Cible de sécurité CSPN

TRANGO Hypervisor

TRANGO Virtual Processors

Sommaire

Tableau de révision

Révision	Date	Auteur	Commentaires
0.1	26/05/2008	Trango VP	Révision initiale
1.0	02/06/2008	Trango VP	Prise en compte des remarques de la DCSSI
1.1	17/06/2008	TrangoVP	Mise à jour de la version évaluée Précision de vocabulaire sur FS6

1 Identification du produit

Organisation éditrice	TRANGO Virtual Processors
Lien vers l'organisation	www.trango-vp.com
Nom commercial du produit	TRANGO Hypervisor
Numéro de la version évaluée	Release 1.5.61
Catégorie de produit	Matériel et logiciel embarqué

2 Glossaire

Terme	Définition
VM ou VM/OS	Virtual Machine / Machine Virtuelle : environnement d'exécution isolé dans lequel s'exécute une application autonome ou un système d'exploitation.
VM hostile	VM dont le code malicieux a pour objectif l'accès à des données sensibles à l'extérieur de son environnement d'exécution, ou de perturber le fonctionnement du système.
VM sensible	VM dont le code et/ou les données sont sensibles. Une VM sensible doit être conçue dans le respect du guide utilisateur, de manière à ne pas divulguer volontairement ces informations.
VPU	Instance de processeur virtuel (Virtual Processor Unit) : vue du processeur « physique » offerte par l'hyperviseur à chaque VM.

3 Argumentaire (description) du produit

3.1 Description générale du produit

TRANGO Hypervisor permet l'exécution sécurisée et simultanée de plusieurs environnements d'exécution sur des plates-formes mono ou multi-coeurs.

Chaque environnement d'exécution est composé d'un processeur virtuel (VPU), avec son propre espace d'adressage où sont affectées mémoire et périphériques. Ces environnements d'exécution isolés les uns des autres sont aussi appelés « machines virtuelles » (VMs).

Une VM peut faire fonctionner tout programme qui s'exécute normalement sur un processeur réel: applications autonomes, systèmes d'exploitation temps réel, ou systèmes d'exploitation « évolués » (Linux par exemple).

Le partitionnement des ressources matérielles par TRANGO Hypervisor assure l'isolation de chaque VM.

La conception de TRANGO Hypervisor prend en compte les problématiques de sécurité et de performance:

- l'isolement des VMs est une caractéristique intrinsèque et non une option. Cette conception garantit un haut niveau de sécurité.
- la taille réduite de son code est un atout pour la sécurité : la faible empreinte mémoire

