Next Generation Secure Computing Base (NGSCB)

Cyril Voisin
Chef de programme Sécurité
Microsoft France

Microsoft

Préambule

- Nom de code initial du projet interne à Microsoft de renforcement de l'intégrité et de la sécurité de la plateforme : Palladium (dans la mythologie grecque, statue ayant la propriété de garantir l'intégrité et la sécurité de la ville qui la possédait…)
- Compte tenu du fait que Palladium est un nom déjà utilisé par une autre entreprise, Microsoft a annoncé le 24 janvier 2003, un changement de nom :
  « Palladium » s'appelle maintenant *Next-Generation Secure Computing Base* (NGSCB)
- Avec un nom aussi compliqué, on est à peu près sûr que personne ne l'a déjà déposé… :-)

Sommaire

- Introduction et motivation
- Aperçu de l'architecture
- Noyau de sécurité (Nexus)
- Fonctionnalités fondamentales
- Agents
- Politique
- Matériel
- Anonymat
- Quelques mythes
- Résumé

Le PC aujourd'hui

Application "sécurisée"

Fausse DLL système

Jeux

Virus

P2P / Chat

(avec backdoor)

Attaque

Application *plus* sécurisée

Attaque Réseau

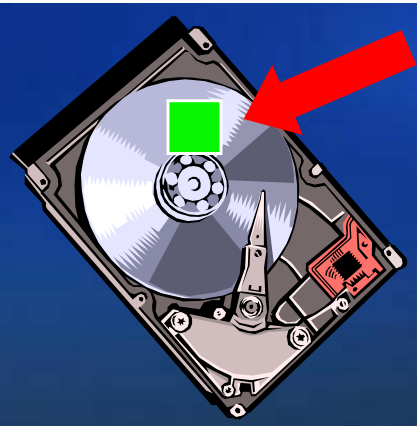
Mode utilisateur

Cheval de Troie

Système d'exploitation

Attaque

Pilote Pilote Pilote



Attaque

Mode noyau

Les buts de NGSCB

- Quelques façons de le dire…
  - « Protéger le logiciel du logiciel »
  - « Permettre d'enrichir la sécurité par des notions d'intégrité de la plateforme (machine,logiciel) »
  - « Rendre le PC aussi sécurisé qu'il est flexible »
  - « Permettre aux applications Windows sur un PC d'être autant dignes de confiance que leurs consoeurs s'exécutant dans un autre environnement »

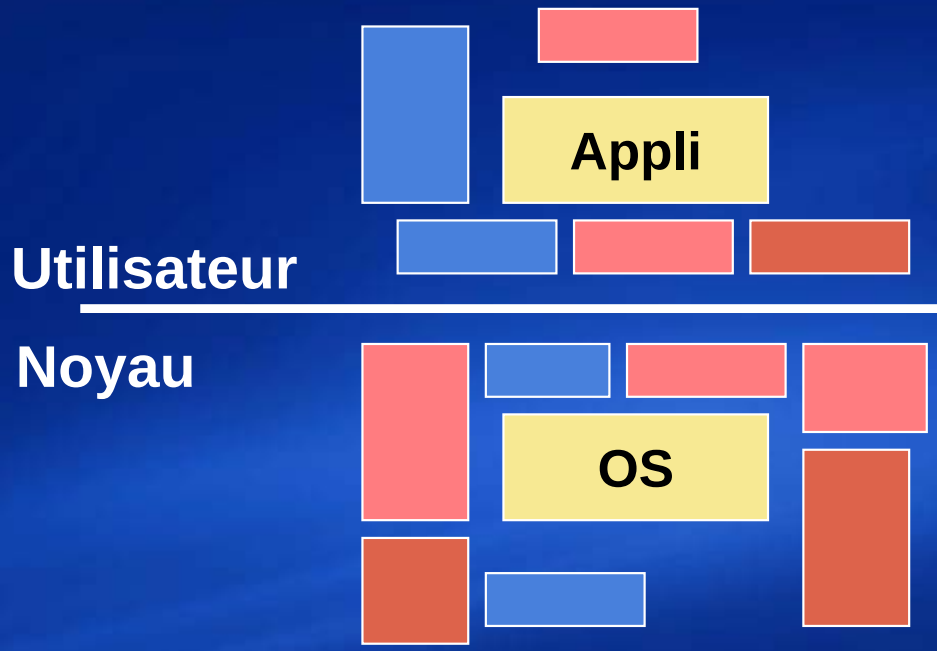
Les principes fondateurs

1. NGSCB sera construit à partir des plus hauts standards en matière de sécurité et de respect de la vie privée.
2. Un PC NGSCB doit être capable de *booter* tout OS compatible NGSCB et d'exécuter des logiciels en provenance de tous les fournisseurs tout comme les PC d'aujourd'hui.
3. Le *Trusted Computing Base* (TCB) de Microsoft sera disponible (les sources) pour examen.
4. Un PC NGSCB doit être capable d'exécuter les applications et les *drivers* d'aujourd'hui.
5. Quiconque peut écrire des applications Windows pour un PC pourra écrire des applications tirant parti de NGSCB.
6. NGSCB n'arrêtera pas le piratage.
7. Il n'est pas nécessaire de disposer des informations sur l'utilisateur pour permettre à NGSCB de fonctionner.
8. NGSCB peut ne pas être capable de résister à des attaquants disposant d'un accès physique à une machine mais empêchera toute attaque de type BORE (*Break Once, Run Everywhere*).
9. NGSCB permettra la mise en place de tout type de politique de sécurité et de respect de la vie privée.
10. Les systèmes NGSCB donneront les moyens de protéger la vie privée mieux que tout système d'exploitation aujourd'hui.

Qu'est-ce que NGSCB ?

- NGSCB est un ensemble de nouvelles fonctionnalités de sécurité de Windows
  - Faisant appel à du nouveau matériel et de nouveaux logiciels (Nexus et agents)
  - Pour offrir de nouvelles protections en matière de sécurité et de respect de la vie privée
- L'objectif est de
  - « protéger le logiciel du logiciel »
  - mettre en service et protéger un *Trusted Computing Base* (TCB) décentralisé dans le cadre de systèmes « ouverts »

