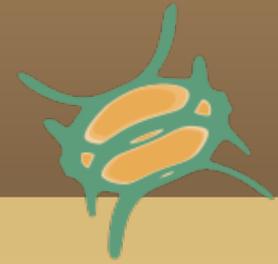


netifera

Une Plate-Forme Distribuée d'Évaluation
de la Sécurité des Systèmes d'Information



Qui sommes-nous?

Philippe Mathieu-Daudé

pmd@netifera.com

Claudio Castiglia

claudio@netifera.com

<http://netifera.com>

Agenda

- 
- Outils de Sécurité Réseau
 - Quelques Limitations des Outils Actuels
 - La Plate-Forme Netifera
 - Les Applications basées sur Netifera
 - Démonstration
 - L' Architecture de Netifera
 - Le Peludo
 - Questions



Outils de Sécurité Réseau

- Qu'est-ce qu'un Outil de Sécurité Réseau?
 - Inventaire et cartographie du réseau
 - Scan de ports et découverte des services
 - Scan de vulnérabilité
 - Exploit de vulnérabilité
 - Écoute de paquets et contrôle du trafic
 - Récupération de mots de passe
 - Détection d'intrusion et de logiciel malveillant
 - Test d'application web



Quelques Limitations

- Peu d'Intégration et d'Interopérabilité
 - Besoin de scripts sur mesure (par exemple pour convertir les données d'un outil à un autre)
 - Répétition de tâches ennuyeuses
 - Difficile de se concentrer sur le problème principal
- Manque de bonne documentation, de guides de référence
- Parfois confus, difficile à comprendre ou fastidieux



La Plate-Forme Netifera

- Est une Plate-Forme Distribuée
 - Extensible, Évolutive
 - Les tâches peuvent être distribuées et parallélisées
- Intègre toute l'Information
 - Le modèle du réseau se construit au fur et à mesure que l'information est recueillie
- Les données collectées sont disponible pour tous les Outils



La Plate-Forme Netifera

- Portable
 - S'exécute sur n'importe quel Système sans avoir à changer le code source
 - Indépendant du Système d'Exploitation et de l'Architecture
- Fournit les fonctions basiques nécessaires aux Outils
 - Accès au système de fichiers, processus, mémoire, réseau, écoute/fabrique/injection de paquets, analyse de protocoles, ...

La Console Netifera

The screenshot displays the Netifera application interface, which is a network scanner and web crawler. The interface is divided into several panes:

- Browser:** Shows the URL `http://www.ossir.org/windows/`.
- Network Tree:** Displays a hierarchical view of the scanned network. The root is `195.83.224.0/24`, which contains:
 - `web.ossir.org (195.83.224.2)`
 - `www.ossir.org (195.83.224.3)`
 - `TCP [22,25,80]`
 - `22/tcp SSH [OpenSSH 3.9p1]`
 - `25/tcp SMTP [Sendmail 8.13.1]`
 - `80/tcp HTTP [Apache 2.0.52]`
 - `http://www.ossir.org/`
 - `/`
 - `/association/adh.pdf`
 - `/association/adh.ps`
 - `/association/index.shtml`
 - `/association/jo.html`
 - `/association/sponsoring`
 - `/association/statuts.htm`
 - `/base/mail.css`
 - `/bretagne/`
 - `/bretagne/calendrier/index.shtml`
 - `/bretagne/calendrier/index2007.shtml`
 - `/bretagne/cr/20081007.shtml`
 - `/bretagne/cr/20081218.shtml`
 - `/bretagne/cr/20090217.shtml`
 - `/bretagne/cr/20090423.shtml`

- Tasks Console:** Shows the status of various tasks:
- `Crawl http://www.ossir.org/ at 195.83.224.3:80/tcp` (Running)
- `Reverse lookup 195.83.224.0/24` (Running)
- `TCP connect scan 195.83.224.3` (Completed (6 seconds))
- Map:** A satellite map showing the location of `www.ossir.org (195.83.224.3)` in Evry, France. A tooltip for the selected `80/tcp HTTP [Apache 2.0.52]` entry shows the response:

```
HTTP/1.1 200 OK
Date: Thu, 07 May 2009 23:49:32 GMT
Server: Apache/2.0.52 (Fedora)
Accept-Ranges: bytes
```

The status bar at the bottom indicates "Local Probe" and "76M of 127M".

