Escuela Politécnica Superior

UAM UNIVERSIDAD AUTONOMA DE MADRID

Evaluación de dispositivos IPSEC para el establecimiento de redes privadas virtuales

José María Sierra
Departamento de Informática
Universidad Carlos III de Madrid

INTRODUCCIÓN

Seguridad en las TIC

- Se acentúan la necesidad de mejorar su seguridad
- El incipiente número de amenazas de los S.I.
  - La incesante interconexión de sistemas y redes.
  - La creciente utilización de las redes de ordenadores para la transmisión de informaciones sensibles.
  - El aumento de la capacidad técnica de un ataque de red
- Necesaria la adaptación de la infraestructura de red
  - Los mecanismos de seguridad.
  - Los protocolos de seguridad de propósito general.
  - Los protocolos de seguridad se propósito especifico

INTRODUCCIÓN

Las TIC y la sociedad

- Internet es un pilar para los avances sociales, comerciales y científicos
- El intercambio de información como catalizador de la colaboración y el progreso
  - *i2010 a european information society for growth and employment (UE, 2005)*
  - La interconexión solo puede venir de la mano de una mejora importante de la seguridad de las redes de ordenadores
  - Necesidad de estandarización para la interoperatividad

INTRODUCCIÓN

Internet Protocol Security

- Arquitectura de seguridad IPsec
  - Servicios de seguridad opcionales en el nivel de red (IETF)
  - Incluido en IPv6 Draft Standard (1998)
- IPsec incluye dos protocolos de seguridad
  - Cabecera de autenticación (AH)
    - Servicios de Integridad y autenticación
    - Mecanismos de firma digital o funciones resumen con clave
  - Encapsulación segura del campo de carga (ESP)
    - Servicios Confidencialidad, integridad y autenticación
    - Mecanismos de cifrado del campo de carga, firma digital o funciones resumen con clave

INTRODUCCIÓN

Internet Protocol Security

- IPsec incluye dos modos de funcionamiento
  - Modo Tunel y Modo Transporte
- Protocolo para la gestión y negociación de parámetros de seguridad
  - Asociación de Seguridad (SA)
  - *Internet Security Association and Key Management Protocol*
  - Protocolo IKE e IKEv2

INTRODUCCIÓN

Protocolos de Seguridad

- Desajuste de las implementaciones
  - No utilización de algoritmos criptográficos estandarizados, o implementación deficiente de los mismos
  - Interpretación arbitraria de lo descrito en el estándar
  - Modificaciones y optimizaciones que los fabricantes realizan sobre lo establecido en el estándar para aumentar el valor competitivo de sus productos
- Falsa sensación de seguridad

Evaluación IPsec

- Necesidad de un baremo comparativo entre soluciones de seguridad
- Validación
  - Del proceso de desarrollo o del diseño del protocolo
  - Ligada a pruebas de caja blanca
  - Limitaciones de las pruebas de caja negra
- Evaluación
  - Generalmente pensadas para sistemas de comunicaciones sin seguridad
  - Nuevos trabajos del IETF (RFC 2544 y RFC 3511)

Análisis de conformidad

- Análisis de conformidad con el estándar
  - Referencia
    - Adecuación a organizaciones de referencia (IETF, NIST, NSA, ...)
    - Adecuación a implementaciones de referencia (OpenSwan y PlutoPlus)

TÍTULO	FECHA
RFC4301 Security Architecture for the Internet Protocol.	Diciembre 2005
RFC4302 IP Authentication Header	Diciembre 2005
RFC4303. IP Encapsulating Security Payload	Diciembre 2005
RFC4304. ESN Addendum to IPSEC DoI for ISAKMP	Diciembre 2005
RFC4308. Cryptographic Algorithm Implementation Requirements for ESP and AH	Diciembre 2005
RFC4306. Internet Key Exchange version 2	Diciembre 2005
Cryptographic Algorithm Implementation Requirements For ESP And AH	Agosto 2004
IP Encapsulating Security Payload (ESPv3)	Marzo 2005

EVALUACIÓN IPSEC

Análisis de conformidad

- Análisis de conformidad con el estándar
  - Pruebas de Algoritmos
    - Algoritmos de cifrado y resumen
    - Modos de cifrado D-H
  - Pruebas de protocolos
    - IKE / ISAKMP
      - Funcionamiento como *Iniciator* o *Responder*
      - Parámetros configurables
        - Autenticación (secreto, RSA o X509), ...
    - ESP (modo túnel y modo transporte)
    - AH (modo túnel y modo transporte)
  - Aspectos no incluidos en el estándar
    - Encaminamiento, alta disponibilidad, ...

