M2 SECRETS

Politique de sécurité et aspects juridiques

Examen 2020

Aucun document n'est autorisé.

Exercice 1 : Attaques Actives et Passives

1. Citer deux moyens physiques pour injecter une faute dans un composant et les expliquer brièvement.
2. Citer deux applications de la rétro-conception matérielle de composants.
3. Donner deux types d'observations physiques mesurables susceptibles de contenir des informations sur les secrets manipulés par un appareil au cours de l'exécution d'un algorithme cryptographique.
4. On note $p(x,y)$ le coefficient de corrélation linéaire de Pearson entre les vecteurs x et y. Soient $u = (1,2,3,4,5)$, $v = (1.9,4.1,6.1,7.9,10.1)$ et $w = (1,4,9,16,25)$. Qu'est-ce qui est le plus grand entre $p(u,v)$ ou $p(u,w)$? Pourquoi ?
5. On considère un registre de 8 bits préchargé à la valeur 0. On note e l'éenergie dégagée lors de la transition d'un bit de l'état 0 à l'état 1. Donner une estimation en fonction de e de la valeur physique observée sous l'hypothèse d'une fuite en poids de Hamming, lorsque le registre prend la valeur 255.

Exercice 2 : Attaques Passives sur la Vérification d'un code PIN

1. Ecrire un pseudo-code implantant la vérification d'un code PIN composé de 4 digits et évaluer sa complexité en temps.
2. Vérifier la résistance de votre implantation vis-à-vis d'une attaque utilisant le temps mis par le matériel pour faire la vérification. Eventuellement, corriger votre implantation pour qu'elle résiste à ce type d'attaque.
3. Vérifier la résistance de votre pseudo-code contre des attaques consistant à injecter des fautes durant les calculs pour retrouver la valeur du code PIN.
4. Proposer des contre-mesures qui permettraient à votre pseudo-code de résister aux attaques par fautes exhibées précédemment.

Exercice 3 : CEM & SSI, entre compromis et agression

1. Indiquer les différentes menaces "non logicielles" pesant sur les systèmes informatiques isolés d'Internet.
2. Quelles menaces particulières font peser les interfaces radio intégrées à un système ? brouillage,
3. Sur quels paramètres peut jouer un attaquant pour capter les signaux RF émis par un système ?

4. Quels durcissements peut-on apporter à un système afin de limiter les risques inhérents à l'utilisation des liens radios ?
5. En quoi les radios logicielles impactent-elles la sécurité des systèmes informatiques ?
6. Citer quelques exemples de sites directement impactés par les menaces d'origines électromagnétiques.

Exercice 4 : Démarche de Sécurisation

"Garder à l'esprit le besoin de sécuriser un système avec des solutions **pérennes**, **pragmatiques** et, si possible, **à moindre coût**."

Mise en situation sur un cas pratique : Une entreprise située en centre-ville occupe la totalité d'un immeuble de 5 étages dont 2 en sous-sol. L'immeuble est mitoyen de locaux privatifs sur ses deux côtés. L'arrière de l'immeuble est ouvert sur un jardin arboré. Les informations sensibles sont réparties dans plusieurs bureaux et dans différentes étages.

Trois systèmes d'information distincts sont utilisés :

— Réseau Internet de confort disponible en Wifi ;
— Réseau de bureautique Intranet dont la disponibilité est stratégique pour le fonctionnement de l'entreprise. Ce réseau est doté d'un chiffreur d'artère permettant l'accès au réseau informatique de la maison mère ;
— Réseau de développement très sensible car manipulant le savoir-faire de l'entreprise.

Deux profils d'attaquants identifiés :

— Recherche d'un accès gratuit à Internet ;
— Concurrents cherchant à découvrir les secrets de fabrication et à perturber le fonctionnement de l'entreprise.

Question : Proposer une démarche globale de sécurisation du site décrit ci-avant et justifier celle-ci (entre 20 et 30 lignes). En particulier, votre argumentaire devra aborder les points suivants : quelle est l'échelle du système ? Le périmètre de sécurité est-il défini ? Modifiable ? Quels sont les chemins de fuites ? Et pour chaque chemin de fuite, quelles sont les protections les mieux adaptées pour se protéger contre les menaces d'origines électromagnétiques ?

Pour vous aider vous trouverez ci-dessous quelques termes relatifs au domaine : mise à la terre, canalisation de chauffage, secteur, signaux de servitudes, cage de Faraday, regroupement de bureaux, durcissement de l'infrastructure, ferraillage, durcissement des cloisons, détection, regroupement d'équipements, déplacement d'équipements, isolation galvanique, durcissement des équi- pements, réaction modification des paramètres de fonctionnement, fonctionnement sur batterie, baie CEM, mesures organisationnelles, signaux faibles, équipotentialité, filtre, canalisation d'eau, faradisation légère, déplacement de bureaux