

GIDRE

Detección de Nuevos Ataques mediante Grid



Olimpia Olguín Tinoco
Manuel García-Cervigón
Manuel Medina Llinàs



Atención: No se permite la reproducción total o parcial de este material sin el permiso del autor

- Introducción
- Motivación
- Objetivos
- Características
- Propuesta
- Grid
- Enlaces de interés

USA → Gusano Morris, 1988

Departamento de Defensa Nacional → Carnegie Mellon
CERT/CC (Computer Emergency Response Team
Coordination Center)

Europa → Alemania + Noruega, Francia, Holanda, 1992

España → UPC → esCERT, inicios 1995, Dr. Manel

lédina

Madrid → IRIS-CERT, finales 1995



Principales objetivos de esCERT-UPC

- Informar sobre vulnerabilidades de seguridad y amenazas.
- Divulgar y poner a disposición de la comunidad información que permita prevenir y resolver incidentes de seguridad.
- Realizar investigaciones relacionadas con la seguridad informática.
- Educar a la comunidad en general sobre temas de seguridad.

Colaboración

- esCERT es miembro de TF-CSIRT (Task Force-Collaboration of Incident Response Teams).
- Forma parte de EPCI (European Private CERT Initiative) una agrupación de CERTs europeos privados.
- esCERT en el ámbito mundial participa en el FIRST, principal foro de coordinación de los diferentes CERTs de todo el mundo.
- Se colabora en la Iniciativa Europea de Firma Electrónica (EESSI).

1. Multiplicación de Sistemas informáticos.
2. Computer Industry Almanac → Usuarios de internet en 2005 1 millón.
3. Violaciones de seguridad (FTP, servidor web,) debido a fallos de programación.
4. En 2003 CERT/CC registró 137.529 incidente, 2005 5,990 vulnerabilidades
5. Amenaza: virus de correo, DDoS y Scanning indiscriminado.

