# Modernisation, développement d'applications et DB2 sous IBM i

*Technologies, outils et nouveautés 2013-2014*

13 et 14 mai 2014 – IBM Client Center Paris, Bois-Colombes

## S3 - Bonnes pratiques de sécurité sous IBM i

*Mardi 13 mai – 14h00-15h30*

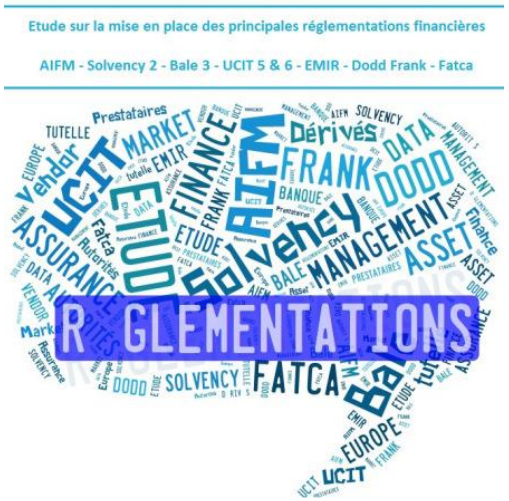
Pascal THENON – pthenon@astech.com

# **Bonnes pratiques** de sécurité sous IBM i

1. **La sécurité informatique n’est pas seulement une question technique**

# Evaluation des Risques & Politique Sécurité

DISPONIBILITE




ISO/IEC 27001:2005

SECURITE

ISO 27001 CERTIFICATION EUROPE

PCI DSS COMPLIANT

CLUSIF

INTEGRITE

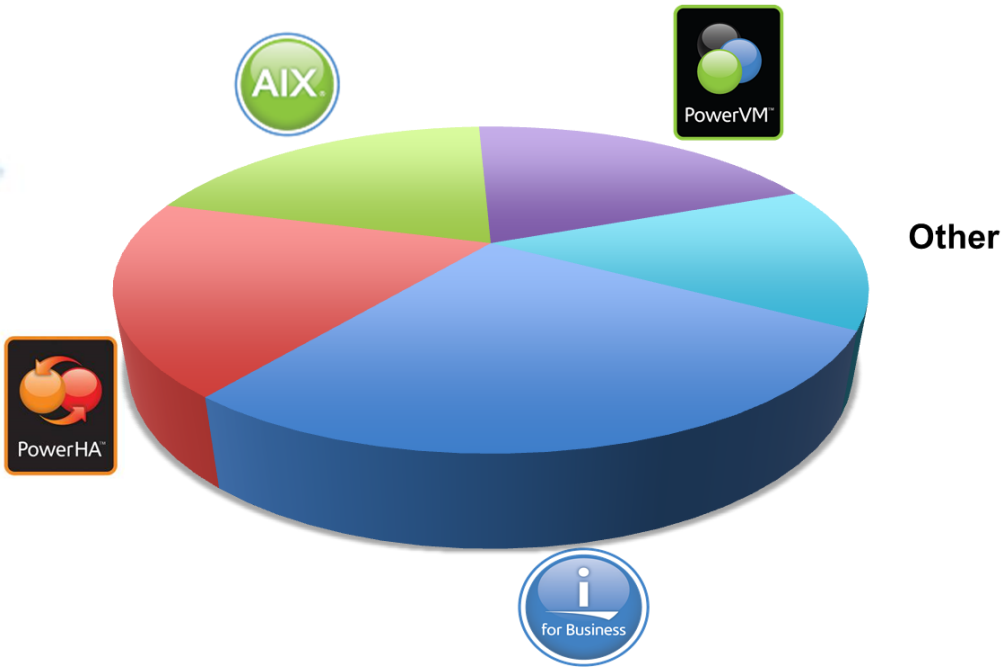
CONFIDENTIALITE

ANSSI Agence nationale de la sécurité des systèmes d'information

# **Bonnes pratiques** de sécurité sous IBM i

1. La sécurité informatique n’est pas seulement une question technique
2. **Périmètre IBM i**

# IBM i (aka AS/400) : un « mort » encore bien vivant ...


*Source : Alison Butterill*
*IBM i Product Offering Manager*

%age Contribution to Power SW Revenue in in 2013

# IBM i : environnement OS comme les autres ?

1. What are the 2 processor speeds on Power750 Express? **3.5 / 4.0 GHz**
2. Does 720 Express have Chip Kill memory? **Yes**
3. What is the size of L2 Cache per core on Power 720 Express? **256**
4. What is the maximum SAS Speed on Power 740 Express? **3 Gbps**
5. How many average IBM i customers care? **0**

# Run my business … not my computer

IBM North America Power Systems

IBM

## IBM i Strategy


### Power Solutions

- Delivering an integrated platform focused on leading industry applications
- Providing flexible solutions delivery options for ISVs and MSPs
- Enabling clients to transform their customer experience via mobile solutions

### Open Platform for Choice

- Confirming IBM's commitment to IBM i, with next major release in 2014
- Growing IBM i solutions options via open source languages and applications
- Extending IBM i solutions portfolio with Linux and AIX application choices


### The *Integrated* Promise of IBM i

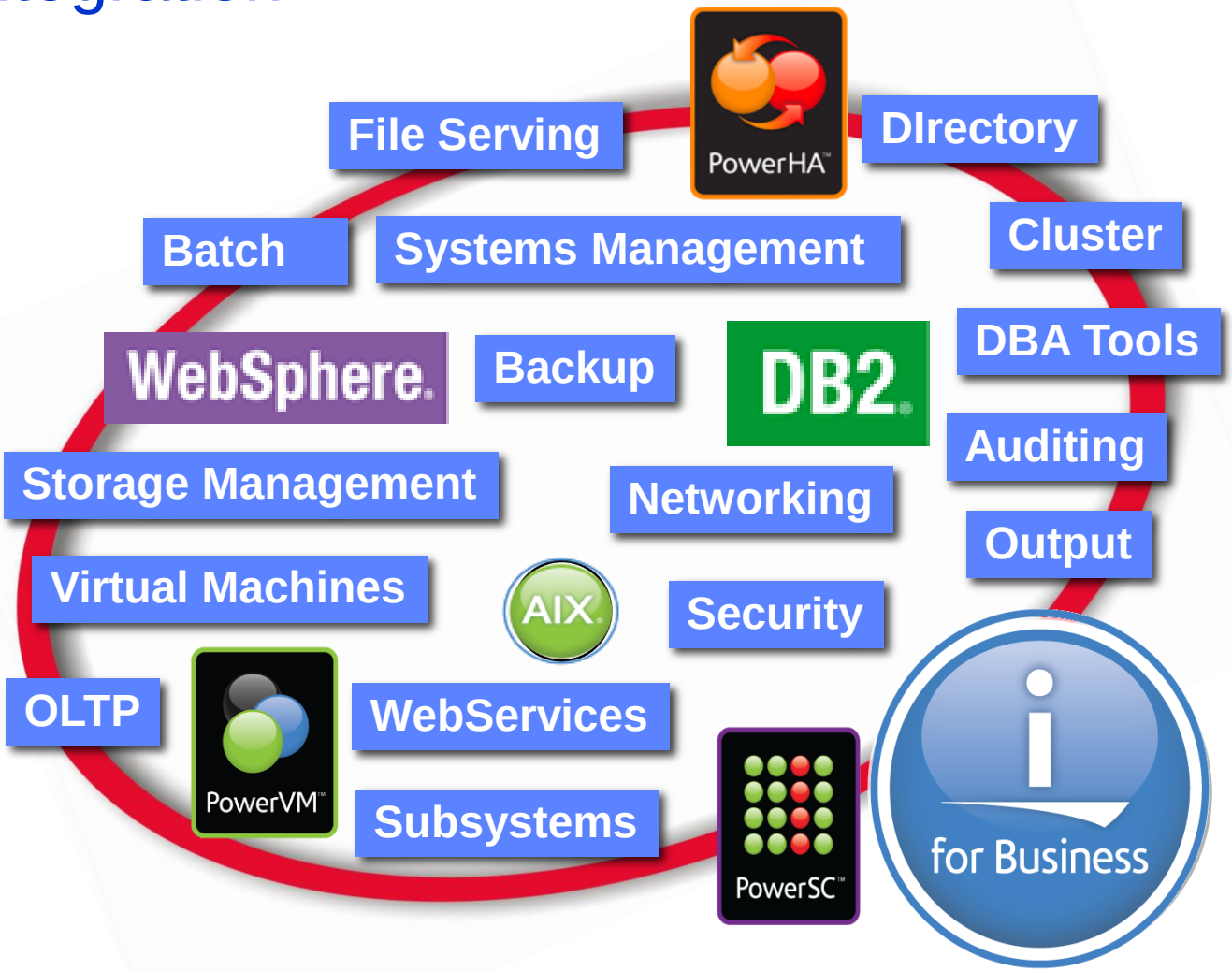
- Deliver a simple, high value platform for business applications
- Provide exceptional security and resiliency for critical business data
- Leverage IBM systems, storage and software technologies

