisationnelles qui permettent de les réaliser.

2.3.1 Se protéger contre un environnement potentiellement hostile

OBJ 1

Menaces internes et externes

Le système se protège contre les menaces provenant de l'extérieur de son périmètre, mais aussi de ses propres constituants ;

OBJ 2

Communications

Les communications entre les constituants du système sont authentifiées et sont limitées au strict nécessaire ;

OBJ 3

Utilisateurs et commandes

Les entités interagissant avec le système sont authentifiées avant toute commande et les informations qu'ils fournissent sont strictement validées ;

Les entités évoquées dans le précédent objectif sont les utilisateurs physiques, mais aussi les utilisateurs logiques interagissant avec le système depuis l'extérieur.

OBJ 4

Menaces physiques

Les dispositifs déployés sont protégés contre les menaces physiques directes ;

OBJ 5

Sécurité par défaut

Les dispositifs déployés sont protégés par défaut, avant même toute configuration.

2.3.2 Concevoir la sécurité tout au long de la vie du dispositif

OBJ 6

Initialisation et propagation de la confiance

La confiance entre dispositifs s'appuie sur des secrets correctement protégés et disposant d'une gestion complète de leur cycle de vie.

OBJ 7

Maintien en condition de sécurité

Le maintien en condition de sécurité des dispositifs est assuré par des mises à jour logicielles applicables de façon réaliste dans leur cadre d'emploi ; l'état de sécurité des dispositifs est public ;

2.3.3 Maîtriser les fonctions de sécurité

Les objectifs ci-dessous visent à limiter la présence de failles dans le système et l'effet de celles-ci sur sa sécurité, afin de réduire autant que possible le coût du maintien en condition de sécurité.

OBJ 8

Composants éprouvés

Les composants logiciels ou matériels utilisés dans des fonctions de sécurité sont éprouvés et un suivi de leurs vulnérabilités est assuré ;

OBJ 9

Méthode de développement

La méthode de développement logiciel et les outils utilisés pour la mettre en œuvre tiennent compte des bonnes pratiques de sécurité ;

OBJ 10

Minimisation

L'utilisation de composants ou logiciels standards n'inclut pas de service ou d'interface inutile ;

OBJ 11

Maîtrise de l'état des dispositifs

L'intégrité des fonctions des dispositifs est garantie ;

OBJ 12

Journalisation

Les événements relatifs à la sécurité du système sont journalisés et accessibles à l'analyse ;

OBJ 13

Prise en compte des risques systémiques

Les risques systémiques liés aux déploiements massifs de dispositifs, et à l'atteinte à leur disponibilité ou à leur bon fonctionnement, sont intégrés dans l'analyse de la menace.

Les risques systémiques peuvent menacer le bon fonctionnement du système, mais aussi être sans rapport avec celui-ci, comme par exemple dans le cas d'attaques par déni de service.

2.3.4 Assurer une protection continue des données sensibles

OBJ 14

Protection des données

La confidentialité et l'intégrité des données sont assurées durant leur stockage et durant leur transport ;

OBJ 15

Interface avec des systèmes tiers

Une politique de gestion des données exportées vers un SI distant est définie et appliquée ;

OBJ 16

Données utilisateurs

Les données appartenant aux utilisateurs restent sous leur contrôle.

2.3.5 Objectifs et architecture type

Les différentes interactions de l'architecture présentée figure 2.1 appellent chacun un sous-ensemble particulier des objectifs précédents :

- A (communication entre dispositifs) : OBJ 1 - Menaces internes et externes, OBJ 2 - Communications, OBJ 5 - Sécurité par défaut, OBJ 6 - Initialisation et propagation de la confiance, OBJ 10 - Minimisation
- B (envoi de données des disposifs vers l'infrastructure) : OBJ 2 - Communications, OBJ 6 - Initialisation et propagation de la confiance, OBJ 13 - Prise en compte des risques systémiques, OBJ 14 - Protection des données, OBJ 16 - Données utilisateurs
- C (interaction avec l'environnement) : OBJ 13 - Prise en compte des risques systémiques
- D (interactions les dispositifs et les utiliateurs physiques) : OBJ 3 - Utilisateurs et commandes, OBJ 4 - Menaces physiques, OBJ 5 - Sécurité par défaut
- E, F (exposition des dispositifs et de l'infrastructure à des réseaux extérieurs comme Internet) : OBJ 1 - Menaces internes et externes, OBJ 2 - Communications, OBJ 3 - Utilisateurs et commandes, OBJ 5 - Sécurité par défaut, OBJ 10 - Minimisation
- G (communication entre l'infrastructure et des ressources nuagiques tierces) : OBJ 1 - Menaces internes et externes, OBJ 2 - Communications, OBJ 14 - Protection des données, OBJ 15 - Interface avec des systèmes tiers, OBJ 16 - Données utilisateurs
- H : OBJ 1 - Menaces internes et externes, OBJ 2 - Communications,OBJ 5 - Sécurité par défaut

L'infrastructure centrale (*1*) et les dispositifs connectés (*2*) appellent eux-mêmes les objectifs suivants :

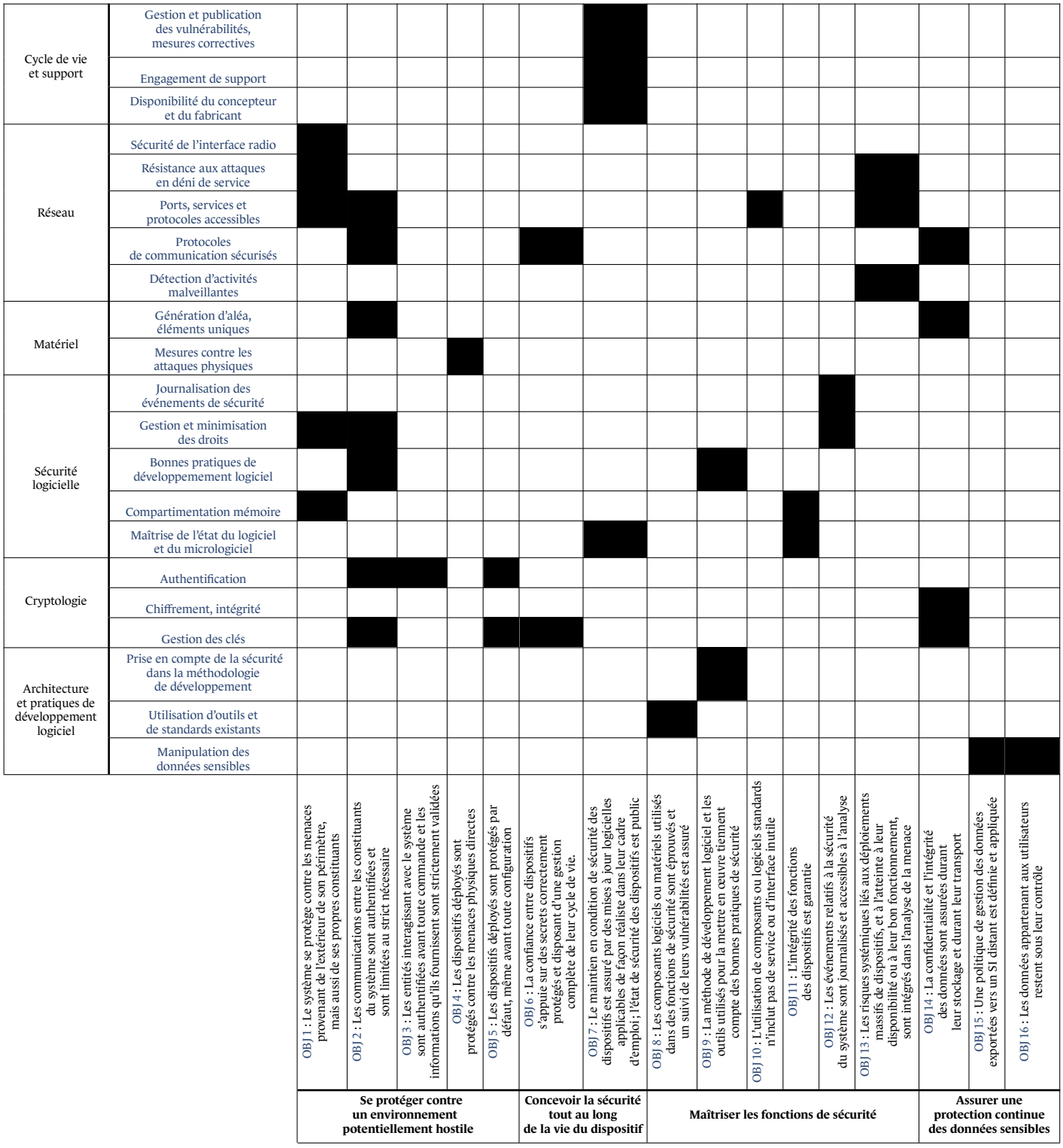
- *1* : OBJ 16 - Données utilisateurs
- *2* : OBJ 5 - Sécurité par défaut, OBJ 7 - Maintien en condition de sécurité