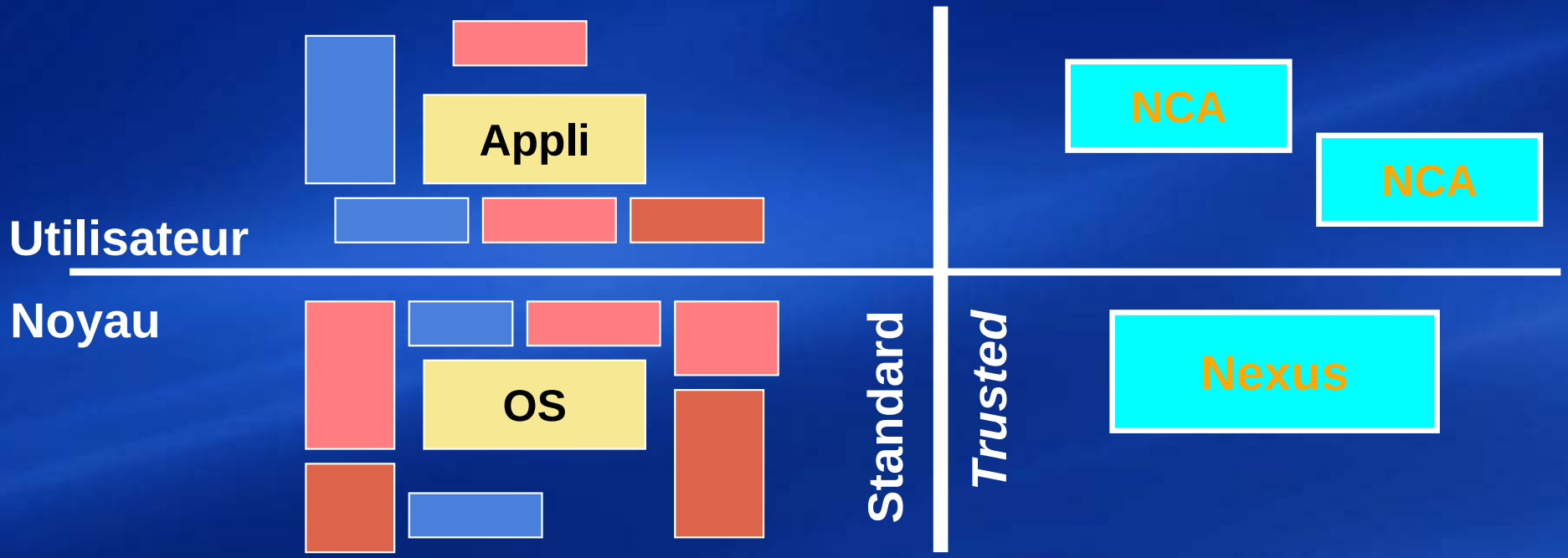
NGSCB « vu d'avion » (1/3)



- Comment préserver la flexibilité et l'extensibilité qui ont tant contribué à la richesse de l'écosystème du PC, tout en fournissant à l'utilisateur final un environnement sûr ?
- En particulier, comment peut-on garder quoi que ce soit de secret, quand des composants du noyau enfichables contrôlent la machine ?

NGSCB « vu d'avion » (2/3)

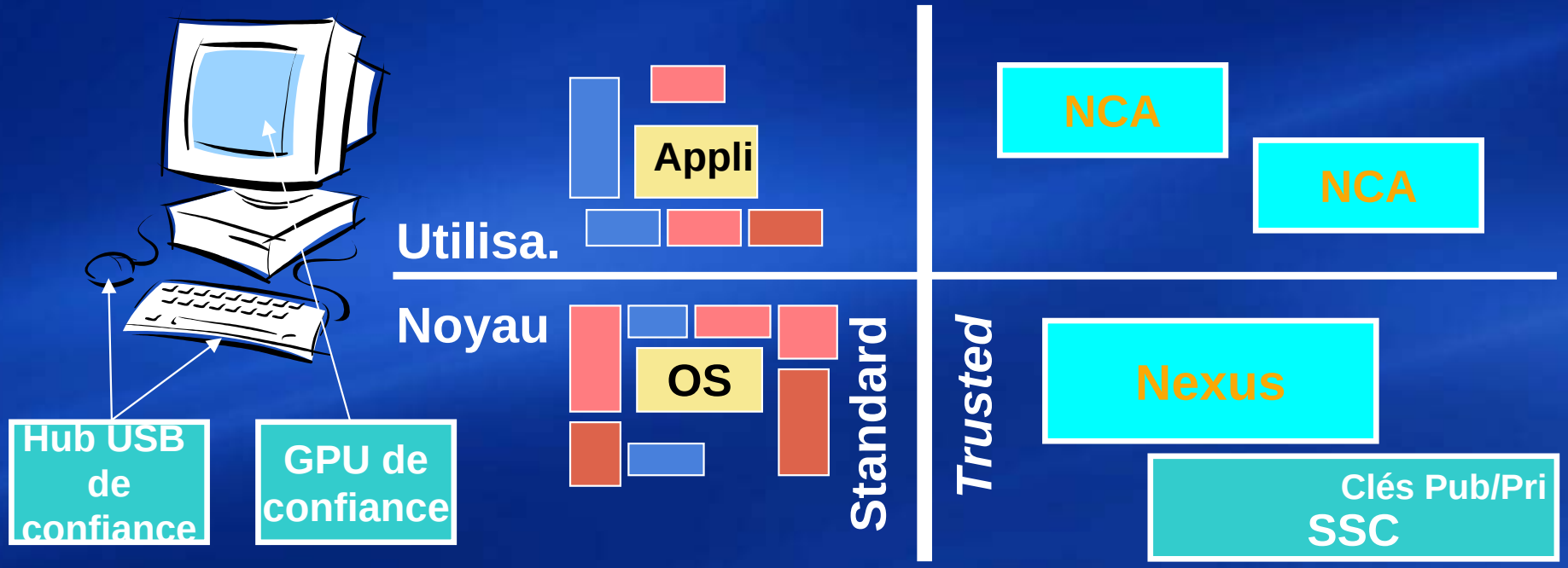
- La solution : subdiviser l'environnement d'exécution en ajoutant un nouveau mode au CPU



- Le CPU est soit en mode « standard » soit en mode « *trusted* »
- Les pages de la mémoire physique peuvent être marquées comme « *trusted* ». Les pages dites « *trusted* » ne peuvent être accédées que lorsque le CPU est en mode « *trusted* »

NGSCB « vu d'avion » (3/3)

- Les agents ont aussi besoin de laisser l'utilisateur entrer des secrets et d'afficher des secrets pour l'utilisateur