7

# **Bonnes pratiques** de sécurité sous IBM i

1. La sécurité informatique n'est pas seulement une question technique
2. Périmètre IBM i
3. **Avoir conscience des spécificités IBM i et bâtir son projet de sécurité**

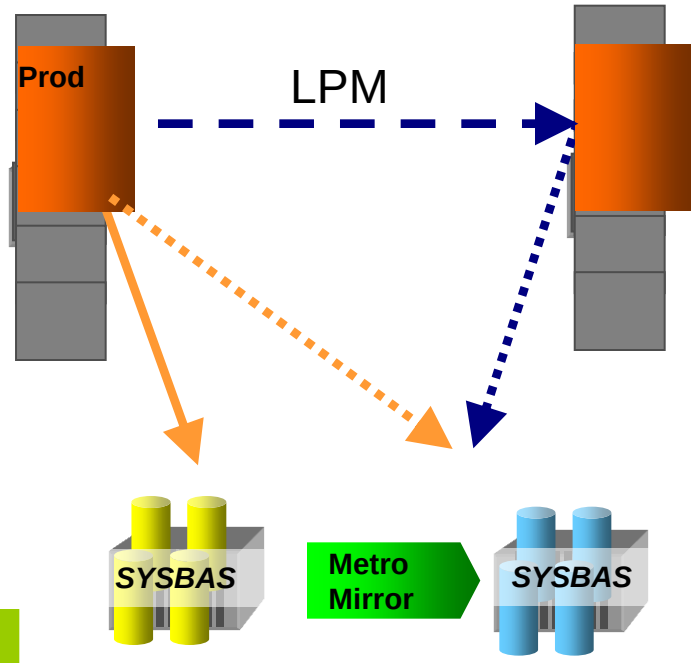
# IBM i = intégration

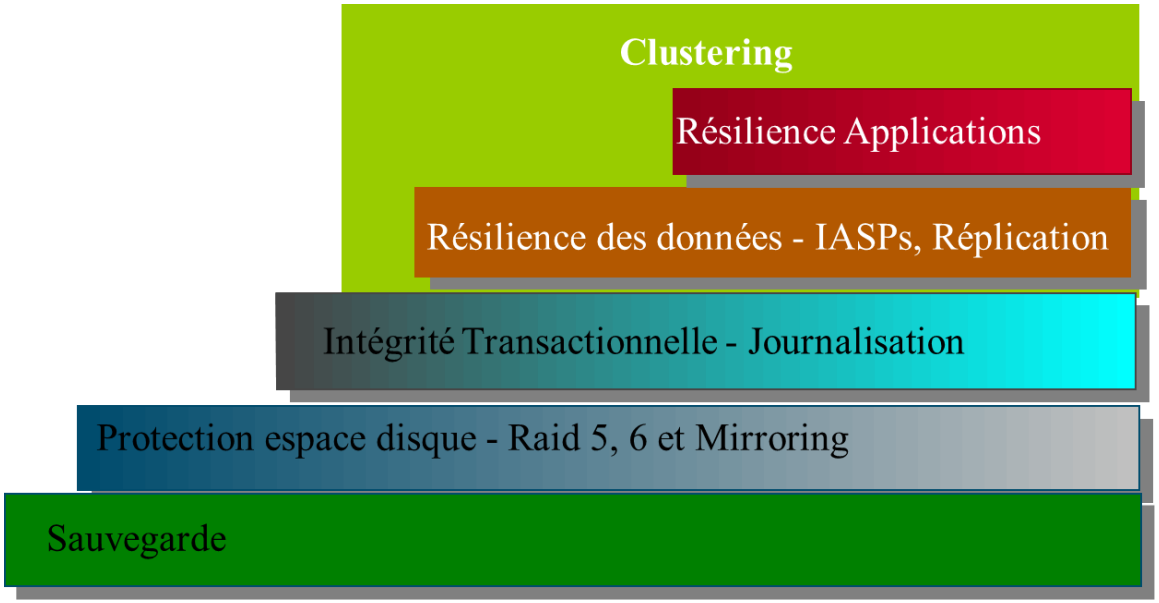


# **Quelle** sécurité ?

# Disponibilité

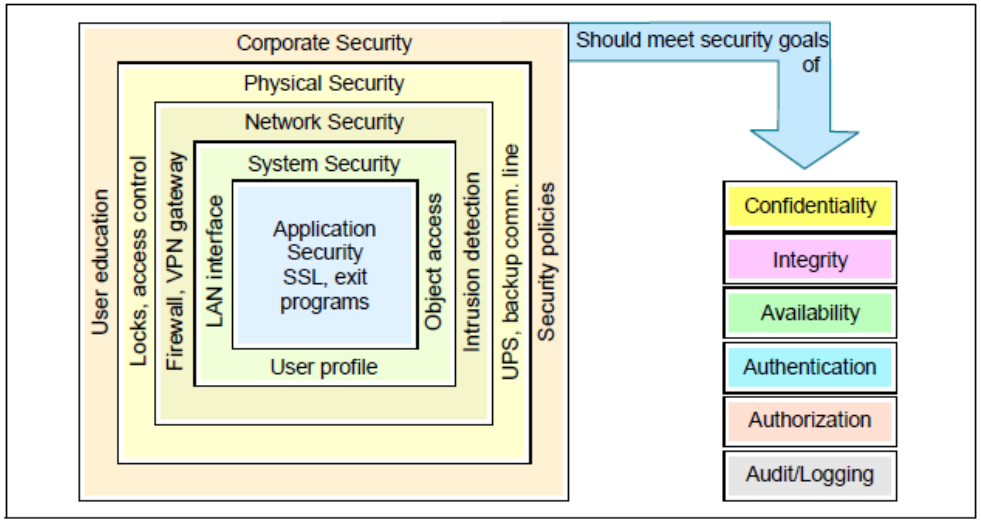
- RTO / RPO
- ASP / iASP
- V7R2 : PowerHA HyperSwap

