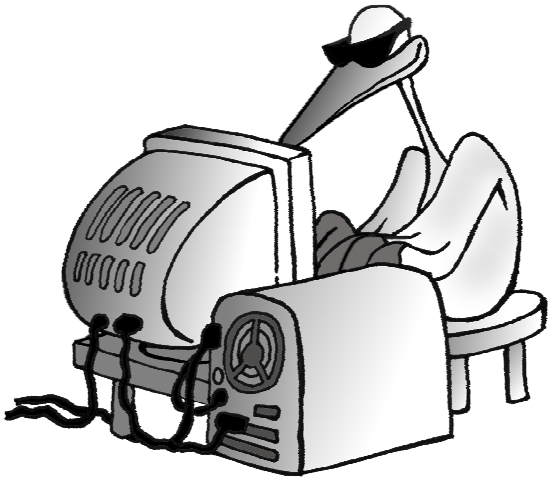
OSSIR – Groupe Sécurité Windows
Sécurité de Windows Mobile

Roderick ASSELINEAU (MAPS/NSS)

Hacker, oui mais pourquoi ?



➔ Des motivations diverses

- Le jeu (hacker)
- Le profit (utilisateur malintentionné)
- L'espionnage
  - Mafia
  - Espionnage industriel
  - Organisations gouvernementales ?

➔ Des dangers bien réels !

- Installation de backdoors et attaques par rebond
- Pertes de données
- Vol de l'utilisateur

La répartition des OS mobiles en 2005

➔ Quelques chiffres …

Worldwide total smart mobile device market
Market shares by operating system Q1 2005, Q1 2004

OS vendor	Q1 2005 shipments	% share	Q1 2004 shipments	% share	Growth Q1'05/Q1'04
Total	10,782,380	100.0%	5,930,010	100.0%	82%
Symbian	6,618,370	61.4%	2,402,790	40.5%	175%
Microsoft	1,976,970	18.3%	1,368,400	23.1%	44%
PalmSource	1,131,310	10.5%	1,303,730	22.0%	-13%
RIM	758,300	7.0%	379,990	6.4%	100%
Others	297,430	2.8%	475,100	8.0%	-37%

Source: Canalys estimates © 2005 canalys.com ltd.
Smart mobile device market: handhelds, wireless handhelds, smart phones

➔ Symbian et Windows Mobile sont majoritaires

Pourquoi choisir d'étudier WinCE ?

- **Windows CE est le concurrent direct de SymbianOS**
- **Les sources sont disponibles**
  - Compréhension facilitée
  - Audit possible
- **L'API est très documentée**
- **Windows a un lourd passé en terme de sécurité**
  - Possibilité de découvrir de nouvelles attaques
  - Possibilité de portage de techniques pour Windows 2k/XP

Terminaux testés

- **Pocket PC M{1,2}000 et SmartPhone E{1,2}00**
  - Windows Mobile 2002 / 2003
    - Basé sur Windows CE
  - GSM/GPRS
  - IrDA
  - Bluetooth
  - Wi-Fi

Les mécanismes de sécurité

- **Le niveau de privilège d'un processus**
  - Est déterminé par un mécanisme de signature
    - Clef publique de l'intégrateur hardcodée en ROM
  - Ne peut être changé
- **Les différents niveaux d'exécution**
  - *OEM_CERTIFY_TRUST* (tous les droits)
    - Le code est signé par l'intégrateur
  - *OEM_CERTIFY_RUN* (droits limités)
    - Le code n'est pas signé
    - Ne peut utiliser les *Trusted API*
  - *OEM_CERTIFY_FALSE* (aucun droits)
    - Le programme ne peut être chargé
- **Le mécanisme parfait ?**