Enfin, les objectifs suivants sont pertinents indépendamment de l'architecture déployée :

- OBJ 5 - Sécurité par défaut
- OBJ 7 - Maintien en condition de sécurité
- OBJ 8 - Composants éprouvés
- OBJ 9 - Méthode de développement
- OBJ 11 - Maîtrise de l'état des dispositifs
- OBJ 12 - Journalisation
- OBJ 13 - Prise en compte des risques systémiques

2.4 Correspondance entre objectifs de sécurité et recommandations techniques

Le tableau ci-dessous indique les recommandations techniques pertinentes pour permettre d'atteindre les objectifs de sécurité énumérés au paragraphe 2.3.



3
Recommandations techniques

Objectif

Ce chapitre présente les différentes recommandations techniques proposées dans chaque catégorie listée au chapitre 2.

Il est rappelé que, comme indiqué au paragraphe 1.2, les recommandations techniques se voient attribuer un niveau matérialisé par un nombre d'étoiles compris entre 1 et 3. Une étoile est attribuée aux mesures à mettre en œuvre en priorité ; 3 étoiles indiquent au contraire une complexité de mise en œuvre élevée, ou un emploi limité aux niveaux d'assurance de sécurité les plus élevés. Certaines recommandations n'ont pas de niveau attribué, lorsque la complexité de mise en œuvre d'une mesure ne peut pas être estimée en raison de la diversité des situations couvertes par ce guide.

3.1 Architecture et pratiques de développement logiciel

3.1.1 Manipulation des données sensibles

3.1.1.1 Relation avec une infrastructure distante

Comme vu au paragraphe 2.2, des dispositifs connectés peuvent faire partie d'une architecture interconnectée de composants comprenant, outre les dispositifs connectés eux-mêmes, une infrastructure distante du point de vue du client final qui récolte, traite et/ou stocke des données issues des dispositifs connectés. Les données qui transitent entre les dispositifs et l'infrastructure distante sont potentiellement sensibles prises une par une ; elles peuvent présenter un caractère de sensibilité plus élevé encore une fois agrégées (entre utilisateurs, au cours du temps, etc.).

R 1 *

Collecte des données

Les données collectées auprès d'un utilisateur doivent être clairement identifiables par lui et leur collecte doit être nécessaire aux fonctions fournies.

R 2 *

Protection des données

Le transport et le stockage des données doit faire l'objet d'une protection adaptée en confidentialité et en intégrité.

Voir à ce propos également les recommandations R 24, R 25 et R 53.

R3*

Données dans une infrastructure distante

Les données sensibles confiées à une infrastructure distante doivent se voir appliquer une politique de gestion limitant les possibilités d'usage indésirable (emploi non conforme aux objectifs initiaux, vol, etc.).

Cette politique fixe

- une règle de rétention des données : délai au-delà duquel celles-ci sont effacées en cas d'absence d'utilisation, etc. ;
- la désensibilisation appliquée lors de l'agrégation de données (par exemple anonymisation, mais plus généralement suppression de toute information inutile à l'agrégat) ;
- le contrôle des utilisateurs finaux sur leurs données : généralement, la possibilité d'effacement, et la sélection des usages. Ce principe issu de la protection des consommateurs peut s'avérer pertinent pour des services fournis à des personnes morales.

Il existe des contraintes réglementaires pouvant s'appliquer à la collecte de données par une telle infrastructure, comme le Règlement Général pour la Protection des Données européen, entré en vigueur depuis mai 2018.

Le contrôle exercé par l'infrastructure distante sur les dispositifs connectés présente également un enjeu de sécurité qui doit être pris en compte dans la conception d'un système. La limitation des vulnérabilités liées à un tel contrôle comprend les mesures suivantes :

R4*

Minimisation des droits de l'infrastructure sur les dispositifs connectés

Les commandes que l'infrastructure peut émettre en direction des dispositifs connectés doivent être limitées au minimum requis par les fonctions attendues.

Il ne doit par exemple pas subsister en production de commandes uniquement utiles au déboguage du système.

R5*

Protection en intégrité des commandes

L'infrastructure doit s'authentifier avant de pouvoir émettre des commandes vers les dispositifs ; l'intégrité du flux de commandes émises doit être assurée. La confidentialité des commandes doit également être assurée dès lors que celles-ci véhiculent des informations sensibles.

La protection de l'intégrité du flux de commande implique, outre la garantie d'intégrité de chaque commande, la protection contre l'altération de leur succession, en particulier contre le rejeu de commandes passées. Une façon classique d'obtenir cette propriété est le calcul et la vérification de motifs d'intégrité sur chaque commande incluant une description non ambiguë de la position de la commande dans le flux. Une telle description fait généralement intervenir un compteur (dit *compteur anti-rejeu*) indiquant la position de la commande dans le flux. En cas de division du flux de commande en plusieurs flux logiques interdépendants (par exemple, deux sens de communication), la description de la position d'une commande doit permettre d'identifier le flux logique auquel elle appartient afin d'empêcher la réutilisation d'une commande dans un flux logique différent de son flux originel.

3.1.1.2 Données et fonctions sensibles dans un système connecté

R6

Environnement pour la réalisation de tâches sensibles

Il est recommandé de situer la réalisation de tâches sensibles dans un environnement présentant une exposition minimale aux attaques.

