THALES

THALES UNDERWATER SYSTEMS

LA PROTECTION CEM DES SITES MILITAIRES

B. GRANGIER Le 28 mars 2007 Conférences Hyper 2007

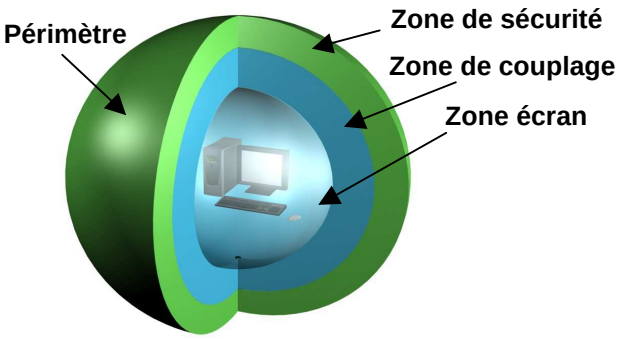
Cette présentation est relative à la protection des systèmes d'information contre la menace provoquée par la propagation des signaux parasites par conduction et rayonnement. L'objet principal est de présenter les règles de sécurité applicables à l'installation des matériels de traitement des informations de manière à limiter la propagation des signaux parasites générés.

Le sujet abordé est donc basé autour de la compromission électromagnétique qui se définie comme étant la révélation des informations confidentielles à des personnes qui n'ont pas à connaître ces informations. Quelques exemples montrent comment capturer illicitement l'information par l'intermédiaire des signaux parasites compromettants (SPC) en exploitant la corrélation entre les signaux parasites et l'information.

Cette protection contre les SPC passe par des études de CEM globale (de la conception jusqu'à la fabrication et l'installation d'un équipement) afin de réduire les niveaux de parasites. Cette réduction des parasites s'obtient par :

- Un choix judicieux des composants,
- Un blindage qui empêche les signaux créés de sortir d'une enceinte,
- Le filtrage qui permet de désadapter les connexions aux autres appareils reliés au même réseau d'alimentation,
- L'étude des câbles de liaisons,
- La mise à la terre,
- L'utilisation de cage de Faraday.

Les règles d'anticompromission ou TEMPEST (qui concerne la compromission de type électromagnétique) nécessitent des mesures drastiques sur les systèmes ainsi que des mesures d'atténuation apportée par les bâtiments de manière à corréler zonage d'un bâtiment avec niveau d'émission parasite d'un système suivant les normes TEMPEST. Le Zonage TEMPEST consistant à définir à l'intérieur d'un bâtiment plusieurs zones présentant, pour un signal rayonné, une atténuation dont la valeur se situe dans une plage donnée. L'objectif du durcissement TEMPEST (équipement / système) étant de supprimer le risque TEMPEST (exploitation des SPC).



L'organisme Français qui s'occupe de la politique SSI (Sécurité des Systèmes d'Information), de la sécurité, de l'approbation des plans de test des industriels, du test (AMSG-720B, AMSG-788A et AMSG-784B) ainsi que de l'agrément des matériels et du zonage des sites (495/SGDN et AMSG-799A) est le service DCSSI qui dépend des services du Premier Ministre.

En conclusion il est très facile d'espionner avec des moyens simples la majorité des réseaux informatiques. L'utilisation de composants blindés, la réalisation d'équipotentialité répondant aux exigences des hautes fréquences ainsi que l'emploi de moniteurs à faible rayonnement électromagnétique permettent de réduire le risque d'être écouté.

Pour plus de renseignements veuillez trouver ci-après mes coordonnées :

Bernard GRANGIER
Thales Underwater Systems
525 Route des Dolines
BP157
06903 Sophia Antipolis Cedex

Tel: +33 (0)4 92 96 48 45
Fax: +33 (0)4 92 96 33 60
Email: Bernard-bg.grangier@fr.thalesgroup.com