Chapitre IV Sécurité des systèmes embarqués

SAIDI SIEF Ali

Chapitre IV Sécurité des systèmes embarqués

IV.1.Introduction :

- **La sécurité** se décline de nombreuses manières, par exemple dans le cadre des transactions électroniques mais également dans la protection des données, des informations, des personnes et des biens. Dans ce contexte, la sécurité comprend en particulier celle des systèmes, des logiciels, des protocoles, des architectures globales, des composants matériels, des réseaux tant filaires ou optiques que radios, des équipements d'extrémités, des moyens de stockage de l'information.
- **Par ailleurs,** la sécurisation des systèmes d'information repose sur de nouvelles techniques de sécurisation algorithmique, mais aussi sur des principes physiques comme la cryptographie quantique ou la cryptographie par chaos

Chapitre III Sécurité des systèmes embarqués

IV.1.Introduction :

La sûreté de fonctionnement **des systèmes (tels que les centrales nucléaires, les avions et engins spatiaux, les systèmes industriels de production continue (électricité, pétrole, chimie), les grands ouvrages de génie civil (barrages, ponts, plateformes pétrolières), les véhicules et les infrastructures des systèmes de transport routiers et ferroviaires)** passe par la conception d'algorithmes de traitement in-situ des données numériques ainsi disponibles. Sur la base des informations et connaissances disponibles (instrumentation, modèles), il s'agit alors en particulier d'opérer une véritable perception (détection, localisation, diagnostic) et réaction (correction, tolérance, maintenance) par rapport aux événements imprévus ou d'évolutions ou de déviations par rapport à un état ou un comportement de référence normal, souhaitable ou nominal.

Chapitre III Sécurité des systèmes embarqués

IV.2.Cryptologie :

IV.2.1 Introduction :

La cryptologie est la science du secret, elle se divise en deux branches :

> La cryptographie : qui étudie les différentes possibilités de cacher, protéger ou contrôler l'authenticité d'une information;

> La cryptanalyse : qui étudie les moyens de retrouver cette information à partir du texte chiffré (de l'information cachée) sans connaître les clés ayant servi à protéger celle-ci, c'est en quelque sorte l'analyse des méthodes cryptographiques.

Chapitre III Sécurité des systèmes embarqués

IV.2.Cryptologie :

IV.2.2 Confidentialité :

La confidentialité est historiquement le premier but des études en cryptographie : rendre secrètes des informations.

Cela se réalise par un chiffrement mathématique des données qui utilise comme paramètre une clé. Le chiffrement consiste à appliquer une suite d'opérations sur un texte clair, pour obtenir un texte chiffré, aussi appelé cryptogramme, ne pouvant être déchiffré que par l'entité qui possède la clé adéquate.

IV.2.Cryptologie :

IV.2.2 Confidentialité :

Il existe deux catégories de chiffrements:

· Le chiffrement symétrique également appelé le chiffrement à clé secrète:

· Le principe est de chiffrer le texte clair avec une clé et de le déchiffrer avec la même clé ou une clé dérivée de celle-ci. La clé n'est connue que par les deux entités s'échangeant des informations.

Chapitre III Sécurité des systèmes embarqués

IV.2.Cryptologie :

IV.2.2 Confidentialité :

Le chiffrement asymétrique également appelé le chiffrement à clé publique: Les clés utilisées pour le chiffrement et le déchiffrement sont différentes et ne peuvent être déduites l'une de l'autre par un observateur extérieur sans la connaissance des informations nécessaires. Une des clés peut être connue de tous tandis que l'autre doit rester secrète. Le but étant que tout le monde puisse à l'aide d'une clé publique chiffrer des données que seule l'entité possédant la clé secrète puisse déchiffrer. La vision d'un ensemble de textes chiffrés ne doit apporter aucune information sur le texte clair, c'est ce qu'on appelle la notion de sécurité sémantique (propre au chiffrement asymétrique).

IV.2.Cryptologie :

IV.2.2 Confidentialité :

Dans le cadre de la sécurité dans les systèmes temps réel qui doivent respecter des contraintes de temps, nous nous intéresserons plus particulièrement au chiffrement symétrique qu'il est préférable d'utiliser car le chiffrement asymétrique a été montré comme plus complexe au niveau du temps de calcul.

IV.2.Cryptologie :

IV.2.3. Intégrité et authentification :

Le réseau reliant les entités n'étant pas toujours sûr, il est important de contrôler la provenance des informations et de s'assurer qu'elles n'ont pas été modifiées en chemin, ce sont respectivement les principes d'authentification et d'intégrité des données.

Afin de garantir ces deux principes, on utilise des codes d'authentification de message (MAC: Message Authentication Code). Un MAC est un code envoyé avec le message, il est aussi appelé *hachage* ou *empreinte* du message. Le hachage correspond au message et permet de garantir la validité de celui-ci. Il est obtenu à partir d'un algorithme MAC qui prend deux paramètres en entrée: le message dont on désire garantir l'intégrité et une clé secrète connue des deux entités s'échangeant ce message.