Incremento de intrusos

Incremento de vulnerabilidades

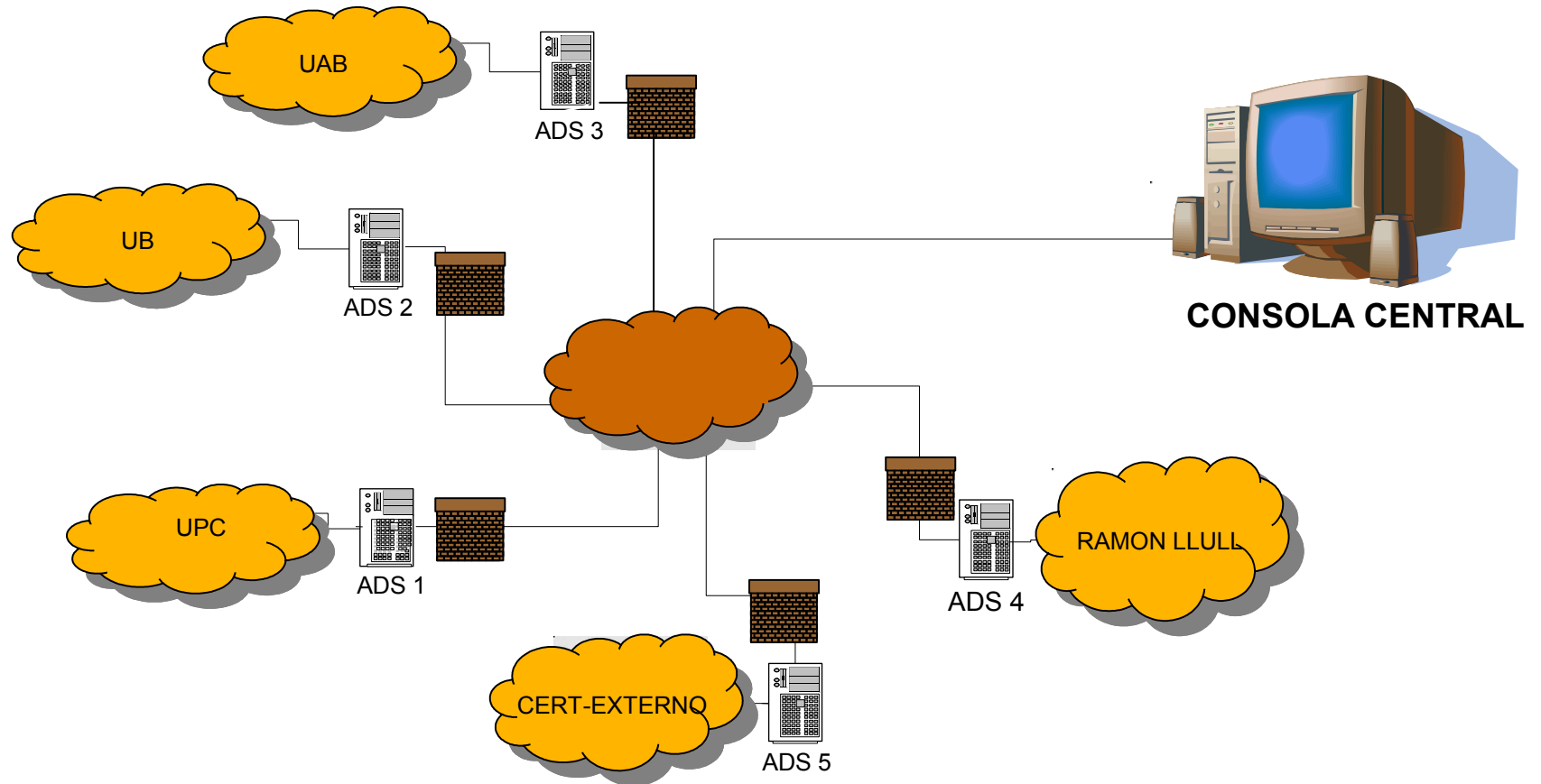


- Existen herramientas de seguridad, pero el **tiempo de respuesta es elevado**.
- Ejemplo: Un administrador no puede tomar medidas hasta que no le informan de un nuevo gusano o visualiza los logs de un firewall.
- ¿Qué ocurre?
 - **Falta de herramientas** que permitan la detección de ataques desconocidos.
 - **Falta de mecanismos** eficientes para la transmisión de información de los nuevos ataques descubiertos.
 - **Falta de mecanismos** que permitan analizar grandes cantidades de información para detectar posibles ataques y de esta manera prevenirlos.

- Nuestro proyecto permitirá:
 - Desarrollar un conjunto de **herramientas innovadoras** para la **detección de anomalías** en la red producidas por ataques distribuidos no conocidos.
 - Desarrollar así mismo una herramienta de **toma de decisiones** mediante el análisis de datos que ofrece la minería de datos y la **compartición de recursos** que permite la tecnología grid.
 - Descarga de trabajo en los sensores por medio de grid.
 - Dotar en definitiva a la red de un sistema robusto que permita la **detección precoz de todo tipo de ataques recibidos**.
 - La alta disponibilidad en caso de que la Consola Central se dañe.

- Uso de IDSs con técnicas de detección de anomalías (ADS).
- Captura y análisis de tráfico con ADS.
- Generación de una política de reacción ante el ataque.
- Distribución de esta política hacia los firewalls y usuarios externos.
- Implantación de las políticas (manual o automática) en los firewalls considerando los servicios críticos.

TOPOLOGÍA



FUNCIONAMIENTO

1.CAPTURA Y ANÁLISIS DE TRÁFICO

- Esta captura la realizará cada ADS, integrado por:
 - IDS por detección de anomalías
 - IDS por firmas
- Posteriormente se analiza utilizando técnicas de **Minería de datos**, para encontrar la correlación entre los eventos y determinar qué tráfico es **anómalo**.
- Ejemplo: Aumento del número de paquetes en el puerto 80.

FUNCIONAMIENTO

2.GENERACIÓN DE UNA FRASE Y MENSAJE

Cuando se encuentra tráfico anómalo se genera un “frase”.

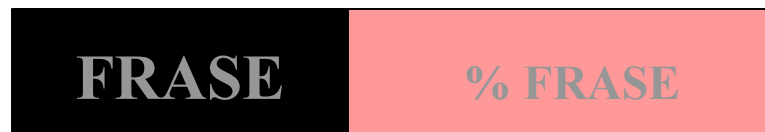
- Una frase se considera una fluctuación sobre el tráfico normal.
- La frase está formada por: protocolo, puerto y payload.

Protocolo	Puerto	Payload	...
-----------	--------	---------	-----

FUNCIONAMIENTO

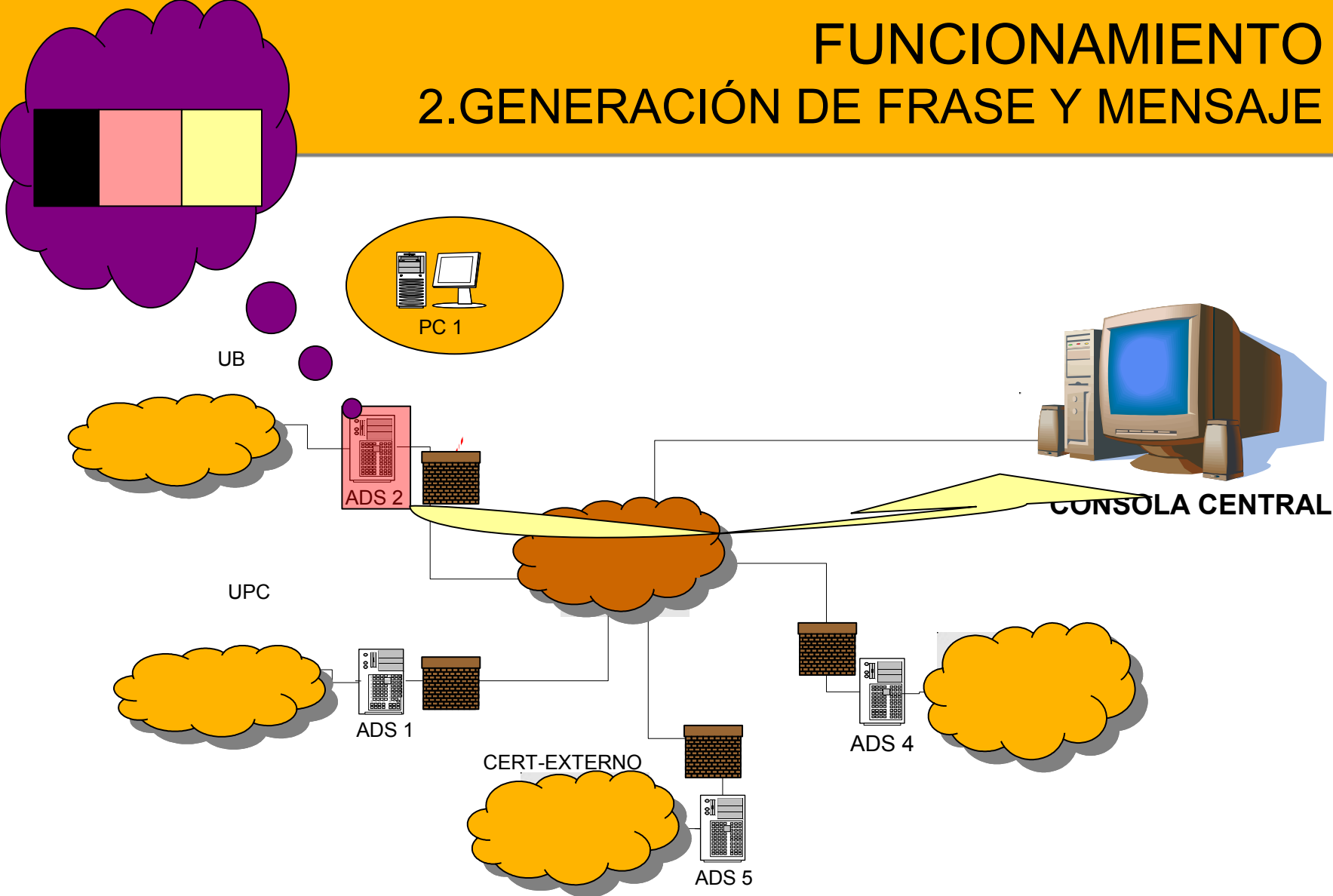
2.GENERACIÓN DE FRASE Y MENSAJE

- El ADS generará una Mensaje formado por:
 - Frase
 - El porcentaje de aparición de dicha frase sobre el tráfico normal.
- Cada ADS enviará los mensajes a una base de datos de la consola central de forma cifrada.
- Se guardará un registro de los mensajes en cada ADS.



FUNCIONAMIENTO

2.GENERACIÓN DE FRASE Y MENSAJE



Cuando llega un mensaje a la consola:

Comprueba si otros ADS han enviado la misma frase.

1. Si la frase no estaba registrada, la consola ordena al ADS que la ha enviado que genere una REGLA ESQUELETO DE FIREWALL.
2. Después se realiza la segunda comprobación:
 1. Si un porcentaje a definir de ADS sobre el número total de ADS's a detectado el mismo tráfico se generará una ALARMA GLOBAL.

FUNCIONAMIENTO

3.REGISTRO DEL MENSAJE EN LA CONSOLA

ID	ADS	Frase	% tráfico	Regla
1	UB	Aumento de tráfico puerto 80	X %	Bloquear el tráfico al puerto 80
2	UAB			
4	UPC	Aumento de tráfico puerto 80	Y %	
5	Rovira i Virgili	Aumento de tráfico puerto 80	Z %	
6				
7	UPC			

FUNCIONAMIENTO

4.GENERACIÓN DE LA REGLA

- Una vez enviada la regla esqueleto desde la consola cada ADS la adecuará a su Firewall. Para ello es precisa una Base de Datos de elementos para cada Red.

- REGLA ESQUELETO:

Filtrar el puerto 80 desde la IP x al servidor Web

- REGLA ADECUADA A UNA RED:

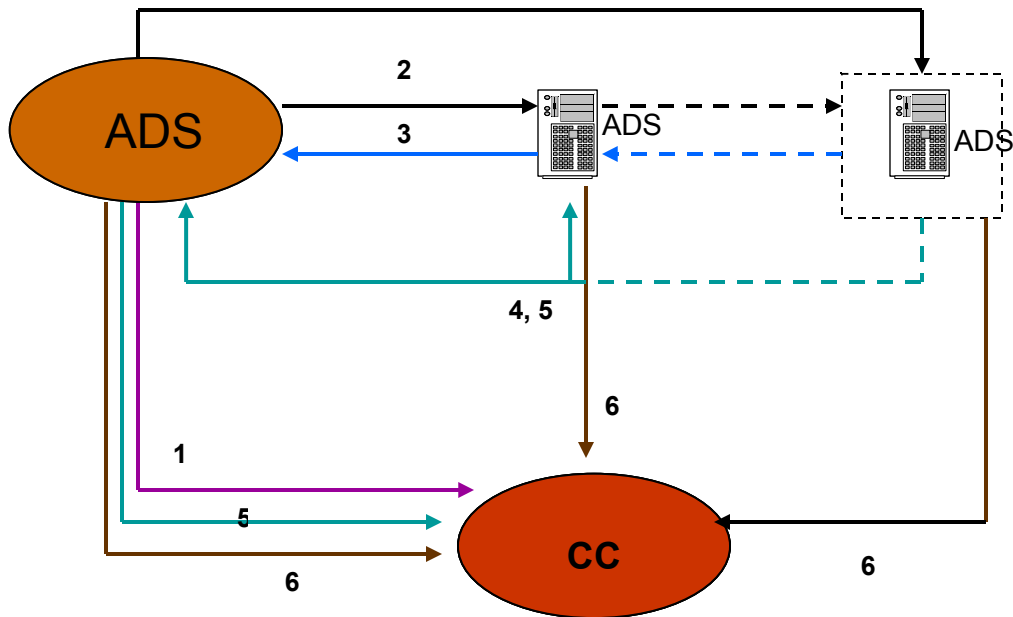
Filtrar el puerto 80 desde la IP x a la IP 192.168.2.3

- Adecuar la reglas a usuarios externos con otro tipo de Firewalls.
- Se definirán servicios críticos de cada red.
- Si la regla incluye un servicio crítico no se implantará automáticamente.

Alta disponibilidad

- Cada elemento de la red GRID será monitorizado por otro elemento. Principalmente la Consola Central, ya que cuando deja de funcionar uno de los ADS toma su lugar.
- En el caso que la consola tenga un problema grave otro ADS podrá realizar sus funciones, gracias al histórico de mensajes guardados en cada ADS.

OTROS OBJETIVOS ALTA DISPONIBILIDAD



- Uso de GRID para enviar parte del tráfico a procesar a otras máquinas.
- De esta forma se podría reducir la carga de trabajo de los ADS.
- La plataforma globus permitiría generar nuevas aplicaciones para la gestión de la creación de estadísticas de minería de datos de forma distribuida.

Grid Computing “Uno para todos y todos para uno”

Conjunto heterogéneo de redes avanzadas, ordenadores, dispositivos de almacenamiento, de visualización, instrumentos científicos, etc.

- Permite gestionar y distribuir la potencia de cálculo disponible, sumando la de todos los ordenadores conectados.
- Utiliza protocolos de comunicación basados en estándares abiertos y permite convertir una red global en un **“superordenador virtual”**.

Algunos servicios:

- Control en el reparto de trabajo
- El seguimiento de su ejecución de los procesos
- Gestión de recursos
- Gestión remota de procesos
- Control de tráfico en ambos sentidos
- Seguridad y soporte a monitorización

Objetivos:

- Potencia de cálculo → Reducción en el tiempo de procesamiento
- Almacenamiento
- Costos bajos.
- Colaboración a nivel mundial

Campos de Aplicación:

- Astrofísica
- Medicina
- Investigación
- Finanzas
- Academia
- Seguridad

www.cert.org

www.escert.org

www.ugr.es

www.gridcat.org

www.grid.org

www.c-i-a.com

DetECCIÓN de Nuevos Ataques mediante Grid

Olimpia Olguín → oolguin@escert.upc.edu

Manel Garcia-Cervigón → manu@escert.upc.edu

Manel Medina → medina@escert.upc.edu