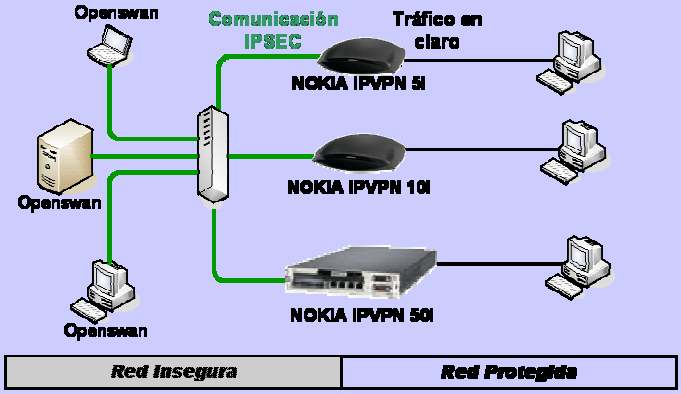
EVALUACIÓN IPSEC

Evaluación del Rendimiento

- Análisis de la eficiencia y estabilidad de la implementación
- Definición de entornos de prueba para ESP y AH
  - Definición de escenarios
    - Tráfico UDP, TCP simétrico, TCP asimétrico (puro o mixto) y tráfico a ráfagas (puro y mixto)
  - Realización de estudios sobre:
    - Ancho de banda ofrecido por combinaciones de escenarios y algoritmos
    - Volúmenes de conexiones activas según escenarios, velocidades de transmisión y tamaños de mensajes
    - Tiempos mínimos por protocolo

Evaluación del Rendimiento

- Esquema de la arquitectura utilizada



Evaluación del Rendimiento

- Eficiencia en la gestión de Asociaciones de Seguridad (IKE)
  - Capacidad de establecimiento de nuevas conexiones
    - Conexiones sin tráfico
      - Capacidad de la BB.DD. de A.S.
    - Conexiones con tráfico
      - Distintas velocidades de transmisión por conexión
  - Capacidad en ráfagas de nuevas conexiones
    - Influencia de la velocidad de transmisión por cada canal
    - Influencia del número de conexiones previas
  - Tiempos mínimos de negociación

EVALUACIÓN IPSEC

Evaluación del Rendimiento

- Capacidad en ráfagas de nuevas conexiones

	NOKIA IPVPN 5i 24 AS	NOKIA IPVPN 10i 24 AS	NOKIA IPVPN 50i 40 AS
500 Kbps	2 pet./seg	2 pet./seg	12 pet./seg
1 Mbps	0,5 pet./seg	0,5 pet./seg	12 pet./seg
1 Mbps	0,13 pet./seg	0,13 pet./seg	10 pet./seg
1 Mbps	0,05 pet./seg	0,05 pet./seg	10 pet./seg

EVALUACIÓN IPSEC

Otros aspectos

- Evaluación del rendimiento en cluster
  - Funcionamiento en alta disponibilidad
  - Reparto de carga
- Protección de la información de encaminamiento
- Otras funcionalidades particulares
  - Self-Learning
  - Self-Healing

CONCLUSIONES

Conclusiones

- Aumento del uso de protocolos de seguridad en Internet
- ciclo de vida de los protocolos de seguridad
- Diferentes implementaciones IPSEC que desean diferenciarse en el marco comercial
- Suites de funcionamiento flexibles
- Tablas de interoperatividad

CONCLUSIONES

Conclusiones

- Validación remota de interoperatividad
  - IPsec-WIT
- Guías para la configuración de IPSEC
  - Suites de funcionamiento
- Gestión de políticas de interconexión IPSEC
  - SEC-POINT

Evaluación de dispositivos IPSEC para el establecimiento de redes privadas virtuales

José María Sierra
Departamento de Informática
Universidad Carlos III de Madrid