La Sonde Netifera



La Sonde Netifera

- Contient toute la Plate-Forme Netifera... sans l'Interface Graphique
- Un Nœud de la Plate-Forme Distribuée
- Possède son propre Modèle des Données
- Autonome, Indépendant (pas besoin d'être connecté à la Console)



La Sonde Netifera

- L'information collectée est envoyé a la Console
 - Le Modèle de la Console intègre l'information provenant des Sondes
 - L'utilisateur est capable d'Analyser et d'Explorer les Données de toutes les Sondes
 - Permet de voir le Réseau sous différents Points de Vue



La Sonde Netifera

- Les outils et autres composants peuvent être installés, mis à jour, désinstallés, à chaud, à la demande, au travers du réseau
- Installation Facile
 - Envoie d'un seul fichier exécutable (choix de l'administrateur système)
 - Injection dans un processus sous forme de *shellcode* (choix du *pentester*)
 - Pas de dépendances externes





Exemples

- Évaluation de la Sécurité des Systèmes d'Information
- Administration Réseau
 - Gestion homogène d'un grand nombre de Systèmes hétérogènes
- Surveillance Réseau
 - Détection d'Attaques Distantes
 - Surveillance du bon Fonctionnement des Serveurs et de leurs Services
 - Cartographie de Réseaux
- Recherche Réseau

