Seguridad en Sistemas Distribuidos

TEMA 2
Protocolos de Autenticación en redes

José María Sierra

Departamento de Informática
Universidad Carlos III de Madrid

Aspectos de seguridad

- La autenticación remota supone un reto para la seguridad
  - Deben evitarse los ataques de repetición
  - Mantener la confidencialidad de los secretos
- Canales seguros para la autenticación
- Mecanismos de sincronización temporal o empleo de contenidos que permitan asegurar la frescura de la comunicación (nonce)

KERBEROS

- Fiabilidad
- Seguridad
- Escalabilidad
- Transparencia

KERBEROS

- Diseñado para permitir el acceso de usuarios a servicios.
  - Red Distribuida
- Existen tres amenazas principales:
  - Suplantación .
  - Ip-spoofing.
  - Ataques de repetición.

KERBEROS

- Su funcinamiento se base en el empleo de un servidor de autenticación (AS) que participa en la autenticación entre usuarios y servidores
- Basado en criptografia simétrica
- Se establece una solución a un problema muy habitual de seguridad
  - Empleado desde su diseño hasta nuestros días.
- Dos versiones: v4 y v5

Kerberos Version 4

- Terminología empleada:
  - C = Client
  - AS = authentication server
  - V = server
  - ID_c = identifier of user on C
  - ID_v = identifier of V
  - P_c = password of user on C
  - ADc = network address of C
  - K_v = secret encryption key shared by AS an V
  - TS = timestamp
  - || = concatenation

Autenticación básica

1) C → AS: IDc || P_c || IDv
2) AS → C: Ticket
3) C → V: IDc || Ticket

Ticket = E_{Kv}[IDc || P_c || IDv]

- Problemas:
  - Cada solicitud al servidor V precisa de la ejecución del protocolo completo (y la intervención del usuario)
  - Envío de la contraseña en claro (Pc)

Autenticación básica mejorada

- Protocolo en tres fases
  - autenticación de usuario, autorización de tipo de servicio, autorización de un servidor
- Conceptos emergentes
  - Además de AS aparece TGS (ticket granting server y el TGT (ticket granting ticket)
  - El TGT permite el uso del TGS
  - El TGS permite el uso de un Servicio determinado

Autenticación básica mejorada

Obtención del Ticket-Granting Ticket

(1) C → AS: IDc || IDtgs

(2) AS → C: $E_{Kc}[Ticket_{tgs}]$

$Ticket_{tgs} = E_{Ktgs}[ID_c||AD_c||ID_{tgs}||TS_1||Tiempo\ de\ vida_1]$

Obtención del Service-Granting Ticket

(3) C → TGS: IDc|| IDv ||$Ticket_{tgs}$

(4) TGS → C: $Ticket_v$

$Ticket_V = E_{Kv}[ID_c||AD_c||ID_V||TS_2||Tiempo\ de\ vida_2]$

Obtención del Service

(5) C → V: $ID_c||Ticket_v$

Autenticación básica mejorada

- Problemas:
  - Tiempo de vida asociado al ticket-granting ticket
    - Si es muy corto → continua petición al usuario
    - Si es muy largo → ventajas para el ataque de repetición
  - El atacante podria utlizar el ticket de servicio antes de que caduque
  - Suplantación de los Servidores

Autenticación en Kerberos v4

Obtención del Ticket-Granting Ticket

(1) C → AS: $IDc \,||\, IDtgs \,||\, TS_1$

(2) AS → C: $E_{Kc}\,[K_{c,tgs} \,||\, ID_{tgs} \,||\, TS_2 \,||\, Tiempo\ de\ vida_2 \,||\, Ticket_{tgs}]$

$Ticket_{tgs} = E_{Ktgs}[K_{c,tgs} \,//\, ID_c \,//\, AD_c \,//\, ID_{tgs} \,//\, TS_2 \,//\, Tiempo\ de\ vida_2]$

Obtención del Service-Granting Ticket

(3) C → TGS: $IDv \,||\, Ticket_{tgs} \,||\, Authenticator_c$

(4) TGS → C: $E_{Kc,tgs}\,[K_{c,v} \,||\, IDv \,||\, TS_4 \,||\, Ticket_v]$

$Authenticator_c = E_{Kc,tgs}[IDc \,//\, ADc \,||\, TS_3]$

$Ticket_V = E_{Kv}[K_{c,v} \,//\, ID_c \,//\, AD_c \,//\, ID_V \,//\, TS_4 \,//\, Tiempo\ de\ vida_4]$