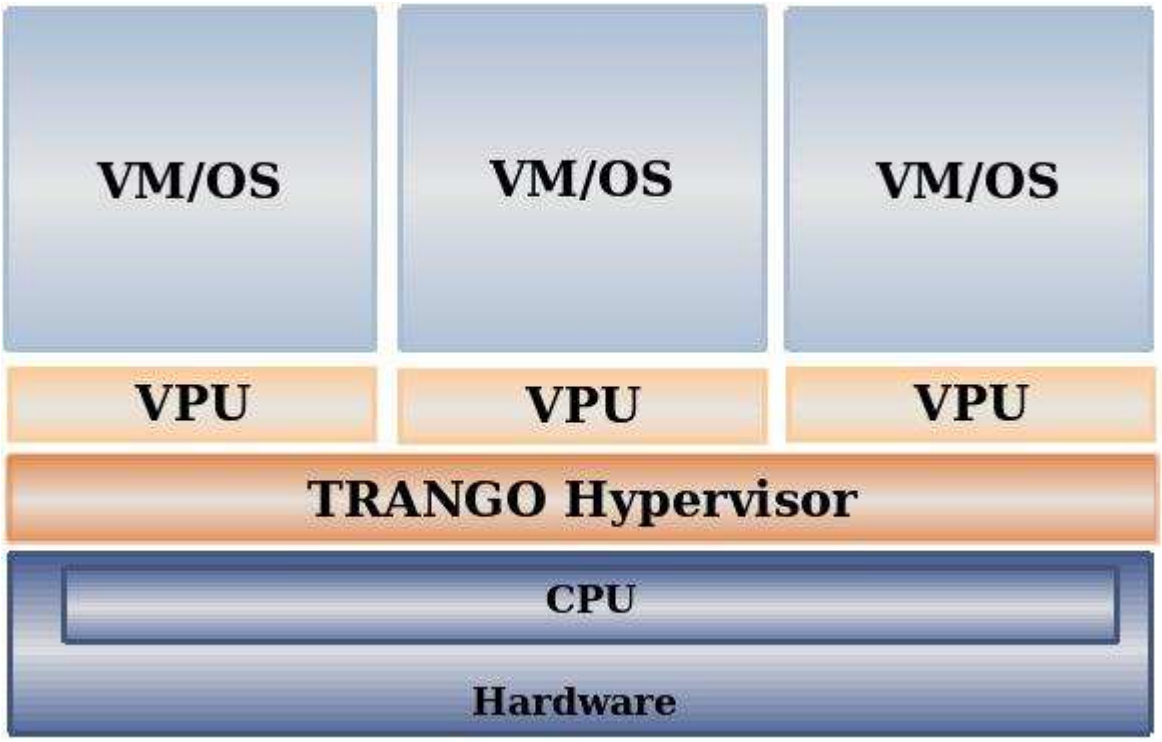
(approximativement 20 Ko) permet l'exécution des VMs critiques en mémoire interne du processeur pour contrer des attaques effectuées contre le matériel.

- Sa conception satisfait les besoins du « temps réel » par une optimisation de l'hyperviseur et un fonctionnement déterministe.

TRANGO Hypervisor fournit les services suivants aux VMs :

- partage sécurisé des ressources (mémoire, CPU, périphériques)
- canaux de communication sécurisés inter-VMs
- gestion dynamique des VMs: création, destruction, gestion des ressources CPU, débuggage

TRANGO Hypervisor est capable de gérer jusqu'à plusieurs centaines de VMs, suivant la plate-forme matérielle.



Exemple de système multi-VPU

3.2 Description de la manière d'utiliser le produit

Le produit est démarré au lancement du système embarqué hôte et reste actif en permanence.

3.3 Description de l'environnement prévu pour son utilisation

L'utilisation de TRANGO Hypervisor, dans le cadre d'un produit de type téléphone mobile, peut être décomposée en deux étapes:

1. intégration

   Cette phase se déroule dans un environnement non hostile, par du personnel qualifié et formé appelé « intégrateur », dans des locaux non publiques.

La phase d'intégration consiste à rassembler tous les composants logiciels du système pour obtenir un exécutable. Ces composants sont l'hyperviseur (binaire), les VMs (binaire), et le fichier de paramètres de configuration (texte) qui doit être généré par l'intégrateur, afin de définir les droits (ressources mémoires, accès au périphériques,…) de chaque VM. Cette étape est réalisée à l'aide d'outils développés et fournis par TRANGO VP (tgo_tools et tgo_mkimage).

2.utilisation

Cette phase se déroule dans un environnement potentiellement hostile, sans qu'il soit fait d'hypothèses sur la compétence et/ou l'hostilité des utilisateurs.

3.4 Description des hypothèses sur l'environnement

L'intégrateur système est considéré comme non hostile et est formé pour exécuter les opérations dont il a la responsabilité en suivant les recommandations du guide d'utilisation de l'hyperviseur.

L'intégrateur dispose des moyens de contrôler les paramètres de configuration afin de les intégrer de façon sûre.

On présume que l'intégrité de l'hyperviseur est assurée durant la phase de démarrage du système, par exemple au travers d'un chargeur d'amorçage sécurisé (secure boot loader).

Les VMs sensibles et non hostiles sont implémentées par un développeur lui-même non hostile et formé pour exécuter les opérations dont il a la responsabilité en suivant les recommandations du guide d'utilisation de l'hyperviseur.