Mais (1/2) …

➔ Quand le code est non signé

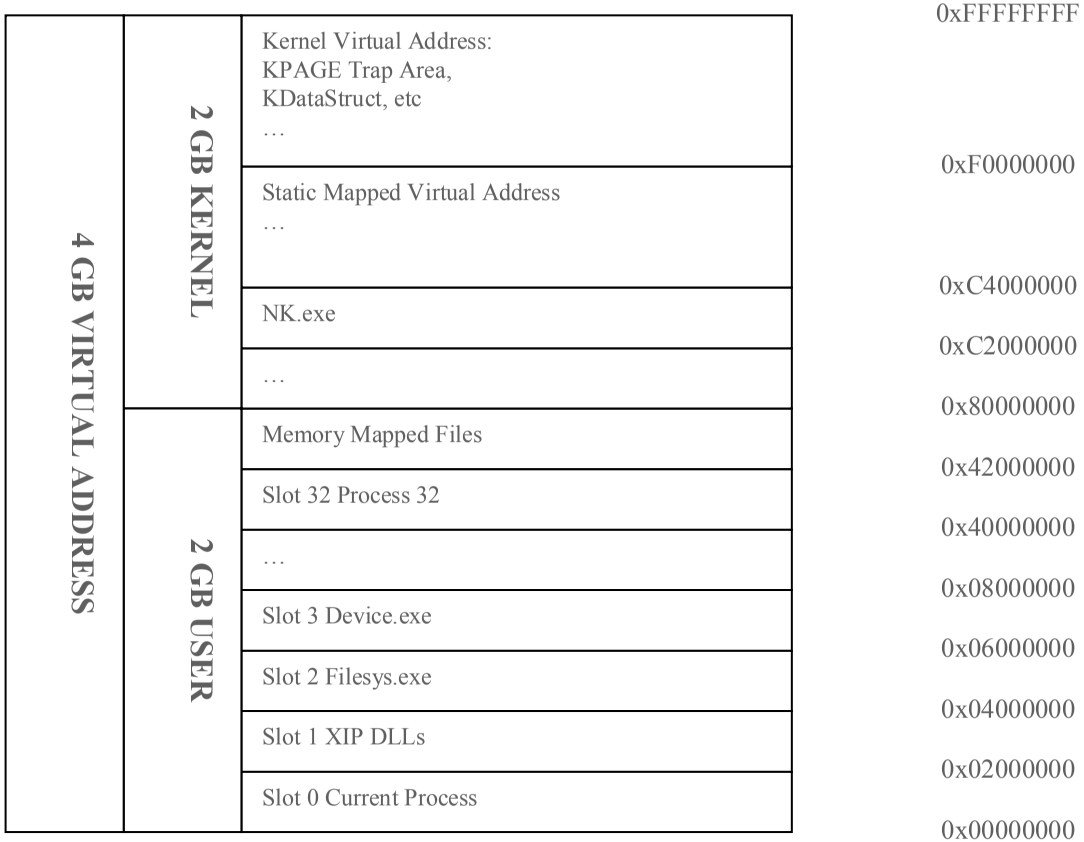
- Le choix de l'exécution est laissé à l'utilisateur
- Il reste cependant dangereux …
  - Accès SIM
  - Appels téléphoniques et émission de SMS
  - Connexions Bluetooth / GPRS

