Metasm

un framework pour code machine

Yoann Guillot

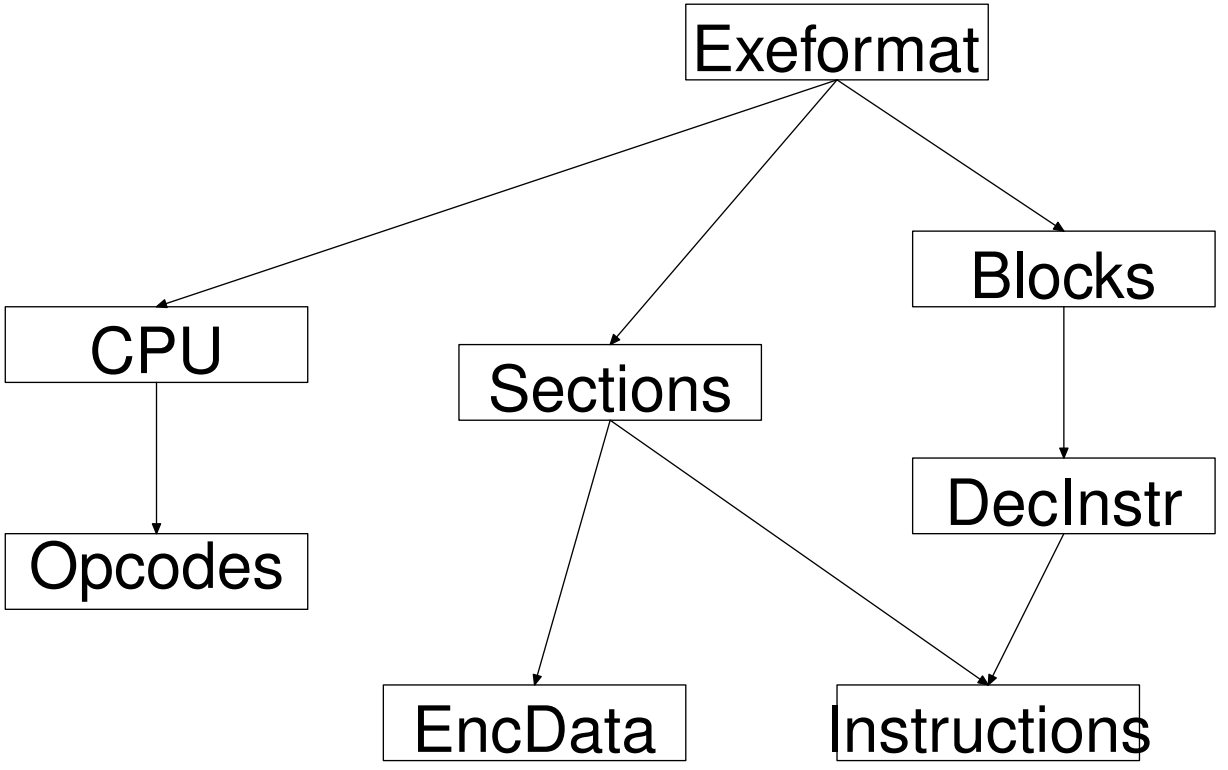
Sommaire

- Présentation du framework
  - Aperçu de l'architecture
  - Fonctionnalités
- Ce qui devient possible
- Exemples

Présentation du framework

- Metasm est un framework de manipulation de code machine
  - Code exécutable multi-architecture (actuellement Ia32 et MIPS)
  - Formats de fichier exécutables Windows et GNU/Linux
  - Interaction avec un système en cours d'exécution
- Ecrit intégralement en Ruby
- Licence LGPL

Architecture interne



Assemblage de code machine

- Fournit une chaine relogeable : `EncodedData`
  - Code machine
  - Relocations
  - Exports
  - Espace virtuel
- Sépare l'assemblage du linkage
- Démonstration

Désassemblage de code machine

- Puissant moteur de backtracking
  - Suit précisément le flot d'exécution
  - Mais manque actuellement de support d'appels externes
  - Permettra de tracer les accès data
- La partie spécifique à une architecture est minimale
- Démonstration

Gestion de fichiers exécutables

- Lecture
  - Depuis un fichier
  - Depuis la mémoire
- Écriture
  - Modification
  - Génération from scratch
- Support de MZ/PE/COFF et ELF

Interaction avec le système d'exploitation

- Abstraction de la mémoire d'un processus cible
  - Lecture/écriture transparente
- Fournit une API générique
- Démonstration

Ce qui devient possible

- Modification arbitraire du processus d'assemblage/désasseblage
- Facilite énormément toute interaction avec du code machine

Intégration à Metasploit3

- Metasploit 3 est écrit en ruby
- Mais le support du code machine est très mauvais
  - Shellcodes en hexa
  - Bidouilles pour “patcher” ces shellcodes au runtime
  - Re-bidouille pour lier différents stages
- Avec Metasm :
  - 1 - Shellcodes sous forme de code source
  - 2 - Linkage standard pour les relocations
  - 3 - Linkage standard pour les stages
  - 4 - ????
  - 5 - Profit

Exemples

- Metasm-shell

Exemples

- Lecture d'un ELF MIPS

Exemples

- Compilation d'un exécutable PE

Exemples

- Modification d'un exécutable PE

Exemples

- Hook basique Windows

Exemples

- Hooks avancés Windows

Conclusion

- Merci de votre attention !
- Des questions ?

Download

- Le framework est téléchargeable sur http://metasm.cr0.org/
- Il est en plein développement :
  - des features ne fonctionnent pas de manière satisfaisante
  - l'API risque de changer radicalement
  - use at your own risk!
- je suis joignable sur irc.ofjj.net, chan #metasm
- Happy hacking !