DJ HACK: Distributed Java HAsh craCKer

Proyecto de fin de carrera dirigido por Pablo González Nalda

Unai Gómez Velasco

Depto. de Lenguajes y Sistemas Informáticos

27 de septiembre de 2010

Introducción

Objetivo: desarrollo de una aplicación capaz de realizar ataques hash criptográficos mediante entornos distribuidos.

Finalidad: Proporcionar una herramienta sencilla pero completa para realizar auditorías.

Contenidos de la presentación

Conceptos básicos de la fuerza bruta

- Definición: Metodología encargada de la ruptura de claves mediante la comprobación de todas las combinaciones posibles.
- Elementos:
  - Longitud la clave $\Longrightarrow$ n
- Alfabeto $\Longrightarrow$ b
- Complejidad: b^n combinaciones posibles

Diseño del algoritmo de la fuerza bruta

- Finalidad: La generación de combinaciones
- Metodologías posibles de implantación
  - Recursividad
  - Iteración

Conceptos

Las palabras clave en la explicación del proyecto son:

- Palabra matemática: Array en $base_{longitudDiccionario}$
- Intervalo: El número mínimo de palabras a procesar.
- Palabra auxiliar: Palabras de corte a desplegar

Generación de palabras auxiliares

Se debe de establecer:

1. Un intervalo
2. La longitud de la palabra
3. El alfabeto a utilizar

Realiza una suma sucesiva en base a la longitud del alfabeto

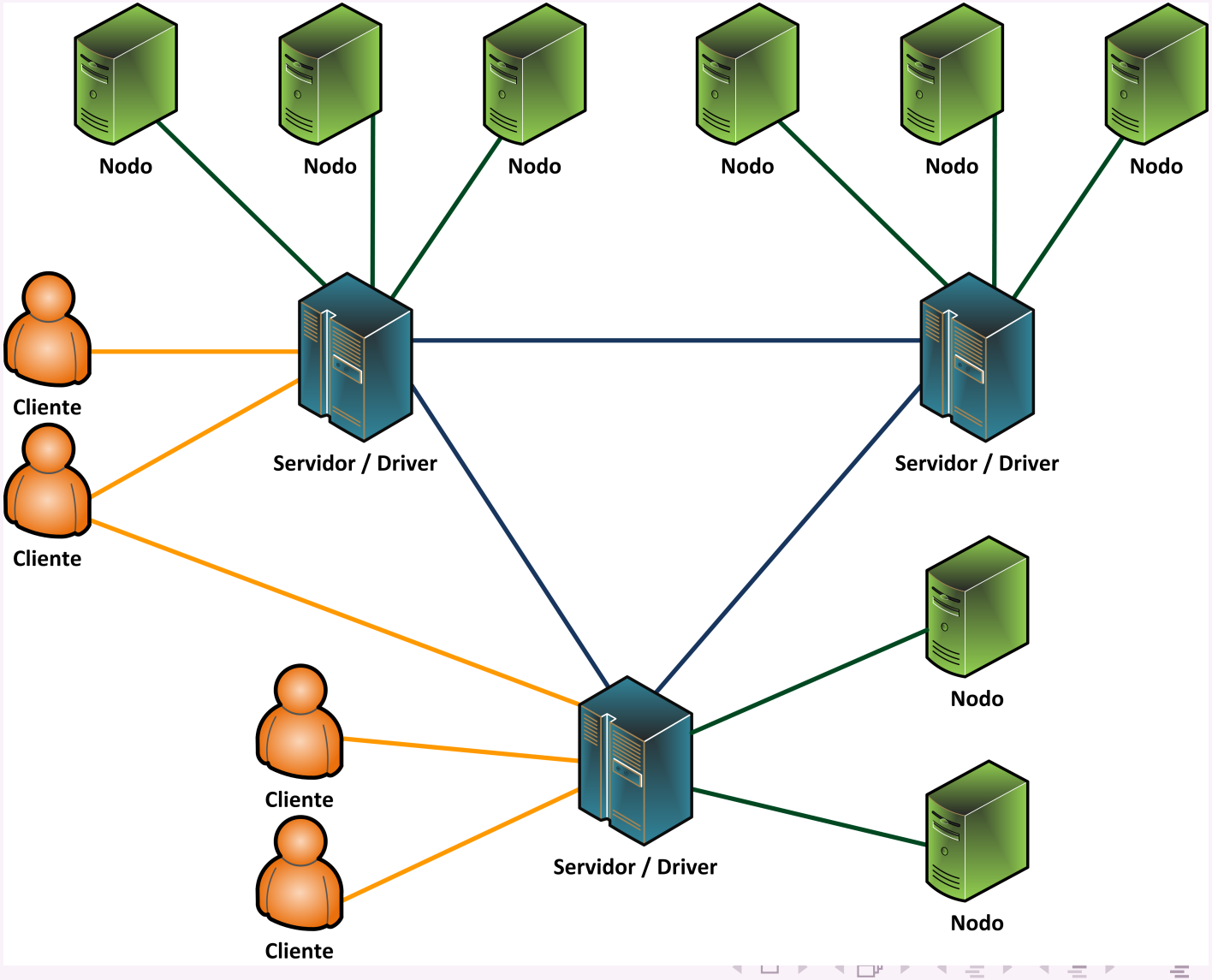
Se obtiene un conjunto de palabras auxiliares

Estructuras en JPPF

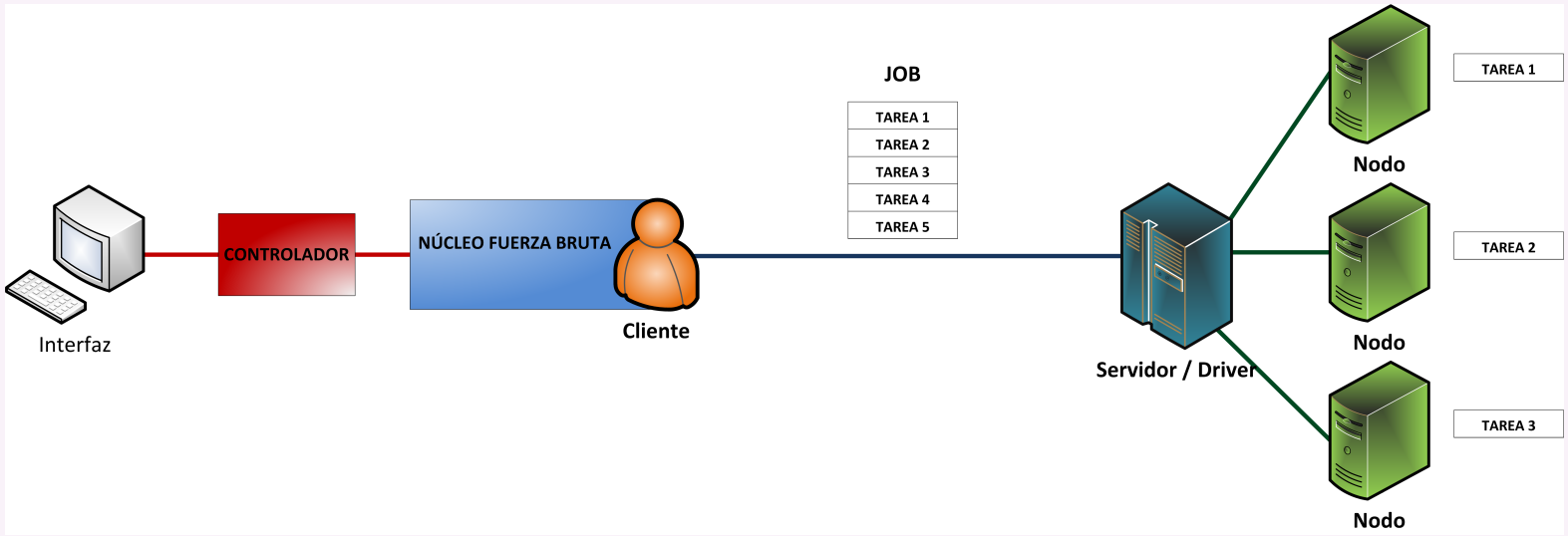
JPPF se compone de dos estructuras de datos elementales:

- task o tarea
- Job o trabajo

Topología de la red en JPPF



Adaptación de JPPF a DJ HACK



Instalación del MemoryDataProvider

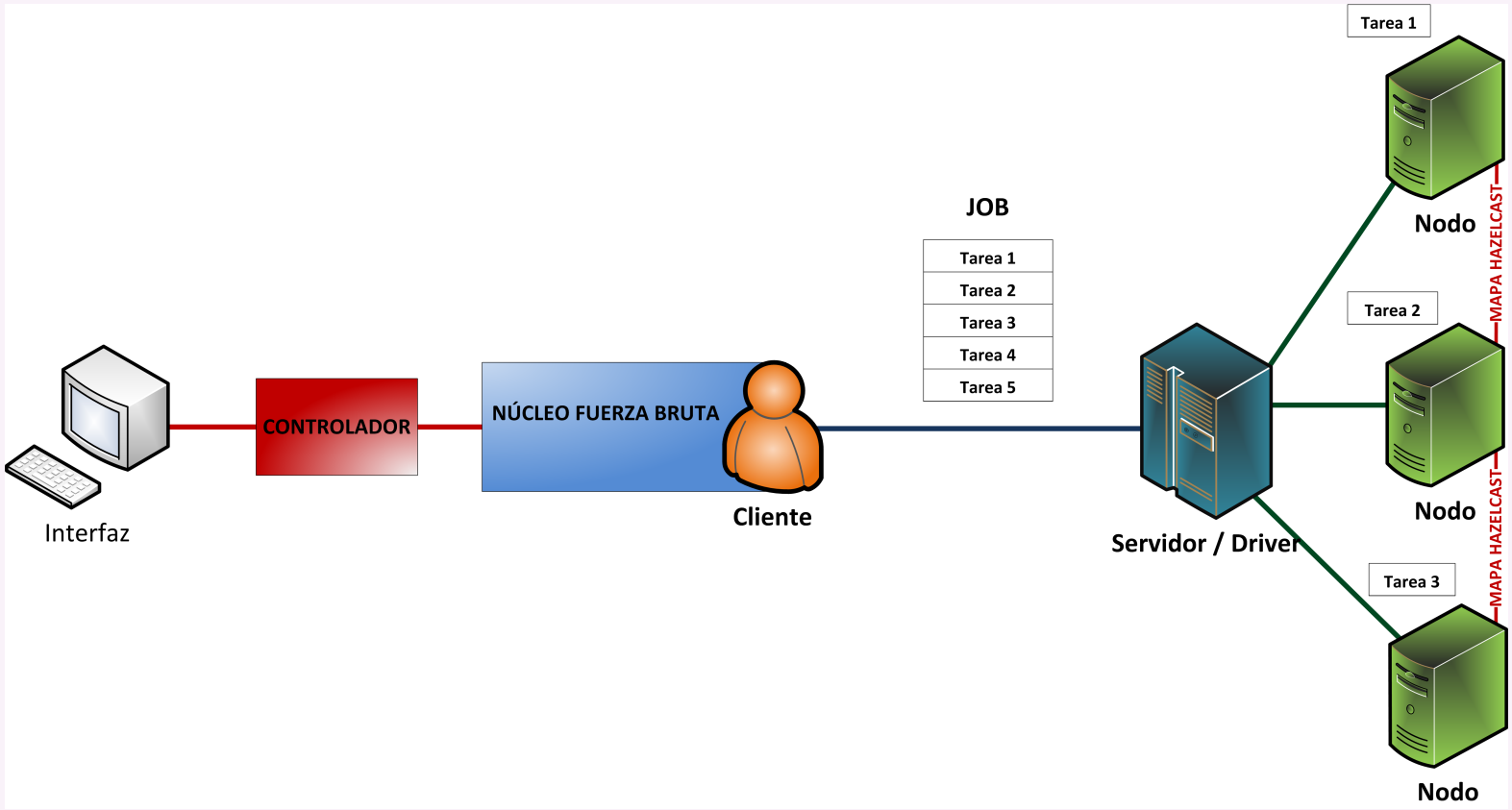
Elementos comunes a todas las tareas, no tienen por qué transmitirse constantemente.

