Descon2

XXIII Grupos de Trabajo 2007
E.T.S.I. Telecomunicación
Universidad Politécnica de Madrid.

Rafael Calzada

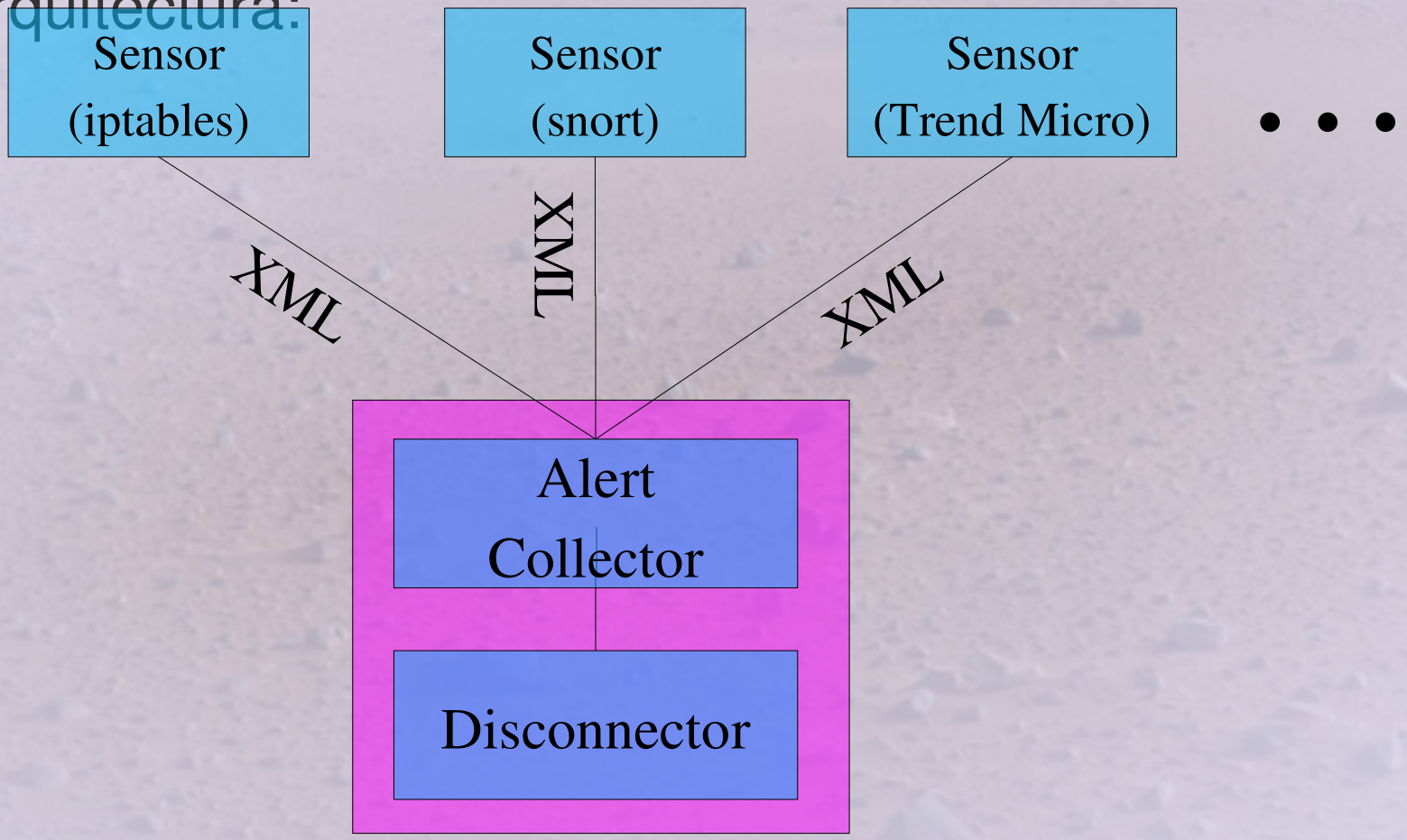
Universidad Carlos III de Madrid

Índice

- Introducción
- Versión Actual
  - Requisitos
  - Instalación
- Cambios a corto plazo
  - SNMP puro
  - IDMEF

Introducción

- Agregador de eventos de seguridad
- Arquitectura:



- Requisitos para el Colector
  - Instalación estándar de perl
  - Módulos adicionales:
    - Mail::Sendmail (libmail-sendmail-perl)
    - XML::Simple (libxml-simple-perl)
    - Unix::Syslog (libxml-simple-perl)
    - Net::SNMP (libnet-snmp-perl)
    - Expect (libnet-snmp-perl)
    - Net::Telnet::Cisco (libnet-snmp-perl)
- Requisitos para los sensores
  - Instalación estándar de perl
  - Módulos adicionales:
    - XML::Simple (libxml-simple-perl)

- Localización de IPs
  - Emplea SNMP y conexiones Telnet a los conmutadores
    - Traducción IP -> MAC, consulta SNMP al encaminador
    - Localización MAC, Telnet a los conmutadores de backbone
    - Necesario CDP para “descubrir” la ruta a la dirección MAC

Instalación

- Disponible en:
  - https://nuberu.uc3m.es/descon2/descon2v1.tar.gz
- Descomprimir
  - Copiar los módulos propios a un directorio de módulos de perl (p.e. /etc/perl)
    - Directorio Descon2
- Configurar el colector de alertas
  - Fichero colector.cfg
    - Coste máximo
    - Tiempo de desconexión
    - Facilidad Syslog
    - Direcciones de correo
- Probar el colector de alarmas

Detector snort

- Permite monitorizar ciertas alertas de snort
  - Para cada tipo de alarma, podemos fijar:
    - El coste
    - Dirección IP origen de la alarma
      - La IP origen de snort (p.e. escaneo)
      - La IP destino de snort (p.e. la alerta de id=root(0)
      - Ambas (un troyano gestionado desde el maestro)
    - El tiempo de vida
- Para desarrollar sensores
  - Ver INSTALL-ES.txt
  - Utilizar sample-detector.pl como plantilla

Cambios a corto

- Migración a SNMP puro (módulo SNMP::Info)
  - Para evitar problemas con nuevos conmutadores
  - Supresión de conexiones Telnet
  - Admite conmutadores de otros fabricantes con protocolos de descubrimiento (LLDP, etc)
- Migración a IDMEF
  - RFC 4765
    - Admite más información, y afinar la sensibilidad del colector.
  - Compatible hacia atrás
    - Aprovechando la extensibilidad de IDMEF

- Muchas gracias por vuestra atención