# Sécurisation des annuaires

Christian.Claveleira@CRU.fr

JRSSI 2010

# Risques liés aux annuaires de personnes

- Non conformité avec la réglementation
- Accès injustifié à des tiers à des données à caractère personnel
- Récupération de données à des fins commerciales
- Altération non autorisé de contenu

L'établissement est responsable de l'usage et de la protection de ses annuaires

# Périmètres

- Annuaires internes :
  - données professionnelles destinées aux personnels
  - Accessibles au sein de l'établissement
  - Dans certains cas accessibles depuis l'extérieur

Accès de type intranet

- Annuaires publics :
  - Sous-ensemble de l'annuaire interne
  - Accessibles depuis l'extérieur sans contrôle d'accès

Accès extranet -> les plus préoccupants

# Type d'accès

- Direct LDAP
  - Applications du SI
  - Carnets d'adresses d'outils de messageries individuels (Thunderbird, Evolution, Entourage, Outlook, Carnet d'adresses,...)
- Web
  - Consultation via un navigateur Web
  - L'annuaire est en back-end et n'est pas forcément LDAP (SQL par exemple)

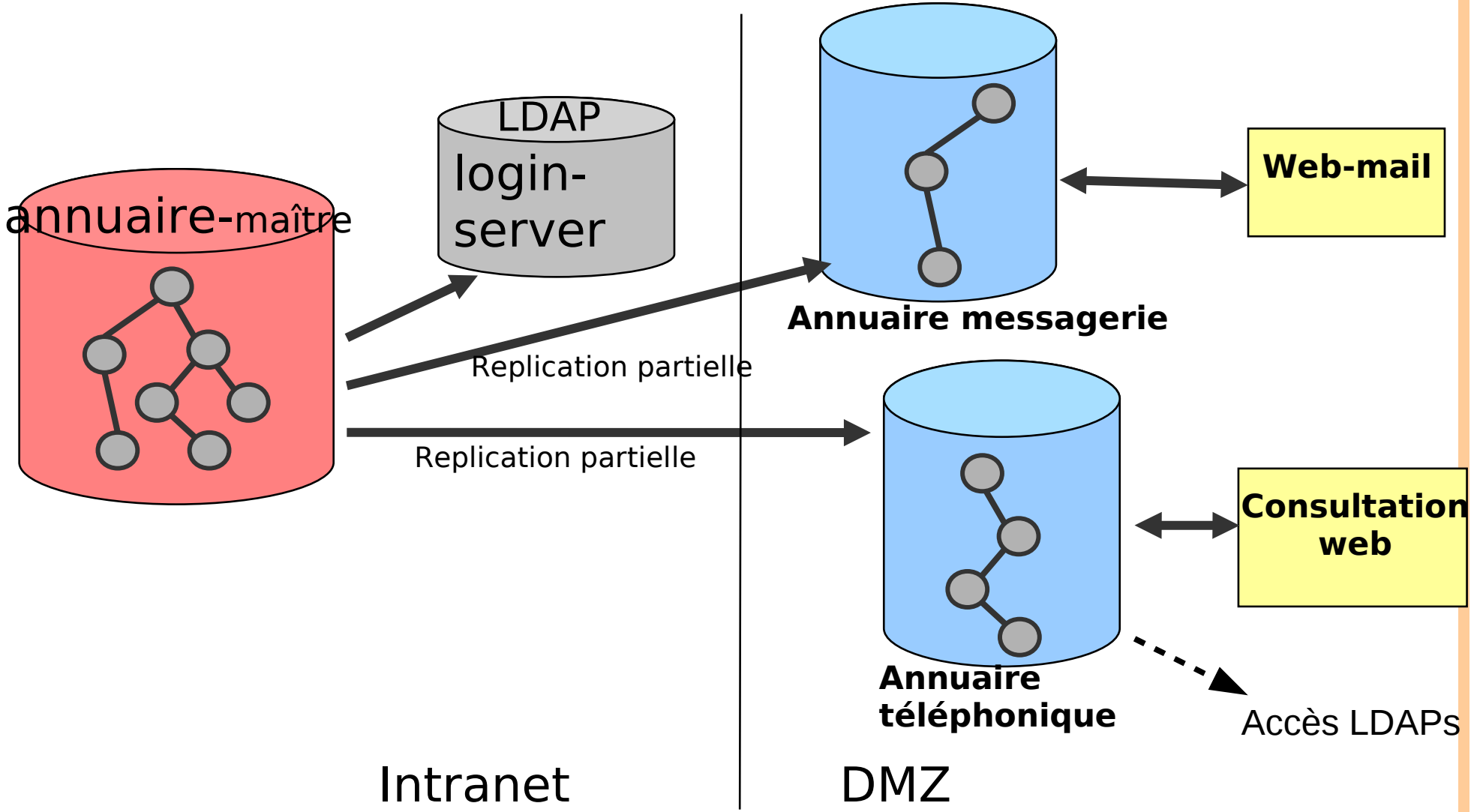
# Contrôle d'accès

- LDAP (SQL) : c'est au serveur de savoir qui a accès à quoi -> contrôle réseau, authentification, ACLs (gestion délicate)
- Web : le contrôle est fait à priori par l'interface d'interrogation et peut être renforcé par le back-end

# Conseils d'architecture

- Ne pas utiliser l'annuaire maître pour les applis de type pages blanches/jaunes
- Affecter un serveur dédié ne contenant qu'une réplication partielle de l'annuaire en DMZ
- Imposer un nombre maximum de réponses raisonnable au niveau du serveur
- Ne pas donner d'accès superflus à l'interface d'interrogation
- Si accès LDAP externe utiliser LDAPs et imposer une authentification

# Exemple d'architecture



# Le problème des jokers (wildcards)

- Permettent de faire des recherches sur une partie du nom (*dupon**)