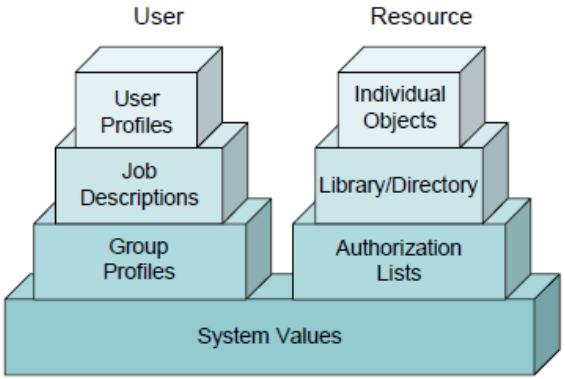


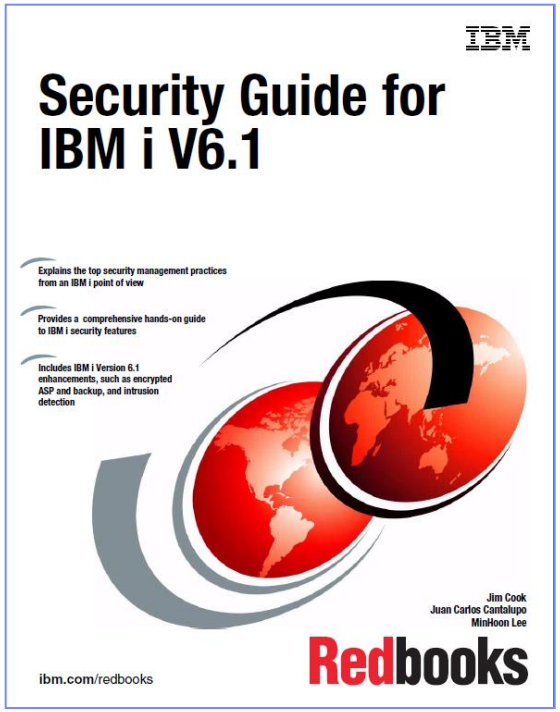




PowerHA™

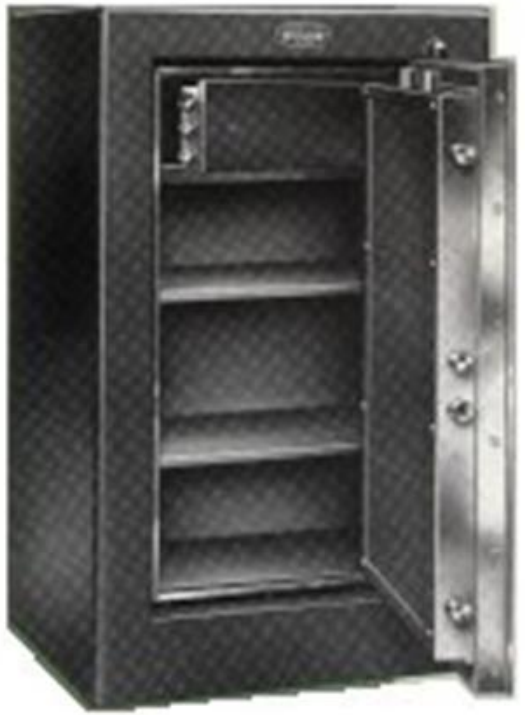
# Sécurité **native IBM i**



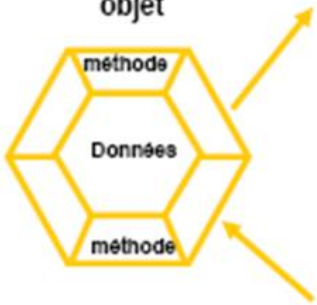



# Sécurité IBM i : c'est **Automatique ?**



# Architecture IBM i : **Orientation Objet**

Encapsulation objet




**Chaque objet System i contient l'équivalent numérique d'une étiquette sur les informations nutritionnelles et les ingrédients**

Chaque type d'objet dispose d'un jeu de règles régissant son utilisation.
Ces règles sont mise en œuvre par le système d'exploitation et ne peuvent être mises en question, ce qui assure l'intégrité de l'objet.

**Description de l'objet**

**Propriétés de l'objet**
- Type d'objet (ex. fichier, programme,…)
- Règles d'utilisation (comportement)

**Droits d'usage de l'objet**
- Qui peut y accéder
- Actions autorisées (ex. utilisation, …)

**Ingrédients de l'objet**

**Contenu de l'objet**
- Informations que contient réellement l'objet, données ou instructions

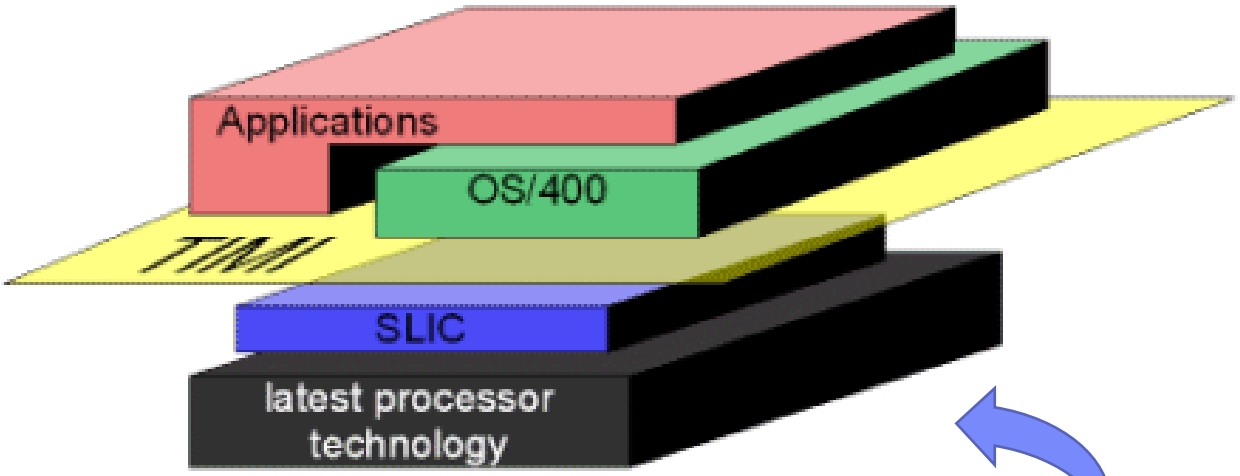
L'accès au contenu d'un objet et son utilisation sont régis par les propriétés et droits d'usage de l'objet, ce qui assure l'intégrité de toute information (données) ou programme (exécutable) que contient l'objet.