Obtención del Servicio

(5) C → V: $ID_c \,||\, Ticket_v \,||\, Authenticator_c$

(6) V → C: $E_{Kc,v}\,[TS_5+1]$

$Authenticator_c = E_{Kc,v}[IDc \,//\, ADc \,||\, TS_5]$

TEMA 2. Parte 2

Protocolos Seguros de Acceso

Introducción

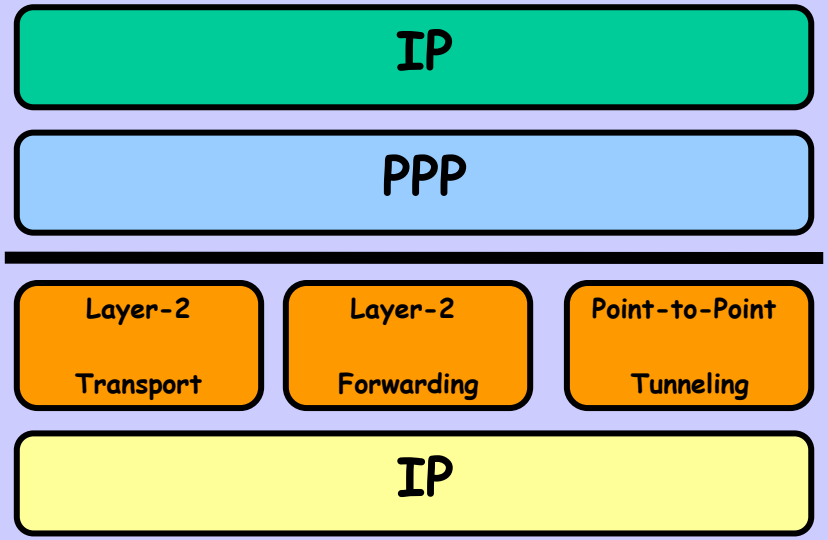
- Túneles de encapsulación de protocolos (Tunneling)
  - La transmisión de paquetes de datos de un determinado protocolo encapsulados en otro, de manera que el contenido del paquete original puede llegar inalterado a su destino, creando una conexión virtual extremo a extremo a través de una red.
  - En distintos niveles de la pila de red:
    - Nivel 2 (Enlace):, PPP, PPTP, L2F, L2TP, MPLS, ...
    - Nivel 3 (Red): L2TP, MPLS, IPSEC, GRE, ...

Introducción

- Repaso al protocolo PPP
  - Es un protocolo para encapsular IP por línea serie que corrige las deficiencias de SLIP.
  - Consta de tres partes:
    - Especificación de la encapsulación de paquetes
    - Protocolo de Control de Enlace (LCP), para establecer, configurar y testear el enlace.
    - Familia de Protocolos de Control de Red (NCPs), para poder especificar distintas familias de protocolos de niveles superiores y sus parámetros.

Protocolos de nivel 2

- Incluyen servicios de seguridad previos al establecimiento de la comunicación



Protocolos de nivel 2

- PPTP (Point-to-Point Tunneling Protocol):
  - Protocolo desarrollado por Microsoft y normalizado por la IETF (RFC 2637)
  - Permite el tráfico seguro de datos desde un cliente remoto a un servidor corporativo privado
  - PPTP soporta múltiples protocolos de red (IP, IPX, NetBEUI…)
- L2F (Layer 2 Forwarding):
  - Protocolo desarrollado por Cisco Systems
  - Precursor del L2TP
  - Ofrece métodos de autenticación pero carece de cifrado de datos

Protocolos de nivel 2

- L2TP (Layer 2 Tunneling Protocol):
  - Estándar aprobado por la IETF (RFC 2661)
  - Mejora combinada de PPTP y L2F
  - No posee cifrado o autentificación por paquete, por lo que ha decombinarse con otro protocolo de seguridad
  - Combinado con IPSec ofrece la integridad de datos y confidencialidad exigidos para una solución VPN
  - Permite el encapsulado de distintos protocolos (IP, IPX,NetBEUI…)

Seguridad en el protocolo PPTP

- PPTP proporciona dos servicios de seguridad básicos:
  - Autenticación
  - Confidencialidad
- PPTP Utiliza la seguridad de PPP para asegurar las comunicación sobre el túnel
  - Autenticación de usuario PPP (PAP, CHAP, MS-CHAP, MS-CHAPv2, EAP).
  - Confidencialidad y cifrado PPP (MPPE). RC4 con claves de 40 o 128 bits.