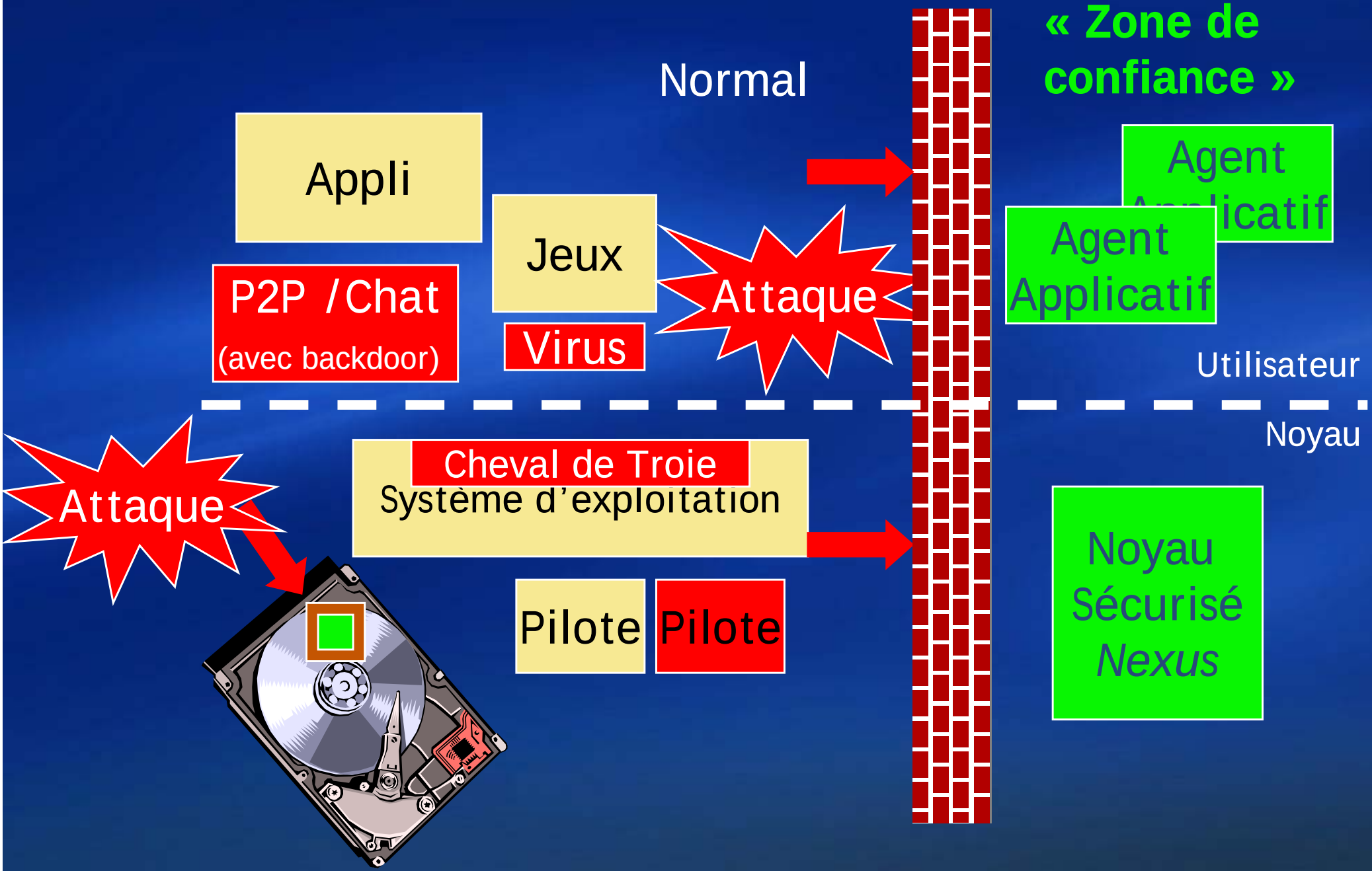


- Les entrées sont sécurisées par un « hub » USB de confiance pour le clavier et la souris qui permet de transporter une conversation sécurisée avec le *Nexus*
- Les sorties sont sécurisées par un GPU de confiance qui transporte une conversation chiffrée avec le *Nexus*
- Ceci permet une sécurité de bout en bout

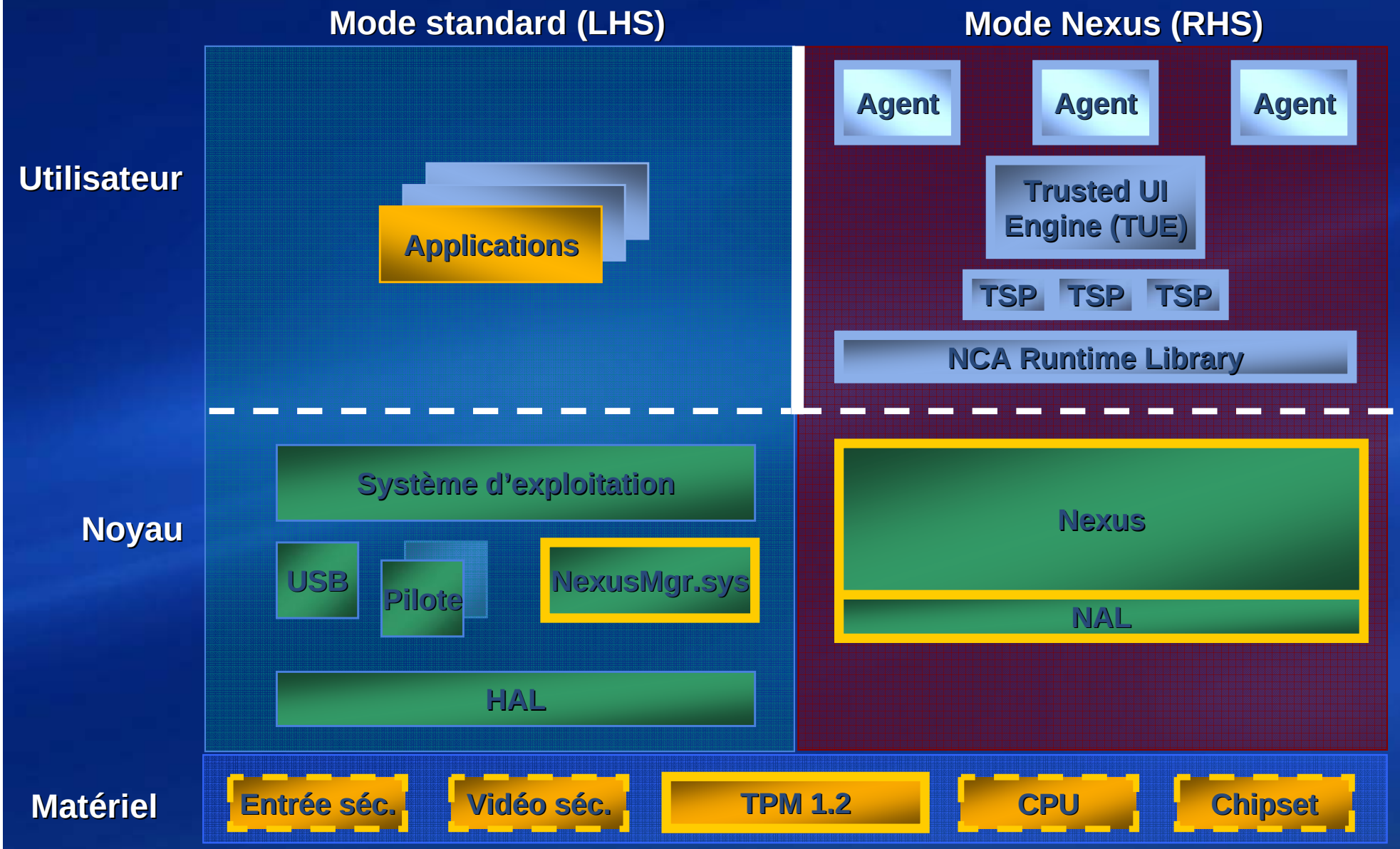
Ce qui tourne du côté gauche (LHS)