IV.2.Cryptologie :

IV.2.3. Intégrité et authentification :

La probabilité que des données différentes possèdent le même hachage est très faible, c'est ce qu'on appelle une « collision ». La probabilité de trouver une collision et que le message possédant le même hachage soit compréhensible par le récepteur est quasi nulle. Une modification même très légère des données provoque un changement radical au niveau du hachage obtenu. Si une modification a lieu entre la source et la destination, le hachage ne correspondra plus aux données et celles-ci seront rejetées par le récepteur.

Le fait d'utiliser une clé secrète partagée entre les deux entités en plus de la fonction de hachage garantit l'authenticité des données étant donné qu'un attaquant ne connaissant pas la clé ne peut envoyer des informations accompagnées d'un hachage correct de celles-ci.

IV.2.Cryptologie :

IV.2.3. Intégrité et authentification :

Différentes méthodes existent pour créer une empreinte du message:

· une fonction de hachage utilisant une clé en paramètre en plus du message (ex : HMAC);

· un chiffrement par blocs (comme les méthodes CBC-MAC).

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :

IV.3.1. Types d'attaquants (menaces) :

· Terroristes (but : destruction) ;
· Ennemis (but : causer des désagréments) ;
· Espions, services de renseignement (gouvernementaux, industriels) (but : informations) ;
· Concurrents industriels (but : prise de part de marché) ;
· Pirates (but : vol) ;
· Hackers (but : défi, jeux).

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :

IV.3.2. Objectifs des attaques :

· Accéder aux données privées et secrètes pour accéder à un niveau supérieur d'information (exemple: clé de cryptage pour décoder un message crypté) ;
· Accéder aux données privées pour les modifier ou les détruire ;
· Copier les données de conception pour reconstruire ou améliorer un système ;
· Prendre en main un système pour le détourner de sa fonction ou pour le détruire.

IV.3. Les menace de sécurités :

IV.3.3. Sources d'attaques dans les systèmes embarqués

Les systèmes embarqués sont exposés de plusieurs attaques, dont la cause principale est la faiblesse et les fautes résultant lors de la phase d'implémentation des mécanismes de sécurité fonctionnelle et leurs algorithmes de cryptographie. Avec ces faiblesses les attaquants peuvent contourner complètement, ou d'affaiblir de manière significative la solution de sécurité. Les raisons sont les suivantes :

IV.3. Les menace de sécurités :

IV.3.3. Sources d'attaques dans les systèmes embarqués

IV.3.3.1. Le fonctionnement dans un environnement non fiable

Il est facile de concevoir un système embarqué sûr si on base sur la sécurité physique naturelle du système (personne ne peut ouvrir le système) ou de supposer que les parties du système ne sont pas accessible par des entités malveillantes. Cependant, les systèmes embarqués ont parfois besoin de travailler dans des relations complexes, où un dispositif souhaite mettre une partie sécurisé dans la main des autres, en assurant que la deuxième partie ne peut pas modifier les parties internes du dispositif . Par exemple : une banque peut conserver des informations pertinentes dans une carte à puce qui est dans les mains de ses clients, toute en assurant que le client ne peuvent pas manipuler la carte ou de modifier les informations qu'elle contient.

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :

IV.3.3. Sources d'attaques dans les systèmes embarqués

IV.3.3.2. Vulnérabilité introduite à travers les réseaux

Il y a pas mal de systèmes embarqués qui ont la capacité de se connecter aux réseaux, ce qui les expose à de nombreuses sources d'attaque, en d'autre terme, il n'est plus nécessaire d'avoir la possession physique de l'appareil afin de briser ses mécanismes de sécurité. Les appareils avec connectivité sans fil, ou ceux qui se connectent à Internet sont les plus vulnérable.

IV.3. Les menace de sécurités :

IV.3.3. Sources d'attaques dans les systèmes embarqués

IV.3.3.3. L'exécution des logiciels téléchargés

Afin de fournir et enrichir les fonctionnalités des systèmes embarqués et les personnalisé pour l'utilisateur final, il est parfois nécessaire d'avoir la capacité de télécharger et exécuter des logiciels non fiable (approuvés), (avec des virus, chevaux de trois, etc...) qui peuvent être la source des vulnérabilités.

IV.3.3.4. Processus de conception complexe

Il peut ne pas être possible de pré-valider chaque composant du système pour assurer la sécurité de celle-ci. En d'autre terme, même si chaque composant du système est assuré en soi, il est possible que la composition des pièces expose des nouvelles vulnérabilités. La prise en compte de la sécurité lors de la conception des systèmes embarqués

IV.3. Les menace de sécurités :

IV. 3.4. Classement des attaques :

Il est possible de classifier les attaques en se basant sur 2 critères : L'objectif fonctionnel et les méthodes utilisées afin d'exécuter ces attaques.