Les tâches sensibles incluent les traitements utilisant des données sensibles comme des secrets, ou les actions d'administration sur le système.

Exemple

Dans un système de contrôle d'accès, l'utilisation de lecteurs de badge "transparents", qui ne font que relayer l'information vers un élément central situé dans un local sécurisé et responsable des décisions sensibles, est préférable à l'exécution de ces mêmes opérations dans les lecteurs eux-mêmes.

3.1.2 Utilisation d'outils et de standards existants

R7*

Emploi de composants éprouvés

Dans le domaine des communications, sécurisées ou non, le concepteur doit privilégier l'emploi de

- standards existants, en particulier pour ce qui concerne la cryptographie et les communications réseau (protocoles existants dont les propriétés de sécurité sont bien comprises)
- bibliothèques logicielles éprouvées, en particulier pour la cryptographie, l'interprétation de protocoles et le décodage des données (*parsing*).

R8*

Maintien en condition de sécurité des composants tiers

L'usage de bibliothèques logicielles tierces doit s'accompagner de mesures organisationnelles permettant le suivi de leurs vulnérabilités publiées, et la correction de celles-ci par le déploiement de mises à jour logicielles.

3.1.3 Prise en compte de la sécurité dans la méthodologie de développement

Concernant la méthodologie de développement, le lecteur pourra se référer au guide "Agilité et sécurité numériques : méthode et outils à l'usage des équipes projet" [4], et également la politique de contribution aux logiciels libres de l'état de la DINUM [22], en particulier la partie concernant les bonnes pratiques de développement (document 'pratique.md'). Nous retenons de cette source les recommandations suivantes :

R 9 *

Tests

Des tests fonctionnels et unitaires doivent être employés, avec un niveau de couverture satisfaisant, afin de garantir la qualité du code produit.

R 10 **

Fuzzing

Le fuzzing doit être utilisé pour détecter des comportements anormaux dans le logiciel, notamment en présence de données malformées.

3.2 Cryptologie

De façon générale, l'annexe B du Référentiel Général de Sécurité (RGS) [11, 12, 13] définit des recommandations et des règles pertinentes pour l'emploi de mécanismes cryptographiques. Son contenu s'applique en particulier aux sous-sections de ce paragraphe.

Une recommandation très générale concernant l'emploi de mécanismes cryptographiques, quelle que soit leur fonction, est de s'en tenir à des mécanismes standardisés à l'état de l'art. Pour les fonctions cryptographiques usuelles, le lecteur pourra se référer au guide de sélection de mécanismes cryptographiques de l'ANSSI [9] qui vient compléter le RGS.

Certains dispositifs disposant de ressources limitées peuvent présenter des performances insuffisantes pour l'emploi de mécanismes cryptographiques usuels.

Dans le domaine de la cryptographie symétrique, des algorithmes économes en ressources existent, visant une implémentation matérielle ou logicielle.

Pour ce qui concerne les implémentations matérielles, le lecteur pourra consulter le rapport du NIST sur la cryptographie légère [21] et la norme ISO/IEC 29192 [23] qui définit trois algorithmes de chiffrement par blocs "légers" : PRESENT, CLEFIA et LEA.

L'algorithme SKINNY [17] peut également être considéré, aussi bien pour des implémentations matérielles que logicielles. Enfin l'AES est accéléré sur de nombreuses architectures, ce qui le rend accessible même dans certains contextes contraints.

3.2.1 Gestion des clés

La gestion des clés constitue le socle de toutes les opérations cryptographiques. La sécurité des données sensibles manipulées par un dispositif connecté ne pourra en général être plus élevée que celle des clés cryptographiques qu'il possède. Il est le plus souvent nécessaire de pouvoir stocker des clés de façon confidentielle et intègre ; pour certains usages, l'intégrité d'une valeur utilisée dans une opération cryptographique suffit à garantir les propriétés attendues de la fonction (c'est le cas par exemple d'un certificat permettant d'authentifier un élément de l'environnement). La capacité a garantir la confidentialité ou l'intégrité de valeurs stockées doit être appréciée en fonction des attaques probables dans l'environnement du dispositif.

En l'absence de capacité adéquate de gestion des clés, un dispositif connecté devra donc traiter et stocker aussi peu d'informations sensibles que possible. Il ne sera pas non plus capable d'authenti-

fier son environnement de façon convenable, ce qui peut constituer un problème sérieux lorsque celui-ci n'est pas *a priori* de confiance.

Au delà de ces constats initiaux, nous extrayons quelques recommandations de l'annexe B.2 du RGS qui traite en détails de la gestion des clés.

Dans cette section, un *secret* désigne soit une clé symétrique, soit la partie privée d'une biclé asymétrique.

3.2.1.1 Création des clés

Les clés sont soit générées *ex nihilo*, soit dérivées de secrets existants, soit obtenues à partir d'un protocole complexe comme un mécanisme d'échange de clé. Dans le premier cas, les clés sont générées à partir d'une source d'aléa qui doit être adaptée à un usage cryptographique ; voir recommandation R 48. Dans les autres cas, des mécanismes cryptographiques à l'état de l'art doivent être employés.

3.2.1.2 Stockage des clés

R 11 *

Protection des secrets

La protection en confidentialité, et en intégrité lorsque cela est nécessaire, des clés privées et secrètes, par une combinaison de moyens organisationnels et techniques, doit être assurée de façon continue durant toutes les phases de leur vie.

Les mesures techniques permettant la protection des secrets incluent l'emploi d'autres secrets et de mécanismes cryptographique qui permet de créer une hiérarchie de secrets interdépendants et, pour des secrets racine qui ne peuvent bénéficier de telles mesures, des protections de nature matérielle ou logicielle.

3.2.1.3 Association entre clés et entités

Les clés sont associées à une entité physique (dispositif) ou virtuelle (p.ex. un utilisateur logique). La bonne association entre une entité et les secrets qu'elle possède conditionne les propriétés de sécurité de toutes les opérations cryptographiques ultérieures impliquant ces secrets. Cette association a deux aspects :

- La garantie que seuls les dispositifs détenteurs légitimes de secrets y ont accès, qui provient des mesures organisationnelles assurant la sécurité de l'initialisation des secrets dans les entités destinataires (*mise à la clé*) et des mesures techniques protégeant les secrets (p.ex. *secure enclave*).
- L'assurance d'intégrité des informations concernant l'association entre secrets et identités. Dans le cas de clés publiques, cette intégrité peut reposer sur des certificats, pourvu que leur procédure de création ne possède pas de faille permettant à un attaquant de substituer sa propre clé publique à la clé authentique d'une identité du système. Dans le cas d'un système reposant

sur la cryptographie symétrique, le maintien de cette bonne association dans le temps repose généralement sur la protection en confidentialité et intégrité des clés dans les dispositifs d'administration du système ; mais comme dans le cas de clés publiques, l'existence d'associations incorrectes entre clés et sécurité doit être empêchée dès leur création.

R 12

Affectation des clés

La bonne association des secrets avec leurs détenteurs légitimes doit être garantie.

