3TI
Sécurité des réseaux informatiques
2015-2016

Sécurité des bases de données et du Cloud Computing

V. Van den Schrieck

Analyse de la sécurité des BDD

1. Quels sont les avoirs à protéger?
2. Quelles sont leurs vulnérabilités?
3. Quels sont les risques?
4. Quelles sont les contre-mesures possibles?
5. Quels sont les risques résiduels?
6. Comment valider la politique de sécurité?

Difficulté dans la sécurisation des DB

- Complexité!
- SQL
- Personnel dédié
- Hétérogénéité

Injections SQL

```
var ShipCity;
ShipCity = Request.form("ShipCity");
var sql = "select * from OrdersTable where ShipCity = ‘"
+ ShipCity + "’";
```

Canaux d'injection

- Input utilisateur
- Variables du serveur
- Injection de second ordre
- Cookies
- Input physique

Attaques In-Band

- Tautologie : `SELECT info FROM user WHERE name= ' ' OR 1=1 -- and pwd = ' '`
- Commentaire de fin de ligne `--`
- Requêtes « piggybacked »

Attaque par inférence

- Requêtes illégales/Illogiques
  - Page d'erreur par défaut trop bavarde!
- Injection SQL à l'aveugle
  - Questions true/false, observation du résultat

Attaque Out-of-Band

- Utilisation d'un canal différent
  - Ex : Email
  - connectivité sortante laxiste

Contre-mesures

- Codage défensif
  - Validation de l'input
  - Insertion SQL contrôlée
  - SQL DOM : API/classes permettant la validation des types de donnée et l'échappement des input
- Détection
  - Sur base de signature
  - Sur base d'anomalie
  - Sur base d'analyse de code

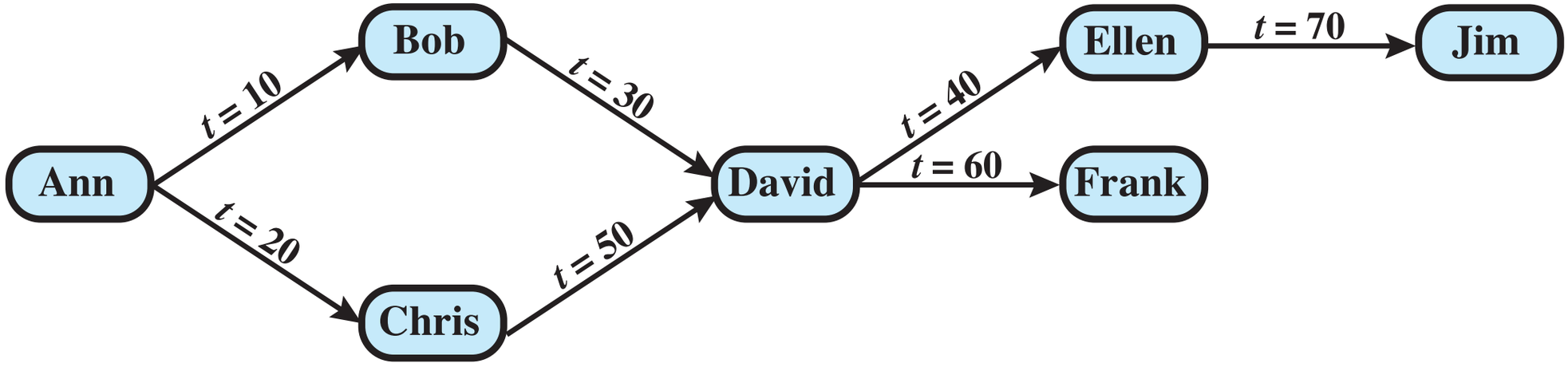
Contrôle d'accès aux DB

- Administration centralisée
- Administration par le propriétaire
- Administration décentralisée

Définitions des accès avec SQL

```
GRANT  {privileges|role}
 [ON   table]
TO {user|role|PUBLIC}
 [IDENTIFIED BY password]
 [WITH GRANT OPTION]
```