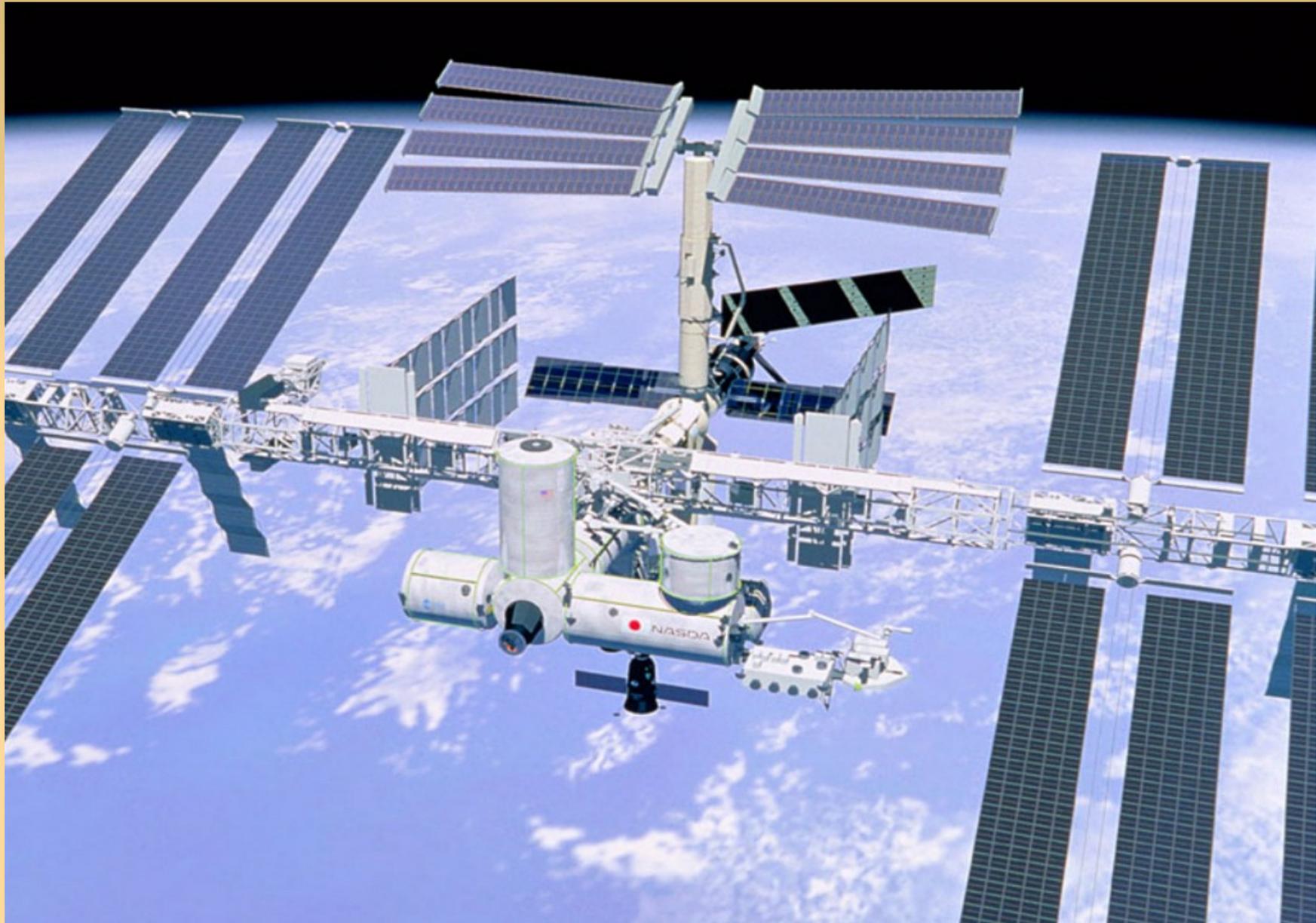


DEMO

Video

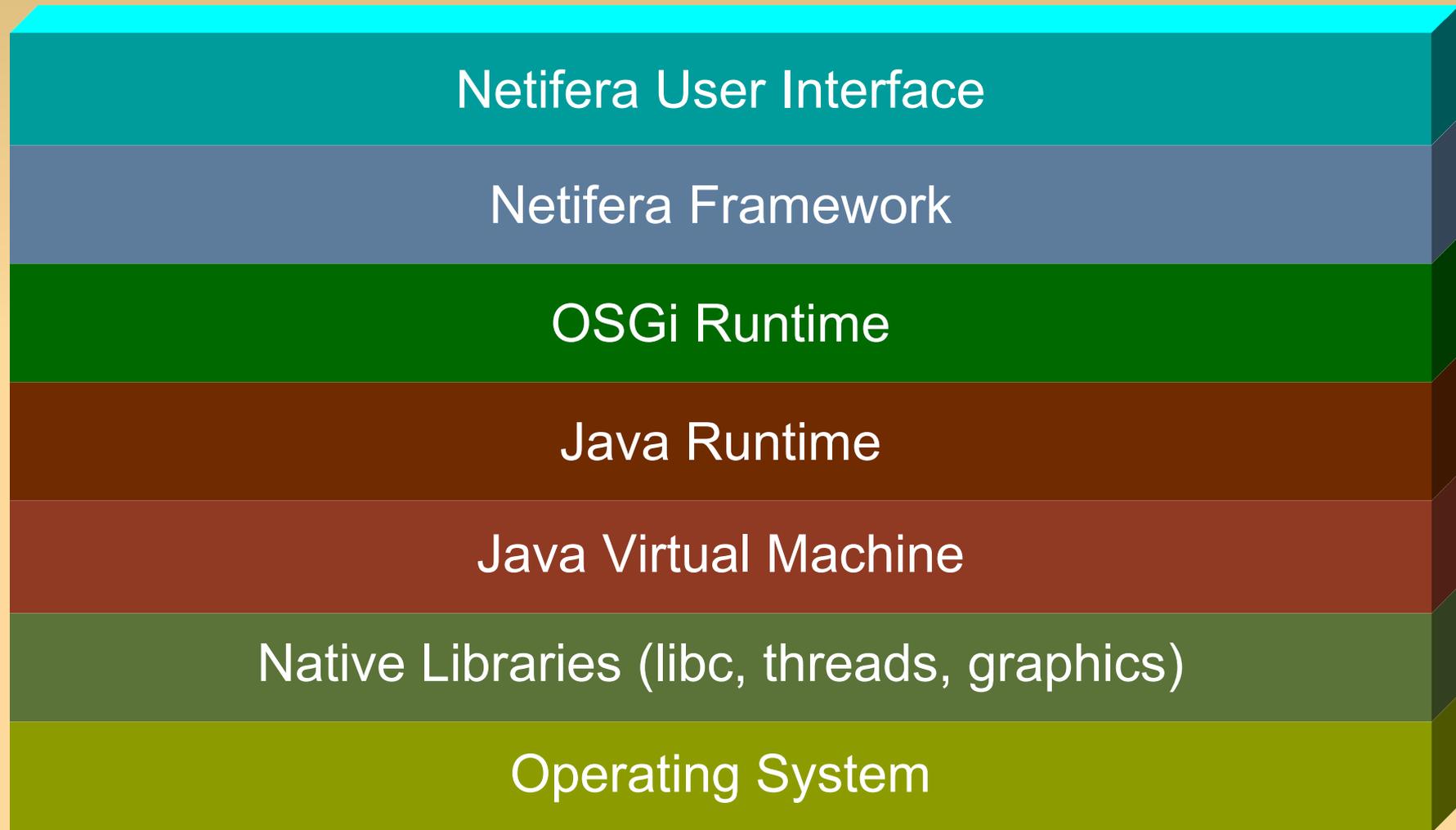
La Machine Virtuelle Java Comme Shellcode