Exemple

Dans un échange de clé non authentifié entre deux participants A et B, un attaquant E peut s'insérer dans la communication et négocier séparément une clé commune avec A et B (*man-in-the-middle*). Alors la clé que A (resp. B) croit détenir en commun avec B (resp. A) est en fait partagée avec E ; cette tromperie de A et B compromet la sécurité de toutes les communications ultérieures entre A et B utilisant les clés négociées.

Exemple

Il est parfois possible de générer des biclés publiques/privées directement sur les dispositifs utilisateurs de la clé privée. Cette pratique, qui assure que la clé privée n'est jamais transportée, combinée avec la protection en confidentialité de celle-ci, empêche le clonage des dispositifs qui emploient les biclés. À elle seule, elle n'assure cependant pas la bonne association entre le dispositif et sa biclé dans le reste du système, car rien ne protège *a priori* la production de certificats liant les clés publiques des dispositifs et leurs identités. Une façon d'assurer cette protection est de demander une preuve de possession par l'identité déclarée de la clé privée associée à une clé publique - à travers la signature ou le déchiffrement d'un défi - avant de signer la clé publique pour produire un certificat.

3.2.1.4 Usages multiples d'un secret

Les clés partagées entre de nombreuses entités ou usages sont à éviter autant que possible, en raison des risques accrus liés à la divulgation de tels secrets.

R 13

Secrets maîtres

Les clés doivent être cloisonnées autant que possible par usage et par identité, et le système être conçu de telle sorte que la connaissance d'une clé ne compromette pas d'autres clés, afin de contrarier la propagation latérale d'un attaquant.

Les clés embarquées dans des dispositifs réputés perdables sont particulièrement concernées par cette recommandation.

R 14 *

Rôles uniques pour les clés publiques

En cas d'usage de cryptographie à clé publique, les clés privées doivent être individualisées par dispositif et par fonction.

En cas d'usage de cryptographie symétrique, les mécanismes de *dérivation de clé* permettent de construire à partir d'un secret unique autant de clés que nécessaire pour des usages distincts ou pour des entités distinctes.

R 15 *

Emploi de secrets symétriques dérivés

L'emploi d'une même clé symétrique pour des entités ou des usages distincts doit être évité par l'utilisation de mécanismes de dérivation de clé.

3.2.1.5 Compromissions et durée de vie des clés

L'impact d'une compromission peut être réduit par les mesures de cloisonnement présentées dans les paragraphes précédents. Il peut également l'être en agissant sur la durée de vie des clés concernées, soit en réaction à une compromission, soit de façon indépendante de celle-ci.

R 16 *

Durée de vie des clés

Chaque clé doit avoir une durée de vie choisie en fonction de la probabilité et des conséquences de sa compromission.

R 17 ***

Révocation de dispositifs

Lorsque le niveau de sécurité visé le justifie, il doit être possible d'exclure les dispositifs compromis du système sans affecter le fonctionnement du reste du système.

Le problème de la détection de la compromission est toutefois difficile à traiter dans le cadre de systèmes à bas coût.

3.2.2 Authentification

3.2.2.1 Généralités

R 18 *

Authentification et actions sensibles

Dès lors qu'un dispositif peut être commandé ou configuré, ou fournir de l'information sensible, il ne doit pas être possible de dialoguer avec celui-ci sans s'être préalablement authentifié.

R 19 *

Unicité des secrets d'authentification

Les secrets employés (clés ou mots de passe) ne doivent pas être communs à plusieurs dispositifs, même avant configuration.

Il faut en particulier éviter les authentifiants par défaut qui ne seront jamais changés et qui permettent des attaques de grande ampleur par le réseau ou la probabilité élevée de prise de contrôle d'un dispositif en cas d'interaction directe.

Pour garantir l'emploi d'authentifiants uniques, plusieurs approches sont possibles qui correspondent à différents compromis entre facilité d'implémentation, facilité d'emploi et sécurité :

- à la première initialisation et à chaque réinitialisation usine, le dispositif utilise des secrets qui lui sont propres, physiquement indiqués sur le dispositif (et qui sont produits par un générateur de qualité cryptographique). Il faut alors éviter que ces secrets soient observables par d'autres personnes que les utilisateurs légitimes (par exemple, par l'inscription sous l'appareil dans le cas d'une box Internet) ; cette approche présente l'inconvénient d'utiliser les mêmes authentifiants à chaque initialisation, mais est la plus simple pour l'utilisateur ;
- à la première initialisation et à chaque réinitialisation usine, une étape de configuration obligatoire permet à l'utilisateur de renouveler les secrets d'authentification ; tant que cette opération n'est pas effectuée les fonctionnalités principales du dispositif sont désactivées, et il présente une connectivité limitée. Cette méthode permet un renouvellement des secrets à chaque initialisation mais permet toutefois le choix par l'utilisateur de secrets peu aléatoires ;
- à la première initialisation et à chaque réinitialisation usine, le dispositif tire aléatoirement des secrets qu'il communique à l'utilisateur. Cette méthode nécessite une interface pour communiquer ces secrets, et un générateur aléatoire compatible avec cet usage.

3.2.2.2 Authentification de machine à machine

R 20 *

Emploi de protocoles à l'état de l'art

Les protocoles d'authentification employés doivent être à l'état de l'art cryptographique, en particulier ne pas permettre le rejeu des communications d'authentification, ni les tentatives d'énumération exhaustive des secrets d'authentification.

3.2.2.3 Authentification d'humain à machine

On suppose ici qu'un humain s'authentifie à l'aide d'un mot de passe. Les alternatives ou compléments à cette méthode emploient en général un élément en la possession de l'utilisateur qui s'authentifie, et cet élément met en œuvre un protocole cryptographique d'authentification, de sorte que l'on est ramené au cas de l'authentification de machine à machine traité au paragraphe précédent.

R 21 *

Empreintes pour l'authentification par mot de passe

Lorsqu'une authentification par mot de passe est mise en œuvre, le stockage de l'empreinte du mot de passe doit employer une technique à l'état de l'art utilisant un mécanisme de dérivation à sens unique avec sel ; ce sel doit être choisi indépendamment pour chaque dispositif et chaque identifiant. La dérivation doit être la plus lente possible compte tenu des contraintes de temps de réponse et de consommation afin de

contrarier les tentatives d'énumération de mots de passe candidats.

En tout état de cause, le mot de passe ne doit pas être stocké en clair ni sous forme chiffrée [3].

Le sujet du choix d'une fonction de dérivation n'étant pas traité dans les annexes du RGS, le lecteur pourra utilement consulter le guide du NIST [18] sur le sujet, qui propose une solution très utilisée (PBKDF2) et dont le temps de calcul est paramétrable. Pour obtenir une résistance accrue face aux attaques par énumération de mots de passe, il possible d'utiliser Argon2 [16] ou scrypt [19].

R 22 *

Contrôle du nombre d'essais d'authentification par mot de passe

Lorsque cela est possible, le nombre d'essais d'authentification doit être limité et/ou des délais croissants entre chaque essai doivent être imposés.

Le guide de l'ANSSI [15] contient des recommandations complètes concernant l'authentification multifacteurs et par mots de passe.