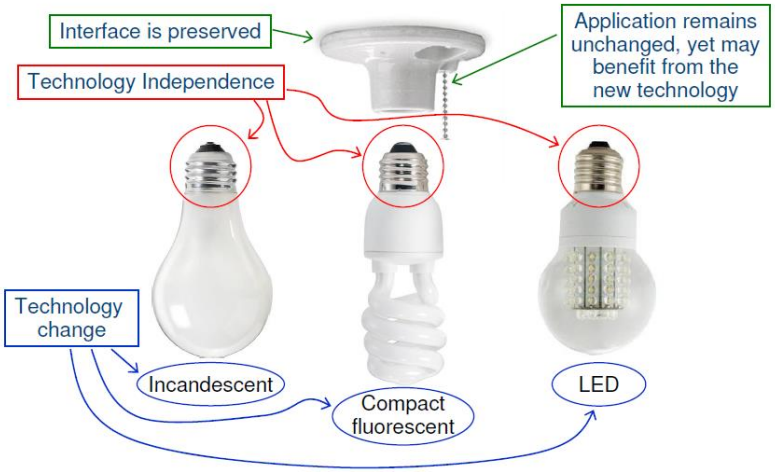
Des droits d'usage particuliers peuvent être associés aux objets. Cela permet de contrôler les droits et responsabilités qui peuvent être attachés à un objet, Assurant encore un peu plus l'intégrité de l'objet et de son contenu.

***Des défenses naturelles contre les intrus et les attaques virales***

Vérifiez-le vous-mêmes : www.securityfocus.com !!!

# Technology Independant Machine Interface




Les principales fonctions SECURITE de l'IBM i sont gérées au sein du SLIC

# Le résultat …

Figure 5 summarizes numbers of advisory notices issued by the company between the beginning of 2008 and the end of June 2012 for the most recent versions of IBM i, Red Hat Enterprise Linux (RHEL) and SUSE Linux Enterprise Server (SLES), and for Windows Server 2008.

| SEVERITY | WINDOWS SERVER 2008 | RHEL Server 5 | RHEL Server 6 | SLES 10 | SLES 11 | IBM i 7.1 | i5/OS 6.x |
|---|---|---|---|---|---|---|---|
| Extremely critical | 3 | 1 | 0 | 0 | 0 | 0 | 0 |
| Highly critical | 64 | 93 | 61 | 134 | 88 | 0 | 0 |
| Moderately critical | 34 | 185 | 84 | 79 | 53 | 0 | 6 |
| Less critical | 73 | 175 | 85 | 60 | 66 | 0 | 5 |
| Not critical | 5 | 53 | 31 | 18 | 14 | 0 | 0 |
| TOTAL ADVISORIES | 179 | 507 | 261 | 291 | 221 | 0 | 11 |

Source: Secunia

**Figure 5:** ***Comparative Vulnerability Data: January 2008 Through June 2012***

Figure 6 shows lifetime vulnerabilities; i.e., the number of vulnerabilities recorded by Secunia since each version was introduced. Multiple vulnerabilities may be documented in a single advisory notice.

| | WINDOWS SERVER 2008 | RHEL Server 5 | RHEL Server 6 | SLES 10 | SLES 11 | IBM i 7.1 | i5/OS 6.x |
|---|---|---|---|---|---|---|---|
| Release Date | February 2008 | March 2007 | November 2010 | July 2006 | March 2009 | April 2010 | January 2008 |
| Lifetime Vulnerabilities | 352 | 1,871 | 906 | 3,557 | 1,889 | 0 | 16 |

Source: Secunia

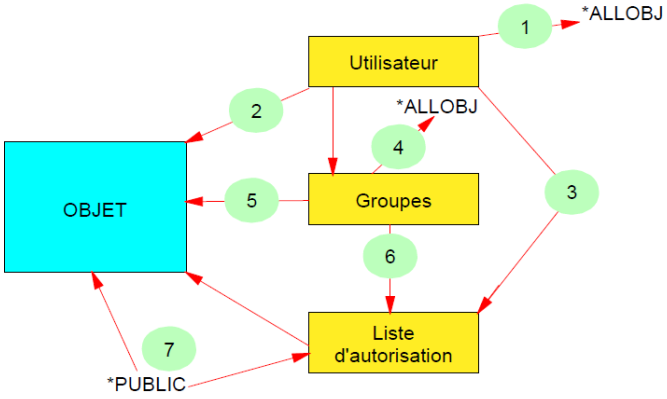
**Figure 6:** ***Comparative Vulnerability Data: Lifetime Totals***

# Le projet de sécurité IBM i (1/2)

**… parce que le reste n'est PAS automatique**

## Sécurité « Interne »

- Droits sur les OBJETS




## Sécurité « Périmétrique »

- Contrôle d'Accès
- Confidentialité données critiques

**sans oublier Sécurité Système et Traçabilité**

# Le projet de sécurité IBM i (2/2)

- Conception des applications
  - Documentation
  - Propriété des objets
  - Droits
    - *PUBLIC
    - Privés
    - Listes d'Autorisation
  - Adoption de droits
  - « User Profile Swap »


- Outils du marché
  - Exploitation des données d'audit
  - Limiter le besoin de développements complexes avec risques d'impacts opérationnels (Point d'exit, Profile Swap, … )

# **Bonnes pratiques** de sécurité sous IBM i

1. La sécurité informatique n’est pas seulement une question technique
2. Périmètre IBM i
3. Avoir conscience des spécificités IBM i et bâtir son projet de sécurité
4. **Intégrité Système & Réseau**

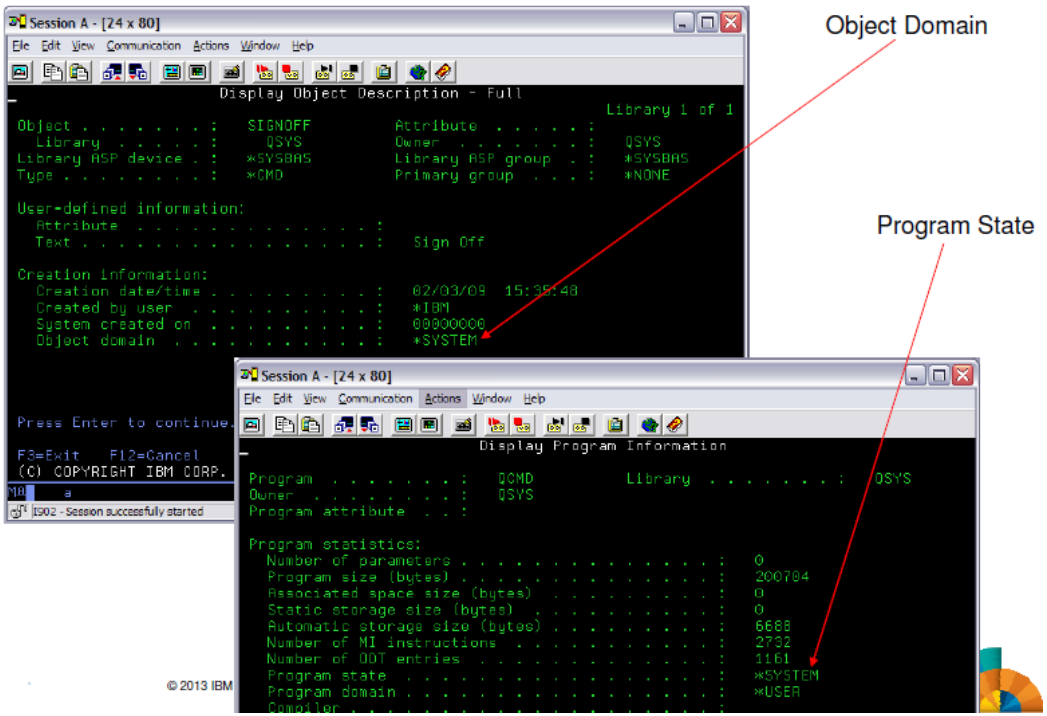
# Valeurs Système IBM i

- Intégrité
  - QSECURITY
  - QALWOBJRST
  - QFRCCVNRST
  - QVFYOBJRST
- Audit
  - QAUDCTL
  - QAUDLVL / QAUDLVL2
  - QAUDENDACN
  - QAUDFRCLVL
  - QCRTOBJAUD
- Autres : QA


- QALWUSRDMN - Consider value QTEMP
- QINACTITV - Set to a reasonable number of minutes
- QINACTMSGQ - *ENDJOB/*DSCJOB
- QMAXSIGN - Consider setting to 3
- QMAXSGNACN - Set to disable device and profile

# Intégrité IBM i

## Object Domain, Program State




Programs running *SYSTEM state can access both *USER and *SYSTEM domain.
Programs running *USER state can only access *USER domain objects.