Autorisations en cascade



DB RBAC

- Trois catégories « naturelles » :
  - Propriétaire de l'application
  - Utilisateur final de l'application
  - Administrateur
- Ex : Microsoft SQL Server
  - Fixed Server Roles
  - Fixed DB Roles
  - User-defined Roles

Inférence

Name	Position	Salary ($)	Department	Dept. Manager
Andy	senior	43,000	strip	Cathy
Calvin	junior	35,000	strip	Cathy
Cathy	senior	48,000	strip	Cathy
Dennis	junior	38,000	panel	Herman
Herman	senior	55,000	panel	Herman
Ziggy	senior	67,000	panel	Herman

(a) Employee table

Position	Salary ($)
senior	43, 000
junior	35,000
senior	48,000

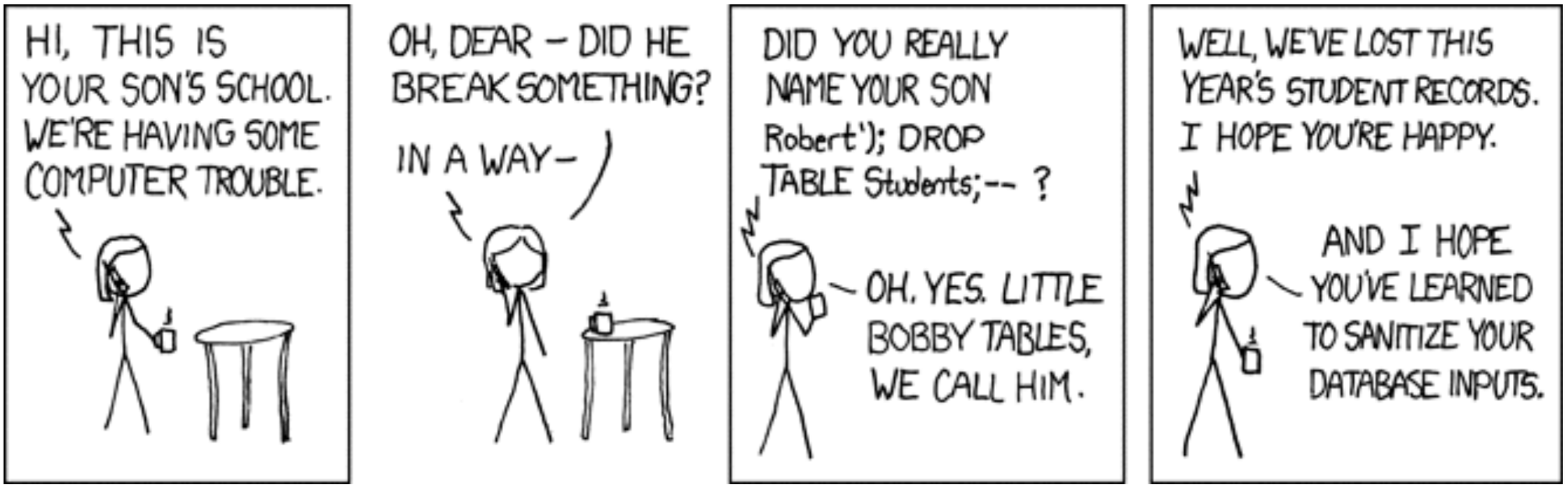
Name	Department
Andy	strip
Calvin	strip
Cathy	strip