3.2.3 Confidentialité et intégrité des données

R 23 *

Protection des communications

Les flux de données sensibles échangées entre les constituants d'un système connecté, et entre ce système et des réseaux externes, doivent être protégées en confidentialité et en intégrité par des moyens cryptographiques à l'état de l'art.

Comme dans le cas de la recommandation R 5, la protection de l'intégrité des flux implique, outre l'intégrité des échanges individuels, la protection contre l'altération dans la succession des échanges, et en particulier contre le rejeu de messages.

R 24

Protection locale des données non volatiles

Les données sensibles stockées dans la mémoire long terme d'un dispositif (flash, EEPROM, SSD, disque dur, etc.), doivent être protégées en confidentialité et en intégrité.

R 25 ***

Protection locale des données volatiles

Les données sensibles stockées dans la mémoire volatile d'un dispositif doivent être protégées en confidentialité et en intégrité.

Cette dernière recommandation nécessite l'emploi d'une racine de confiance matérielle ; voir la recommandation R 47.

3. Dans ce second cas, la clé de déchiffrement doit être accessible par le dispositif qui vérifie le mot de passe et la sécurité obtenue n'est guère meilleure que dans le cas d'un stockage en clair.

3.3 Sécurité logicielle

3.3.1 Maîtrise de l'état du logiciel et du micrologiciel

R 26 *

Minimisation de la surface d'attaque

Un effort de minimisation du système doit être fait : seuls les applications, exécutables, pilotes nécessaires au bon fonctionnement des dispositifs doivent être présents.

La présence d'outils de déboguage, et l'activation de fonctionnalités uniquement utiles pour du diagnostic et susceptibles de faire fuir de l'information sensible, sont en particulier à proscrire.

Le guide de l'ANSSI [1] pourra être mis à profit pour la sécurisation et la minimisation d'un système Linux.

La vérification du logiciel aux différentes étapes du démarrage d'un dispositif (chaîne de démarrage sécurisée) permet de renforcer considérablement l'assurance que le micrologiciel exécuté est authentique.

R 27 ***

Chaîne de démarrage sécurisée

Il est recommandé d'assurer l'intégrité logicielle des dispositifs par une chaîne de démarrage sécurisé lorsque la criticité des fonctions du dispositif le justifie.

Cette mesure ne protège cependant pas de vulnérabilités dans le logiciel lui-même. Par ailleurs, le premier logiciel exécuté (Boot ROM) n'est pas modifiable, et la présence de vulnérabilités dans celui-ci compromet donc de façon irrémédiable la fonctionnalité offerte par une chaîne de démarrage sécurisée.

3.3.2 Mises à jour logicielles

R 28 *

Mises à jour de micrologiciel

Les mises à jour de micrologiciel doivent être possibles, afin de permettre la correction d'erreurs, en particulier de vulnérabilités.

R 29 *

Authentification et versionnage des mises à jour

Les mises à jour de micrologiciel doivent disposer d'un numéro de version et être authentifiées. L'authentification porte sur le logiciel lui-même, mais aussi sa version et toute information pouvant influer sur la décision d'installer ou non le micrologiciel.

R 30 *

Mécanisme anti-rollback

L'installation d'une version de logiciel plus ancienne que la version déjà déployée (*rollback*) doit être interdite par défaut, afin d'empêcher les attaques exploitant une version de micrologiciel comportant des vulnérabilités connues et déjà corrigées.
La possibilité de déroger à cette interdiction, si elle est jugée nécessaire, doit être contrôlée par un mécanisme d'administration authentifié.

R 31 *

Vérification locale de l'authenticité des mises à jour

Il est recommandé de faire vérifier l'authenticité d'une mise à jour par le dispositif à qui celle-ci est destinée.
Si la vérification d'authenticité est faite par un autre dispositif que celui mis à jour, le transfert de confiance entre ces deux composants doit être assuré par un mécanisme adapté.

Das le second cas, une commande correctement authentifiée de mise à jour, transmise du dispositif vérificateur au dispositif cible, et permettant elle-même de vérifier l'intégrité de la mise à jour, peut par exemple être employée.

R 32 *

Numéros de version logicielle et matérielle

Il doit être aisé de déterminer la version du micrologiciel et des logiciels employés, et en cas d'existence de plusieurs versions du matériel, un identifiant de celle-ci.
En revanche, ces informations ne doivent être disponibles à distance qu'après une authentification pour un rôle pertinent.

L'objet de cette dernière recommandation est de permettre de déterminer aisément si une mise à jour est applicable, sans toutefois divulguer sans raison une information potentiellement utile à une attaque.

3.3.3 Compartimentation mémoire

R 33 **

Compartimentation des applications et services

Les applications ou services s'exécutant sur un dispositif connecté doivent être compartimentées afin de limiter les conséquences d'une prise de contrôle par un attaquant de l'une d'entre elles. Cela implique l'emploi d'un noyau système contrôlant l'accès aux ressources (mémoire, périphériques), et donnant aux applications les accès minimaux nécessaires à leur bon fonctionnement. Les espaces mémoire des différentes applications doivent être distincts, avec impossibilité pour une application de lire ou d'écrire en dehors de son espace, sauf dans des zones explicitement dédiées à la communication inter-applications.

La recommandation ci-dessus s'appuie sur des fonctionnalités matérielles pour faire respecter un tel cloisonnement, comme une MMU (*Memory Management Unit*, unité de gestion de la mémoire) ou d'une MPU (*Memory Protection Unit*, unité de protection de la mémoire).

R 34 **

Compartimentation dans un système multi-utilisateurs

Lorsque le système d'exploitation est multi-processus et multi-utilisateur (au sens du système, et non de la personne physique qui utilise le dispositif), les différentes fonctionnalités offertes par le dispositif doivent être portées par des applications (processus) différents avec des droits utilisateurs adaptés à leurs besoins.

R 35 *

Compartimentation des processus interagissant avec l'environnement

Lorsque le système d'exploitation est multi-processus et multi-utilisateur, les applications en interaction directe avec l'extérieur (capteurs, actionneurs, échanges réseaux) doivent s'exécuter avec des privilèges adaptés. En particulier, ils ne doivent pas s'exécuter avec des privilèges élevés (de type *root* ou super-utilisateur).

Le lecteur est invité à se référer à ce sujet au guide ANSSI concernant le cloisonnement système [14].

3.3.4 Bonnes pratiques de développemement logiciel

Les outils de développement permettent d'inclure dans le code généré des protections contre l'exploitation de certaines failles logicielles, comme par exemple la détection de débordement de pile, et ce d'autant plus qu'ils sont récents.

R 36 *

Outils de développement à jour

Une chaîne de développement à jour pour la cible matérielle visée doit être employée.

R 37 *

Durcissement du code

Les protections offertes par les outils de développement pour durcir le code doivent être employées.

Les outils de développement permettent une analyse statique rudimentaire du code détectant la présence d'erreurs communes.

R 38 *

Avertissements fournis par les outils de développement

La génération d'avertissements par les outils de développement doit être activée et les problèmes détectés doivent être corrigés.

Le lecteur pourra consulter des recommandations concernant des langages spécifiques, par exemple pour le langage C [8] ou Rust [7].