Seguridad en el protocolo PPTP

- Comunicación en PPTP de dos tipos
  - Control
    - Creación de un control de conexión PPTP
    - Conexión lógica que representa el túnel PPTP.
    - El servidor utiliza el puerto TCP 1723 y el cliente un puerto dinámico.
    - Determina los ID de la cabecera GRE entre cliente y servidor que identifican el túnel PPTP específico.
    - Mantenimiento del control de conexión PPTP
  - Finalización del control de conexión PPTP
  - Datos
    - Encapsulado y transmisión de datos PPP mediante (GRE). Generic Routing Encapsulation

Seguridad en el protocolo PPTP

- Autenticación
  - Password Authentication Protocol (PAP).
    - Envía la password en texto claro.
  - Shiva Password Authentication Protocol (SPAP).
    - Utiliza cifrado reversible.
  - Challenge Handshake Authentication Protocol (CHAP)
    - Reto-respuesta enviado con la función resumen MD5

Seguridad en el protocolo PPTP

- Autenticación
  - MS-CHAP v1
    - Lan Manager hash function
      - La clave se transforma en una cadena de 14 bytes
      - Minúsculas → Mayúsculas
      - Cifrado con DES de una constante usando cada mitad de 7 bytes como clave → 2 cadenas de 8 bytes
    - • Windows NT hash function
      - La clave se transforma en una cadena de 14 bytes
      - Se convierte a Unicode
      - Se usa MD4 → hash de 16 bytes
    - A Tener en cuenta
      - Conversión a mayúsculas
      - Ausencia de condimento (SALT) en el almacenamiento de claves

Seguridad en el protocolo PPTP

- Proceso de autenticación en MS-CHAP
  - El cliente solicita un reto
  - El servidor envía un reto de 8bytes aleatorios
  - El cliente añade 5 bytes a cero al valor obtenido del hash (Lan Manager y WindowsNT)
  - Divide los 21 bytes en 3 claves que son usadas para cifrar con DES el reto → 24 bytes (para cada opción Lan Manager y Windows NT)
  - El servidor analiza uno de los dos bloques de 24 bytes (determinado por el cliente)
- MS-CHAP v2
  - Mejoras de seguridad (no se envía el Lan Manager de la contraseña del usuario)
  - Sigue siendo tachado de inseguro

Seguridad en el protocolo PPTP

- Cifrado en PPTP
  - Protocolo MPPE (Microsoft Point-to-Point Encryption)
    - Cifrado de flujo a través del algoritmo RC4
    - 128 bits de semilla tomados de la aplicación de SHA1 sobre el hash (Windows NT) de la contraseña de usuario y 64 generados durante la negociación MS-CHAP
    - Cada 256 paquetes PPTP, se recalcula una semilla nueva a través de la clave antigua y la clave original.
  - Siguen existiendo debilidades en MPPE
    - P.e.: puede evitarse el cambio de clave cada 256 paquetes

Seguridad en el protocolo L2TP

- El estándar permite que se pueda utilizar la seguridad de PPP para asegurar las comunicación sobre el túnel.
  - Autenticación PPP (PAP, SPAP, CHAP, MS-CHAP, ...)
  - Confidencialidad y cifrado PPP (MPPE).
- Autenticación con EAP Extensible Authentication Protocol
  - Soporta varios tipos de Autenticación
    - EAP-MD5: Desafió/Respuesta.
    - EAP-TLS: Basado en cerificados digitales
    - EAP-RADIUS: Mecanismo proxy de reenvió de datos en un formato EAP especifico a un servidor RADIUS
  - PEAP: Protected EAP
    - Proteje las negociaciones EAP envolviéndolas con TLS.
- L2TP/IPSEC