# QSECURITY = 40 ou 50

## Hardware Storage Protection (HSP) - Object integrity

Program state is compared against object HSP to determine allowable access. Every object has a HSP value.

Object HSP attributes:

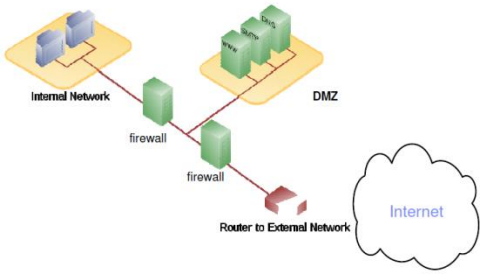
- Allow access from any state (no protection, *USRSPC, *USRQ, *USRIDX)
- Read only in any state (*PGM, *SRVPGM)
- No access in user state (Setting for most objects, 5.3 and prior)
- Enhanced storage protection (5.4 and beyond)

User written programs, running at security level 40 or 50, **MUST** use system interfaces (commands and APIs) to gain access to the objects.

- Authority checking is enforced by the system interface
- Parameter Validation is performed
- Object Domain checking is performed
- Object Hardware storage protection is performed

Direct access by user programs to system objects is not allowed at Security level 40 and 50 due to domain and hardware storage protection attributes.

# Réseaux




- SSL / VPN
- DDM/DRDA : **ADDSRVAUTE** USRPRF(profil_local) SERVER(QDDMDRDASERVER) USRID(profil_remote) PASSWORD(motdepasse)

## Host Based Intrusion Detection/Prevention – 5.4 & 6.1

- **Enable Intrusion detection support on your host system.**
  - Detect "internal" attacks on your systems
- **Real time notification enablement**
  - E-mail, messages, etc. (i.e., pagers, ISV solutions) in addition to IM records
- **Numerous intrusion events audited** – well-known attacks such as "Smurf", "Fraggle", ACK storms, Address Poisoning (both IPv4 ARP poisoning, and IPv6 neighbor discovery poisoning), Ping-Of-Death and many more….
- **"Extrusions" detected** – attacks, scans, traffic regualtion anomalies emanating from your host
- **IPv6 support**
- **GUI – iNav**
  - Management of IDS policies
  - Display of intrusion events as an alternative to viewing the audit journal

## General TCP/IP Security Tips

- Only start TCP/IP servers that are needed
- Prevent applications from using well-known ports
- Turn *IP Source Routing* off
- Allow *IP Datagram Forwarding* only when needed
- Don't leave PPP or SLIP lines waiting in answer state

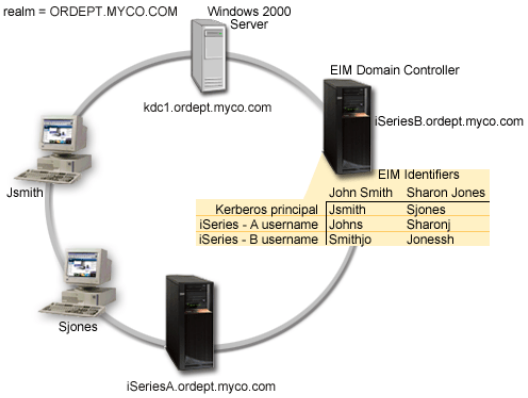
# **Bonnes pratiques** de sécurité sous IBM i

1. La sécurité informatique n'est pas seulement une question technique
2. Périmètre IBM i
3. Avoir conscience des spécificités IBM i et bâtir son projet de sécurité
4. Intégrité Système & Réseau
5. **Gestion des Profils & des Droits**

# Gestion des profils utilisateur

**Bonnes pratiques :**

- Un profil utilisateur = une personne physique = un mot de passe
- Gérer les profils et mots de passe
  - Péremption, Suspension, Suppression, …
  - Attention aux profils particuliers (produits, formation, prestataires, …)
- Attribuer des droits correspondant au besoin et utiliser les profils de groupe
- Ne pas utiliser les profils système : PWD(*NONE) pour QUSER, QPGMR, QSYSOPR
- Accorder des droits spéciaux uniquement quand c'est strictement nécessaire, avec justification et limitation dans le temps
- Gestion des Environnements
  - Pas de développement/test en environnement de production
  - Accès restreint des développeurs à la production
  - Attention aux environnements de secours …



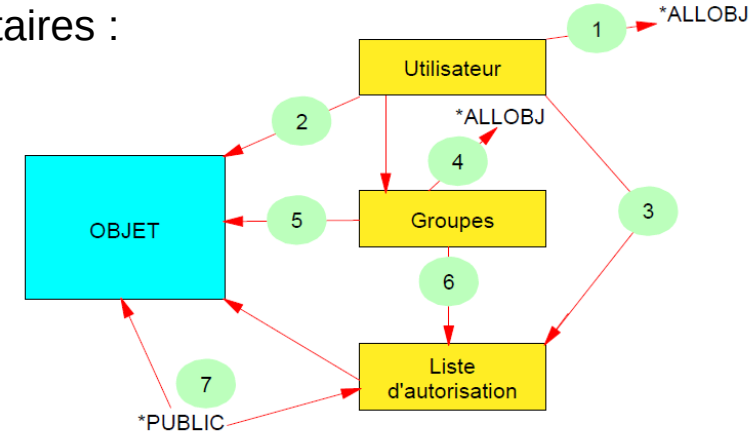

**« Goodies »**

- SSO : EIM, …
- Droits spéciaux temporaires
- Anonymisation des environnement de tests

# Gestion des droits

| | *OBJOPR | *OBJMGT | *OBJEXIST | *OBJALTER | *OBJREF | *READ | *ADD | *UPD | *DLT | *EXECUTE |
|---|---|---|---|---|---|---|---|---|---|---|
| *ALL | X | X | X | X | X | X | X | X | X | X |
| *CHANGE | X | | | | | X | X | X | X | X |
| *USE | X | | | | | X | | | | X |
| *EXCLUDE | | | | | | | | | | |

- Plusieurs méthodes, éventuellement complémentaires :
  - Droits publics
  - Droits privés
  - Liste d'autorisation
  - Profil de groupe
  - Adoption de droits (non valable pour l'IFS)
  - Swap




- Et le plus difficile : **maintenir cette sécurité à jour**. Attention aux nouvelles versions et patchs qui entrainent des régressions ou aux dérogations temporaires qui durent …
- Attention aux Back Door utilisant l'adoption de droits !