- Windows tel qu'on le connaît aujourd'hui (mais aussi les autres OS actuels comme Linux…)
- Les applications et pilotes
- Les virus aussi
- Tout logiciel, à quelques rares exceptions près. En effet, le nouveau matériel ne permet pas certains "mauvais" comportements :
  - Copie directe de mémoire d'un endroit au suivant
  - Passage du processeur en mode réel

Architecture NGSCB



NGSCB


Mode standard (LHS)
Mode Nexus (RHS)
Utilisateur
Noyau
Matériel
Applications
Agent
Agent
Agent
Trusted UI Engine (TUE)
TSP
TSP
TSP
NCA Runtime Library
Système d'exploitation
USB
Pilote
NexusMgr.sys
HAL
Nexus
NAL
Entrée séc.
Vidéo séc.
TPM 1.2
CPU
Chipset

Environnement en mode Nexus

- Fonctions basiques d'un OS
  - Gestionnaire/chargeur de processus et threads
  - Gestionnaire de mémoire
  - Gestionnaire d'E/S
  - Moniteur de référence de sécurité
  - Gestion des interruptions et abstraction du matériel
- Mais ce n'est pas un OS complet
  - Pas de système de fichiers
  - Pas de réseau
  - Pas de pilotes en mode noyau
  - Pas de Direct X
  - Pas d'ordonnancement (on s'appuie sur des processus *shadow LHS* qui appellent les threads RHS)
  - Pas de…
- Le Nexus s'appuie sur la partie standard pour la stabilité et les services (il ne dépend pas de cette partie pour la sécurité)

Que fournit le Nexus aux NCA?

- Un environnement d'exécution séparé protégé pour les agents ou *Nexus computing agents* (NCA)
- Les NCA peuvent
  - Etre autonomes
  - Fournir des services aux applications de la partie standard
- L'utilisateur indique au *Nexus* quels NCA sont autorisés à s'exécuter (la politique d'exécution du *Nexus* utilise les identités des NCA)
- Le *Nexus* scelle les secrets pour tout NCA et peut « attester » de l'identité du NCA

Identité de Nexus

- Le propriétaire de la machine définit les Nexus qui peuvent s'exécuter (en spécifiant leurs *hashes* respectifs)
- Démarrer un Nexus (noyau de sécurité) provoque le calcul du *hash* du Nexus par le SSC qui le stocke dans un registre en lecture seule (PCR)
  - Si on change le Nexus, son identité change
  - Le PCR détermine les clés auxquelles le Nexus a accès
- **Aucune signature particulière n'est requise pour exécuter du code**
  - Si l'utilisateur indique que le code correspondant à une valeur de hachage est autorisé à s'exécuter, celui-ci s'exécutera

Le Nexus (suite)

- Le mode noyau du mode Nexus ne permet pas d'ajouter du code à la volée (tout le noyau de sécurité est chargé au démarrage de ce dernier et doit correspondre à son empreinte chargée dans le PCR)
- Le Nexus peut être démarré et arrêté à n'importe quel moment (et redémarré plus tard)

Initialisation du *Nexus*

- L'amorçage du *Nexus* est initié par le système d'exploitation principal
  - Techniquement, c'est un chargement, pas un amorçage
  - Le code du *Nexus* est chargé en mémoire physique
  - A souvent besoin du support du *chipset* afin de permettre l'exclusion des maîtres du bus
- Etapes pour initialiser un *Nexus* :
  - *Reset* du CPU
  - Protection du *Nexus* des maîtres du bus (y compris les DMA)
  - Détermination de l'identité du *Nexus*
    - Calcul du hachage de la séquence d'instructions du *Nexus*
  - Passage du contrôle au *Nexus*

Politique pour le *Nexus*

- Tout ce qui tourne aujourd'hui tournera sur les systèmes NGSCB
- La plate-forme pourra exécuter tout *Nexus*
  - Le propriétaire de la machine aura la responsabilité de choisir le Nexus qu'il voudra utiliser
- Le *Nexus* Microsoft pourra exécuter toute application
  - L'utilisateur aura la responsabilité de choisir les applications qu'il voudra exécuter
- Le *Nexus* Microsoft interopérera avec tout fournisseur de service réseau
- Le code source du *Nexus* Microsoft sera rendu disponible pour analyse détaillée

Caractéristiques NGSCB

- Toutes les capacités des applications tirant parti de NGSCB s'appuient sur les 4 fonctionnalités clé suivantes :
  - Isolation forte des processus (mémoire cloisonnée – établissement du TCB)
  - Secrets pour le logiciel (stockage scellé – persistance de l'état du TCB)
  - Chemin sécurisé (échanges « dignes de confiance » pour l'utilisateur)
  - Authentification du logiciel (attestation - extension du TCB)
- Les 3 premières permettent de se protéger contre du code malicieux
- L'attestation permet d'ajouter à l'authentification de l'utilisateur celle du logiciel, ou bien de la machine ou bien de services
- Assertions de sécurité, permissions et authentification fondées sur des références (*credentials*)
  - Lampson, Rivest, Abadi, etc.

Menaces prises en charge par la version 1

- Modification de données
  - L'isolation forte des processus empêche les applications mal intentionnées de modifier vos données ou votre code pendant qu'il s'exécute. Le stockage scellé vérifie l'intégrité des données quand il les descellent
- Divulgation d'informations
  - Le stockage scellé évite que des applications mal intentionnées puissent accéder à vos données chiffrées
- Répudiation
  - L'attestation vous permet de vérifier que vous traitez avec une configuration (application+machine) en laquelle vous avez confiance
- Usurpation d'identité
  - Le chemin sécurisé permet à l'utilisateur de s'assurer qu'il traite avec la bonne application et réciproquement, de s'assurer qu'on traite avec le vrai utilisateur, pas une application qui se fait passer pour l'utilisateur

Détails supplémentaires pour la version 1

- Synchronisée avec la prochaine version cliente de Windows, nom code *Longhorn* (version alpha fournie fin octobre 2003 aux développeurs professionnels sur la plateforme Microsoft lors de la conférence PDC; sortie en 2005/2006)
- Focalisée sur les applications d'entreprise
- Exemples :
  - Signature de document
  - Messagerie instantanée sécurisée
  - Applications internes pour visualiser des données sensibles
  - Plug-in pour messagerie sécurisée

