Etude des aspects cybersécurité de la directive RED

Thierry Didi,
Mai 2025
Tidiwi

Dans un article précédent je me suis intéressé à la sécurisation des objets connectés, telles que promue par la communauté européenne ou par des organisations à but non lucratif.

À la suite d'un échange avec un industriel et de la lecture d'un post sur LinkedIn, j'ai constaté que les nouvelles exigences en matière de cybersécurité introduites par la directive RED restent encore méconnues de certains acteurs du secteur. Leur impact sur la mise sur le marché des produits semble souvent mal évalué : certains en minimisent les conséquences, pensant qu'un simple passage en laboratoire suffira, tandis que d'autres anticipent à l'inverse un redesign complet de leurs équipements. Pourtant, l'échéance approche rapidement, avec une entrée en vigueur prévue dès août 2025.

Aussi, j'ai décidé d'analyser de manière neutre la nouvelle directive RED et les standards associés.

Cette nouvelle version introduit trois nouveaux articles :

- 3.3§d : « *radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service* »
- 3.3§e : « *radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected* »
- 3.3§f : « *radio equipment supports certain features ensuring protection from fraud* »

Pour chacun de ces trois articles, j'ai choisi d'aborder les sujets suivants :

- Quels produits sont concernés,
- Quelles nouvelles contraintes sont applicables à ces produits,
- Quelles actions doivent être mises en œuvre par les fabricants pour s'y conformer.

Ce document n'a pas vocation à remplacer les normes associées à la directive RED. Son objectif est plutôt de mettre en évidence les types de menaces contre lesquelles les équipements devront se prémunir pour satisfaire aux exigences de cette directive. Il revient ensuite à chaque fabricant ou responsable de conformité :

- D'identifier les normes applicables,
- De déterminer si l'équipement entre dans le champ des nouveaux articles concernés,
- De mettre en œuvre, si nécessaire, les fonctionnalités requises,
- Et de constituer la documentation technique appropriée, afin de démontrer la conformité du produit.

Ce document est basé sur une étude personnelle des directives européennes et des normes associées. Il n'a donc aucune valeur juridique et se base uniquement sur ma compréhension des textes et ma connaissance des systèmes embarqués. Si vous avez des remarques ou des suggestions d'amélioration, n'hésitez pas à m'en faire part par email : thierry.didi[at]tidiwi[dot]com.

Introduction

Ce document ne s'intéresse qu'aux trois nouveaux articles qui traitent de sécurité, et pas à la conformité à la directive RED de manière globale.

Il est important de souligner qu'il n'existe pas d'outil de mesure permettant de vérifier automatiquement la conformité d'un produit aux exigences des standards de cybersécurité associés à la directive RED. La conformité repose avant tout sur l'analyse menée par les concepteurs du produit, qui devront documenter dans le dossier technique RED la manière dont chaque contrainte a été prise en compte et satisfaite. Le recours à un organisme notifié ne dispense donc pas de cette évaluation, laquelle ne peut être réalisée que par les équipes en charge de la conception.

Il est aussi important de noter qu'un fabricant peut effectuer une procédure d'auto-certification[1] de son produit s'il a intégré dans son produit (et documenté) les contraintes indiquées dans les standards harmonisés :

> *«Radio equipment which is in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the essential requirements set out in Article 3 covered by those standards or parts thereof.»* [2]

Avant de rentrer dans les détails des contraintes et des solutions, il est important de définir certains des termes employés dans ce document et dans les spécifications :

- **Actif de sécurité (Security Asset)**
  Paramètre sensible ou confidentiel ou fonction qui assure la confidentialité des *données à caractère personnel* d'un utilisateur, d'un *actif lié au réseau* de télécommunications, ou d'un *actif financier*.
  Par exemple, la position GPS d'un utilisateur est une *donnée à caractère personnel* qui est un *Actif lié à la vie privée* – mais une fonction qui stocke ces données est elle aussi un *actif de sécurité*. Le code de cette fonction fait donc partie des éléments à protéger, au même titre que les données de position elles-mêmes.

[1] ANNEXE II de la directive RED
[2] Article 16 de la directive RED

- **Actif lié à la vie privée (Privacy Asset)**
  Permet d'identifier directement ou indirectement un *utilisateur* (personne physique) – par exemple une adresse IP, un nom d'utilisateur, un identifiant, une adresse MAC … La protection des actifs liés à la vie privée est traitée dans l'article 3.3(e) de la directive RED. Ces actifs sont les suivants :
  - **Données à caractère personnel**[3]
    Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

  - **Données relatives au trafic**[4]: toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation.

  - **Données de localisation**[5]: toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un *utilisateur* (personne physique) d'un service de communications électroniques accessible au public.

- **Actif financier (Financial Asset)**
  Toute ressource liée à la gestion de valeur monétaire. La protection des actifs financiers est traitée dans l'article 3.3(f) de la directive RED.

- **Actif réseau (Network Asset)**
  Toute ressource liée au réseau dont la compromission pourrait perturber le fonctionnement du réseau (protocoles de communication, interfaces Ethernet filaire, WIFI, Bluetooth, interface de gestion à distance (SSH …), mots de passe SSH ou WIFI ...). La protection des actifs réseau est traitée dans l'article 3.3(d) de la directive RED.