3.5 Description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système qui ne sont pas fournis avec le produit.

TRANGO Hypervisor est conçu pour fonctionner sur un processeur qui possède au moins les caractéristiques suivantes:

- plusieurs niveaux de privilèges
- une unité de gestion de mémoire (MMU)

3.6 Description des utilisateurs typiques concernés (utilisateurs finaux, administrateurs, experts…) et de leur rôle particulier dans l'utilisation du produit.

Le contexte d'emploi organisationnel et relatif au personnel pour le produit est le suivant :

- l'intégrateur système qui est responsable de la configuration correcte et sûre du système. Il est également en charge d'intégrer l'hyperviseur, les VMs et le fichier de configuration associé.
- les développeurs de VMs qui possèdent le contrôle du développement de leur propre VM fournie à l'intégrateur système.
- l'utilisateur final de la solution intégrée, par exemple d'un téléphone mobile.

3.7 Définition du périmètre de l'évaluation, à savoir les caractéristiques de sécurité du produit concernées par l'évaluation.

Le périmètre de l'évaluation couvre l'hyperviseur, TRANGO Hypervisor, à l'exception des fonctions suivantes qui seront désactivées par l'intégrateur dans le fichier de configuration du système, durant la phase d'intégration (voir Description de l'environnement prévu pour son utilisation pour plus de détails sur la phase d'intégration):

- supervision (modification des paramètres d’exécution autorisés) ;
- monitoring et micro-monitoring (lecture d’informations du système) ;
- débuggage (déroutement du flot d'instruction) ;
- gestion de l'énergie (arrêt de certaines fonctionnalités et/ou VMs).

Le périmètre de l'évaluation couvre uniquement les attaques logicielles réalisées au travers de l'interface de l'hyperviseur.

4 Description de l’environnement technique dans lequel le produit doit fonctionner

4.1 Matériel compatible ou dédié

Le produit TRANGO Hypervisor est un logiciel embarqué, qui nécessite un système matériel pour pouvoir s'exécuter. Ce système devra être considéré comme un support, et est donc en dehors du périmètre de l'évaluation. Ce système est un téléphone mobile destiné au grand public, basé sur un processeur de type ARMv6.

Cet appareil mobile est achitecturé autour d'un processeur embarqué OMAP2430 (TI). Divers composants fonctionnels gravitent autour de ce processeur:

- Un contrôleur mémoire (DRAM et FLASH), connecté via un bus mémoire
- Un affichage de type LCD, connecté via un bus RGB et un bus SPI
- Un gestionnaire Radio-Baseband, connecté via un bus SPI
- Un gestionnaire d'alimentation et clavier, connecté via un bus I2C

Les interfaces externes sont:

- une liaison série de type UART, normalement utilisée uniquement pour la mise au point
- une liaison USB (servant aussi de support à une liaison ethernet)
- un canal radio

4.2 Système d’exploitation compatible : type, version, correctifs…

Le produit TRANGO Hypervisor ne nécessite pas de système d'exploitation pour fonctionner.

5 Description des biens sensibles que le produit doit protéger

Le produit protège les biens suivants :

- B1 : Les paramètres de configuration (intégrité) qui gèrent les droits des différentes VMs
- B2 : Le contrôleur d’interruptions (intégrité) qui gère notamment l’allocation du temps CPU entre les différentes VMs
- B3 : Les ressources matérielles (disponibilité et intégrité) affectées aux différentes VMs
- B4 : Les données sensibles et le code des VMs (confidentialité et intégrité)
- B5 : Les données et le code de l’hyperviseur (intégrité et disponibilité)

6 Description des menaces

Les différents agents menaçants sont :

1.les développeurs hostiles implémentant des VMs malveillantes en vue de recueillir de l'information sensible, de perturber ou d'influer sur le comportement des autres VMs

2.les utilisateurs hostiles tentant de recueillir de l'information sensible ou d'influer sur le comportement des VMs

L'intégrateur système n'est pas considéré comme un attaquant potentiel, par hypothèse.