R 39

Utilisation d'outils d'analyse statique

Il est recommandé d'employer des outils d'analyse statique sur les portions de code sensibles pour détecter et éliminer des erreurs pouvant se déclarer à l'exécution.

Différents outils d'analyse statique produisent des garanties de nature variable. Certains logiciels sont en mesure de prouver l'absence d'erreurs particulières (division par zéro, déréférencement de pointeur nul, etc), tandis que d'autres effectuent une analyse de nature uniquement heuristique, qui peut comporter des faux positifs (code sans erreur indiqué comme pouvant en comporter) et des faux négatifs (des erreurs ne sont pas vues).

Lorsque l'on dispose d'une spécification formelle d'une portion de code, un travail spécifique peut permettre de prouver que le comportement du code est conforme à la spécification, ce qui constitue un niveau très élevé de garantie de correction de l'implémentation.

3.3.5 Gestion et minimisation des droits

R 40 *

Minimisation des droits utilisateur

Les utilisateurs extérieurs interagissant avec le dispositif (par la connexion réseau ou toute autre interface) doivent avoir des droits limités en fonction des actions qu'ils peuvent légitimement effectuer et de leur niveau d'authentification. Si différents rôles utilisateurs existent, les droits attribués aux utilisateurs doivent refléter ces rôles et l'association entre un utilisateur et son rôle doit donc être explicite.

Le paragraphe 3.3.3 traite de la minimisation des droits des applications et processus.

3.3.6 Journalisation des événements de sécurité

R 41 **

Durée de rétention et droits d'accès à la journalisation

Tous les événements pertinents pour la sécurité des dispositifs vis-à-vis des menaces envisagées (connexions réussies ou en échec, redémarrages prévus ou non, erreurs, etc.) doivent être enregistrés avec une durée de rétention et des droits d'accès permettant une analyse a posteriori.

R 42 **

Journaux en lecture seule

Les journaux d'événements ne doivent pas être modifiables ou effaçables.

Les événements liés à la sécurité sont primordiaux pour l'analyse d'incidents. Les événements métier peuvent également être utiles à cette fin et être inclus dans le périmètre de la recommandation précédente.

R 43 **

Journalisation déportée

Il est recommandé de remonter les événements vers des équipements déportés (syslog, etc) dans les situations où cette pratique permet de mieux protéger les journaux.

3.4 Matériel

3.4.1 Mesures contre les attaques exploitant des propriétés matérielles

Les attaques sur un dispositif permises par l'environnement, exploitant des faiblesses de l'implémentation matérielle et visant à extraire ses secrets ou à perturber le bon fonctionnement de ses fonctions de sécurité, doivent être envisagées et contrées.

La technicité de ces attaques est très variable : il peut s'agir dans les cas les plus simples de l'utilisation d'un contact d'un composant donnant accès à des fonctions de debug. Au contraire, dans les scénarios les plus élaborés, un canal auxiliaire (comme le temps nécessaire à un calcul, la consommation de courant ou le rayonnement électromagnétique pendant celui-ci) peut être exploité pour obtenir des informations sensibles ; un composant réalisant des opérations sensibles peut également être perturbé pour provoquer activement la fuite de secrets.

R 44 *

Sécurité matérielle et accès aux composants

Les fonctionnalités de deboguage et de reprogrammation (e.g. JTAG, SWD) doivent être inaccessibles en production. Suivant les capacités du matériel employé, ceci peut être réalisé de différentes façons :

- Désactivation définitive de ces fonctions par utilisation de fusibles prévus à cet effet ;
- Activation et mise à la clé d'un mécanisme d'authentification de l'utilisateur des commandes de déboguage.

Si aucun de ces mécanismes n'est disponible, les contacts des interfaces de déboguage doivent *a minima* être rendus d'accès difficile sur le PCB des dispositifs.

En cas d'utilisation d'un mécanisme d'authentification pour l'interface de déboguage, les recommandations du paragraphe 3.2.1 s'appliquent.

R 45 **

Protection des communications entre composants

Les bus de communication exposés sur le PCB (SPI, I2C, UART, etc.) doivent être protégés en intégrité et/ou en confidentialité si ces bus véhiculent des données sensibles comme des secrets ou du code à exécuter.
Lorsque des mémoires, volatiles ou non, sont physiquement séparées des unités de traitement, et sont amenées à stocker des éléments sensibles (comme des clés ou du code critique), elles doivent être chiffrées et/ou protégées en intégrité par des secrets stockés dans une zone de confiance du composant principal du système (BootROM ou SRAM interne du SoC, flash interne des MCU, etc.).

R 46 ***

Perturbations du matériel et canaux auxiliaires

Les perturbations du matériel ne doivent pas permettre un contournement de ses mesures de sécurité.
Les attaques par canaux auxiliaires, exploitant ou non de telles perturbations, ne doivent pas permettre d'extraire des secrets des dispositifs dans les conditions d'interaction avec ceux-ci compatibles avec leur usage prévu.

Pour se protéger de ces attaques, une attention particulière devra être portée à l'implémentation des fonctions utilisant des éléments secrets (par exemple redondance des tests, temps d'exécution ne dépendant pas des valeurs secrètes manipulées, etc.)

L'emploi d'un élément de sécurité certifié renforce considérablement la confidentialité et l'intégrité des secrets détenus vis-à-vis des attaques physiques et logiques, à condition que le code s'exécutant sur un tel environnement ne présente pas de vulnérabilité exploitable. L'emploi d'un environnement d'exécution sécurisé au sein d'un processeur ou d'un SoC (System on Chip) peut également jouer ce rôle, principalement contre les attaques logiques.

R 47

Emploi d'un environnement dédié aux fonctions de sécurité

Il est recommandé d'employer un environnement d'exécution sécurisé intégré à un SoC, ou un élément de sécurité certifié, pour les traitements de données dont la confidentialité ou l'intégrité doit être garantie.

L'utilisation d'un environnement de confiance matériel ou logiciel destiné à l'exécution des tâches sensibles est un cas particulier de mesure de cloisonnement comme discuté au paragraphe 3.3.3.

3.4.2 Génération d'aléa, éléments uniques

R 48 *

Génération d'aléa de qualité cryptographique

Un dispositif doit être capable de générer des valeurs aléatoires de qualité cryptographique dès lors qu'elles sont requises par un protocole mis en œuvre par celui-ci.

Une source d'aléa cryptographique est nécessaire pour générer des clés, mais aussi dans tout cas d'usage nécessitant une garantie concernant l'entropie des valeurs produites : défis dans les protocoles de défi/réponse, vecteurs d'initialisation cryptographiques (IVs), etc.

R 49 *

Génération de valeurs uniques

Un dispositif doit être capable de générer les éléments uniques (*nonces*) nécessaires dans les protocoles qu'il met en œuvre, par l'emploi d'éléments aléatoires ou d'une mémoire à long terme convenablement protégée.

3.5 Réseau

3.5.1 Ports, services et protocoles accessibles

R 50 *

Requêtes d'origine inconnue

Les requêtes dont l'origine n'est pas maîtrisée ne doivent pas être traitées.