Intérieur de la Plate-Forme

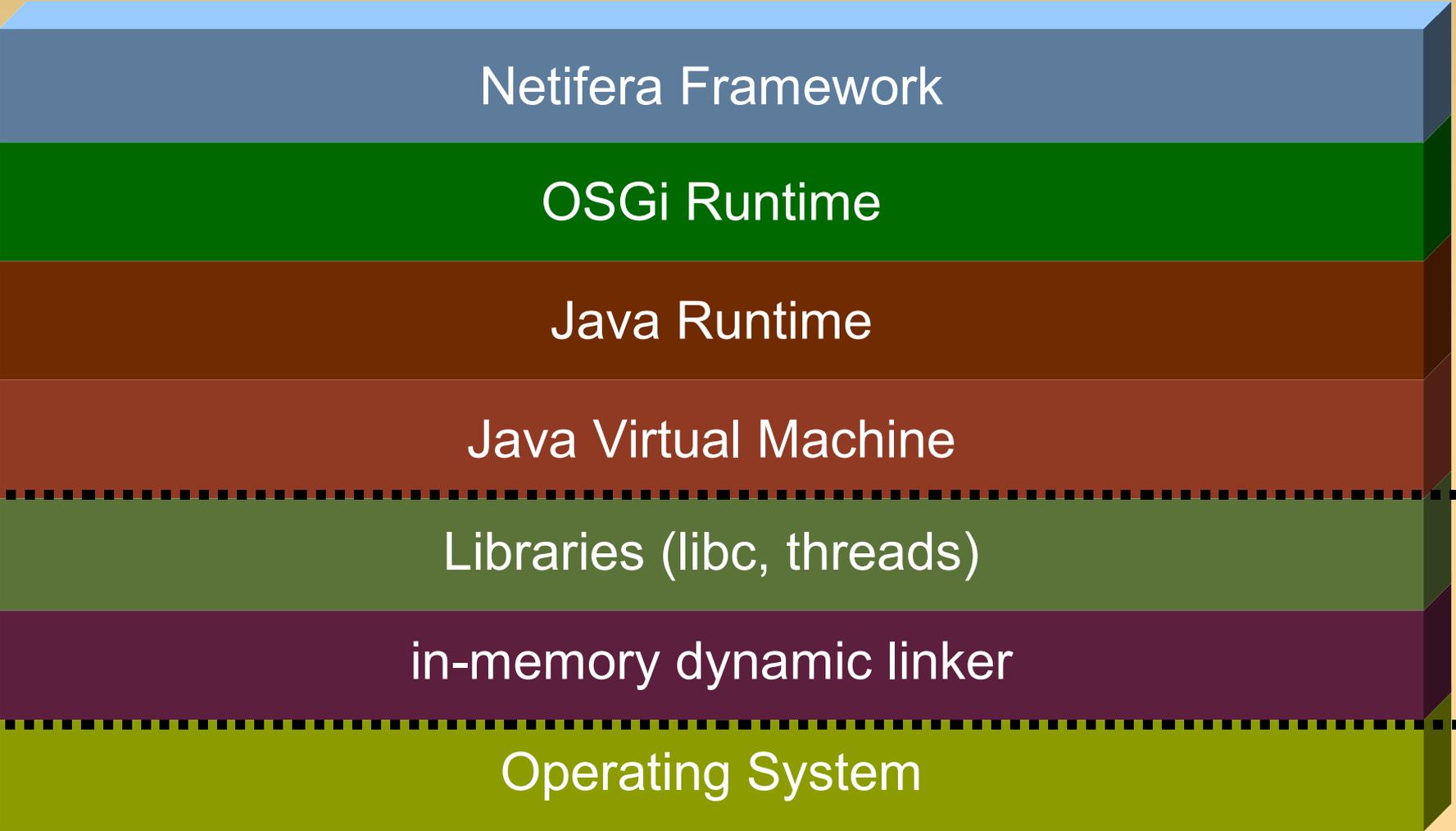




L'Architecture de la Console



L'Architecture de la Sonde



Netifera Framework

OSGi Runtime

Java Runtime

Java Virtual Machine

Libraries (libc, threads)