- **Dossier Technique RED :** Pour prouver la conformité d'un appareil à la directive RED, le constructeur doit rédiger un dossier technique. Le contenu minimal de ce dossier technique est décrit dans l'Annexe V de la directive RED.

- **Etat Sortie d'usine** : Etat d'un équipement à sa sortie d'usine, ou lorsqu'il est réinitialisé à un état par défaut.

- **Utilisateur**[6] : toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service.

[3] article 4 du règlement européen (EU) 2016/679
[4] Article 2, point (b) du règlement européen (EU) 2002/58/EC
[5] Article 2, point (c) du règlement européen (EU) 2002/58/EC
[6] Article 2, point (a) du règlement européen (EU) 2002/58/EC

- **Failles de sécurité connue (Known Vulnerabilty)**: Il existe plusieurs bases de données qui décrivent les vulnérabilités publiquement connues dans des logiciels open source ou commerciaux. Ces bases de données contiennent la description de la faille de sécurité, les effets possibles, et les correctifs éventuels.

La nouvelle directive RED

Comme indiqué dans un autre article dédié à la sécurité des objets connectés[7], Il existe trois standards harmonisés qui permettent de garantir la conformité à la directive RED. Ces standards sont :

- EN 18031-1:2024 : Common Security Requirements for Internet Connected Radio Equipment. Permet de vérifier la conformité à RED 3.3-§d
- EN 18031-2:2024 : Common Security Requirements Equipment Processing Personal Data : Permet de vérifier la conformité à RED 3.3-§e
- EN 18031-3:2024 : Common Security Requirements for Equipment Processing Virtual Money or monetary value : Permet de vérifier la conformité à RED 3.3-§f

Chacun de ces standards peut amener ou ne pas amener de nouvelles contraintes sur un produit, que ce soit au niveau de l'électronique ou du logiciel.

Cette directive ne s'applique pas aux équipements médicaux ou aux appareils de diagnostic in vitro, aux équipements automobiles, aux équipements destinés à l'aviation civile, au télépéage routier, qui sont couverts par d'autres directives[8].

Les sections qui suivent s'intéressent à ces contraintes dans les cas de la protection du réseau, de la protection de la vie privée et de la protection contre les fraudes. Pour des raisons d'intérêt personnel, je me suis intéressé en premier lieu à la protection des données personnelles, et les sections sont donc listées dans cet ordre :

- Protection des données personnelles.
- Protection du réseau.
- Protection contre les fraudes.

[7] https://tidiwi.com/shared-files/3944/?Technical%20Paper%20Securit%C3%A9-V1-fr.pdf
[8] Point (15) et (16) du RÈGLEMENT DÉLÉGUÉ (UE) 2022/30 DE LA COMMISSION

L'article 3.3§e : La protection des données personnelles

Les appareils concernés par l'article 3.3§e

La spécification EN 18031-2:2024 introduit des contraintes liées à la cybersécurité. Ces contraintes sont destinées à protéger les *actifs de sécurité (Security Assets)* et les *actifs liés à la vie privée* (Privacy Assets) intégrés à l'appareil. Ces contraintes s'appliquent seulement si l'appareil gère des *données à caractère personnel, données des relatives au trafic, des données de localisation* (donc associées à un *utilisateur,* personne physique). Dans ce cas, ces contraintes s'appliquent :

- *Si l'appareil dispose d'une connexion à internet*
- *Ou si l'appareil est un jouet ou un équipement destiné exclusivement au suivi des enfants,*
- *Ou si l'appareil est un accessoire portatif connecté (montre connectée, capteur porté sur le corps …)*

Autrement dit, si l'appareil ne peut être associé — ni directement, ni indirectement — à une personne physique, alors les exigences liées aux actifs de sécurité et à la vie privée ne s'appliquent pas.

Toutefois, la notion d'association avec un utilisateur doit être interprétée au sens large : Dès lors que l'appareil embarque un identifiant (par exemple un numéro de série, une adresse MAC ou une adresse IP) pouvant être lié à une personne physique via une plateforme distante (comme un service cloud), les exigences de cette spécification deviennent applicables.

Il faudra bien sûr justifier tous ces faits dans le *Dossier Technique*[9] qui atteste de la conformité de l'équipement à la directive RED.

Les contraintes introduites par l'article 3.3§e

Dans un premier temps, le constructeur doit lister tous les *actifs de sécurité* et les *actifs liés à la vie privée* à protéger. Il doit aussi lister tous les accès possibles légitimes ou illégitimes, à ces actifs.

Ensuite, pour chacun de ces actifs de sécurité, il devra garantir (et documenter et justifier) comment il répond aux contraintes suivantes :

- **Contrôle d'accès** : il s'agit de protéger l'accès en lecture ou en écriture aux *actifs liés à la vie privée* (Privacy Assets) et aux *actifs de sécurité* (Security Assets). Cette protection s'applique bien sûr aux utilisateurs légitimes, mais aussi aux utilisateurs malveillants qui pourraient essayer d'obtenir ces données au moyen des interfaces radio (Bluetooth, Wifi, Cellulaire …) qui sont intégrées à l'équipement. En revanche, si l'environnement dans lequel l'équipement est utilisé dispose lui-même de mesures de contrôle d'accès « physique » ou « logique », il n'est pas nécessaire d'implémenter ce type de mesure dans l'équipement lui-même. Ces mesures devront être documentées dans le *Dossier Technique RED*.
  Les jouets et les appareils destinés au suivi des enfants intègrent d'autre besoin en termes de contrôle d'accès des parents ou des personnes responsables de la garde des enfants.

- **Authentification** : Pour chaque type de contrôle d'accès identifié, il s'agit de demander une authentification avant d'autoriser une entité externe à lire ou manipuler des *actifs de sécurité* ou des *actifs liés à la vie privée*. Des modes d'authentification différents seront implémentés sur les interfaces utilisateur (par exemple username/password, biométrie, pin code …) et sur

[9] Le contenu du document technique est précisé dans l'annexe V de la directive RED

les interfaces réseau (TLS …). Cette contrainte ne s'applique pas si l'environnement dans lequel l'équipement est utilisé dispose de mesures de contrôle d'accès, ou si l'accès à certaines informations personnelles, en lecture uniquement, fait partie de l'utilisation normale de l'équipement (par exemple, affichage du nom de l'utilisateur sur l'écran de l'appareil, ou lecture d'une clé publique d'un algorithme de chiffrement asymétrique).

Si des mots de passe « usine » sont définis, ils doivent être unique pour chaque appareil ou demander à être modifiés à la première utilisation, éventuellement par un mot de passe vide. Des contraintes similaires s'appliquent aux autres mots de passe qui protègent des *actifs de sécurité* ou des *actifs liés à la vie privée*.

En fonction du type de données personnelles manipulées par l'équipement, cette spécification peut demander une authentification à deux facteurs.

La spécification impose aussi que les mécanismes d'authentification aient une robustesse minimum. S'ils sont basés sur des mots de passe, les mots de passe doivent avoir une certaine complexité. S'ils sont basés sur des certificats, l'appareil doit être en mesure de vérifier la validité des certificats grâce à signature et une chaine de confiance par exemple.

Par ailleurs, l'appareil doit être protégé pour éviter qu'un acteur malveillant qui enregistrerait une communication de contrôle d'accès ne soit ensuite capable de la rejouer pour obtenir l'accès à une ressource protégée (« Replay Attack »).

Enfin, l'appareil doit se protéger contre les attaques par force brute, où un utilisateur malveillant dispose d'un temps infini pour tester un grand nombre de mots de passe.

- **Mises à jour sécurisées** : si l'appareil contient des *actifs de sécurité* ou des *actifs liés à la vie privée*, il doit implémenter au moins une méthode pour mettre à jour le logiciel, ou tout au moins les composants logiciels, qui manipule(nt) ces données, sauf si ce logiciel est stocké en ROM (Read Only Memory) ou si d'autres mesures permettent de protéger ces actifs durant toute la vie du produit. Par exemple
    - Pour des systèmes très basiques comme des capteurs, une de ces mesures peut être le remplacement du produit.
    - L'équipement peut faire partie d'un système qui protège ces actifs contre les vulnérabilités.

  L'intégrité des logiciels téléchargés doit être vérifiée, c'est-à-dire qu'il ne doit pas être possible d'installer un logiciel qui ne provient pas d'une source autorisée.

  L'équipement doit être capable de se mettre à jour automatiquement, ou à la suite d'une action de l'utilisateur.

- **Stockage Sécurisé** : si l'appareil mémorise de manière permanente (donc en mémoire non volatile) des *actifs de sécurité* ou des *actifs liés à la vie privée*, ces données doivent être stockées de manière sécurisée (typiquement via des algorithmes de chiffrement) et protégées contres les modifications (typiquement via des signatures). Le mode de protection à implémenter dépend du type de données à stocker et de leur durée de stockage.

- **Sécurité des communications** : si l'appareil échange avec d'autres appareils des *actifs de sécurité* ou des *actifs liés à la vie privée*, il doit utiliser des protocoles de communication sécurisés. Ces protocoles assurent en général la confidentialité des données, la vérification de l'intégrité des données, et une protection contre les attaques de type « Replay Attacks ». Ces protocoles doivent être conformes aux bonnes pratiques en matière de sécurité.

- **Mécanisme de traces** : si l'appareil gère des *actifs de sécurité* ou des *actifs relatifs à la vie privée*, il doit mettre en place un système de log pour tracer toutes les manipulations de ces données. Typiquement, les événements à tracer sont : la création, la modification, la destruction d'*actifs de sécurité*, ou les tentatives d'accès infructueuses (« Access Denied »).

  Les événements générés doivent être horodatés (avec un timestamp absolu ou relatif en fonction des possibilités de l'appareil) puis stockés en mémoire non volatile, sauf s'ils sont stockés à l'extérieur de l'appareil (dans le cloud par exemple).

- **Possibilité de supprimer les données** : L'appareil doit fournir une procédure qui permet de détruire toutes les *données à caractère personnel*. Cette procédure sera notamment utilisée en cas de retrait du produit du marché, ou en cas de cession du produit par exemple.

- **Notification des utilisateurs** : L'appareil doit implémenter un mécanisme de notification de l'utilisateur en cas modification des *actifs de sécurité* ou des *actifs liés à la vie privée*. Cette contrainte ne s'applique pas si l'utilisateur est notifié par des mécanismes extérieurs à l'appareil (par email ou SMS par exemple).

- **Gestion des clés de chiffrement** : Sauf justification très précise, les clés de chiffrement utilisées pour protéger les données ou les communications doivent avoir une longueur minimum de 112bits, sauf cas spécifiques qui doivent être documentés.

  Les clés de chiffrement qui sont préinstallées dans les appareils doivent être uniques pour chaque appareil. Il ne doit pas être possible de dériver facilement ces clés à partir du numéro de série ou d'une autre donnée de l'appareil. Cette unicité ne s'impose pas :
  - Si ces clés sont utilisées pour établir une relation de confiance initiale et dans des conditions contrôlées,
  - Si la fonctionnalité associée à la clé impose que ces clés soient communes (par exemple pour une mise à jour du firmware).

- **Fonctionnalités des équipements** : l'équipement ne doit pas intégrer de *faille de sécurité connue* (known Vulnerability) qui compromettrait les *actifs de sécurité* ou les *actifs liés à la vie privée*, à moins que :
  - A la suite d'une analyse de risque, les conséquences de ces vulnérabilités aient été acceptées,
  - Une solution technique ait permis de ramener le risque à un risque résiduel

  Pour ce faire, le fabricant doit maintenir une liste des modules logiciels et des composants matériels intégrés à son produit et qui sont utilisés pour gérer *les actifs de sécurité* ou les *actifs liés à la vie privée*.

Par ailleurs, la spécification recommande de limiter les fonctionnalités et les interfaces réseau disponibles en mode *sortie d'usine* au strict minimum requis pour la première mise en service de l'appareil.

Pour limiter la surface d'attaque de l'appareil, toutes les interfaces non utiles pour le fonctionnement de l'appareil doivent être inhibées (typiquement l'interface JTAG, les ports TCP/UDP non utilisés, les ports série non utilisés …).

Toutes les données d'entrée utilisées pour manipuler les *actifs de sécurité* ou les *actifs liés à la vie privée* doivent être vérifiées. Typiquement, l'objectif est de protéger l'appareil contre des attaques de type injection de code[10], où un attaquant pourrait forcer l'appareil à exécuter un code malveillant intégré dans une requête.

- **Cryptographie** : Les algorithmes de cryptographie utilisés pour protéger les données au repos ou en transit doivent suivre les bonnes pratiques.

[10] https://owasp.org/www-community/attacks/Code_Injection

L'article 3.3§d – ne pas perturber les ressources réseau

La spécification EN 18031-1:2024 introduit des contraintes liées à la cybersécurité. Ces contraintes sont destinées à protéger les *actifs de sécurité (Security Assets)* et les *actifs liés au réseau* (Network Assets) intégrés à l'appareil.

Les appareils concernés par l'article 3.3§d

Cet article s'applique à tout équipement radioélectrique capable de communiquer par lui-même sur l'internet, qu'il communique directement ou par l'intermédiaire d'un autre équipement [11] c'est-à-dire que ces équipements connectés à l'internet exécutent les protocoles nécessaires pour échanger des données avec l'internet, directement ou au moyen d'un équipement intermédiaire.

Il s'applique donc évidemment aux appareils dotés d'une interface d'accès au réseau cellulaire (2G,3G,4G,5G ..), aux équipements dotés d'une interface WIFI qui se connectent à internet via un point d'accès WIFI par exemple.

Par ailleurs, il s'applique à toutes les interfaces de communication de ces équipements, que ces interfaces soient des interfaces Radios ou filaires[12].

Un appareil qui n'a pas vocation à se connecter sur internet (par exemple un système d'ouverture de porte de garage) n'est donc pas concerné.

Il reste une ambiguïté, à mon avis, qui concerne l'applicabilité de l'article 3.3§d aux équipements :

- Qui se connectent en Bluetooth à une application mobile (un cardiofréquencemètre utilisé pour le sport par exemple),
- Ou qui se connectent via un interface radio (par exemple Zigbee, ou un protocole radio propriétaire) à une gateway qui est elle-même connectée à internet (un capteur d'ouverture de porte dans un système d'alarme de maison par exemple).
- Ou qui se connectent à un réseau Lora public ou privé.

D'après mes recherches sur internet, ces équipements seraient concernés par cet article puisqu'ils se connectent « indirectement » à internet. Mais cette information provient souvent de site de cabinets de consultants et pas de sites officiels de la communauté européenne.

Mais ma lecture personnelle du texte de la directive me laisse penser que ce n'est pas le cas puisque ces équipements n'implémentent pas les protocoles nécessaires pour échanger sur internet (à savoir TCP/UDP/IP). Il n'y a donc pas de raison qu'ils puissent perturber le réseau.

Pour ce type d'équipements, il faudra donc approfondir cette question auprès d'experts en droit, ou auprès de la commission européenne, pour savoir si l'article 3.3§d est applicable ou non.

Les contraintes introduites par l'article 3.3§d

Si l'appareil entre dans le cadre d'application de l'article 3.3§d, on peut facilement transposer les contraintes associées à la protection des *actifs liés à la vie privée* à la protection des *actifs réseau*.

Dans ce cas, les actifs concernés sont les *actifs réseau* plutôt que les *actifs liés à la vie privée*.

- **Contrôle d'accès** : transposition du contrôle d'accès de l'article 3.3§e

[11] Article premier du RÈGLEMENT DÉLÉGUÉ (UE) 2022/30 DE LA COMMISSION
[12] Point (8) du RÈGLEMENT DÉLÉGUÉ (UE) 2022/30 DE LA COMMISSION

- **Authentification** : transposition de l'article 3.3§e

- **Mises à jour sécurisées** : transposition de l'article 3.3§e

- **Stockage Sécurisé** : transposition de l'article 3.3§e

- **Sécurité des communications** : transposition de l'article 3.3§e

- **Gestion des clés de chiffrement** : transposition de l'article 3.3§e

- **Fonctionnalités des équipements** : transposition de l'article 3.3§e

- **Cryptographie** : transposition de l'article 3.3§e

- **Résilience** : L'équipement doit se protéger pour limiter les effets d'une attaque de type Denial Of Service sur ses interfaces en contact avec le réseau. Par exemple, il peut filtrer les paquets à l'entrée, ou inhiber temporairement l'interface attaquée en cas de suspicion d'attaque …

- **Supervision du réseau :** Si l'équipement est lui-même une passerelle pour router le trafic d'autres équipements vers l'internet, il doit implémenter des fonctions de surveillance du réseau pour détecter les tentatives de Déni De Service qui pourraient provenir d'une de ses interfaces.

- **Contrôle du trafic :** Si l'équipement est lui-même une passerelle pour router le trafic d'autres équipements vers l'internet, il doit implémenter des fonctions d'analyse du trafic provenant des autres équipements pour détecter si un équipement génère un trafic suspect susceptible de perturber le réseau. Si un type de trafic suspect est détecté, l'équipement doit prendre des mesures pour protéger le réseau (bloquer certaines adresses IP, certains ports …).

L'article 3.3§f – La protection contre les fraudes

Les appareils concernés par l'article 3.3§f

Cet article ne concerne que les équipements qui permettent au détenteur ou à l'utilisateur de transférer de l'argent, de la valeur monétaire ou une monnaie virtuelle[13] telle que définie à l'article 2, point d), de la directive (UE) 2019/713 du Parlement européen et du Conseil[14].

Cet article s'applique donc uniquement à un nombre très restreint d'équipements (typiquement les terminaux de paiement …).

Les contraintes introduites par l'article 3.3§f

Si l'appareil entre dans le cadre d'application de l'article 3.3§f, on peut facilement transposer les contraintes associées à la protection des *actifs liés à la vie privée* à la protection des *actifs financiers*.

Dans ce cas, les actifs concernés sont les actifs réseau plutôt que les actifs liés à la vie privée.

- **Contrôle d'accès** : transposition de l'article 3.3§e
- **Authentification** : transposition de l'article 3.3§e
- **Mises à jour sécurisées** : transposition de l'article 3.3§e
- **Stockage Sécurisé** : transposition de l'article 3.3§e
- **Sécurité des communications** : transposition de l'article 3.3§e
- **Mécanisme de traces** : transposition de l'article 3.3§e
- **Gestion des clés de chiffrement** : transposition de l'article 3.3§e. Par ailleurs, les équipements qui manipulent des données financières doivent implémenter un boot sécurisé, pour s'assurer que le firmware qui est en cours d'exécution est un firmware authentique.
- **Fonctionnalités des équipements** : transposition de l'article 3.3§e
- **Cryptographie** : transposition de l'article 3.3§e

[13] «monnaie virtuelle»: une représentation numérique de valeur qui n'est ni émise ou garantie par une banque centrale ou une autorité publique, ni nécessairement attachée à une monnaie établie légalement et qui ne possède pas le statut juridique d'une monnaie ou d'argent, mais qui est acceptée comme moyen d'échange par des personnes physiques ou morales et peut être transférée, stockée et échangée par voie électronique ;
[14] Point (14) du RÈGLEMENT DÉLÉGUÉ (UE) 2022/30 DE LA COMMISSION

Les techniques à mettre en œuvre

En fonction des contraintes à respecter, les techniques à implémenter pour respecter la directive RED sont les suivantes :

La Cryptographie

La cryptographie intervient dans les domaines du contrôle d'accès, de l'authentification, du stockage sécurisé des données et des mises à jour sécurisées.

En termes de sécurité il est toujours recommandé d'utiliser des librairies open source qui ont été validées par un grand nombre d'utilisateurs, et dont les failles sont rapidement détectées et corrigées. A contrario, il est vivement déconseillé d'implémenter soi-même les algorithmes de cryptographie, car il est quasiment certain que l'implémentation réalisée contiendra des failles.

Dans le domaine du logiciel embarqué, la librairie mbedTLS[15] développée par ARM est largement utilisée car elle est adaptée aux processeurs ne disposant pas de très grandes capacités en termes de mémoire. Elle implémente la plupart des algorithmes de cryptographie modernes symétriques (notamment AES, DES et 3DES) ou asymétriques (notamment RSA, DH, ECC). Elle permet donc de calculer ou de vérifier des signatures suivant plusieurs algorithmes, de manipuler les certificats X.509, ou d'effectuer des opérations de chiffrement/déchiffrement de données. Elle implémente aussi les protocoles TLS/DTLS utilisés dans les protocoles de communication sécurisés. Cette librairie permet donc de gérer la confidentialité des données, la vérification de l'authenticité d'un tiers, la vérification de l'intégrité d'un message ou d'un fichier.

Il existe bien sûr d'autres librairies comme openSSL, librairie open source qui est plutôt utilisée dans le monde linux, ou wolfSSL qui est associée à une licence commerciale.

La gestion des clés de chiffrement

Même si on utilise des algorithmes de cryptographie très modernes, ils seront complètement inefficaces si les clés de chiffrement utilisées sont facilement accessibles. Les équipements utilisent des clés symétriques pour chiffrer les données, et des algorithmes asymétriques pour calculer ou vérifier des signatures, ou pour exécuter les protocoles de communications sécurisés comme TLS ou DTLS.

Les clés de chiffrement doivent donc être protégées. Il existe plusieurs manières de réaliser cette opération en fonction des possibilités présentes sur la carte électronique :

- Le stockage des clés en flash interne du processeur
  La méthode la plus basique pour protéger les clés de chiffrement consiste à stocker ces clés dans la mémoire flash interne du processeur, pourvu que cette mémoire flash ne soit pas accessible depuis l'extérieur (donc notamment, le JTAG devra être désactivé). Les ne doivent pas non plus être stockés dans l'image du firmware mais dans une zone dédiée de la mémoire car l'image du firmware pourrait être facilement accessible, notamment lors d'un upgrade. Cette méthode n'est pas la plus sécurisée mais elle peut suffire à garantir la confidentialité des clés.

[15] https://github.com/Mbed-TLS/mbedtls

- Le stockage des clés en flash externe
- Si le processeur ne dispose pas de flash interne, les clés seront nécessairement stockées en flash externe … Il faudra nécessairement les chiffrer elles-mêmes avec une clé générée par le firmware. La sécurité sera alors assez minimaliste, mais sera suffisante si elle est correctement justifiée dans le document technique.

- Les MPUs[16]
  La plupart des microcontrôleurs récents basés sur les architectures ARM Cortex-M our ARM Cortex-A, qui sont largement utilisés dans l'internet des objets (IOT), intègrent un MPU. Il s'agit d'un « module » intégré au processeur qui permet de protéger certaines parties de la mémoire pour qu'elles ne soient accessibles que par du code qui s'exécute en mode privilégié. Si les algorithmes de chiffrement s'exécutent en mode privilégié alors que le code applicatif (y-compris l'OS temps réel) s'exécute en mode non privilégié, les clés seront protégées.

- ARM Trustzone™
  Certains processeurs ARM Cortex-M (et aussi Cortex-A) intègrent une fonctionnalité nommée ARM Trustzone. Cette fonctionnalité permet de complètement séparer un firmware en deux firmwares distincts, comme si le processeur était composé lui-même de deux processeurs avec leurs propres vecteurs d'interruption et leur propre mémoire. Cette fonctionnalité permet de créer deux « environnements d'exécution » nommés SPE (Secure Processing Environment) et NSPE (Non Secure Processing Environment). Les algorithmes de chiffrement s'exécuteront donc en SPE, alors que le reste du code s'exécutera en NSPE. Les clés de chiffrement ne seront bien sûr accessibles qu'au code qui s'exécute en SPE.

- Le Secure Element
  C'est l'option la plus efficace, mais aussi la plus complexe et la plus coûteuse. Elle consiste à équiper la carte électronique d'un composant spécialisé qui sera responsable de stocker les clés de chiffrement et de réaliser les opérations de cryptographie. Ces composants sont conçus pour résister aux attaques les plus complexes comme les attaques par canal auxiliaire (« side channel attacks »). Une fois les clés configurées en usine, elles ne peuvent pas être relues par un logiciel. Il est toutefois possible de les mettre à jour à partir du firmware de l'appareil. Par exemple, les composants ATECC608B de Microchip, ou STSAFE-A110 de ST Microelectronics peuvent être utilisés. Il existe bien sûr d'autres références chez les fournisseurs de circuits intégrés.