L'objectif de cette recommandation est de réduire la surface d'attaque des dispositifs et de limiter les possibilités de cartographie de systèmes connectés à Internet.

L'origine des connexions aux dispositifs peut être contrôlée par une authentification cryptographique ou, dans certains cas, par l'organisation du réseau dans lequel ils s'inscrivent. Il est par exemple envisageable de placer les dispositifs devant communiquer entre eux sur un réseau d'*overlay* privé les isolant de menaces extérieures. Un tel réseau fournit également un point de contrôle en cas de compromission, en permettant de couper au besoin la connexion entre le réseau privé et les réseaux externes comme Internet.

R 51 *

Minimisation des services exposés

Seuls les services nécessaires au fonctionnement du dispositif doivent être activés.

3.5.2 Résistance aux attaques en déni de service

Un service ne doit pas pouvoir être utilisé pour participer à des (D)DoS. En particulier, l'usage du protocole UDP, qui permet de falsifier l'origine d'une communication, doit faire l'objet d'une attention particulière, afin de ne pas permettre à un attaquant de diriger des réponses vers une cible de son choix.

R 52 *

UDP et attaques par réflexion

Le protocole UDP ne doit pas être employé en cas de risque de détournement de celui-ci pour des attaques par réflexion.

3.5.3 Protocoles de communication sécurisés

Pour assurer l'authentification de l'origine d'une connexion, ainsi que la confidentialité et l'intégrité des échanges, les mécanismes de sécurité implémentés dans les protocoles standardisés tels que IPsec [3] ou TLS [6] sont à préférer à des mécanismes *ad hoc* fournis par des applications, comme indiqué au paragraphe 3.2.

R 53 *

Protection des données en transport

Dès lors que la confidentialité ou l'intégrité de données transmises fait partie des objectifs de sécurité du système, des protocoles de communication éprouvés assurant ces propriétés, comme TLS ou IPsec, doivent être employés.

Le paragraphe 3.2 couvre des aspects connexes à la mise en oeuvre de ces protocoles, en particulier la gestion des clés qui y jouent le rôle de racine de confiance.

3.5.4 Sécurité des interfaces radiofréquence

Une interface radiofréquence présente des risques d'interaction non désirée, à une distance difficile à estimer car elle dépend de l'équipement de l'attaquant : ces risques doivent être pris en compte dans l'analyse de sécurité et contrés. Certains d'entre eux sont identifiables de façon générique :

1. emploi non autorisé d'une fonctionnalité d'un dispositif connecté par radio. Par exemple, emploi à l'insu du porteur d'un badge de contrôle d'accès ou d'un moyen de paiement sans fil, en relayant au besoin de façon bidirectionnelle les messages entre deux équipements légitimes ;
2. mise en cause de la disponibilité de fonctionnalités par brouillage ;
3. collecte d'informations ou pistage d'un dispositif diffusant des identifiants uniques ou toute information de valeur ;

Ces risques peuvent être éliminés ou limités par les mesures suivantes :

1. Une action locale sur le dispositif conditionnant les actions sensibles (bouton pour activer le dialogue radio de contrôle d'accès par exemple) est une solution appropriée pour contrer ces menaces quand l'interaction avec le dispositif est de nature binaire (autorisation ou interdiction d'accès par exemple). Elle ne suffit en revanche pas nécessairement pour des fonctions plus complexes, comme par exemple le paiement, où l'utilisateur doit connaître le montant de paiement qu'il approuve. L'action de celui-ci doit alors être couplée avec l'information sur l'opération autorisée (ici la présentation du montant). De plus, dans le cas du paiement, l'utilisation d'un code lie le dispositif à son propriétaire. Si un tel dispositif de confirmation locale de l'action n'est pas applicable, la mesure des temps de réponse des dispositifs qui communiquent peut limiter les possibilités de relai de signaux. Il est à noter qu'une attaque en relai est possible même dans le cas où les deux participants d'une communication radio procèdent à une authentification mutuelle ; les méthodes de nature cryptographique ne sont pas en mesure de contrer ce type de menace.
2. Dans les cas où une menace sur la disponibilité d'une communication radiofréquence fait peser un risque sur la sécurité du système, des mécanismes d'étalement de spectre ou d'adaptation dynamique des canaux radio utilisés peuvent être employés. Ces solutions rendent le brouillage plus difficile mais n'en éliminent pas la possibilité ;
3. Les identifiants uniques permettant de pister un dispositif mobile (par exemple, une adresse MAC) doivent être rendus aléatoires ; plus généralement, il faut éviter de diffuser toute information publiquement, et privilégier au contraire les communications avec des pairs authentifiés via des canaux protégés par des moyens cryptographiques.

Les considérations précédentes sont résumées dans les recommandations suivantes.

R 54 *

Déblocage d'actions sensibles

Lorsque cela est pertinent, la réalisation d'actions sensibles par le dispositif doit être conditionnée à une action de son porteur.

R 55 **

Canaux radio et brouillage

Les risques résultant d'un brouillage, intentionnel ou non, de canaux radiofréquence doivent être minimisés, soit par des mesures rendant les dispositifs résistants à celui-ci, soit par l'adoption d'un comportement adapté en cas de dysfonctionnement de la liaison.

R 56 *

Canaux radio et identifiants traçables

Le risque de traçage des dispositifs mobiles disposant d'une interfaçe radio doit être minimisé, en particulier lorsque ces dispositifs sont portés par des personnes physiques.
En tout état de cause, la diffusion indiscriminée d'identifiants fixes, ou évoluant d'une façon prédictible, doit être évitée.

Les interfaces radiofréquence peuvent également faciliter ou amplifier des fuites d'information secrète par canal auxiliaire. Cette menace entre dans le périmètre du paragraphe 3.4.1 et de la recommandation R 46.

Des recommandations spécifiques au protocoles WiFi sont présentées dans le guide de l'ANSSI [2].

3.5.5 Détection d'activités malveillantes

R 57

Surveillance du système

Si le niveau de sécurité visé le justifie, une surveillance active du réseau de dispositifs déployés, visant à détecter et à caractériser les tentatives d'en compromettre le fonctionnement, doit être effectuée.

Cette surveillance peut prendre place sur le réseau sur lequel transitent les communications du système, mais peut également concerner l'état du parc de dispositifs déployés et les grandeurs qui mesurent son bon fonctionnement. Elle peut enfin s'appuyer sur la journalisation d'événements de sécurité traitée au paragraphe 3.3.6.

R 58 **

Caractérisation des impacts systémiques

Lorsqu'un système connecté est utilisé dans des processus de prise de décision, la possibilité d'influer sur cette prise de décision par une interaction malveillante avec les dispositifs déployés doit être caractérisée et minimisée et les processus de prise de décision doivent être adaptés en conséquence.

3.6 Cycle de vie et support

3.6.1 Point de contact et correctifs

R 59 *

Point de contact

Une entité responsable du suivi fonctionnel et sécuritaire d'un système connecté doit être connue et joignable afin permettre de signaler un dysfonctionnement ou une faille de sécurité du produit.

R 60 *

Réponse aux signalements

Tout signalement de dysfonctionnement ou de faille de sécurité doit recevoir une réponse indiquant les modalités et le délai de sa prise en compte.

