Introduction à la sécurité des systèmes embarqués

email : kadionik@enseirb.fr
web : http://www.enseirb.fr/~kadionik
http://www.enseirb.fr/cosynux/

Patrice KADIONIK
ENSEIRB - IMS

INTRODUCTION

Vulnérabilité des systèmes embarqués

- Les systèmes embarqués mettant en œuvre la connectivité IP sont aujourd ’hui potentiellement vulnérables à une attaque par le réseau.

- Les attaques concernent actuellement les routeurs, les imprimantes réseau... mais rien n ’empêche une attaque d ’une maison individuelle avec son réseau domotique ou d ’une voiture connectées à Internet !

- L ’aspect sécurité d ’un système embarqué doit être maintenant pris en compte lors de sa conception. Ce n ’est pas encore dans la mentalité des concepteurs de systèmes embarqués...

Vulnérabilité des systèmes embarqués

- La sécurité des systèmes embarqués concernent essentiellement les points suivants :
  - Le matériel.
  - Le logiciel embarqué.
  - Les communications avec le monde extérieur.

PARTIE 1 :
QUELQUES DEFINITIONS

Confidentialité

- La confidentialité est la propriété de “secret” attaché aux informations. Seules les entités autorisées à accéder aux ressources le sont.

- Elle est assurée par le contrôle d’accès aux informations et ressources du Système Embarqué (SE). De même, le système embarqué ne peut communiquer des informations qu’aux entités autorisées à recevoir cette information.

- Mise en œuvre de techniques pour assurer la confidentialité :
  - Contrôle d’accès au SE.
  - Contrôle d’accès aux ressources internes dans le SE.

Intégrité

- L'intégrité est la propriété qui assure qu'une information n'a pas été altérée.

- L'altération d'une donnée concerne :
  - Modification, suppression ou ajout sur les données sans en avoir le droit ou l'autorisation de réaliser ces opérations.
  - Modification, suppression ou ajout sur les programmes sans en avoir le droit ou l'autorisation de réaliser ces opérations.

Intégrité

- L'intégrité sur les données est assurée par le contrôle sur les actions d'écriture.
- On peut vérifier que des données ne sont pas altérées en effectuant des contrôles sur les valeurs :
  - Par redondance, par CRC, par signature...
- Ceci peut être fait par matériel ou par logiciel.

Intégrité

- Un programme ayant subit une altération peut avoir des conséquences très importantes :
  - Modifications sur des données des applications.
  - Modifications sur des données du système d'exploitation : table d'autorisations, programmes...
  - Ouverture de nouveaux services.

- L'altération initiale peut être volontaire mais peut aussi être le résultat d'une erreur de programmation !

Classification des attaques

- Les attaques se font par rapport aux propriétés non fonctionnelles :
  - Confidentialité : l'objectif est d'obtenir des informations.
  - Intégrité : l'objectif est de changer, supprimer ou ajouter des informations.
  - Disponibilité : l'objectif est de rendre le dispositif inutilisable par suite de très nombreuses requêtes.

Types d'attaques

- Les attaques physiques : *probing*, électromagnétisme...
- Les canaux cachés : observations précises du comportement en fonctionnement du dispositif. Les observations peuvent porter sur le temps, la consommation électrique...
- Les attaques par injection de fautes.
- Les attaques logicielles : virus, chevaux de Troie, *Deni Of Service*…

PARTIE 2 :
VULNERABILITES MATERIELLES

Attaques physiques

- Dé-packaging : accéder aux éléments à différents niveaux du composant.

- Reconstituer l'architecture du composant :
  - Mémoires.
  - Bus de données.
  - Bus d'adresses.
  - ...

- *Probing* : descente de sondes et action sur le composant.

Attaques physiques

- Les attaques physiques sont plus ou moins complexes. Elles nécessitent de l'outillage.

- Premières étapes à un autre type d'attaque. Ce sont des attaques destructives.

- Contre-mesures :
  - Packaging.
  - Silicium : architecture.
    - Silicium sur plusieurs niveaux.
    - Structures des mémoires aléatoires.
    - Bus chiffré.

Attaques par canaux cachés

- Analyse des consommations :
  - *Power Analysis Attacks* : SPA (*Simple Power Analysis*) et DPA (*Differential Power Analysis*).
- Attaques en temps.
- Attaques par injection de fautes.
- Attaques par champ électromagnétique.

Attaques en courant

- L'exécution d'un programme dans un composant requiert que celui-ci soit alimenté.

- La consommation de courant dans le composant est fonction des opérations réalisées.

- Contre-mesures :
  - Introduction de bruit dans la consommation et/ou le timing.
  - Diminuer les signaux, flot d'exécution constant, flot d'exécution choisi.
  - Cacher l'information sensible.

Attaques en temps

- Il s'agit d'observer finement le temps d'exécution des programmes.
- Les variations sont fonctions des données, mais aussi du matériel et de l'implémentation.
- Dans le cadre de l'exponentiation, les différents calculs peuvent conduire à disposer d'information sur la clé de chiffrement.

Attaques en électromagnétiques

- A l'origine utilisé pour l'étude des rayonnements des écrans CRT.
- Comme pour la SPA et la DPA on a les méthodes SEMA (*Simple Electromagnetic Analysis*) et DEMA (*Differential Electromagnetic Analysis*).
- Contre-mesures :
  - Cage de Faraday.

Attaques par injection de fautes

- Perturber le fonctionnement :
  - Modifier, forcer des valeurs via le *probing* dans les zones de données et/ou de programmes.
  - Modifier et/ou forcer des valeurs spécifiques du PC.
  - Modifier l'horloge, la tension...
- On peut utiliser un faisceau Laser, d'ions lourds.
- Contre-mesures :
  - Durcissement : technologies SOS/SOI.

PARTIE 3 :
VULNERABILITES LOGICIELLES ET COMMUNICATIONS

Attaques logicielles

- Les crackers exploitent :
  - Les erreurs de conception matérielle.
  - Les vulnérabilités logicielles :
    - *Backdoor* mise en place par le programmeur à des fins de tests et laissée dans la version finalisée.
    - Ignorance des standards usuels.
    - Mauvaise programmation : *buffer overflow*, *stack overflow*, test de validité des paramètres d ’entrée…
    - Serveur HTTP vulnérable car léger !

Attaques logicielles

- Exemples d ’attaques (sur routeur, imprimante réseau) :
  - Modification de l ’adresse IP en utilisant SNMP (communauté par défaut : write).
  - Datagramme UDP spécial pour fermer un port socket.
  - Authentification faible.
  - Mot de passe en clair accessible par SNMP.
  - Reset par SNMP.
  - L ’écriture par SNMP d ’une grande chaîne de caractères crashe l ’équipement.

Attaques logicielles

- Soyons optimiste : les exploits sur systèmes embarqués sont rares par rapport à ceux concernant les systèmes classiques (PC, routeur…).
- Il y a peu de documentation accessible à disposition (en ligne) pour le cracker sur le fonctionnement interne (matériel et logiciel) d ’un système embarqué.
- Les attaques classiques par *shell code* sur *buffer overflow* sont inexistantes par il n ’y a pas de shell (sauf avec linux :-( ).
- Le pire des cas est un crash du système embarqué ou son reboot (ce qui est préférable)...

CONCLUSION

Conclusion

- Comme les systèmes embarqués sont massivement communicants, il est important de prendre en compte l'aspect sécurité dès leur conception :
  - Sécurité matérielle.
  - Sécurité logicielle. Les failles d'un système d'exploitation embarqué entraînent une vulnérabilité du système embarqué.
  - Sécurité des communications.

- La prise en compte de la sécurité n'est pas un réflexe pour les concepteurs de systèmes embarqués.

Références

Références :

- Cours de P. Paradinas. CNAM
  http://deptinfo.cnam.fr/~paradinas/
- http://uuu.enseirb.fr/~kadionik/embedded/securite/securite.html