- Très utiles mais peuvent faciliter l'aspiration de l'annuaire suivant
  - Le nombre de caractères minimum imposé dans la recherche
  - Le nombre de jokers permis (**pon**)
  - Le nombre maximum de réponse imposé par l'interface de consultation

# Le problème des jokers (suite)

– Certaines contraintes peuvent être illusoires :
  - Joker compté comme un caractère
  - Espace compté comme un caractère
  - Failles dans l'interface
  - automates d'interrogation rendant les limites caduques

# Recommandations pour un interface de consultation

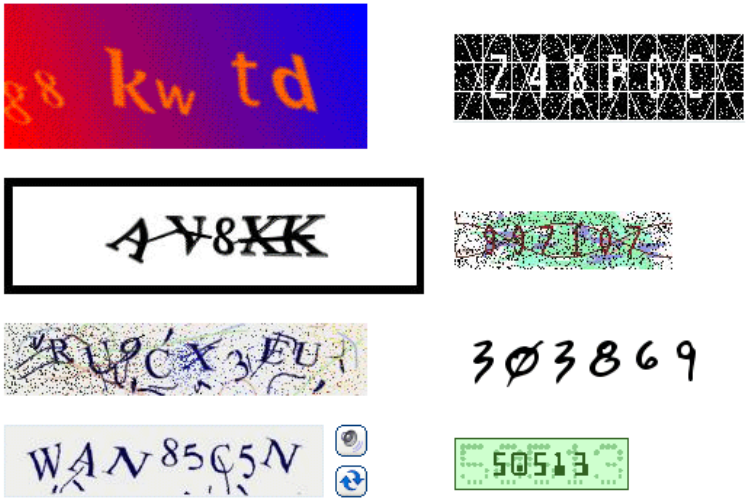
- Limiter le nombre de réponses renvoyées (est-ce utile d'en avoir plus de 10 ?)
  - Par l'interface
  - Par le backend (exemples : *sizelimit* pour OpenLDAP, *sql_select_limit* pour MySQLd)
- Imposer au moins 3 caractères significatifs (impossible au niveau du back-end ?)
- Attention aux paramètres exposés dans les URLs, aux injections SQL, aux erreurs verbeuses,...

# Recommandations pour un interface de consultation (suite)

- Limiter le nombre de requêtes par adresse IP
- Ne pas afficher directement les adresses mail
- Insérer des adresses piège et en surveiller l'utilisation
- Logger et surveiller l'activité de l'interface
- Utiliser un test de turing

# Test de turing

- Principe : poser une question à laquelle seul un humain peut répondre
- Exemple connu : CAPTCHA



- Des variantes plus simples peuvent être envisagées (cases à cocher, opération arithmétique,...)
- Attention aux problèmes d'accessibilité

# Conclusion

- Les interfaces de consultation d'annuaires sont parfois un peu « laxistes »
- Il existe divers moyens pour empêcher toute utilisation abusive
- La plupart sont simples à mettre en œuvre
- Au minimum : un serveur dédié ne contenant que les données nécessaires et une limitation stricte du nombre de réponses

# Questions ?