3.6.2 Engagement de support

R 61 *

Durée de support

Une durée de support en rapport avec la durée de vie attendue des dispositifs doit être indiquée et honorée par le fabricant.

R 62 **

Maintenance au-delà du support

Au delà du support par le fabricant, une procédure doit permettre de transférer la responsabilité du maintien en condition de sécurité des dispositifs. Les fonctions sous le contrôle exclusif du fabricant ou intégrateur et qui sont nécessaires à ce maintien doivent pouvoir passer sous le contrôle des utilisateurs par une action volontaire de ceux-ci.

3.6.3 Gestion et publication des vulnérabilités ; mesures correctives

R 63 *

Politique de gestion des vulnérabilités

Une politique de gestion des vulnérabilités, couvrant la durée de support du produit, doit être proposée. Celle-ci indique comment et sous quels délais sont rendues publiques les vulnérabilités connues du fabricant ; comment le fabricant peut être informé d'une vulnérabilité (voir paragraphe 3.6.1) ; elle explicite également la politique de correction des vulnérabilités ou bogues fonctionnels dans des mises à jour.

Annexe A
Références externes concernant les objets connectés

- Secure by Design, gouvernement du Royaume-Uni
  - Présentation de la démarche globale du gouvernement du Royaume Uni concernant l'amélioration de la sécurité des objets connectés
  - Liste de 13 recommandations essentielles, orientée vers les produits grand public
  - Mapping Security & Privacy in the Internet of Things présente la correspondance entre les recommandations du Royaume Uni et d'autres ensembles de recommandations concernant l'IoT.
- Document de travail IETF "Best Current Practices for Securing Internet of Things (IoT) Devices"
  - Liste de bonnes pratiques de conception, orientée protection réseau
- Document de travail IETF "State-of-the-Art and Challenges for the Internet of Things Security"
  - Protocoles adaptés aux IoT
  - Sécurité et cycles de vie des objets connectés
- Document de travail NIST IR 8200, "Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)".
  - Listes de risques envisagés par grand domaine IoT
  - Énumération très complète des standards susceptibles d'aider à sécuriser l'internet des objets
  - Approches système et objet
- Guide CAP'TRONIC : "PME : Comment maîtriser la cybersécurité de vos objets et systèmes connectés v2", 12/2017
  - Discussion des risques liés à l'absence de prise en compte de la SSI dans la conception de produits ou de services
- OWASP Internet of Things Project
  - Nombreux aspects concrets de la sécurité des objets connectés abordés : par exemple surface d'attaque des objets connectés, ou principes de la sécurité des IoT.

Liste des recommandations

Bibliographie

[1] *Recommandations de configuration d'un système GNU/Linux*.
Guide ANSSI-BP-028 v1.2, ANSSI, février 2019.
https://www.ssi.gouv.fr/reco-securite-systeme-linux.

[2] *Recommandations de sécurité relatives aux réseaux Wi-Fi*.
Note technique DAT-NT-005/ANSSI/SDE/NP v1.0, ANSSI, septembre 2013.
https://www.ssi.gouv.fr/nt-wifi.

[3] *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*.
Note technique DAT-NT-003/ANSSI/SDE/NP v1.1, ANSSI, août 2015.
https://www.ssi.gouv.fr/ipsec.

[4] *Agilité et sécurité numériques : méthode et outils à l'usage des équipes projet*.
Guide ANSSI-PA-041 v1.0, ANSSI, novembre 2018.
https://www.ssi.gouv.fr/administration/guide/agilite-et-securite-numeriques-methode-et-outils-a-lusage-des-equipes-projet.

[5] *Maîtrise du risque numérique - l'atout confiance*.
Guide ANSSI-PA-070 v1.0, ANSSI, novembre 2019.
https://www.ssi.gouv.fr/administration/guide/maitrise-du-risque-numerique-latout-confiance.

[6] *Recommandations de sécurité relatives à TLS*.
Guide ANSSI-PA-035 v1.2, ANSSI, mars 2020.
https://www.ssi.gouv.fr/nt-tls.

[7] *Règles de programmation pour le développement d'applications sécurisées en Rust*.
Guide ANSSI-PA-074 v1.0, ANSSI, juin 2020.
https://www.ssi.gouv.fr/guide/regles-de-programmation-pour-le-developpement-dapplications-securisees-en-rust.

[8] *Règles de programmation pour le développement sécurisé de logiciels en langage C*.
Guide ANSSI-PA-073 v1.2, ANSSI, juillet 2020.
https://www.ssi.gouv.fr/guide/regles-de-programmation-pour-le-developpement-securise-de-logiciels-en-langage-c.

[9] *Guide de sélection d'algorithmes cryptographiques*.
Guide ANSSI-PA-079 v1.0, ANSSI, mars 2021.
https://www.ssi.gouv.fr/guide/mecanismes-cryptographiques.

[10] *Expression des besoins et identification des objectifs de sécurité*.
Guide Version 1.1, ANSSI, janvier 2010.
https://www.ssi.gouv.fr/ebios.

[11] *RGS Annexe B3 : Règles et recommandations concernant les mécanismes d'authentification*.
Référentiel Version 1.0, ANSSI, janvier 2010.
https://www.ssi.gouv.fr/rgs.

[12] *RGS Annexe B2 : Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://www.ssi.gouv.fr/rgs.

[13] *RGS Annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Référentiel Version 2.03, ANSSI, février 2014.
https://www.ssi.gouv.fr/rgs.

[14] *Recommandations pour la mise en place de cloisonnement système*.
Guide ANSSI-PG-040 v1.0, ANSSI, décembre 2017.
https://www.ssi.gouv.fr/guide-cloisonnement-systeme.

[15] *Authentification multifacteurs et mots de passe*.
Guide ANSSI-PG-078 v1.0, ANSSI, septembre 2020.
à paraître.

[16] *Argon2 : the memory-hard function for password hashing and other applications*.
Page web : description, analyse de sécurité, implémentations.
https://www.cryptolux.org/index.php/Argon2.

[17] *SKINNY Family of Block Ciphers*.
Page web : description, analyse de sécurité, implémentations.
https://sites.google.com/site/skinnycipher/home.

[18] *Recommendation for Password-Based Key Derivation*.
Rapport, NIST, décembre 2010.
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf.

[19] *The scrypt Password-Based Key Derivation Function (RFC 7914)*.
RFC, août 2016.
https://tools.ietf.org/html/rfc7914.

[20] *Licence ouverte / Open Licence v2.0*.
Page web, Mission Etalab, 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

[21] *Report on Lightweight Cryptography*.
Rapport, NIST, mars 2017.
http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf.

[22] *Politique de contribution aux logiciels libres de l'état v1.0*.
dépôt git, DINSIC, mai 2018.
https://github.com/DISIC/politique-de-contribution-open-source.

[23] *ISO/IEC 29192-2 :2019 Information technology — Security techniques — Lightweight cryptography — Part 2 : Block ciphers*.
Document normatif, ISO, novembre 2019.
https://www.iso.org/standard/78477.html.

ANSSI-PA-087
Version 1.0 - 2021-08-27

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN