System management mode

Sommaire

- Les différents modes du processeur
- SMM : en détails
- Et on peut en faire quoi ?
- Comment mettre son code en SMRAM ?

Les différents modes du processeur

Real mode

- Utilisé lors du boot et du shutdown.
- Instructions 16bits
- Ram : 1MB
- Présent sur architecture 32 et 64 bits.

Legacy mode

- Gère les niveaux de privilèges mémoire (les rings)
- Instructions 32 bits
- Ram : 4GB max
- Gère le multitâche.
- Présent sur architecture 32 et 64 bits.

Virtual mode

- Est un attribut du legacy mode.
- Instructions : 16bits.
- Gère les niveaux de privilèges.
- Implémente le même environnement que le processeur 8086 d'Intel.

Compatibility mode

- Présent uniquement sur architecture 64bits (X86_64)
- Permet d'éxécuter des programmes 32 bit sans les recompiler.
- Reprend les caractéristiques du legacy mode.

64 bit mode

- Instructions : 64 bits
- Ram : 2^64 - 1 max.
- Reprend les autres caractéristique du legacy mode.

System management mode

- Introduit en 1993 par Intel (copié en 1994 par AMD)
- Instructions: 16bits.
- RAM: 4GB max accessible.
- Gère les opérations sur 32 bits
- Créé pour gérer l'alimentation, la sécurité ou autres.

SMM en détails

Accéder au SMM

- L'interruption SMI (system management interupt) fait rentrer en SMM.
- L'instruction RSM sort du SMM et remet le processeur dans son mode précédent.

SMRAM

- Le SMM a son environement d'éxécution dans une zone de la ram inaccessible depuis un autre mode: la SMRAM.
- Size: 131071(0x1FFFF) octets.

Sauvegarde du contexte

- Lors de l'entrée en SMM le contexte actuel de l'exécution (tout les registres) sont sauvegardé dans la SMRAM
- Lors de l'éxécution de l'instruction RSM le contexte précédement stocké est réstauré et l'éxécution reprend sont cours.

I/O opérations

- Le SMM peut exécuter tout les opérations I/O du Legacy mode.

Exemples d'utilisations

- Emuler de l'hardware.
- Gestion de l'alimentation (laptop).
- Sécurité (detection de malware …).

Et on peut en faire quoi ?

Entrer en SMM

- Il est possible de provoquer une interruption SMI (par exemple esseyant d'accéder à une adresse mémoire particulière).

Modifier le contexte

- Le contexte étant sauvegardé en SMRAM et le SMM ayant tout les droits d'écriture/lecture on peut modifier le contenu des registres sauvegarder (qui seras restauré en sortant de lue SMM).
- Par exemple on peut changer la valeur de RIP.

Modifier des données

- En suivant le même principe que précédement on peut modifier des données aussi bien en ram (même les adresse kernel) que des fichiers

Comment mettre son code en SMRAM ?

Les protections du SMM

- Le bit D_OPEN définie si la SMRAM est accessible en écriture ou pas.
- Le bit D_LCK empêche de modifier le bit D_OPEN.

Le rôle du bios

- Normalement le code dans la SMRAM est écrit par le bios (voir par l'OS pendant le boot).
- Le bit D_LCK doit être activé juste après avoir écrit en SMRAM
- Certains BIOS n'active le bit D_LCK, on peut donc écrire dans la SMRAM puis la vérouiller.

Contourner le BIOS

- Si le bios active bien le bit D_LCK on peut essayer de le contourner.
- Par exemple en flashant une version modifié du BIOS.

Source

- Phrack
- Doc Intel
- Rapport Duflot

Questions ?