Description des menaces :

●M1 : Une VM (on omettra le terme « hostile » quand il n'y a pas risque de confusion) rompt le cloisonnement inter-VMs. Pour ce faire, elle accède aux ressources (mémoire, ressource matérielle) d'une autre VM, lit ou modifie les registres d'exécution de celle-ci ou ouvre un canal de communication non sécurisé inter-VMs.

●M2 : Une VM provoque un déni de service sur les ressources matérielles des autres VMs ou sur l'accès à l'hyperviseur tout entier en s'exécutant en mode privilégié ou en modifiant le comportement du contrôleur d'interruptions de manière à rester prioritaire.

●M3 : Une VM ou un utilisateur hostile modifie le code de l'hyperviseur pour en prendre le contrôle. Cette attaque est réalisée par une exécution du code hostile en mode privilégié ou une modification directe du code hyperviseur visible par la VM.

●M4 : Une VM modifie les mécanismes d'isolation mémoire (MMU) afin de modifier les données de configuration, le contrôleur d'interruption, les données sensibles des autres VMs ou de l'hyperviseur. Cette attaque peut être réalisée par une exécution en mode privilégié ou une modification directe des données utilisées par les mécanismes d'isolation mémoire.

●M5 : Une VM attaque une autre VM à partir des données résiduelles. Pour ce faire :

- la VM hostile récupère les ressources réallouées après destruction de l'autre VM (lecture de données sensibles rémanentes en mémoire);
- ou après libération de ressource mémoire par une VM hostile avec des écritures latentes, puis réallocation et utilisation de ces ressources par une autre VM et enfin écriture retardée (écriture d'informations rémanentes en cache).

●M6 : Une VM modifie les paramètres de configuration en vue d'accéder à une ressource qui lui est interdite ou de provoquer un déni de service en s'octroyant un temps d'allocation CPU important.

7 Description des fonctions de sécurité du produit

TRANGO Hypervisor a pour fonctionnalité principale de fournir les services d'un hyperviseur tout en assurant la sécurité d'exécution des VMs.

Les fonctions de sécurité du produit sont les suivantes :

- FS1 : Cloisonnement inter VMs
  - Chaque VM possède son propre espace d'adressage. L'hyperviseur assure le cloisonnement de chaque espace d'adressage en utilisant la MMU (qui ne peut être gérée que par l'hyperviseur en mode privilégié).
  - L'hyperviseur contrôle également tous les canaux de communication autorisés entre les VMs.

- FS2 : Contrôle du mode privilégié
  - Toutes les VMs ne peuvent s'exécuter qu'en mode utilisateur du CPU, le mode privilégié du CPU ne leur est pas accessible. Seul l'hyperviseur peut exécuter des instructions en mode noyau faisant respecter en cela la politique de sécurité de « séparation des privilèges ».

- FS3 : Sécurité du contrôleur des interruptions
  - L'hyperviseur assure l'exclusion du contrôleur d'interruptions de la liste des périphériques accessibles (en écriture notamment) par les VMs

- FS4 : Sécurité du code et des données de l'hyperviseur
  - L'hyperviseur assure l'exclusion du code et des données de l'hyperviseur de l'espace mémoire accessible par les VMs.

- FS5 : Sécurité de la MMU
  - Ce service assure que les modifications des données utilisées pour les mécanismes d'isolation mémoire sont uniquement faites par l'hyperviseur.

- FS6 : Destruction des informations rémanentes (non réutilisation d'objets)
  - Ce service assure qu'à chaque changement de contexte de VM, l'intégralité du contenu des registres CPU est changée (les registres CPU sont tous réinitialisés avec les valeurs du contexte de la VM à exécuter).
  - La destruction d'une VM s'accompagne de l'effacement systématique de la mémoire avant sa réallocation.
  - Les caches sont systématiquement nettoyés lors de la libération des ressources mémoire

- FS7 : Sécurité du fichier de configuration
  - L'hyperviseur assure l'interdiction de l'écriture des données de configuration par les VMs.