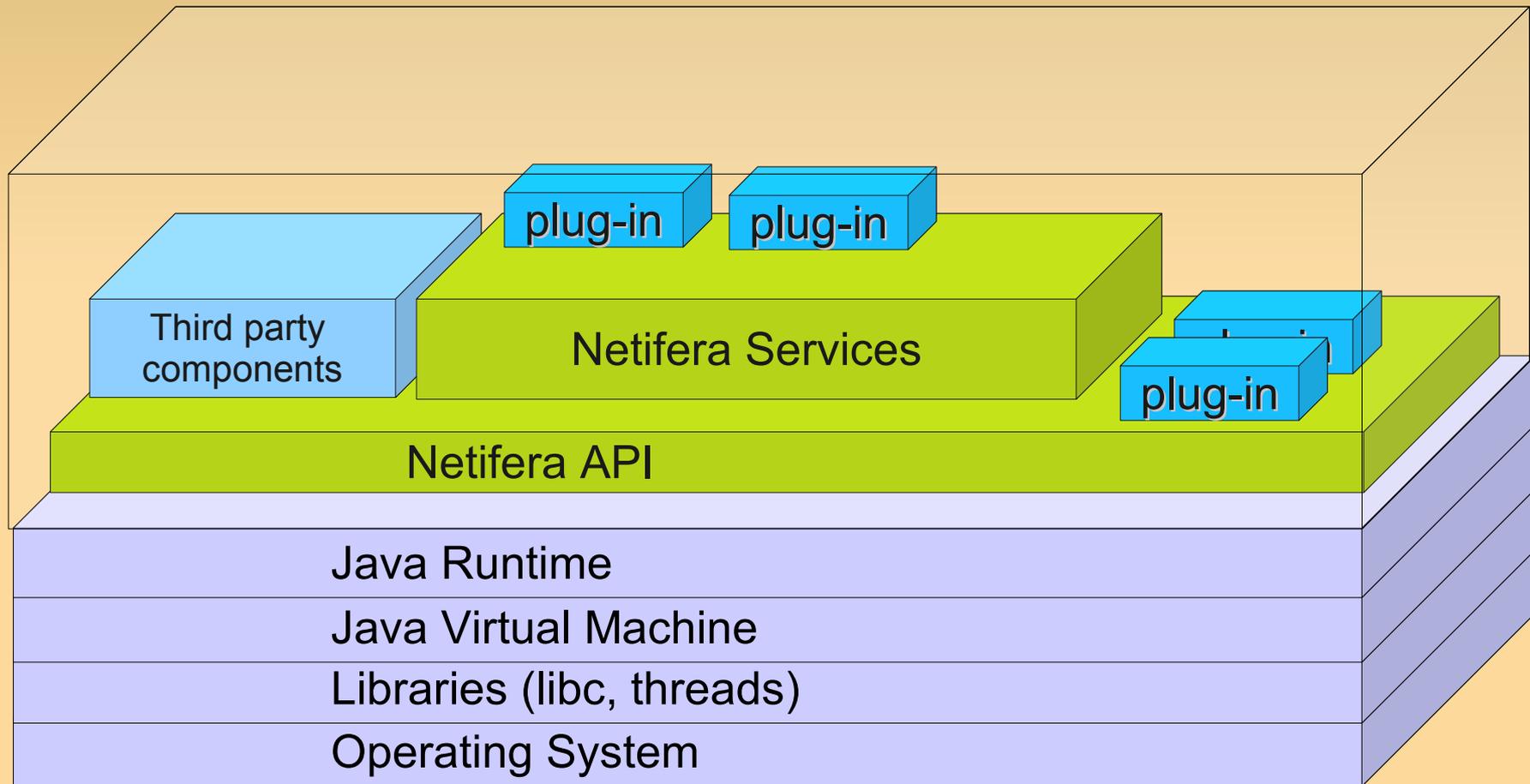
in-memory dynamic linker

Operating System

Peludo

Vue Détaillée de l'Architecture

OSGi Framework



Peludo





L'Objectif

- Une chaîne d'outils pour générer des Applications écrites en langage C
 - Portable
 - Pas de dépendances externes
 - Injectable
 - Petit