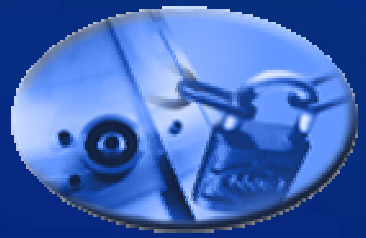
Isolation forte de processus

- Les agents s'exécutent dans un espace mémoire protégé
  - Non accessible à d'autres agents
  - Non accessible au noyau Windows traditionnel
  - Non accessible par le matériel, y compris en mode DMA
- Fonction assurée en collaboration par le matériel et le logiciel NGSCB
  - Le matériel notifie le Nexus de certaines opérations
  - Le Nexus effectue l'arbitrage pour les *page tables*, contrôle les registres, …

Chemin sécurisé

- Entrée sécurisée
  - Session sécurisée entre le périphérique et le Nexus
  - Protège à la fois le clavier et la souris
  - USB pour les postes de travail fixes, intégré pour les portables
- Sortie sécurisée
  - Canal sécurisé entre la carte graphique et le Nexus

Stockage scellé



- Fournit une méthode permettant de chiffrer des données avec une clé enracinée dans le matériel
  - Les données scellées ne peuvent être accédées que par des entités authentifiées
  - Chaque Nexus génère son propre jeu de clés aléatoirement lors du premier chargement
  - Le TPM sur la carte mère protèges le jeu de clés du Nexus
  - Les agents utilisent les services du Nexus pour sceller (chiffrer et signer) des données privées
  - Le Nexus protège la clé de tout autre agent/application, et le matériel empêche tout autre Nexus d'avoir accès à la clé

Attestation

- Si on le demande, le Nexus peut préparer une chaîne qui authentifie :
  - L'agent par *digest*, signé par le Nexus
  - Le Nexus par *digest*, signé par le TPM
  - Le TPM par sa clé publique, signée par son fabriquant ou par le département informatique
- Le propriétaire de la machine définit la politique qui contrôle les formes d'attestation que chaque NCA ou groupe de NCA peut utiliser

Types d'agents

- Agent applicatif – applications autonomes (petites)
  - Toute l'application s'exécute dans la partie de droite (mode Nexus)
  - Les agents applicatifs sont de bons clients pour les applications multi tiers
  - Exemple: application bancaire en ligne
- Agent composant - composants d'une application plus large
  - La majorité de l'application s'exécute dans la partie de gauche (mode standard)
    - Les agents sont utilisés pour des opérations de confiance spécifiques
  - Un proxy de la partie gauche traduit de COM ou .NET vers l'IPC NGSCB
  - Bien pour ajouter des fonctionnalités de confiance à des applications Windows existantes
  - Exemple: composant de signature de document dans un traitement de texte

Manifestes d'agents

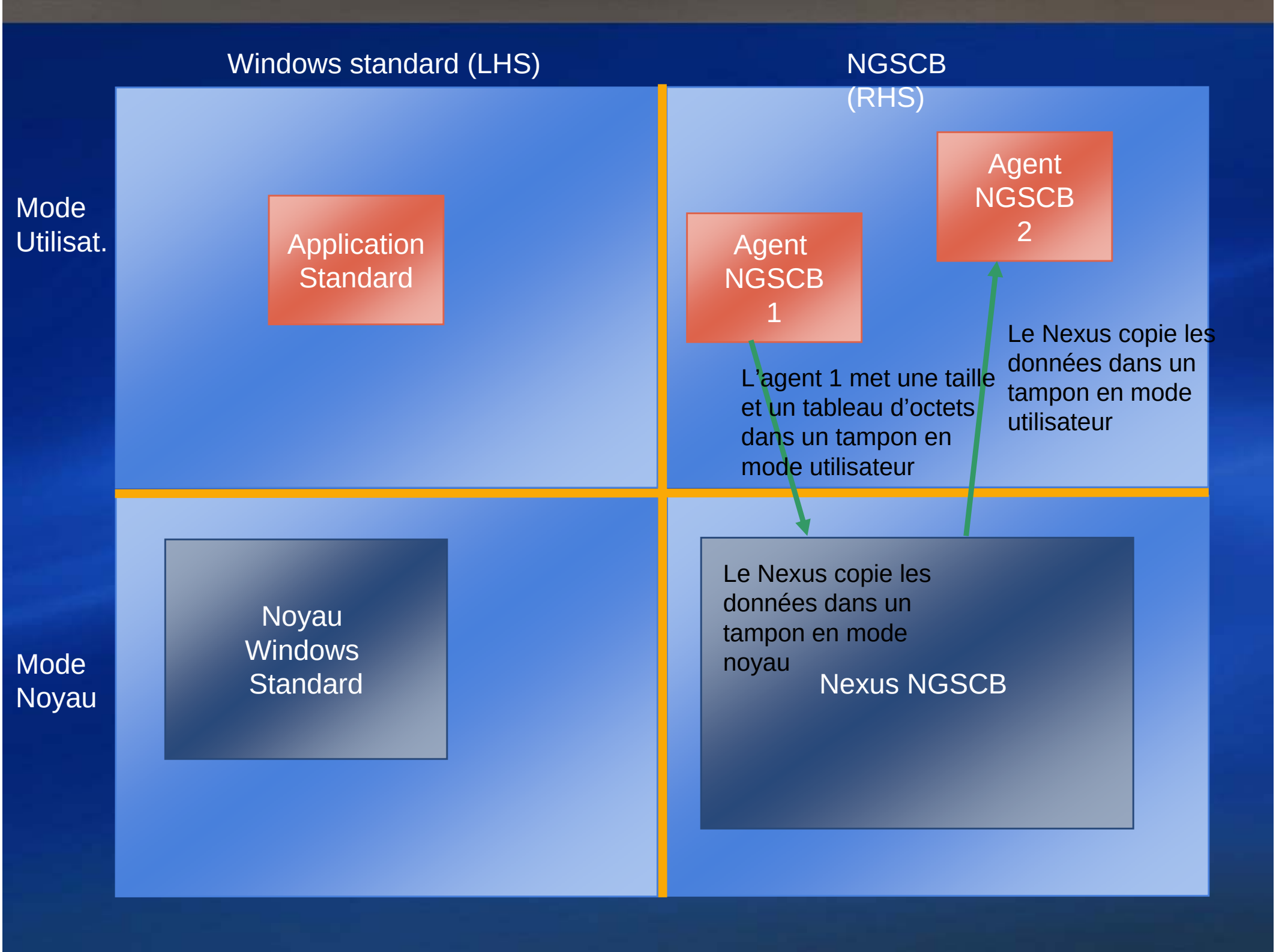
- Fournit les informations à propos d'une application qu'un propriétaire de machine utilise pour déterminer si une application devrait s'exécuter ou non
- Document XML signé qui définit :
  - Les composants de l'agent
  - Les propriétés de l'agent
    - Prérequis systèmes :
      - Appliqués par NGSCB
      - Par exemple : Debuggable = FALSE
    - Propriétés descriptives
      - Non interprétées ni appliquées par le système
      - Par exemple : Version = 1.1.2.2
  - Les requêtes de politique de l'agent (Agent policy requests)
    - C'est-à-dire l'accès à une sortie sécurisée, l'accès en écriture à un compteur, etc.
- Le schéma XML est une extension spécifique pour NGSCB au manifeste standard de Longhorn
- Les requêtes de politique ne sont pas absolues
  - La politique définie par le propriétaire de la machine l'emporte sur les requêtes de politique du manifeste

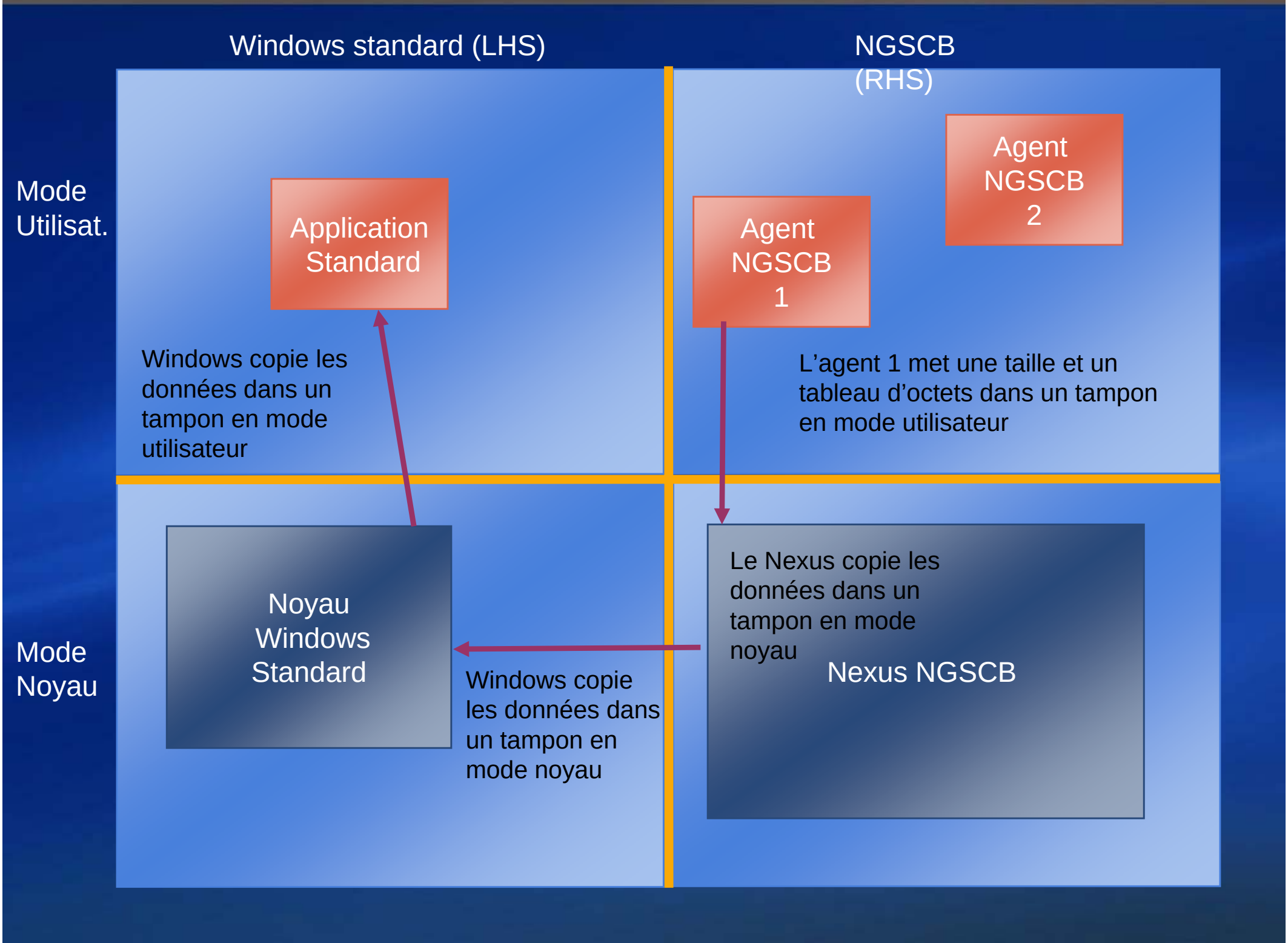
Manifestes : identification du code pour les applications

- Objectif : permettre la gestion
  - Création d'identités par hachage pour des « familles de code »
  - Pas nécessairement un simple condensé de séquences d'instructions
  - Spécifie la mise à jour et le déboguage
- Manifeste : nomme les « familles de code » en utilisant des preuves cryptographiques (hachages, clés de signature, chaînes de certificats) :
  - « Agent de paiement par carte de crédit Visa certifié »
  - « Agent MS-Money + mise à jour »
- Le « condensé de manifeste » peut être utilisé dans le stockage fourni par le *Nexus* et par les fonctions d'attestation

Agents

- Les agents sont monolithiques – pas de DLL
  - Partage de code possible en utilisant des bibliothèques liées statiquement
- La composition des agents est basée sur IPC (*Inter Process Communication*)
  - IPC est bloquante et orientée message
  - Les agents et les processus du mode standard peuvent utiliser IPC
    - Les agents peuvent communiquer avec d'autres agents
    - Les applications standards peuvent communiquer avec les agents qu'elles ont démarré
  - L'accès à l'IPC est contrôlé par politique (policy)


Windows standard (LHS)
NGSCB (RHS)
Mode Utilisat.
Application Standard
Agent NGSCB 1
Agent NGSCB 2
L'agent 1 met une taille et un tableau d'octets dans un tampon en mode utilisateur
Le Nexus copie les données dans un tampon en mode utilisateur
Mode Noyau
Noyau Windows Standard
Le Nexus copie les données dans un tampon en mode noyau
Nexus NGSCB


Windows standard (LHS)
NGSCB (RHS)
Mode Utilisat.
Application Standard
Agent NGSCB 1
Agent NGSCB 2
Windows copie les données dans un tampon en mode utilisateur
L'agent 1 met une taille et un tableau d'octets dans un tampon en mode utilisateur
Mode Noyau
Noyau Windows Standard
Windows copie les données dans un tampon en mode noyau
Le Nexus copie les données dans un tampon en mode noyau
Nexus NGSCB

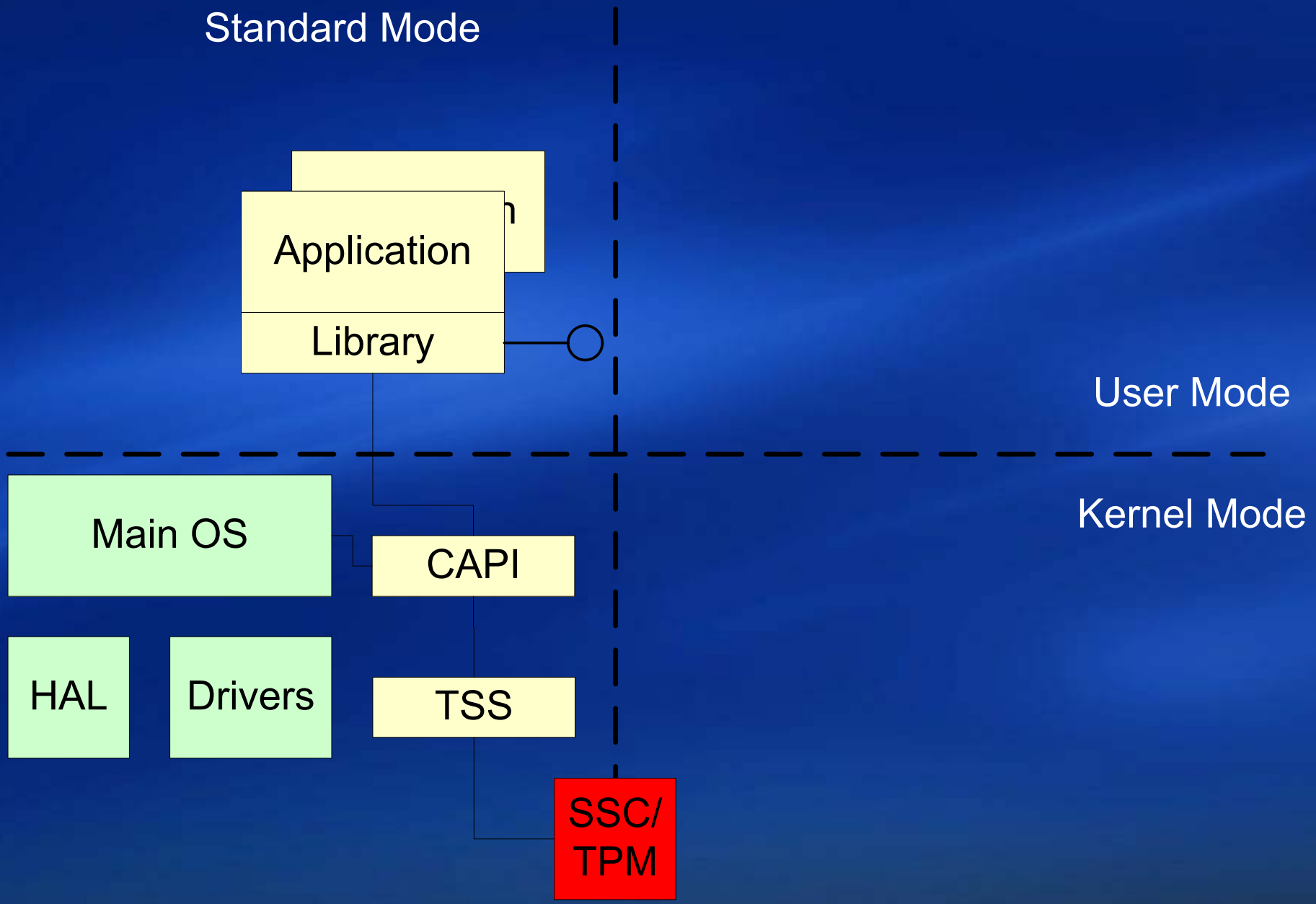
NGSCB Developer Preview

- Permet de :
  - Créer un agent dans Visual Studio
    - Débogage en ligne de commande pour l'instant
  - Simuler le stockage scellé
  - Simuler l'attestation
  - Utiliser l'IPC
- Ne fournit pas
  - Entrées / sorties sécurisées
  - Isolation forte de processus