# Commandes

CHGUSRPRF USRPRF(xxxx) LMTCPB(*YES)

*L'utilisateur ne peut pas exécuter de commande depuis la ligne de commande.*

CHGCMD CMD(xxxx) ALWLMTUSR(*YES)

*Si une commande est définie avec ALWLMTUSR(*YES), elle pourra être exécutée depuis la ligne de commande, même par un utilisateur dont le profil est LMTCPB(*YES).*

# Attention aux fonctions C/S

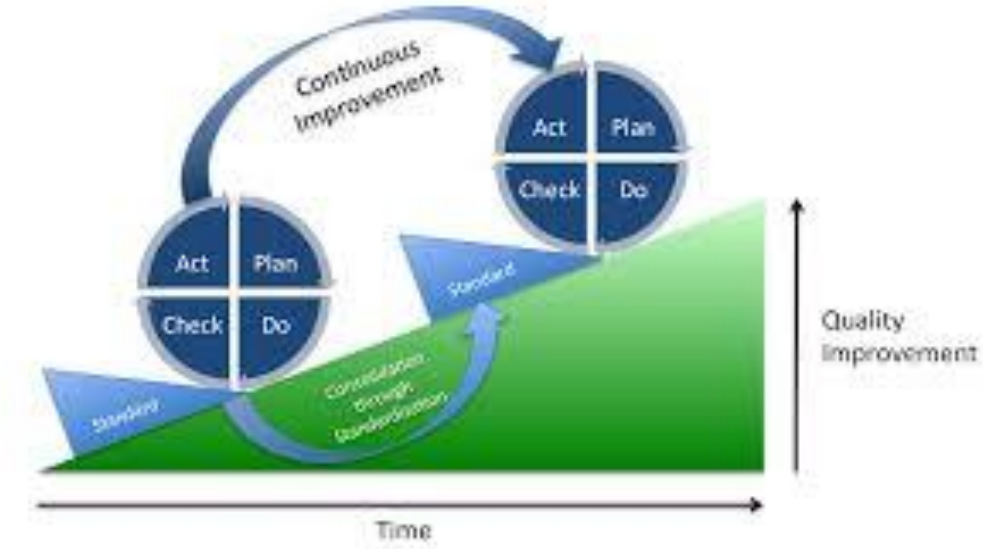
| | |
|---|---|
| 5250 | ***dspsysval qdate*** |
| FTP Server | Quote Rcmd ***dspsysval qdate*** |
| REXEC | RUNRMTCMD CMD('***dspsysval qdate***')<br>RMTLOCNAME(system *IP) RMTUSER(user) RMTPWD( ) |
| Client Access | Rmtcmd //system ***dspsysval qdate*** |
| ODBC / DRDA | CALL QSYS.QCMDEXC ('***dspsysval qdate***', 0000000015.00000) |
| Iseries Navigator | cl:***dspsysval qdate*** |
| DDM | SBMRMTCMD CMD('***dspsysval qdate***') DDMFILE(library/DDMfile) |

# **Bonnes pratiques** de sécurité sous IBM i

1. La sécurité informatique n'est pas seulement une question technique
2. Périmètre IBM i
3. Avoir conscience des spécificités IBM i et bâtir son projet de sécurité
4. Intégrité Système & Réseau
5. Gestion des profils & des droits
6. **P * D * C * A**

# Objectif : amélioration continue

- Sécurité = projet « permanent »
- Intégrer les évolutions de l'environnement
  - Risques
  - Solutions & Technologies

# IBM i V6R1

- Chiffrage des données pour répondre aux obligation légales
  - Sauvegardes réalisées par BRMS (sur bandes ou bandes virtuelles)
    - Option 44 de i5/OS : Encrypted Backup Enablement
  - Chiffrage des données sur disques, uniquement dans les ASP (ASP utilisateurs, iASP)
    - Option 45 de i5/OS : Encrypted ASP Enablement
  - Utilisation de l'algorithme "AES symmetric key"

- Détection et prévention des tentatives d'intrusion
  - Avertissement en temps réel via e-mail ou pagers, audit amélioré, gestion intégrée via Navigator for i5/OS
  - Arrêt progressif des postes de travail à l'origine d'une tentative de "Denial of Service"

- Renforcement de l'intégrite de l'OS lui-même
  - Tous les modules i5/OS exécutables sont signés électroniquement
  - Elimination des programmes modifiés : génération automatique d'un nouveau code machine pour tous les modules i5/OS exécutables


# IBM i V7R1

- DB2 : chiffrage de colonnes
- TR4 : LIVE PARTITION MOBILITY

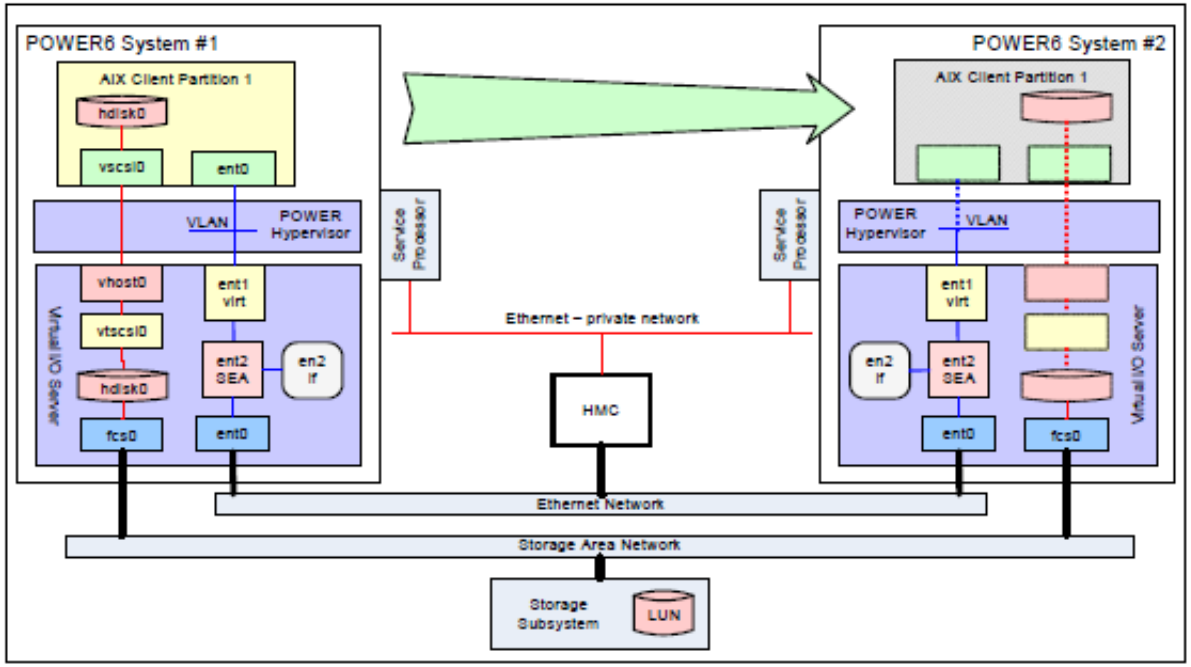



*Figure 1-2 A mobile partition during migration*

# IBM i V7R2

- **Jusqu'à aujourd'hui :**
  - Pour donner ou révoquer des privilèges, il faut  les avoir pour soi-même :
    - Propriétaire ou droit de gestion sur objet
    - *ALLOBJ special authority (*ALLOBJ)