PLD File Format

- C'est un simple format de fichier *TLV*
- Composé de Sections
 - Traditionnels *.code*, *.data*, *.export*, *.import*, *.reloc*
 - *.nimport* (Importations Natives)
 - Supporte la Compression des Données



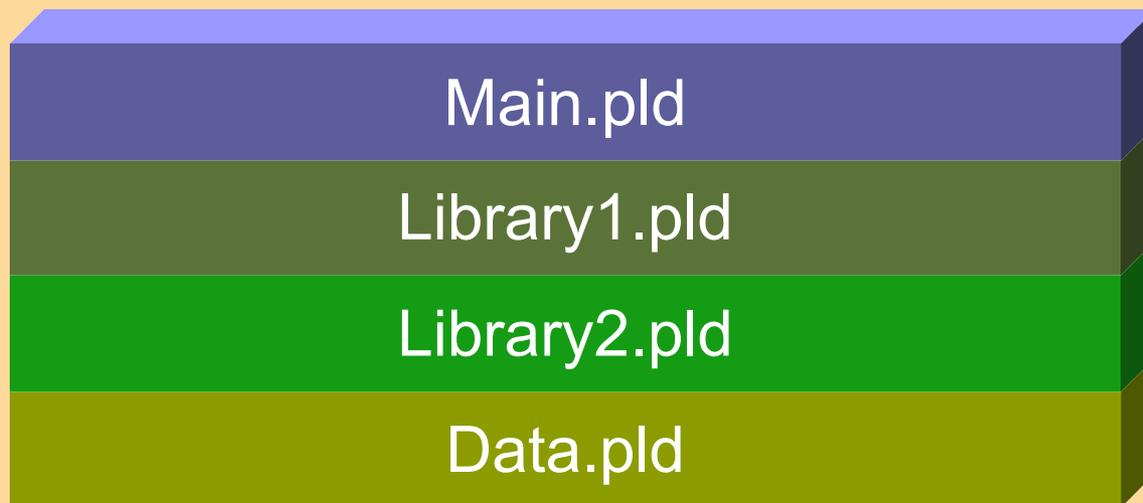
Qu'est ce qu'une Application?

- Les Applications sont composées de:
 - L'Exécutable principal
 - Les Dépendances (les librairies)
 - D'éventuels Fichiers de Données
- Avec Peludo, les Applications sont normalisées au format PLD
 - Entièrement composées de fichiers PLD
 - Les fichiers de données sont embarqués dans de pures PLDs de *.data*