(b) Two views

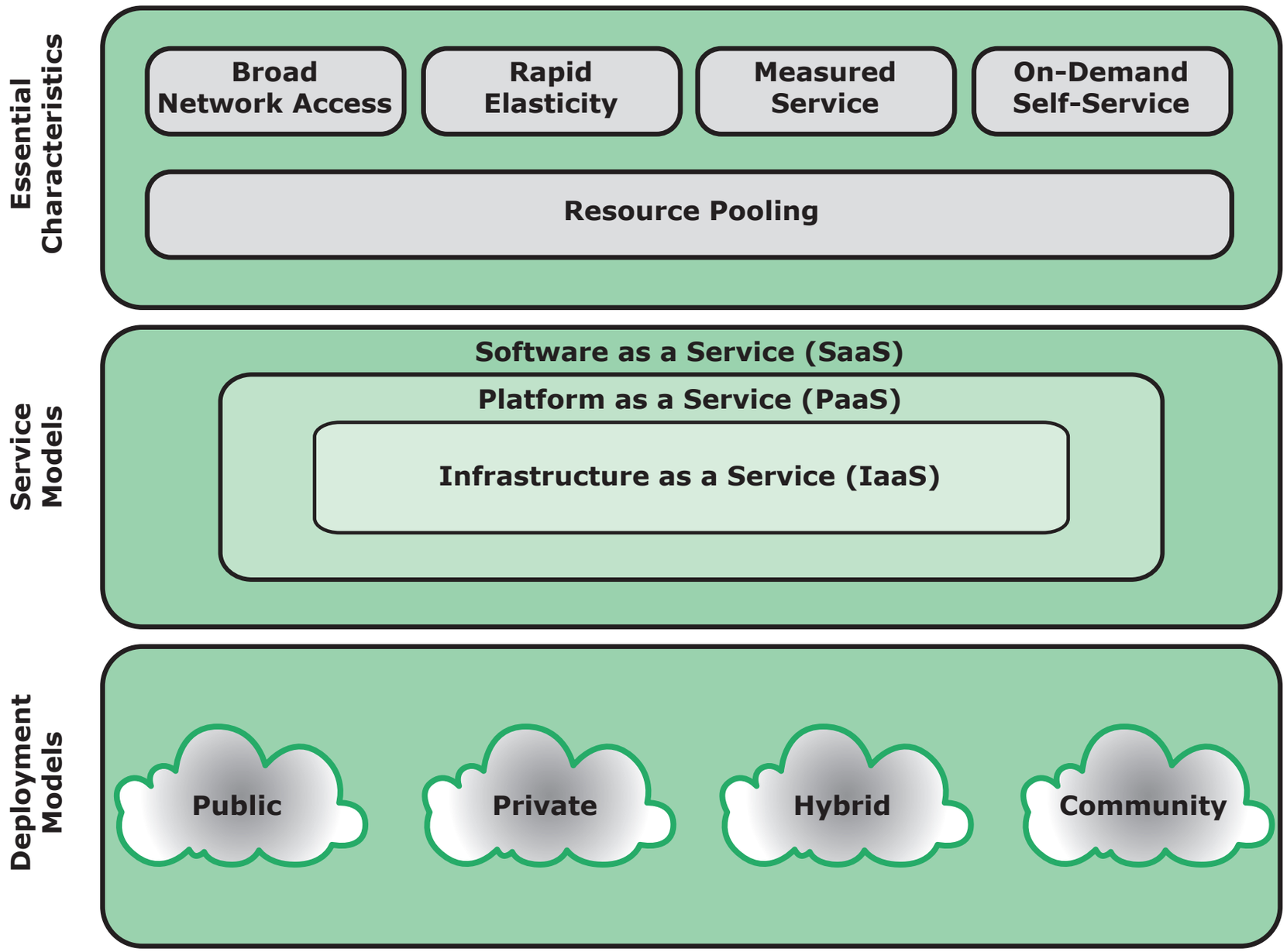
Chiffrement des DB

- Granularité : DB? Ligne? Colonne? Champ?

- Inconvénients :
  - Gestion des clés
  - Manque de flexibilité


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR - DID HE BREAK SOMETHING?
IN A WAY-
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Cloud Computing



Risques de sécurité du Cloud

- Quels sont les risques liés à l'utilisation du Cloud?

Cloud Security as a Service

- Authentification
- Anti-virus/malware/spyware
- Détection d'intrusion
- Prévention de la perte de données
- Business Continuity et Disaster Recovery
- …

Pour la semaine prochaine

- Recherche préliminaire sur les malwares
  - Listez les types de malware et expliquez-les brièvement