IV. 3.4.1. Critère 1 : L'objectif fonctionnel

La Figure suivante montre une classification générale des attaques sur les systèmes embarqués, dont le 1er niveau montre la classification selon l'objectif fonctionnel. Dans ce niveau on peut distinguer 3 types d'attaques :

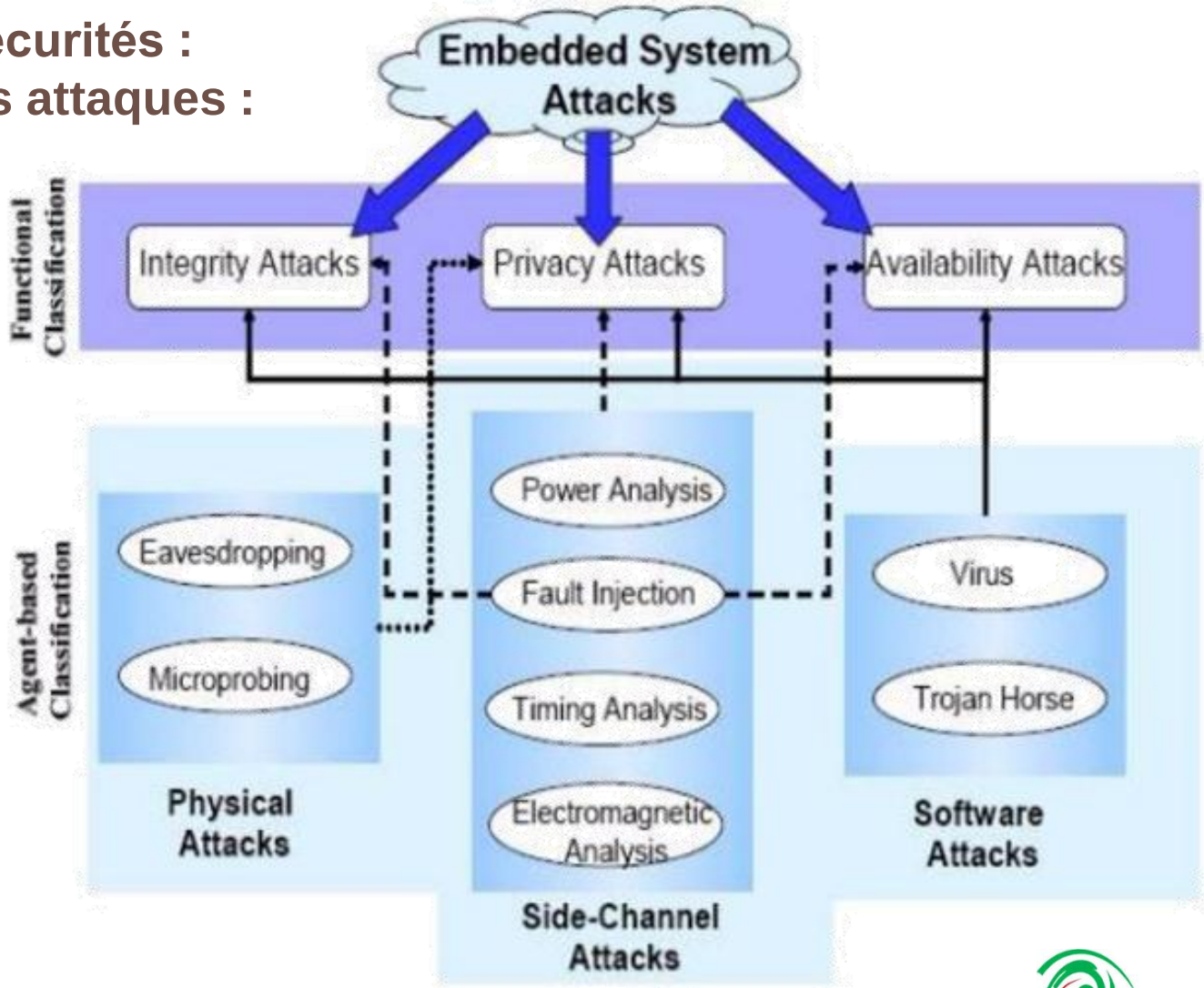
Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :

IV. 3.4. Classement des attaques :

IV. 3.4.1. Critère 1 :

L'objectif fonctionnel



Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :

IV. 3.4. Classement des attaques :

IV. 3.4.1. Critère 1 : L'objectif fonctionnel

IV. 3.4.1.1. Attaques de confidentialité

L'objectif de ces attaques est d'obtenir des informations sensibles stockées, transmises ou manipulées par un système embarqué.

IV. 3.4.1.2. Attaque d'intégrité

Ces attaques tentent de modifier les données ou le code associé à un système embarqué.

IV. 3.4.1.3. Attaque sur la disponibilité

Ces attaques tentent à introduire des erreurs afin de perturber le fonctionnement normal d'un système ou de s'emparer les ressources de tel sorte que le système ne soit pas disponible pur un fonctionnement normal.

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :

IV. 3.4. Classement des attaques :

IV. 3.4.2. Critère 2 : les méthodes utilisées

Dans la même figure précédente, le 2eme niveau et la Figure suivante, présentent une classification des attaques selon les moyens et les agents utilisés pour lancer une attaque. Ces agents sont généralement regroupés en 3 grandes catégories:

IV. 3.4.2.1. Attaque des logiques

Qui se réfèrent à des attaques lancées par des agents logiciels tels que : les virus, les chevaux de trois, etc…

IV. 3.4.2.2. Attaques physiques

Qui se réfèrent à des attaques qui nécessitent une intrusion physique dans le système embarqué.