La Normalisation PLD



Application

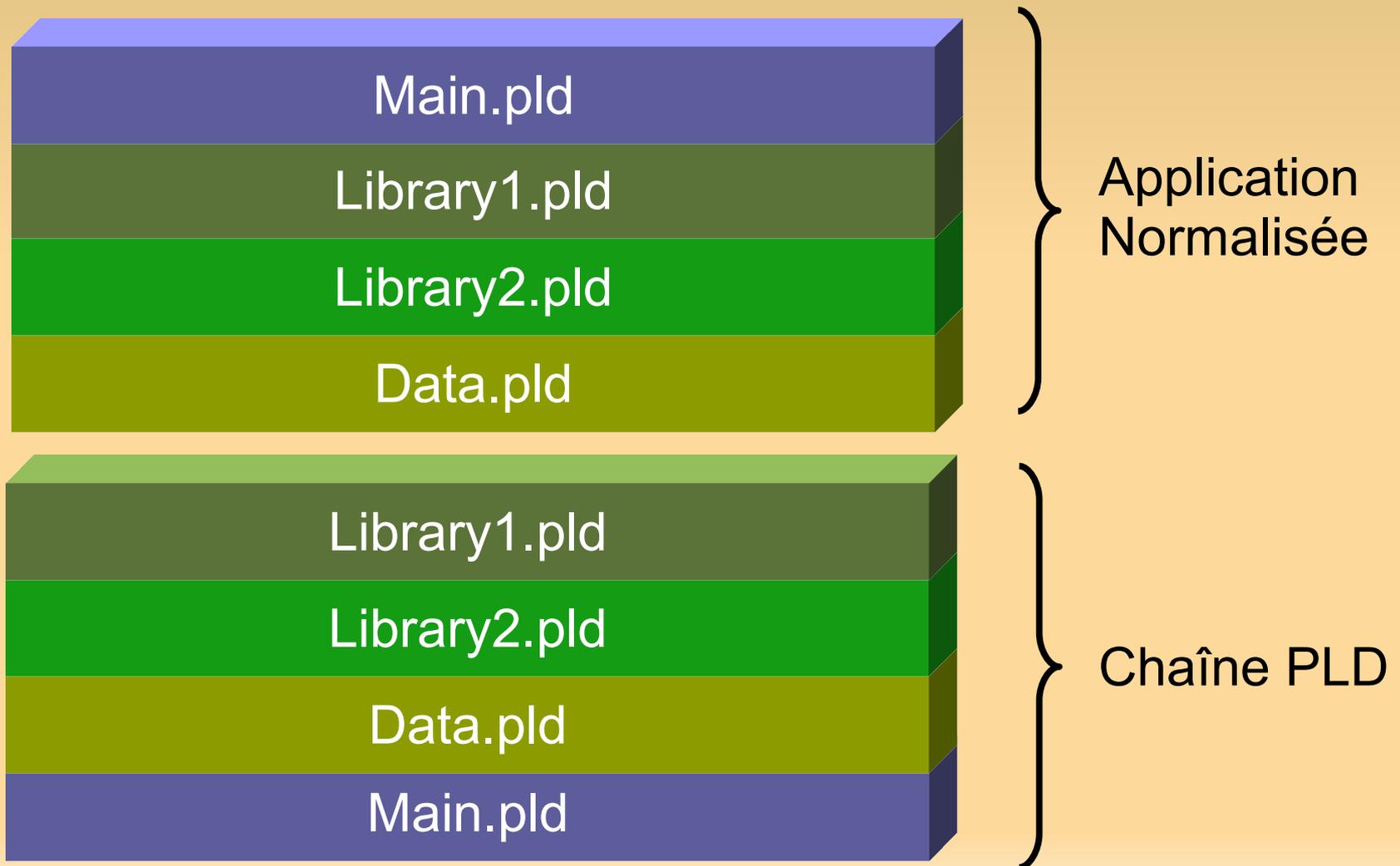


Application Normalisée



La chaîne PLD

- Une chaîne PLD est une succession de fichiers PLD ordonnés suivant leur dépendances





Les Fichiers PLB

- Peludo fournit deux composants:
 - Le code d'amorce (*bootstrap*)
 - Le noyau Peludo (surtout composé du *loader* PLD)
 - Le *loader* PLD est un éditeur de liens (*linker*) qui opère en mémoire et ne touche jamais au système de fichiers
- Un fichier PLB est créé quand une chaîne de PLD est rajoutée à ces deux composants

Les Fichiers PLB

- Peludo fournit deux composants:
 - Le code d'amorce (*bootstrap*)
 - Le noyau Peludo (surtout composé du *loader* PLD)
 - Le *loader* PLD est un éditeur de liens (*linker*) qui opère en mémoire et ne touche jamais au système de fichiers
- Un fichier PLB est créé quand une chaîne de PLD est rajoutée à ces deux composants



- Pour lancer une Application il suffit de sauter dans le premier octet du PLB



Injection

- Pour injecter dans un processus
 - Le processus devrait être exploité (ou créé spécialement) pour recevoir un fichier PLB comme un *shellcode*
 - Le PLB est reçu et lu en mémoire
 - Pour exécuter le PLB, il suffit de sauter au premier octet



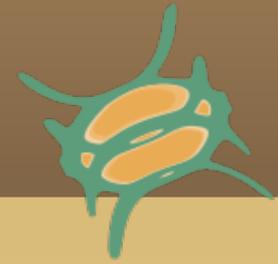
Le PLB de la Sonde Netifera





Merci!

Des Questions?



Pour nous contacter

<http://netifera.com>

info@netifera.com