Mais (2/2) …

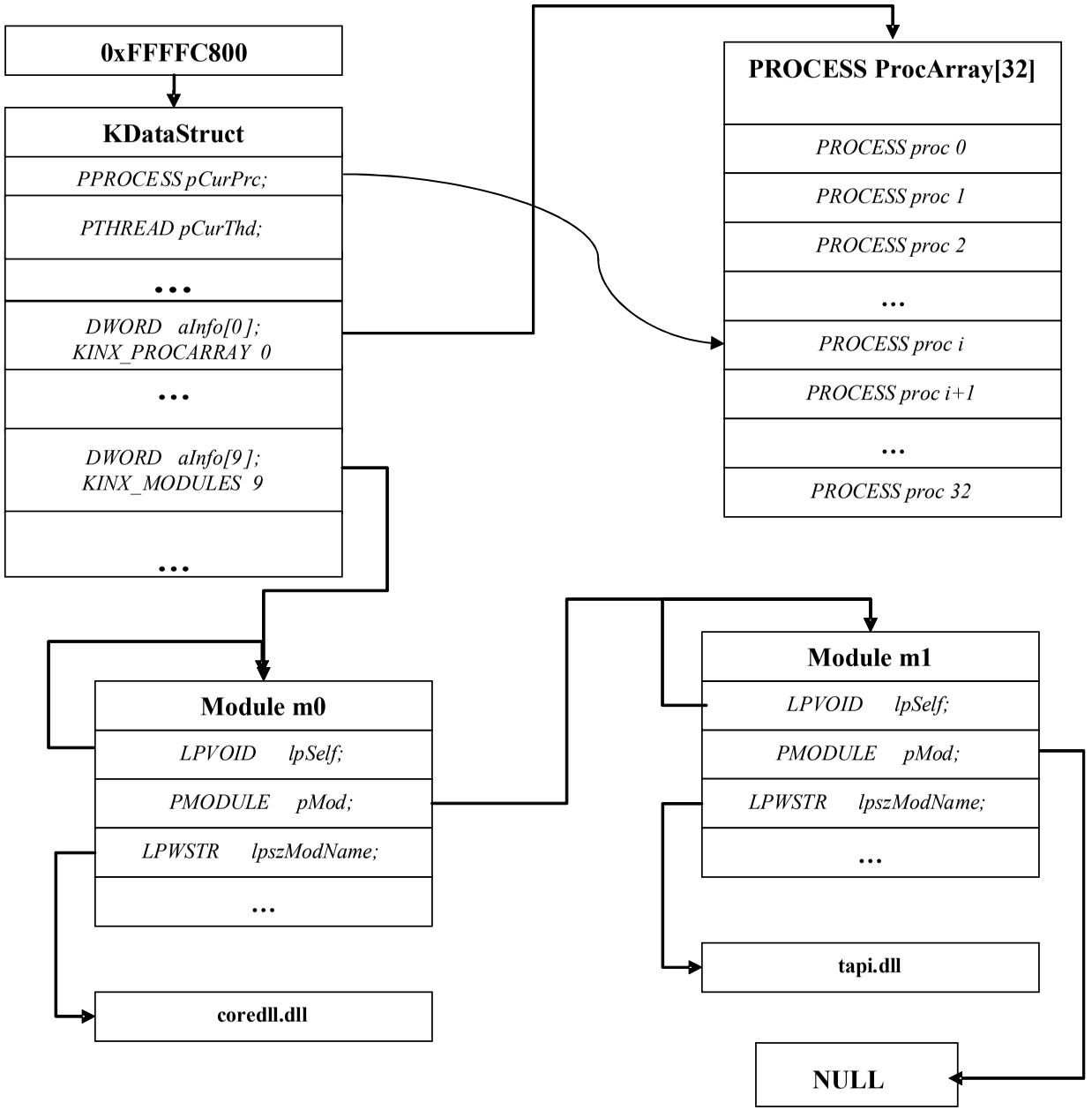
- **Tout intégrateur peut compiler sa propre version de Windows CE**
  - Le choix de l'activation de la signature est fait à la compilation
    - Mécanisme contraignant pour l'utilisateur
- **L'état du parc**
  - Les signatures sont actives sur la gamme des Smartphones
  - Les signatures sont inactives sur la gamme des Pocket PC
- **Possibilité de contournement du mécanisme**
  - Programme Security off

Mode de fonctionnement de la VM

➔ Le principe des slots

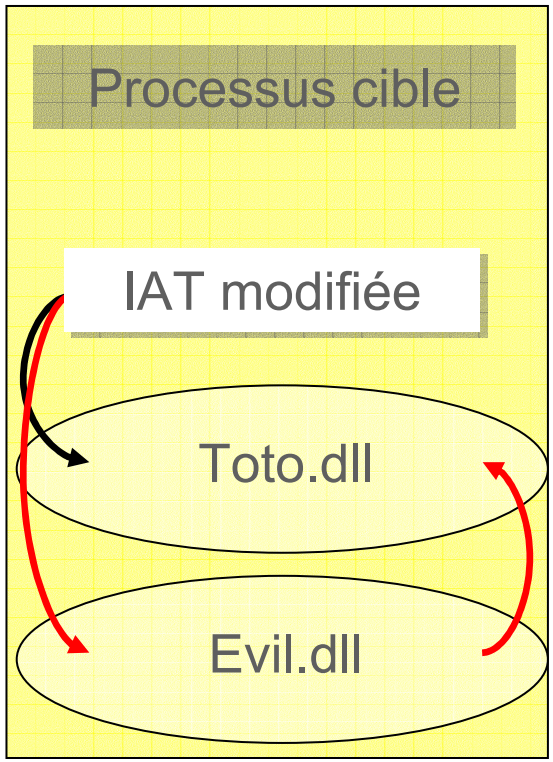


KDataStruct



Comment attaquer le user space ?