IV. 3.4.2.3. Les canaux cachés

Qui se réfèrent à des attaques qui sont basées sur l'observation des propriétés du système lors de l'exécution des opérations de chiffrement par ce dernier. Par exemple : la consommation d'énergie par le système, le temps d'exécution, le comportement dans la présence des failles, etc…

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :
IV. 3.4. Classement des attaques :
IV. 3.4.2. Critère 2 : les méthodes utilisées

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :
IV. 3.4. Classement des attaques :
IV. 3.4.2. Critère 2 : les méthodes utilisées
IV. 3.4.2.1. Les attaques logicielles
IV. 3.4.2.1.1. Infections informatiques, codes malveillants

Programmes simples qui exécutent un programme en tâche de fond. Ils ne peuvent pas se reproduire, ils servent souvent à ouvrir une brèche cachée dans le système pour y faire pénétrer un pirate , par exemple : Cheval de Troie et Bombe Logique (dans le cas de la bombe logique le départ du programme est retardé). Programmes autoreproducteurs par exemple : Un ver est un virus très virulent qui se diffuse de façon planétaire.

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :

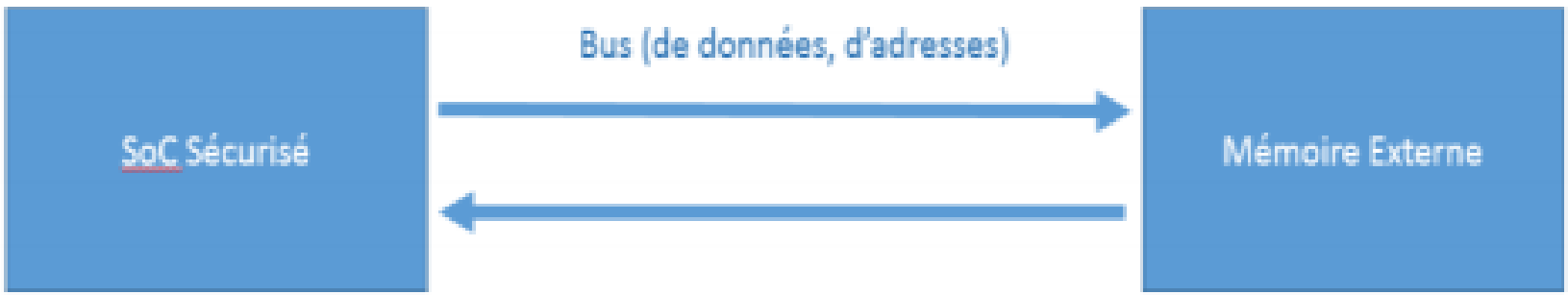
IV. 3.4. Classement des attaques :

IV. 3.4.2. Critère 2 : les méthodes utilisées

IV. 3.4.2.1. Les attaques logicielles

IV. 3.4.2.1.2. Vulnérabilités logicielles

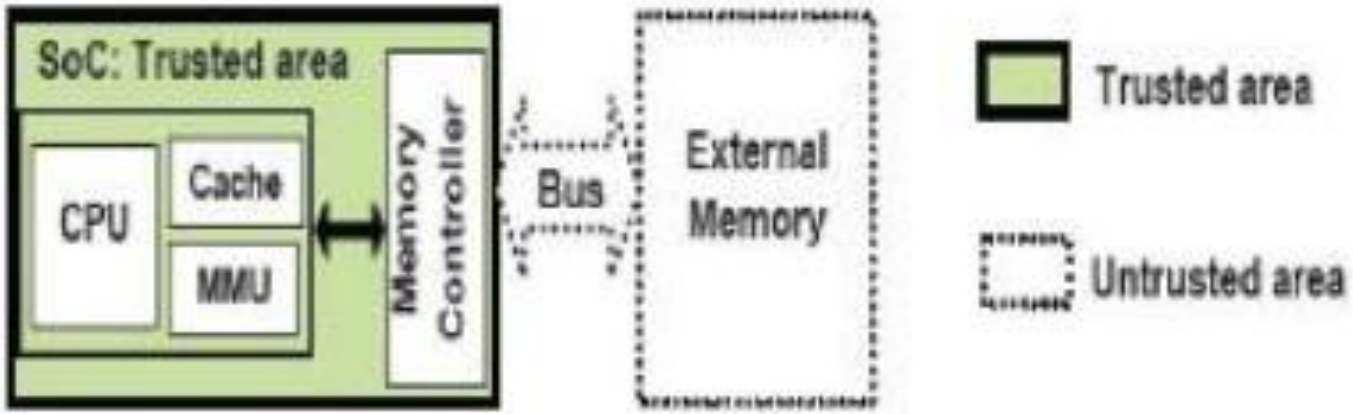
La plus part des systèmes embarqués ont une zone mémoire extérieure au SoC (System on Chip) principal. Des données et des instructions sont échangés entre le processeur et la mémoire sur un ou plusieurs bus (adresse, instruction, donnée) Menaces (logicielle ou matérielle) : Lecture non autorisée de données, Injection de code, Modification des données.



Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :
IV. 3.4. Classement des attaques :
IV. 3.4.2. Critère 2 : les méthodes utilisées
IV. 3.4.2.1. Les attaques logicielles
IV. 3.4.2.1.3. Modèle de menaces

Ici le SoC est dans un environnement sécurisé à contraire de la mémoire externe qui n'est pas dans un environnement sécurisé, voir la [Figure ci-dessous].



Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :
IV. 3.4. Classement des attaques :
IV. 3.4.2. Critère 2 : les méthodes utilisées
IV. 3.4.2.1. Les attaques logicielles
IV. 3.4.2.1.3. Modèle de menaces

Dans ce cas il y'a deux modèles d'attaques :

1. Attaques passives : écoute du bus (bus probing) par analyse hors ligne du code est la reconstitution d'une clé de chiffrement, qui permet de faire une reconstitution de message, ce qui constitue une matière première pour préparer une attaque active.

2. Attaques actives : modification du contenu de la mémoire (memory tampering). Il y'a trois types d'attaques actives sont définies en fonction du choix fait par l'attaquant :

a. Spoofing : injection aléatoire de données. **b. Splicing :** permutation spatial de données. **c. Replay (rejeu)**: permutation temporelle de données. interception d'une écriture/lecture et remplacement par une donnée plus ancienne

Chapitre III Sécurité des systèmes embarqués

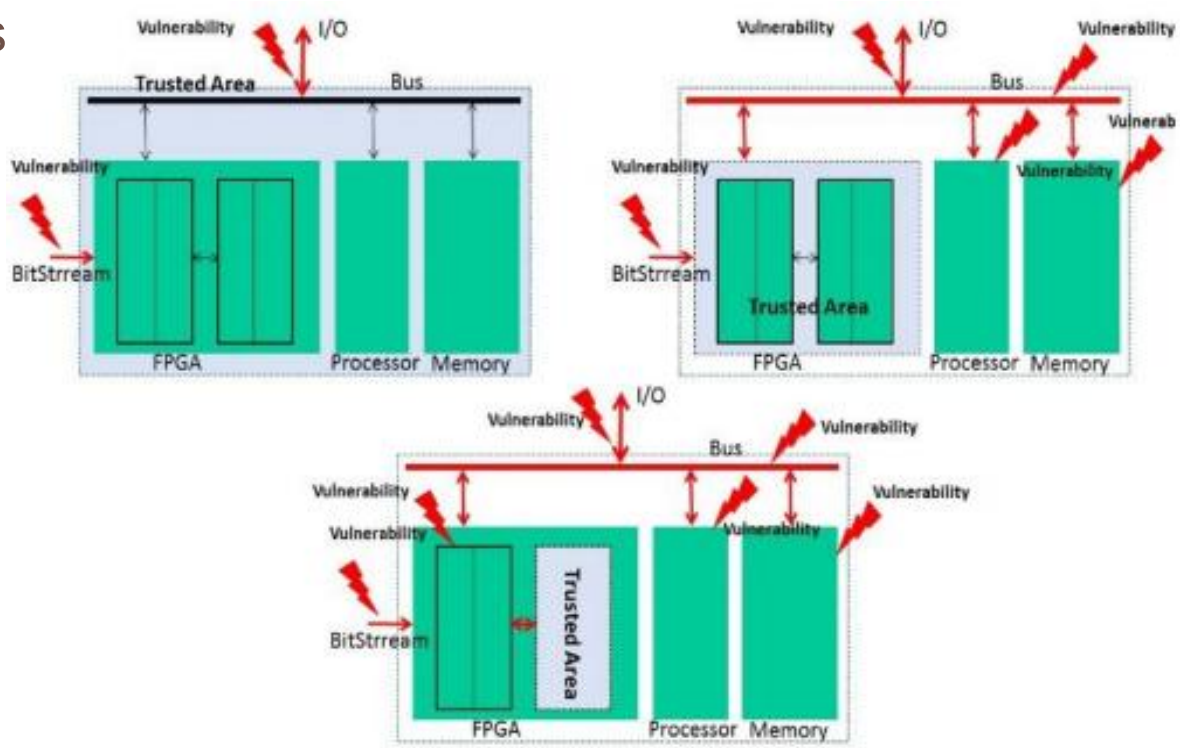
IV.3. Les menace de sécurités :
IV. 3.4. Classement des attaques :
IV. 3.4.2. Critère 2 : les méthodes utilisées
IV. 3.4.2.1. Les attaques logicielles
IV. 3.4.2.1.3. Modèle de menaces

Les objectifs de ces attaques sont : détournement du code, réduire l'espace de recherche pour la reconstruction d'une clé ou d'un message.

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :
IV. 3.4. Classement des attaques :
IV. 3.4.2. Critère 2 : les méthodes utilisées
IV. 3.4.2.2. Les attaques matérielles
IV. 3.4.2.2.1. Vulnérabilités matérielles

Plusieurs types de menaces peut être considérés en fonction de l'environnement et de la possibilité d'accès ou non à l'intérieure du système, voir la [Figure ci-contre].



Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :
IV. 3.4. Classement des attaques :
IV. 3.4.2. Critère 2 : les méthodes utilisées
IV. 3.4.2.2. Les attaques matérielles
IV. 3.4.2.2.2. Attaques physiques irréversibles (Invasive attacks, tampering) :

1. Découpage du circuit intégré.
2. Attaque chimique de la puce.
3. Découpage du layout : reconnaître les structures formées par les différentes couches et les transformer en un circuit électrique équivalent.
4. Analyse microscopique.
5. Reconstruction du layout.

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :
IV. 3.4. Classement des attaques :
IV. 3.4.2. Critère 2 : les méthodes utilisées
IV. 3.4.2.2. Les attaques matérielles
IV. 3.4.2.2.3. Attaques physiques réversibles

Injection de fautes (non-invasive ou semi-invasive attacks) :les attaques par perturbation sont extrêmement puissantes et permettent à un attaquant de casser un système non protégé plus rapidement que n'importe quelle autre attaque par canaux auxiliaires. Par conséquent, ces attaques sont largement utilisées pour valider la sécurité des applications sensibles s'exécutant dans un environnement carte à puce. Et cette attaque est faite par :

1. Glitch : Causer une défaillance électronique ou électrique qui correspond à une fluctuation dans les circuits électroniques ou à une coupure de courant. Ce qui entraîne un dysfonctionnement du matériel informatique, qui occasionne à son tour des répercussions sur les logiciels.

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :
IV. 3.4. Classement des attaques :
IV. 3.4.2. Critère 2 : les méthodes utilisées
IV. 3.4.2.2. Les attaques matérielles
IV. 3.4.2.2.3. Attaques physiques réversibles

2. Flash lumineux qui agit sur les technologies EPROM4 pour modifier une partie du système.

3. Ionisation locales qui se fait par l'utilisation du Laser pour les mémoires CMOS SRAM.

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :
IV. 3.4. Classement des attaques :
IV. 3.4.2. Critère 2 : les méthodes utilisées
IV. 3.4.2.2. Les attaques matérielles
IV. 3.4.2.2.4. Les canaux cachés

Les attaques par canaux cachés (auxiliaires) dans l'environnement de la carte à puce sont composées des quatre catégories présentées ci-dessus :

1. analyse de temps d'exécution : Les algorithmes de cryptographies utilisent souvent des opérations de multiplication et de division. Cependant, ces instructions s'exécutent dans un nombre variable de cycle selon les données d'entrées .Comme dans le cas des attaques à base d'analyse d'énergie, des statistiques du temps d'exécution peuvent être recueillies et analysé afin de déduire la clé de chiffrement.

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :
IV. 3.4. Classement des attaques :
IV. 3.4.2. Critère 2 : les méthodes utilisées
IV. 3.4.2.2. Les attaques matérielles
IV. 3.4.2.2.4. Les canaux cachés

2. analyse de courant/de fréquences radio: Tout le monde connaît que la consommation d'énergie d'un circuit dépend de la commutation d'un signal électrique à l'intérieur d'un fil, ainsi cette commutation elle-même dépend des données. Donc il n'est pas surprenant que la clé utilisé dans un algorithme de cryptographie peut être déduite à partir des statistiques recueillies à partir de la consommation d'énergie sur une vaste gamme de données d'entrées. Ces attaques sont aussi appelées attaque à base d'analyse de puissance, et il a été démontré qu'elles sont très efficaces pour briser les systèmes embarqués tel que les cartes à puce

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :
IV. 3.4. Classement des attaques :
IV. 3.4.2. Critère 2 : les méthodes utilisées
IV. 3.4.2.2. Les attaques matérielles
IV. 3.4.2.2.4. Les canaux cachés

3. analyse du rayonnement électromagnétique : Les attaques à base d'analyse électromagnétique (EMA) ont été utilisé depuis longtemps en utilisant les rayonnements électromagnétique d'une unité d'affichage vidéo afin de reconstruire le contenue de l'écran.

Chapitre III Sécurité des systèmes embarqués

IV.3. Les menace de sécurités :
IV. 3.4. Classement des attaques :
IV. 3.4.2. Critère 2 : les méthodes utilisées
IV. 3.4.2.2. Les attaques matérielles
IV. 3.4.2.2.4. Les canaux cachés
4. attaques par perturbation (Bien que ce dernier type d'attaque n'utilise pas directement les informations disponibles par canaux auxiliaires, il est très souvent classé comme tel dans la littérature) : Les attaques à base d'injection de faute s'appuyé sur la variation et le changement des paramètres externes d'un système embarqué afin d'inciter des fautes dans ses composants .Les fautes injectées peuvent être transitoire ou permanant, et peuvent compromettre la sécurité d'un système dans plusieurs points :
Les fautes peuvent être injectées afin de perturber le fonctionnement normal d'un système afin d'attaquer sa disponibilité. Par exemple : le bus dans un système embarqué (ex : carte à puce) peut être rendu indisponible pour effectuer des communications, ceci est possible par le biais de mettre une valeur constante sur le bus.

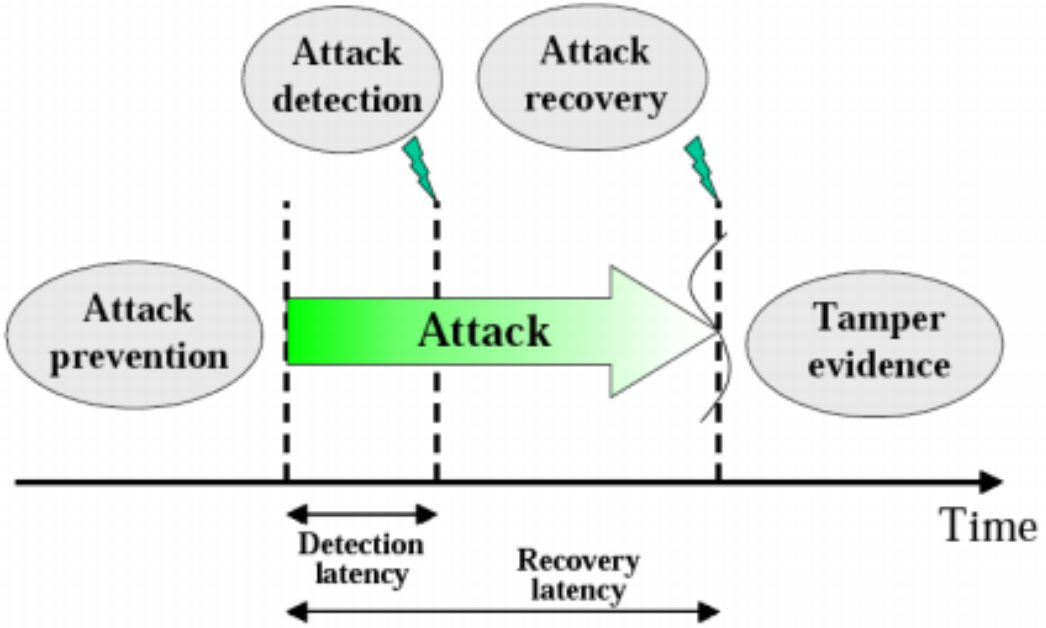
Chapitre III Sécurité des systèmes embarqués

IV.4. Contres mesures (Les contres attaques) :

Dans cette section, on va présenter les techniques qui ont été proposé pour renforcer les systèmes embarqués contre les diverses attaques décrites dans les sections précédentes.

IV.4.1. Classification des contres-attaques:

La [Figure ci-dessous], schématise la classification des contres attaques selon le moment d'intervention.



IV.4. Contres mesures (Les contres attaques) :

IV.4.1. Classification des contres-attaques:

IV.4.1.1. Techniques de prévention

Ces techniques rendre plus difficile de lancer une attaque sur le système embarqué. Ces techniques peuvent inclure : 1. Des mécanismes de protection physique. 2. Concevoir des matériels dont les caractéristiques ne dépend pas des données afin d'éviter les attaques à base d'analyse du temps et d'énergie. 3. Concevoir des logiciels avec des mécanismes d'authentification avant l'exécution.

IV.4.1.2. Détection des attaques

Dans le cas où une attaque est lancée et malgré toutes les techniques de prévention utilisées, les techniques de détection tentent de détecter l'attaque dès que possible. L'intervalle de temps écoulé entre le lancement d'une attaque et sa détection (la latence de détection) représente une période de vulnérabilité et doit être aussi courte que possible. Exemple : La détection d'accès mémoire à partir d'un logiciel malveillant.

IV.4. Contres mesures (Les contres attaques) :

IV.4.1. Classification des contres-attaques:

IV.4.1.3. Recouvrement d'attaque

Une fois l'attaque a été détecté, le système embarqué doit à son tour exécuter les actions appropriées. Le recouvrement des attaques présente les techniques utilisées afin de stopper l'attaque et mettre le système dans un état sûr et opérationnel.

IV.4.1.4. Sauvegarder l'historique

Dans certains cas, il est préférable de laisser l'attaque exécuter et enregistrer les actions effectuées pour des utilisations ultérieures.

IV.4. Contres mesures (Les contres attaques) :

IV.4.2. Technique de conception des contres attaques

Dans cette section, on va présenter les techniques de conception pour contrer chacune des techniques d'attaque présenté dans les sections précédentes.

IV.4.2.1. Protection contre les attaques logiques

Il existe plusieurs techniques qui assurent la sécurité d'un système embarqué contre les attaques logiques. Dans ce qui suite, on va présenter quelques techniques qui assurent la sécurité des systèmes embarqués contre les attaque logiques.

IV.4.2.1.1. Support matériel : Cette approche consiste à l'utilisation d'un module séparé (coprocesseur) qui est dédié au traitement de toutes informations sensible dans le système embarqué [5]. Toute information sensible qui doit être sortir du coprocesseur sera cryptée. Une autre approche matériel consiste à réserver une zone mémoire (volatil ou non, dans la puce ou hors la puce) comme un lieu de stockage sécurisé accessible seulement pour les composants du système confiée. Enfin, il existe d'autres mécanismes de protection de mémoire adoptée dans nombreux système embarqués qui utilisent des matériels de surveillances du bus qui peuvent distinguer entre les accès légal et illégal à ces endroits .

IV.4. Contres mesures (Les contres attaques) :

IV.4.2. Technique de conception des contres attaques

IV.4.2.1. Protection contre les attaques logiques

IV.4.2.1.2. Amélioration du système d'exploitation

L'amélioration des systèmes d'exploitation afin d'assurer la sécurité incluse des modifications dans :

1. La gestion des exceptions.
2. La communication entres processus.
3. Gestion de mémoire.
4. La commutation du contexte.

Car ces derniers présentent la source de la plus part des vulnérabilités. Cependant, il est important de noter que la plus part de ces améliorations nécessite des modifications au niveau architecturale (changement du système de gestion de mémoire).

Enfin, l'isolation des processus est aussi utilisée comme technique qui garantit que les ressources privées d'un processus peuvent être protégé contre un autre processus.

IV.4. Contres mesures (Les contres attaques) :
IV.4.2. Technique de conception des contres attaques
IV.4.2.1. Protection contre les attaques logiques
IV.4.2.1.3. Logiciels de validation et de vérification

Il est connu qu'un très grand nombre des attaques proviennent des vulnérabilités produites par des logiciels confiés. Par conséquent, les moteurs de vérification de logiciels sont de plus en plus importants afin de détecter les erreurs qui rendent le système vulnérable. L'utilisation de la vérification dynamique du code source est utile pour la recherche des erreurs pendant l'exécution. Enfin, des techniques de vérification formelle ont été également appliquées avec succès pour vérifier l'implémentation des protocoles de sécurités.

IV.4. Contres mesures (Les contres attaques) :

IV.4.2. Technique de conception des contres attaques

IV.4.2.2. Protection contre les attaques physiques

IV.4.2.2.1. Processeurs dédiés

Afin de protéger les systèmes embarqués contre les attaques physiques, des techniques de réponses immédiates et d'emballage ont été proposé. Un exemple d'un module cryptographique qui fournit des niveaux très élevés de la sécurité physique est "IBM4758 PCI cryptographic adapter". Dont le dispositif comprend un circuit qui détecte les attaques physique et répondre aux attaque de température et de voltage

IV.4.2.2.2. Chiffrement du bus

La protection contre les attaques sur le bus (bus probing) implique l'utilisation d'un processeur qui crypte toutes les informations envoyées sur le bus. Tel processeur assure que la mémoire et les bus de données et d'adresse ne contiennent que des valeurs cryptés qui sont ensuite décrypté. Alors que ces processeurs ont tendance à atteindre des niveaux de sécurité très élevés, ils restent toujours insuffisants contre les attaques par des canaux cachées. Ce qui nécessite des mécanismes de protection supplémentaire. .

IV.4. Contres mesures (Les contres attaques) :

IV.4.2. Technique de conception des contres attaques

IV.4.2.2. Protection contre les attaques physiques

IV.4.2.2.3. Protection contre les canaux cachés

La majorité des attaques sur les systèmes embarqués sont à base des canaux cachés (Analyse du temps, analyse d'énergie, rayonnement électromagnétique, etc.…). Diverses techniques de protection contre ces attaques ont été proposées afin d'éliminer les symptômes qui rendent un système embarqué vulnérable. L'une de ces techniques est la randomisation qui permet de donner des faut mesures à l'attaquant. L'utilisation d'un signal d'horloge aléatoire est proposée dans comme un moyen efficace d'introduire le non déterminisme dans les processeurs des cartes à puce. Ainsi, l'utilisation des données supplémentaire (donnée de masquage) et l'introduction des bruits permettent de perturber les mesures dans les attaques à base d'analyse d'énergie.

Chapitre III Sécurité des systèmes embarqués

IV.4. Contres mesures (Les contres attaques) :

En plus, afin de renforcer la sécurité des systèmes embarqués, ces derniers doivent être:

1- Symptôme Gratuit (Symptom Free) : ne fournir aucune information par fuite pour éviter les attaques passives.

2- Consciente de sécurité (Security Aware) : être toujours conscient de son état et notamment de sa vulnérabilité dans le but d'être réactif.

3- Conscient d'activité (Activity Aware) : Analyser son environnement pour détecter une activité irrégulière en embarquant des capteurs et des systèmes de surveillance.

4- Système agile (Agile System) : Etre flexible pour pouvoir rapidement répondre à une attaque ou alors anticiper l'attaque.

IV.4. Contres mesures (Les contres attaques) :

En plus, afin de renforcer la sécurité des systèmes embarqués, ces derniers doivent être:

5- Mise à jour du logiciel et de matériel (Software or Hardware update) : Remettre à jour facilement les mécanismes de sécurité en fonction de l'évolution des attaques.

6- Résistance contre les erreurs : Etre résistant aux sabotages et attaques physiques.

7- Efficacité (Efficient) : Rester performant : ressources limités des systèmes embarqués plus contraintes fortes (consommation de puissance et d'énergie, débit, latence, surface).