- **IBM i 7.2 :** Nouveau
  - *Security administration function usage (QIBM_DB_SECADM) will be able to grant or revoke privileges on any object to anyone*
    - *Regardless of whether they have any of the above privileges.*
  - *Users may be authorized to manage security*
    - *BUT NOT BE AUTHORIZED TO SEE OR MODIFY THE DATA.*
  - *Note that:*
    - *A security administrator cannot grant data privileges to himself…only to others.*
    - *Only QSECOFR or another security administrator can grant the security administrator function usage.*

# IBM i V7R2 : DB2 Row and Column Access Control

```
CREATE MASK SSN_MASK ON EMPLOYEE
      FOR COLUMN SSN RETURN
        CASE
          WHEN (VERIFY_GROUP_FOR_USER(SESSION_USER,'PAYROLL') = 1)
            THEN SSN
          WHEN (VERIFY_GROUP_FOR_USER(SESSION_USER,'MGR') = 1)
            THEN 'XXX-XX-' CONCAT SUBSTR(SSN,8,4)
          ELSE NULL
        END
      ENABLE;

ALTER TABLE EMPLOYEE
    ACTIVATE COLUMN ACCESS CONTROL;
```

```
CREATE PERMISSION NETHMO.ROW_ACCESS
ON HOSPITAL.PATIENT
FOR ROWS
WHERE(VERIFY_GROUP_FOR_USER(SESSION_USER,'PATIENT') = 1 AND
          HOSPITAL.PATIENT.USERID = SESSION_USER) OR
          (VERIFY_GROUP_FOR_USER(SESSION_USER,'PCP') = 1 AND
           HOSPITAL.PATIENT.PCP_ID = SESSION_USER) OR
          (VERIFY_GROUP_FOR_USER(SESSION_USER,'MEMBERSHIP') = 1 OR
          VERIFY_GROUP_FOR_USER(SESSION_USER,'ACCOUNTING') = 1 OR
          VERIFY_GROUP_FOR_USER(SESSION_USER,'DRUG_RESEARCH') = 1)   ENFORCED FOR ALL ACCESS
      ENABLE;


ALTER TABLE HOSPITAL.PATIENT
    ACTIVATE ROW ACCESS CONTROL;
```

# **Bonnes pratiques** de sécurité sous IBM i

1. La sécurité informatique n'est pas seulement une question technique
2. Périmètre IBM i
3. Avoir conscience des spécificités IBM i et bâtir son projet de sécurité
4. Intégrité Système & Réseau
5. Gestion des profils & des droits
6. P * D * C * A
7. **Conclusions**

# Et les autres, ils en sont où ?

PowerTech
your security expert

WHITE PAPER

## The State of IBM i Security **2012**

Are my Power Systems™ servers running IBM i (aka System i®, iSeries®, AS/400®) **compliant with government and industry security regulations?**

**Is my data secure** behind the walls of my Power Systems server? Are we able to **detect fraud, data theft, and other deceptive behavior?**

How do I secure my system in the **most efficient and economical way?**

If you're a senior executive or IT manager with responsibility for Power Systems running IBM i, then you're already familiar with these security-related questions. In response to these issues, PowerTech surveyed over 120 Power Systems servers (many from Fortune 100 companies) in 2011. The results, and the universal nature of IBM i vulnerabilities, led us to conclude that if you have IBM i systems in your data center, then your organization probably suffers from similar internal control deficiencies.

IBM i security projects often take a back seat to Windows- and UNIX-platform security, either because it is assumed that an IBM i server is already secure, or because the security professionals or auditors are unsure how to assess this system.

Our goal in releasing this annual study is to help executives, IT managers, system administrators, auditors, and compliance officers understand the important security exposures of IBM i servers and to provide answers to the questions that keep you up at night. >>>

The PowerTech Group, Inc.
www.powertech.com
TEL USA: 253.872.7788
TOLL FREE: 800.915.7700



**FIGURE 10: SYSTEM SECURITY LEVEL**

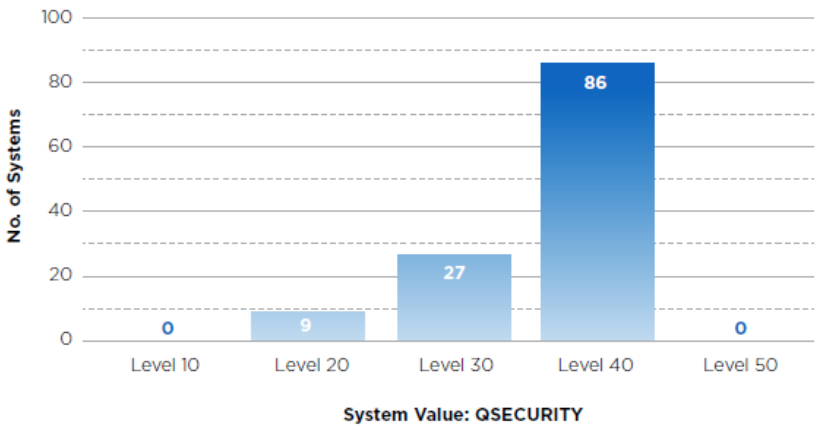



**FIGURE 9: SYSTEMS USING THE IBM I AUDIT JOURNAL**

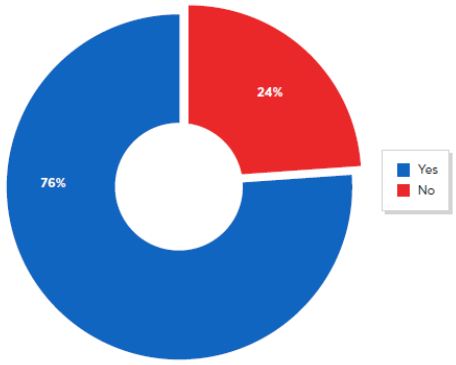



**FIGURE 8: EXIT PROGRAMS IN PLACE**

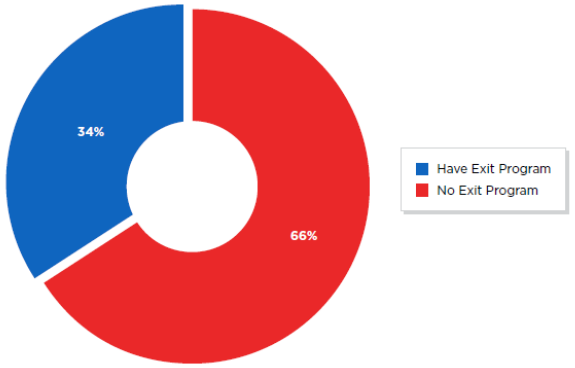


FIGURE 2: POWERFUL USERS (SPECIAL AUTHORITIES)