➔ Infection de processus



Mémoire en partage

LoadLibrary()

Corruption de l'IAT

Processus offensif

DebugActiveProcess()

SetThreadContext()

➔ Définition de hooks

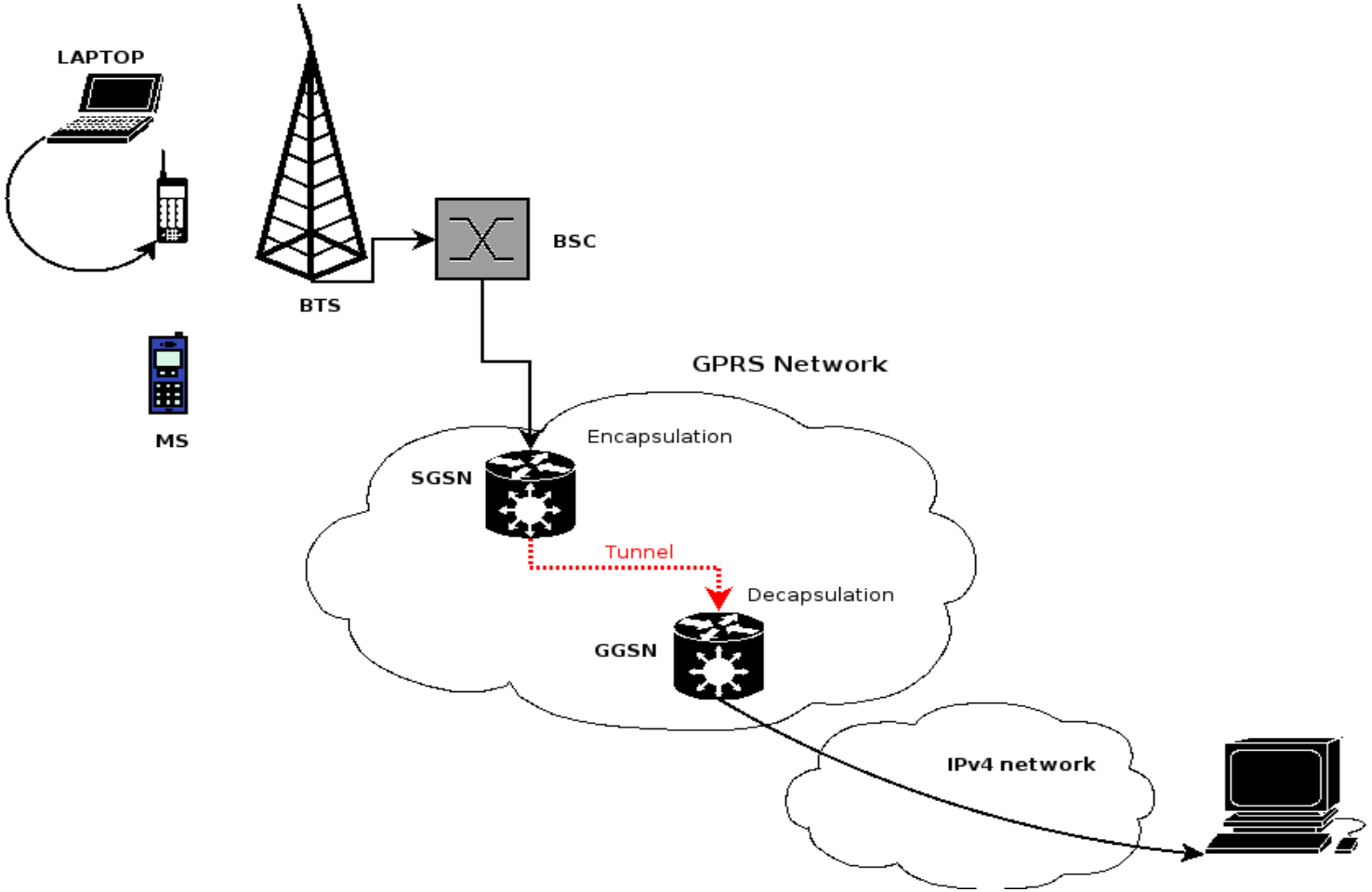
- SetWindowsHookEx()

Comment attaquer le kernel space ?