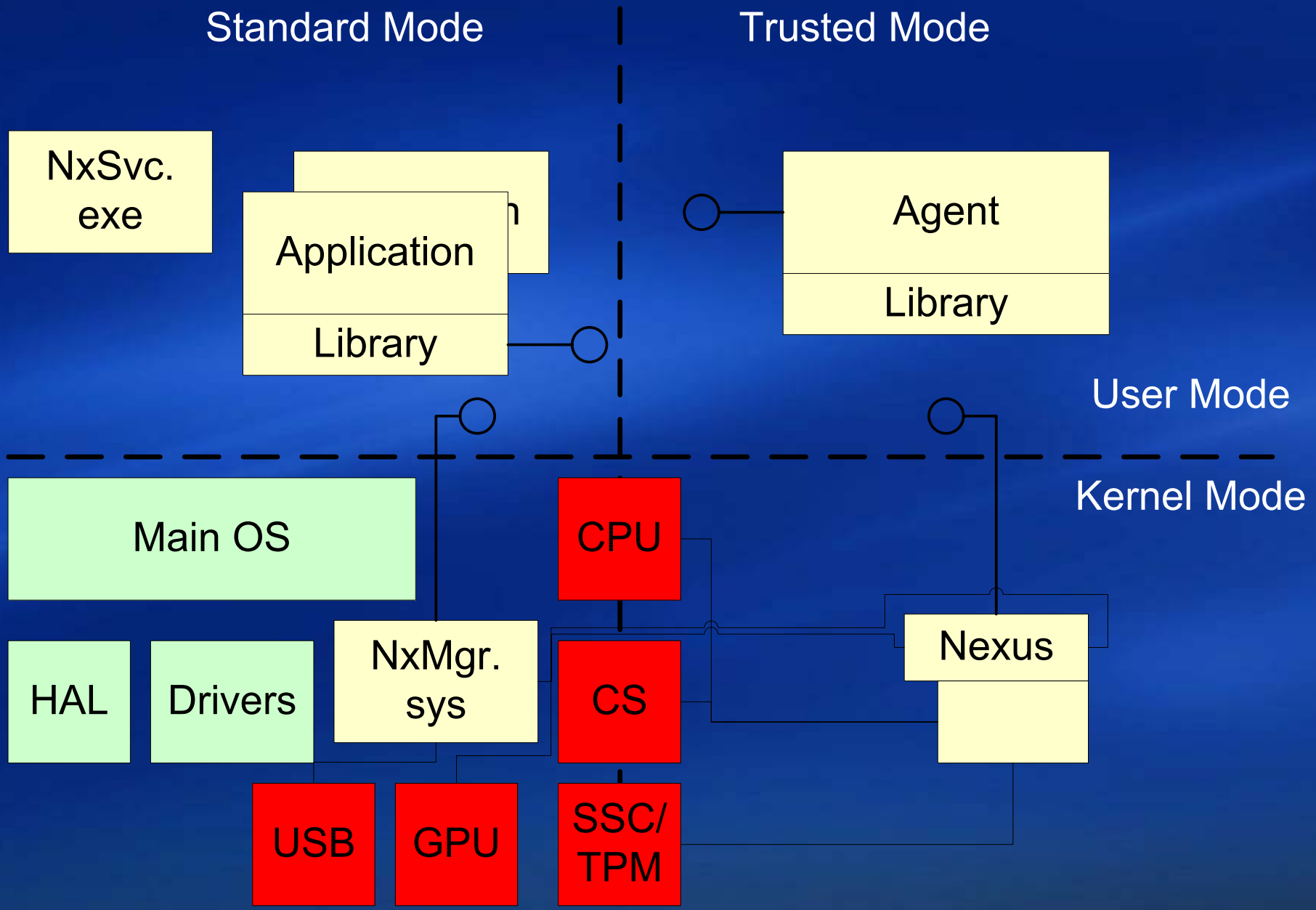
Politique Système

- Définie par le propriétaire de la machine
  - Le propriétaire peut autoriser les utilisateurs à étendre ou modifier la politique
  - Le propriétaire peut choisir de déléguer la politique et les décisions d'approbations à une tierce partie
    - "Utiliser les politiques de l'organisation Truc pour tout agent signé par Bidule"
    - "Utiliser les politiques de ma direction informatique pour tous les agents"
- Exprimée en utilisant des certificats de politique signés au format XrML (signed XrML policy certificates)
- Les ressources contrôlées par la politique système comprennent :
  - Exécuter un agent
  - Répondre à une demande d'attestation
  - Accéder à un secret spécifique
  - Accéder à certaines API NGSCB (comme les API réseau par exemple)
  - Créer un processus enfant
  - Accéder au TUE
- La politique est vérifiée lors de l'exécution pour chaque requête
  - Quelques décisions relatives à la politique sont mises en cache dans le Nexus pour des raisons de performance

TCPA


Standard Mode
Application
Library
User Mode
Kernel Mode
Main OS
CAPI
HAL
Drivers
TSS
SSC/
TPM

NGSCB


Standard Mode
Trusted Mode
NxSvc.
exe
Application
Library
Agent
Library
User Mode
Kernel Mode
Main OS
CPU
HAL
Drivers
NxMgr.
sys
CS
Nexus
USB
GPU
SSC/
TPM

Algorithmes de chiffrement

- La version 1 du SSC nécessite
  - RSA 2048 + PKCS #1 V2.1
  - AES-128
  - SHA-1
  - HMAC (*Keyed-Hashing for Message Authentication*)
  - Un générateur de nombre aléatoires FIPS 140-2
  - Un petit nombre de compteurs monotones
- Le SSC contient au moins une paire de clés RSA, une clé AES-128 et une clé HMAC

Attestation au niveau du SSC

- Il n'y a pas « d'anonymat absolu » à ce bas niveau mais on ne peut utiliser la clé matérielle qu'une seule fois lors de la mise sous tension de la machine
- Pour préserver l'anonymat, il est possible d'utiliser la clé matérielle pour créer des pseudo-identités afin de fournir indirection/anonymat tout en préservant la capacité d'attestation de la plate-forme
  - La capacité de pouvoir créer des pseudo-identités nécessite la présence de tiers de confiance fournissant ce genre de service, ce qui n'est pas le cas aujourd'hui
    - Microsoft cherche à encourager l'émergence de ce type de marchés

Quelques idées fausses « classiques » sur NGSCB

- NGSCB pourra censurer ou interdire du contenu sans la permission de l'utilisateur
  - La mise en place d'une telle politique, tel qu'est conçu NGSCB, n'est absolument pas possible
    - En effet, les applications compatibles NGSCB ne peuvent pas interférer avec d'autres applications NGSCB (de par la conception même de NGSCB) ni avec d'autres applications Windows traditionnelles
- NGSCB mettra hors du marché les fournisseurs non approuvés par Microsoft
  - Il n'y a aucune signature Microsoft requise pour utiliser NGSCB
- NGSCB n'est pas contrôlé par l'utilisateur
  - Tous les programmes NGSCB ne pourront s'exécuter que si ils sont autorisés par l'utilisateur

Quelques idées fausses « classiques » sur NGSCB

- NGSCB est un « super » moyen de répandre des virus
  - Les applications NGSCB ne s'exécutent pas avec des privilèges élevés
- Un NCA de NGSCB n'est pas déboguable
  - Si. Un drapeau dans le manifeste permet de mettre en service le déboguage
- NGSCB surveillera l'utilisation de votre ordinateur et en informera le fournisseur et/ou Microsoft
  - Un des principaux objectifs de conception de NGSCB est d'interdire à quiconque (y compris Microsoft) d'espionner votre machine et de capturer les séquences de caractères entrées au clavier
- D'autres idées fausses en http://www.microsoft.com/france/securite/entreprises/palladium

Résumé (1/2)

- NGSCB sera proposé dans Longhorn
- NGSCB est une combinaison de
  - Nouveau matériel qui crée un environnement sécurisé pour…
  - …un nouveau noyau de sécurité parallèle, appelé Nexus, qui…
  - …permettra l'exécution d'agents dans une partition mémoire sécurisée, et qui …
  - …fournira à ces agents des services de sécurité de façon à ce qu'ils puissent…
  - …fournir aux utilisateurs plus de sécurité et de respect de la vie privée
- Ne pas oublier que :
  - Lorsque le Nexus est éteint, tout fonctionne comme avant
  - Que quand le Nexus est en marche, la partie standard (de gauche) continue à faire fonctionner quasiment tout ce qui tournait avant
  - Le Nexus n'a pas besoin de savoir ce qui s'exécute en mode standard
  - Le matériel devrait permettre l'exécution de n'importe quel Nexus (étape administrative du propriétaire à prévoir)
  - Le Nexus exécutera n'importe quel logiciel que le propriétaire lui demandera d'exécuter

Résumé (2/2)

- NGSCB fournit quatre fonctionnalités clé :
  - Isolation forte des processus
  - Protection des secrets
  - Chemin sécurisé de et vers l'utilisateur
  - Attestation
- Les trois premières de ces fonctionnalités permettent de se protéger contre du code malicieux (virus, chevaux de Troie, etc.)
- L'attestation permet de prouver à des entités distantes des faits à propos des logiciels, des utilisateurs, des machines, des services, etc. que ces entités distantes pourront croire en confiance
- Il reste encore beaucoup de chemin à parcourir. Nous ne connaissons pas les réponses à toutes les questions. Nous sommes intéressés par tous les feedbacks, questions, préoccupations,… Sans œillères ni certitudes.

Ressources

- Livres blancs et spécifications
  - http://www.microsoft.com/ngscb (en anglais)
  - http://www.microsoft.com/france/securite/entreprises/ngscb (en français)
- Questions ? Écrivez en anglais à l'alias suivant :
  - ngscb_qa@microsoft.com
- Inscrivez-vous pour recevoir des infos mises à jour par e-mail (lettre d'info NGSCB)
  - Envoyez un message vide à :
    - wtpiinfo-subscribe@pens.tm500.com
- Article de l'IEEE Magazine : http://download.microsoft.com/download/c/8/0/c80ea683-9900-46ff-9c67-d7f14b0d3787/trusted_open_platform_ieee.pdf