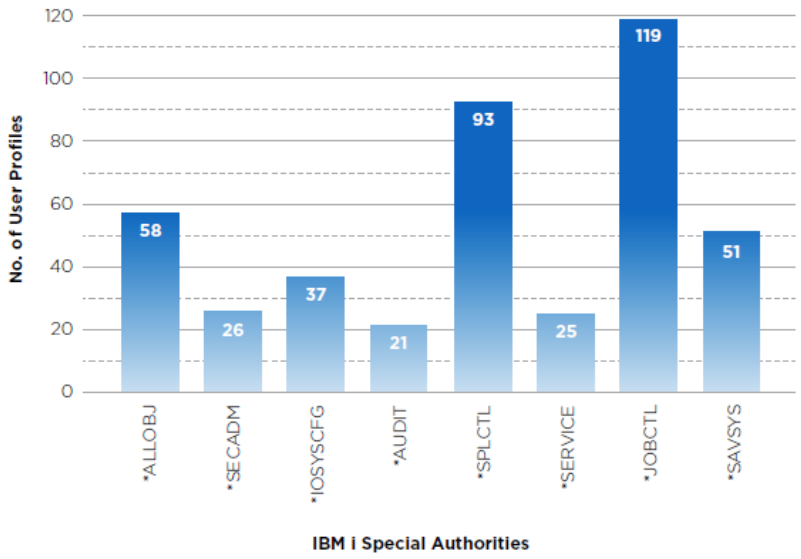



FIGURE 3: INACTIVE PROFILES

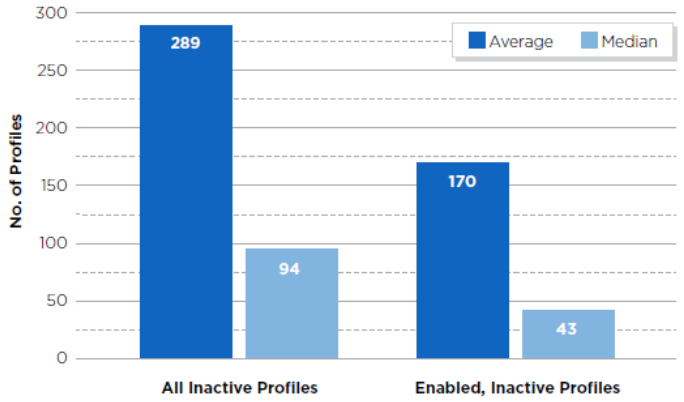



FIGURE 4: DEFAULT PASSWORDS

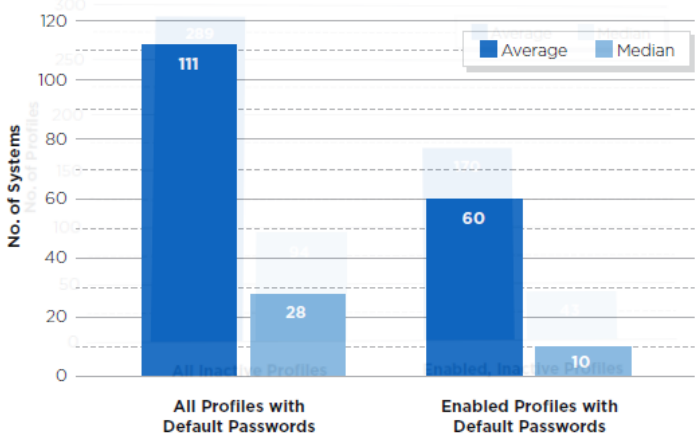
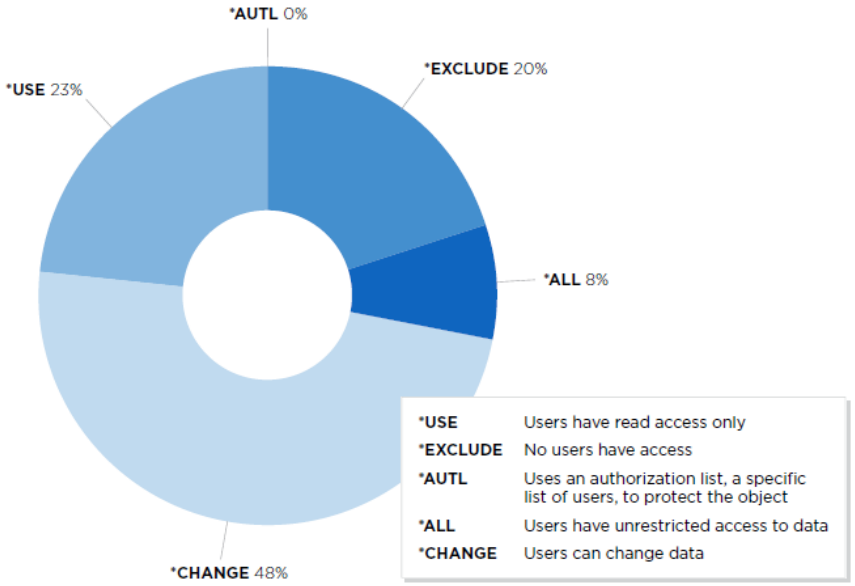
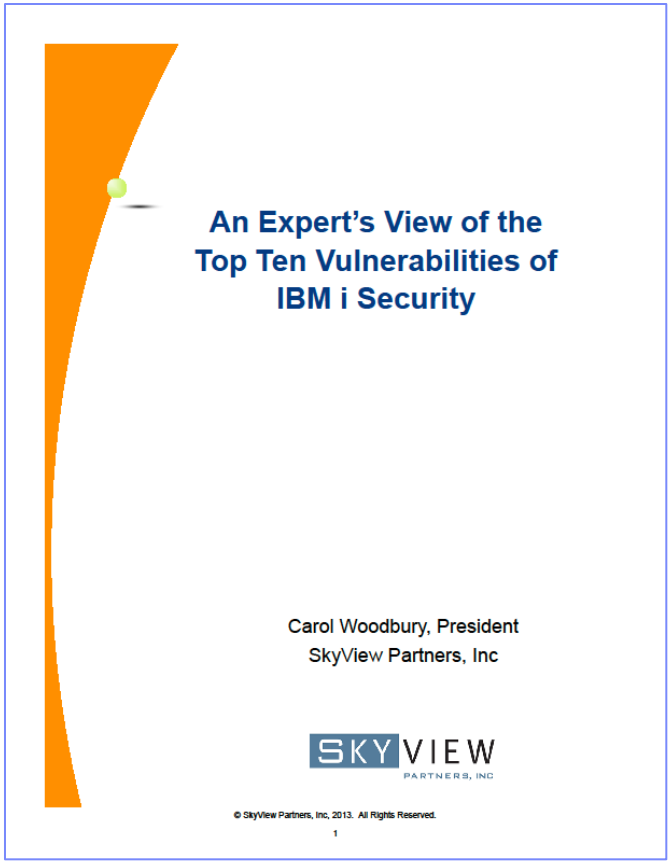



FIGURE 6: *PUBLIC AUTHORITY TO DATA



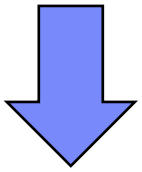
# Vulnérabilités

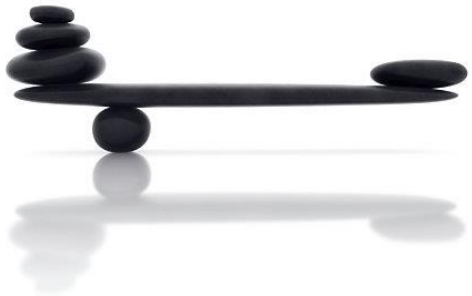
- http://www.youtube.com/watch?v=qKNb0CL3JkU



# Sécurité IBM i


- Vulnérabilités principales
  - Pas d'Audit (ou pas assez)
  - Valeurs système
  - Profils
    - Individuels / Groupe
    - inactifs
  - Fonctions C/S
  - Mots de passe (expirés, défaut, « faibles »)
  - Copies multiples des données
  - Trop d'autorités (droits spéciaux)
  - IFS (partage de Root, …)
  - Vision partielleSécurité « applicative »
- Du déni aux constats … avant les actions





# Conclusion