- Alfabeto
- Intervalo
- Longitud de las claves

Uso del proveedor de datos en memoria.

- Despliegue y serialización de objetos, en el envío de un trabajo
- Agiliza el tráfico de la red

Adaptación de JPPF a DJ HACK



Tolerancia a fallos

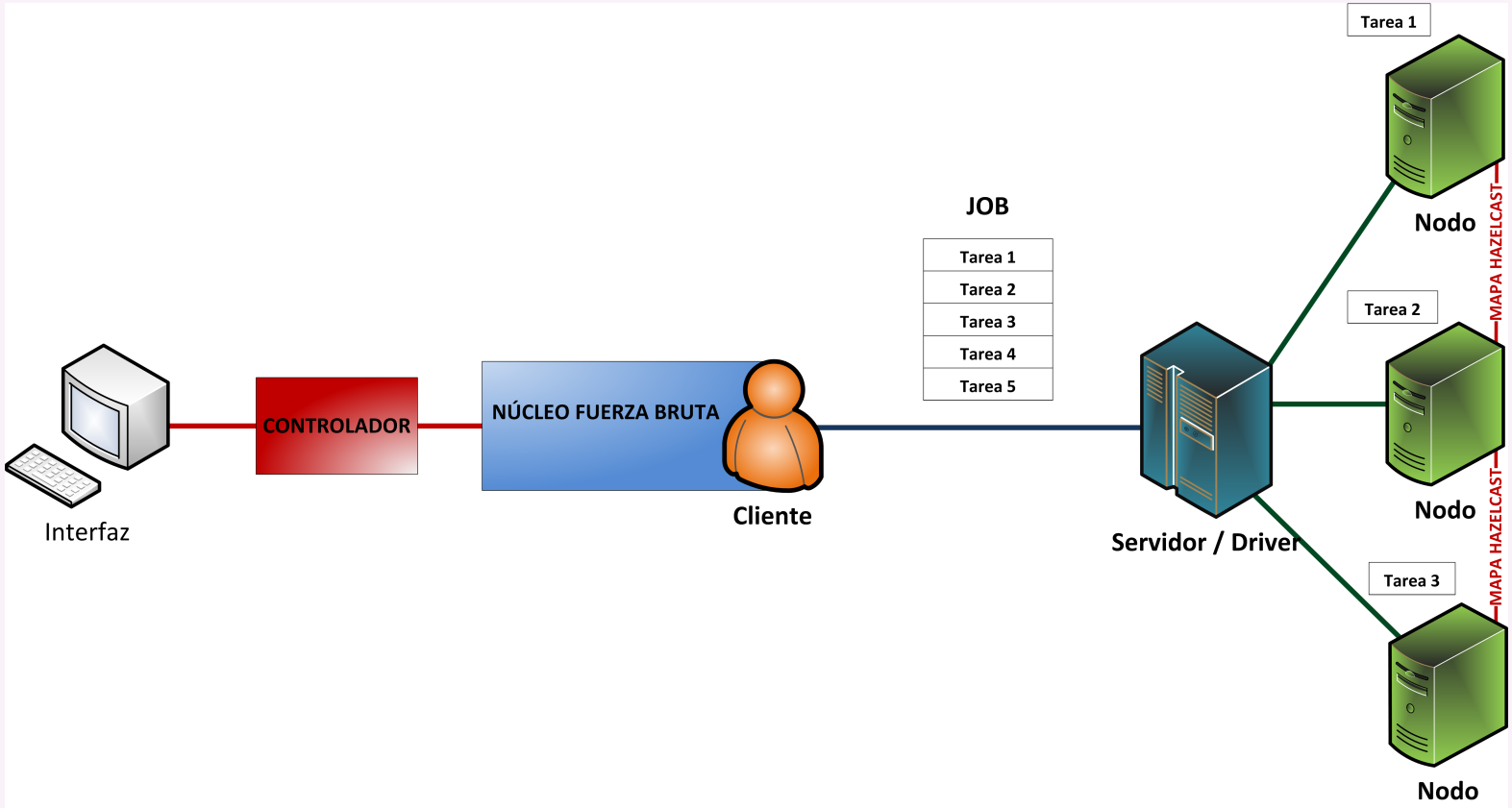
Posible caída total de la red, implica:

- Eliminación del mapa distribuido de Hazelcast

Solución: Conexión con la base de datos por nodo.

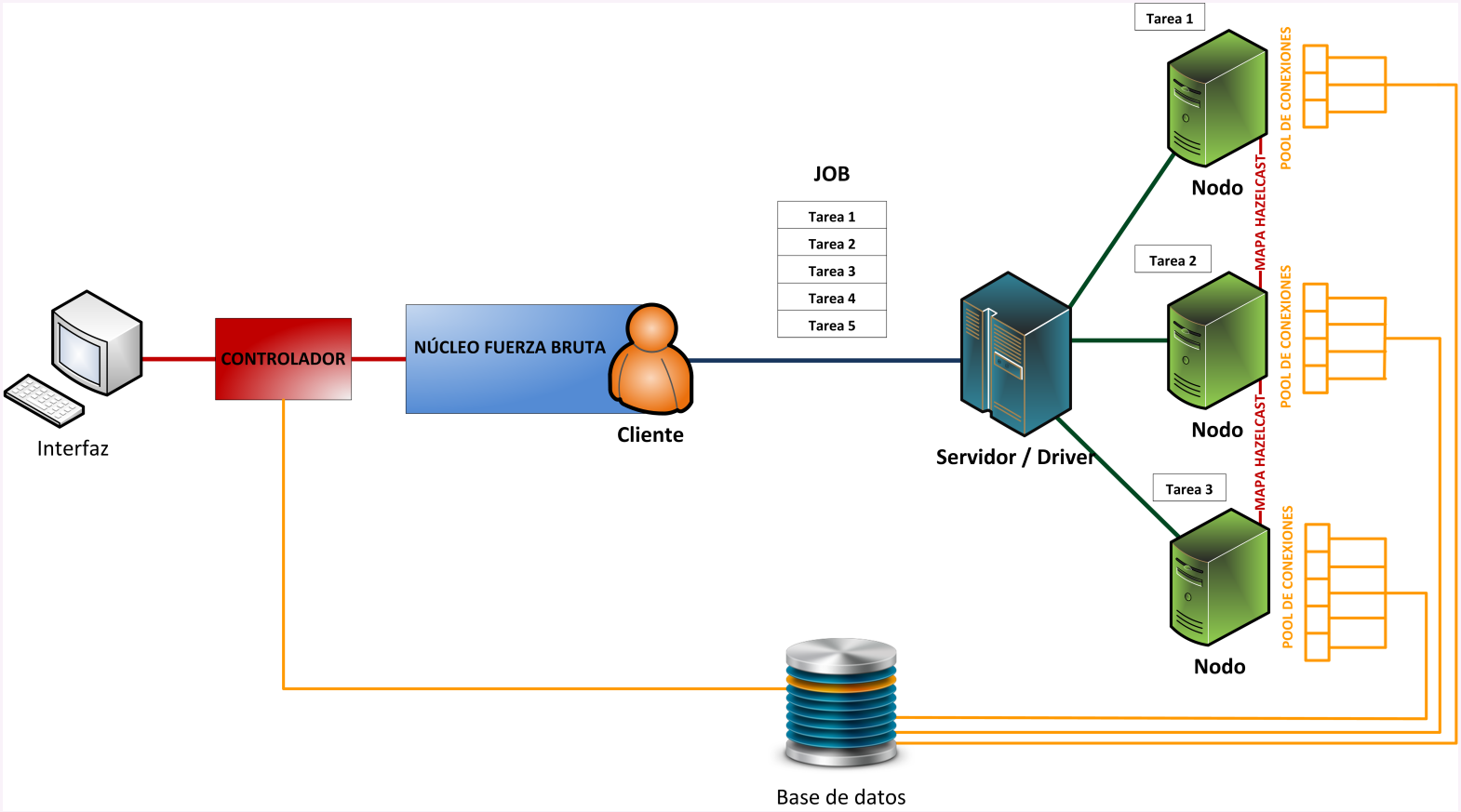
- Problemas de concurrencia entre procesos.
  - Soluciones:
    - Sincronización entre procesos, implica, rendimiento lento.
    - Pool de conexiones

Pool de conexiones



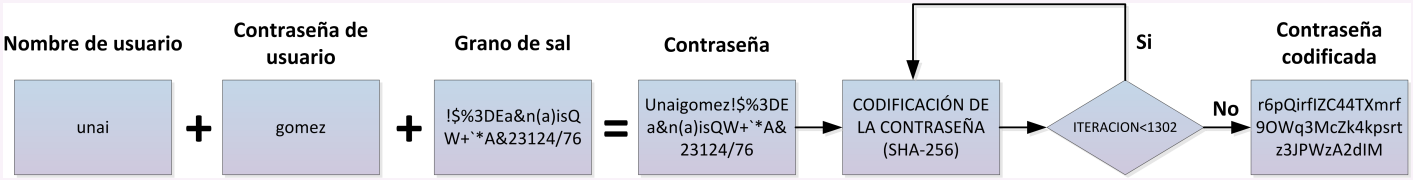
Problemática: Datos relevantes al descubierto

Seguridad en la red



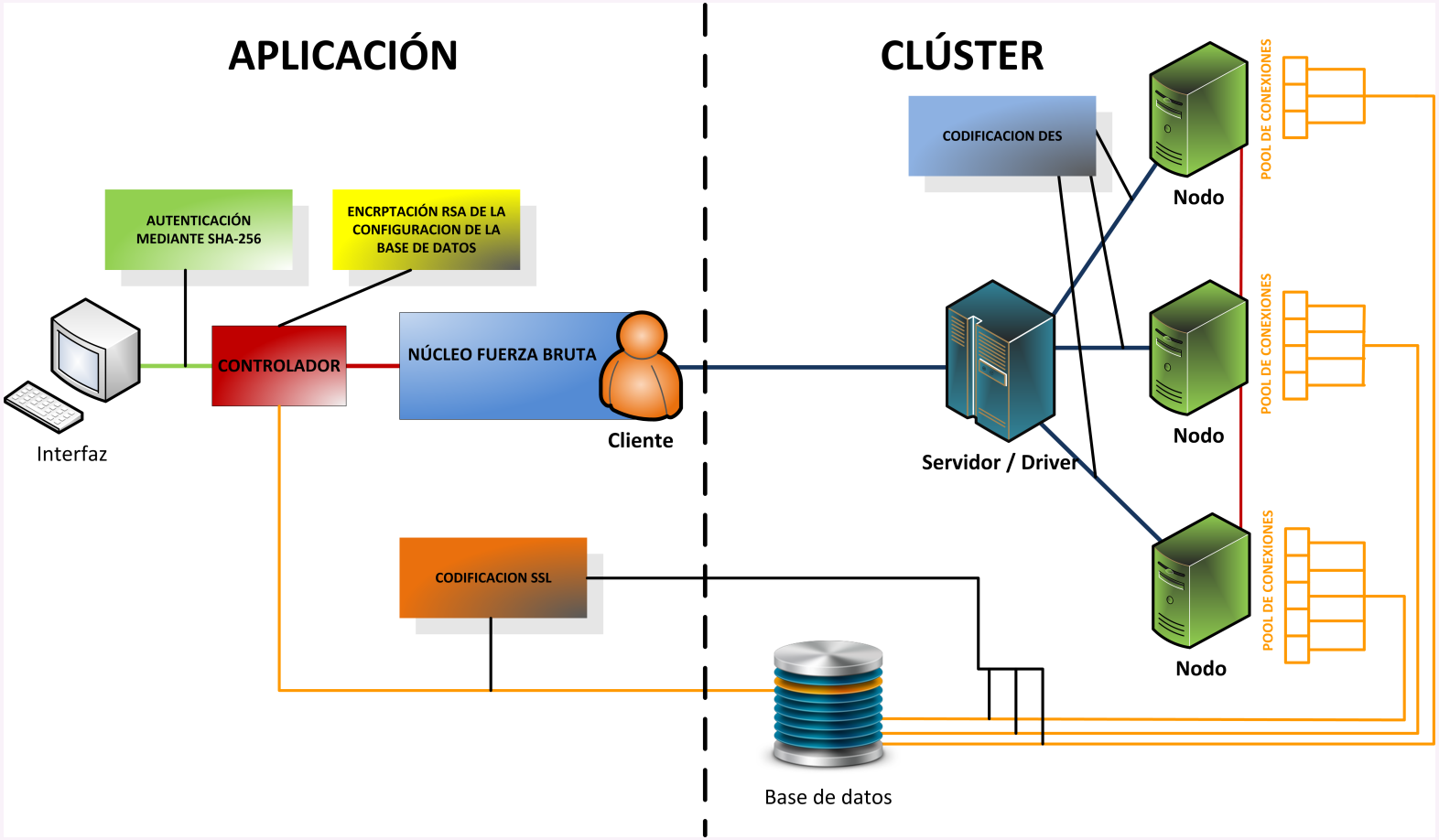
Mecanismos de seguridad

- Autenticación de usuario mediante digestores.



- Encriptación PBE de parámetros de acceso a la base de datos
  - RSA

Diagrama de red



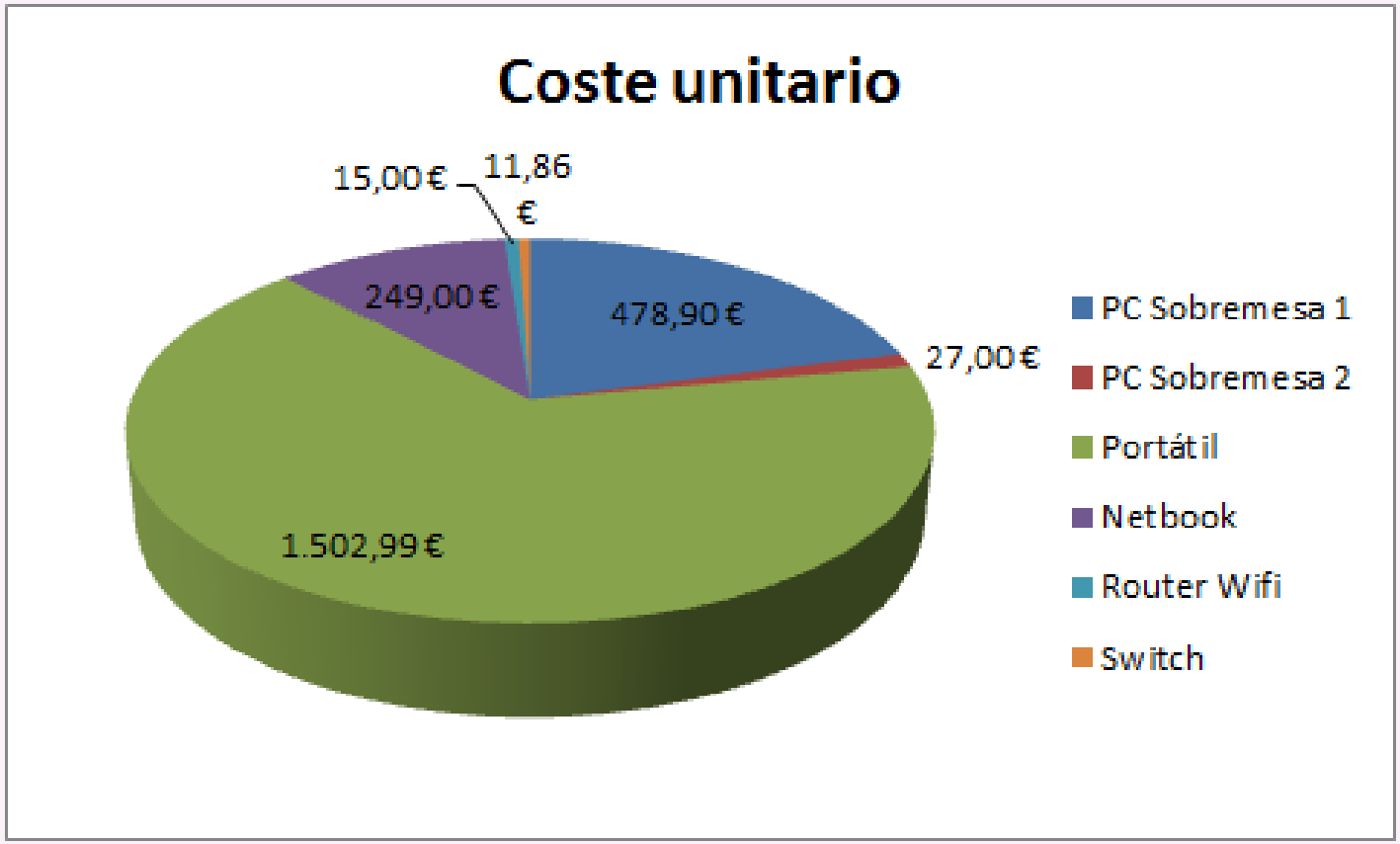
Herramientas y funcionalidades extra

- Capacidad de realizar ataques por diccionario
- Hasheo de claves
- Creación automatizada de nodos y servidores
- Monitorización del clúster en tipo real
- Multiplexación de puertos TPC

Recursos humanos

Concepto	**Tasa estándar**	**Tasa horas extra**
Desarrollador	5,30 €/hora	7,15 €/hora

Recursos materiales hardware



Recursos materiales

Concepto	Coste unitario	Núm. De licencias
MS Project 2010	775,00 €	1
MS Visio 2010	330,00 €	1
Antivirus Nod32	39.95 €	2
Kubuntu Linux	0,00 €	2
Apache Ant	0,00 €	4
NetBeans 6.9.1	0,00 €	1
MySQL Sever 5.1	0,00 €	1
MySQL GUI Tools	0,00 €	1
IPTools 1.98	0,00 €	1

Cuadro: Recursos materiales (Software).

Recursos materiales II

Concepto	Coste unitario	Núm. De licencias
TeXnicCenter 1.0	0,00 €	1
Ghostscript 8.71	0,00 €	1
GWView 4.9	0,00 €	1
MiKTeX	0,00 €	1
Gimp 2.6	0,00 €	1
Biblioteca Swing	0,00 €	1
Biblioteca Jasypt	0,00 €	1
JPPF Framework	0,00 €	1
Hazelcast Framework	0,00 €	1