- Certains SOCs[17] intègrent un Secure Element
  Les SOCs sont largement utilisés dans les objets connectés car ils embarquent le processeur, la partie radio, et intègrent aussi de la mémoire. Les SOCs les plus récents intègrent un Secure Element, c'est-à-dire un processeur de cryptographie et une mémoire protégée pour stocker les clés de chiffrement. Cette solution est encore plus efficace que la précédente puisqu'il est même impossible d'espionner les communications entre le processeur et le Secure Element (même si les Secure Elements sont capables de chiffrer les communications sur les interfaces I2C). C'est le cas notamment de certains SOCs de Silicon Labs, qui utilise le terme Secure Vault™ pour désigner cette fonctionnalité.

[16] Memory Protection Unit
[17] System On Chip

Le stockage sécurisé des données

Toutes les données des *actifs liés à la vie privée*, des *actifs réseaux*, des *actifs financiers* qui sont stockées en mémoire permanente doivent être protégées.

- Idéalement, ces données doivent être stockées dans la flash interne du processeur, si celui-ci en dispose, pour éviter que ces données puissent être espionnées sur le bus de données du processeur au moment où elles sont utilisées.

- Le minimum de protection à implémenter consiste à chiffrer ces données, en général avec un algorithme de chiffrement symétrique (en général AES). Cette protection ne suffit pas à garantir que les données n'ont pas été modifiées depuis leur stockage. Il faudrait donc aussi calculer la signature du bloc de données à protéger (par exemple une signature ECDSA[18]) pour garantir l'intégrité des données à protéger. On aura donc besoin d'une clé symétrique pour le chiffrement des données, et d'une clé privée d'un algorithme asymétrique pour générer la signature.

- Une implémentation plus élaborée proposée par ARM dans ARM Trusted Firmware™ consiste à séparer le code qui gère les données sécurisées pour qu'il s'exécute dans l'environnement SPE (Secure Processing Evironment). Cette implémentation suppose que le SOC implémente ARM Trustzone, qui existe notamment sur les processeurs ARM Cortex M33 ou ARM Cortex M55.

La sécurisation des communications

La sécurisation des communications passe le plus souvent par l'utilisation des protocoles TLS (Transport Layer Security) ou DTLS (Datagram Transport Layer Security). Ces protocoles permettent à un client (l'équipement radioélectrique) de vérifier l'authenticité du serveur auquel il se connecte. Une fois l'authenticité du serveur vérifiée, le serveur peut optionnellement vérifier l'identité du client, mais cela suppose d'avoir stocké (souvent en usine) une clé privée dans la mémoire non volatile de l'équipement. Une fois que cette phase a été exécutée avec succès, le client et le serveur définissent des clés de chiffrement symétrique qui seront utilisées pour chiffrer les messages qu'ils s'échangeront durant cette session. De nouvelles clés seront négociées à chaque nouvelle session.

Toutes les stacks IP fournies avec les SOCs implémentent ces protocoles, et il n'est donc pas compliqué de les utiliser. Cependant, ces protocoles sont basés sur la génération et l'utilisation de certificats X.509, dont la gestion demandera de mettre en place quelques process liés à la sécurité au sein de l'entreprise.

La mise à jour sécurisée des firmwares

Tous les SOCs modernes sont fournis avec un environnement logiciel qui intègre, entre autres modules, des librairies capables de réaliser des mises à jour sécurisées. Ces librairies peuvent vérifier l'intégrité des logiciels, les déchiffrer (s'ils ont été chiffrés avant d'être transmis), et de les stocker en mémoire interne ou externe, en clair ou chiffrés suivant le choix du développeur, et suivant les possibilités du SOC. Si les images des firmwares sont stockées en flash externe, elles devraient

[18] Elliptic curve digital signature algorithm<

idéalement être chiffrées pour protéger l'accès aux « *actifs de sécurité* » qui pourraient s'y trouver (notamment le code qui gère des données critiques).

En revanche, l'implémentation de la récupération des logiciels depuis un serveur est à la charge des développeurs. Pour s'assurer que le logiciel provient bien d'un serveur « officiel », il est indispensable d'authentifier le serveur qui fournit le nouveau logiciel à télécharger. Cette authentification est habituellement réalisée par le protocole HTTPS : le serveur fournit un certificat X.509 qui est vérifié par l'appareil grâce à une clé publique qui lui a été fourni au préalable, souvent au moment de la configuration en usine.

La limitation de la surface d'attaque

Il est recommandé de désactiver toutes interfaces non utilisées. Il s'agit en particulier de l'interface JTAG mentionnée plus haut car elle donne tous les accès à un attaquant.

Au-delà du JTAG, les ports UART qui sont souvent utilisés comme console de debug doivent être inhibés, sauf s'ils sont requis pour fournir d'autres fonctionnalités à l'appareil (comme une console de configuration par exemple) : dans ce cas, cette interface devra être protégée par des mécanismes d'authentification de l'utilisateur, et les données reçues sur cette interface devront être validées avant d'être traitées pour que l'équipement soit protégé contre les attaques de type « injection de code ».

De même tous les ports TCP/UDP inutilisés doivent être fermés.