- **En utilisant les Trusted API**
  - Lecture / écriture dans les données du noyau
    - SetKMode()
  - Chargement d'une dll noyau
    - LoadKernelLibrary()
- **Par l'exploitation d'une faille de sécurité**

Le GPRS (1/2)

➔ Un bref rappel



Le GPRS (2/2)

- **Le monde de l'IP dans celui du GSM**
  - Une technologie connue …
  - Connexion à Internet
    - Quelques ports ouverts
    - NAT
- **Peut être le vecteur d'attaques de grande amplitude**
  - Propagation de Worms/virus
    - Botnet IRC
  - L'anonymat est facile
    - Voler le sac à main d'une vieille dame ;-)
- **L'UMTS, son successeur, un même combat …**

Autre piste intéressante : le Bluetooth

- **Vecteur de propagation idéal**
  - Ondes radio 2.4 GHz
  - Portée correcte en entreprise (20m)
  - Existence d'antennes dédiées (200m ou plus)
- **De nombreuses recherches ont été réalisées**
  - Nécessité de démêler le vrai du faux
  - Trouver des failles génériques
- **Protocole complexe**
  - Failles d'implémentation probables
    - Longues à trouver
    - Difficiles à exploiter
  - Problèmes de mauvaises configurations
    - Spécifiques à certains mobiles

Contrôle à distance du mobile

- **Interface graphique**
  - Permet un contrôle rapide
    - Pratique pour un vol de donnée ponctuel
  - Peu intéressant pour un contrôle massif
- **IRC shell (botnet)**
  - Intégration de commandes simples
    - ps, ls, mkdir, sms, …
  - Upgradable
  - Reverse shell
  - Commande massive par un canal IRC

Comment protéger un mobile ?

- **Machine virtuelle**
  - Procédé efficace
  - Disponible quand ?
  - Potentiellement lent
- **Antivirus**
  - Audit de quelques AV du marché
    - Symantec
    - Air mobile
- **Mécanismes de contrôle d'accès**
  - Avance de Symbian v9 sur ce plan là

Quelques fonctionnalités des virus x86 modernes …

- **Astuces anti-debug**
  - Modification du comportement du programme quand le debugger est détecté
- **Astuces anti-désassemblage**
  - Difficile sur ARM …
- **Astuces anti-heuristique**
- **Anti signature matching**
  - Chiffrement/Obfuscation
  - {Poly,Méta}morphisme

Comment devrait fonctionner un AV pour mobile ?

- **Scan des binaires et fichiers sensibles**
- **Détection de corruption de binaires**
  - EP redirection
- **Analyse comportementale (heuristique)**
  - Des hooks sont nécessaires
- **Capacités d'upgrade**

Qu'est ce que les AV pour mobiles sont réellement capables de faire ?

- **Analyse statique**
  - Mécanisme de signature faible …
    - Se contourne en changeant quelques strings ou opcodes
  - Monitoring de changement sur le système de fichiers
    - Pas forcément implémenté dans les AV
    - Lents quand ils le font (polling)
- **Analyse dynamique**
  - Les AV ne surveillent pas les appels aux API
    - Absence de mécanisme de hook
    - Pas de restriction des API
  - Le processus de l'AV n'est pas protégé
- **De bonnes capacités d'upgrade le plus souvent**

Quelques mots sur les virus pour mobiles d'aujourd'hui

- **Encore en faible nombre**
- **Pas de fonctionnalités avancées**
  - Les mécanismes de signature actuels suffisent pour se prémunir des virus connus
- **Se propagent difficilement**
  - Pas de réel vecteur de propagation
  - Grande hétérogénéité du parc

Conclusion

- **Les mobiles étudiés**
  - Ne sont pas assez sécurisés
    - Mauvaise utilisation des niveaux de sécurité
    - Trop de bugs …
  - Ne possèdent pas de réels mécanismes de protection
    - Les AV ne sont pas encore efficaces
- **Le danger devrait croître**

Des questions ?

@(°_°)@