Cuadro: Recursos materiales (Software).

Presupuesto

Concepto	**Importe**
Recursos de trabajo	4706,4 €
Recursos materiales	57,90 €
Amortizaciones	214,38 €
Total	**4.978,68 €**
Gastos Generales (10 %)	497,86 €
Beneficio (15 %)	746,81 €
Subtotal	**6.223,35 €**
IVA (18 %)	1.120,21 €
Total	**7.343,56**

Cuadro: Presupuesto

Contenidos

Resultados: viabilidad de un desarrollo técnico en los ataques de fuerza bruta distribuidos

Se ha construido una aplicación capaz de

- realizar ataques de fuerza bruta en entornos distribuidos de manera sencilla
- realizar ataques de diccionario
- crear cada componente del grid forma personalizada y totalmente automatizada
- encriptar todas sus comunicaciones con la finalidad de proteger sus datos
- proveer de multiplexación de puertos TCP para entornos con cortafuegos
- monitorizar y modificar cualquier propiedad de los computadores que estén conectados a él online

DJ HACK: Distributed Java HAsh craCKer

Proyecto de fin de carrera dirigido por Pablo González Nalda

Unai Gómez Velasco

Depto. de Lenguajes y Sistemas Informáticos

27 de septiembre de 2010

Contenidos de la presentación