La gestion des vulnérabilités

L'identification des *failles de sécurité connues* (known vulnerabilities) introduites par des librairies externes dans un logiciel embarqué est plus simple à réaliser que dans un logiciel plus complexe. En effet, les logiciels embarqués, du fait de leurs fortes contraintes en taille de code, intègrent moins de librairies externes (open source ou non), qui intègreraient elles-mêmes d'autres librairies externes, etc …

Cependant, il faut tout de même identifier ces vulnérabilités. Cette étape passe par un listing de tous les composants externes intégrés au logiciel, puis par des audits des bases de données de vulnérabilités (par exemple https://nvd.nist.gov, …) pour vérifier si ces composants incluent des *failles de sécurité connues*.

Il existe également des outils d'analyse statique de code spécialement conçus pour les logiciels embarqués, largement intégrés dans les processus d'intégration continue. Ces outils permettent d'analyser le code source des équipements et d'identifier s'il contient des *failles de sécurité connues*.

Toutefois, les piles de communication (Wi-Fi, BLE, Zigbee, Thread, etc.) posent un problème particulier : elles sont souvent fournies en format binaire par les fabricants de SoC, ce qui empêche toute analyse directe du code. Dans ce contexte, il est nécessaire de se rapprocher du fournisseur afin d'obtenir des informations sur les éventuelles vulnérabilités connues affectant ces composants.

La méthode STRIDE est adaptée pour identifier les menaces auxquelles un système est exposé. Cette méthode consiste à étudier 6 catégories de menaces, comme indiqué dans le tableau suivant (extrait de https://en.wikipedia.org/wiki/STRIDE_model):

Threat	Desired property	Threat Definition
Spoofing	Authenticity	Pretending to be something or someone other than yourself
Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere
Repudiation	Non-repudiability	Claiming that you didn't do something or were not responsible; can be honest or false
Information disclosure	Confidentiality	Someone obtaining information they are not authorized to access
Denial of service	Availability	Exhausting resources needed to provide service
Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

Une fois les vulnérabilités identifiées, il faudra soit les corriger, soit les contourner, soit décider que ces vulnérabilités sont admissibles pour le produit. Cette décision sera prise à la suite d'une analyse des risques, qui caractérisera chaque risque en fonction de son impact sur le produit et de sa probabilité dans le contexte d'utilisation de l'équipement.

Le boot sécurisé

Même si l'utilisation d'un boot sécurisé n'est requise que pour les équipements qui gèrent des données financières, son utilisation est largement recommandée dans tous les produits. Il s'agit de vérifier à chaque démarrage si le logiciel qui se trouve en mémoire n'a pas été modifié depuis son téléchargement. Idéalement, l'implémentation d'un boot sécurisé requiert qu'un premier « bootloader » soit stocké en mémoire non modifiable (ROM). En effet, un boot sécurisé n'aurait aucun intérêt s'il était possible de modifier le bootloader lui-même …

En général, les implémentations de boot sécurisé intègrent deux bootloaders :

- Un bootloader non modifiable stocké en ROM (ce bootloader est nommé BL1 dans ARM Trusted Firmware™). Puisque ce bootloader est non modifiable, il contient un strict minimum d'instructions car il ne pourra pas être patché si un bug est découvert. Son rôle est de vérifier l'intégrité d'un deuxième bootloader (nommé BL2 dans ARM Trusted Firmware) et de l'exécuter.
- Ce deuxième bootloader peut intégrer des fonctionnalités plus avancées puisqu'il peut être mis à jour si un bug est découvert. Son rôle sera essentiellement de vérifier l'intégrité de l'application (ou d'un autre bootloader interactif nommé U-Boot dans le cas de linux), puis de l'exécuter. Eventuellement, il pourra implémenter des stratégies de repli vers une version antérieure s'il détecte que le code de l'application (ou de U-Boot) a été modifié de manière anormale.

Comme pour les mises à jour du firmware, les fournisseurs de SOCs fournissent tous des exemples d'implémentations de bootloader sécurisés. Les SOC les plu récents intègrent un premier bootloader BL1 en ROM, et permettent aux développeurs d'implémenter leur propre bootloader (BL2) sur la base des exemples fournis.

A propos de TIDIWI

TIDIWI est une société de conseil spécialisée dans la conception et le développement de projets IOT. Notamment, TIDIWI a une forte expérience dans les protocoles de communication sans fil et dans les systèmes à ultra faible consommation d'énergie.

TIDIWI intervient sur des missions de conseil, de développement de logiciel embarqué, de développement de cartes électroniques, le management d'équipes de développement, la gestion de projets.

Pour plus d'information, visitez le site de Tidiwi : www.tidiwi.com

Ou contacter thierry.didi[at]tidiwi[dot]com

References

- DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014

- RÈGLEMENT DÉLÉGUÉ (UE) 2022/30 DE LA COMMISSION du 29 octobre 2021

- EN 18031-1:2024 : Common Security Requirements for Internet Connected Radio Equipment.

- EN 18031-2:2024 : Common Security Requirements Equipment Processing Personal Data

- EN 18031-3:2024 : Common Security Requirements for Equipment Processing Virtual Money or monetary value

- ARM Trusted Firmware-A : https://github.com/ARM-software/arm-trusted-firmware

- ARM Trusted Firmware-M: https://github.com/TrustedFirmware-M/trusted-firmware-m