CORSO DI FORMAZIONE INTERSTRUTTURA

TUTORIAL KERBEROS 5

Responsabile Enrico M. V. Fasanelli

Lecce, 6 - 9 febbraio 2007

PROGRAMMA DEL CORSO

FASE 1: Sguardo d'insieme
- Cosa è kerberos
- Perché occorre kerberos
- Chi usa kerberos
- Kerberos5 e Windows2000

FASE 2: Primo approfondimento tecnico
- Sistemi di autenticazione
- ABC del protocollo (kerberos 4 e kerberos 5)
- Versioni free e non

FASE 3: La nostra realtà
- L'uso di Kerberos4 nell'INFN (AFS)
- L'uso di Kerberos5 in alcune realtà INFN
- Perché passare a kerberos5

SESSIONE di LAVORO di GRUPPO
(rilevazione situazione di sezione, aree di interesse per kerberos 5, ecc.)

FASE 4: Sezione tecnica
- Installazione e configurazione di un REALM
- Il server Kerberos
- I clients
- Configurazione del DNS
- Openafs con autenticazione kerberos5

FASE 5: Sezione tecnica in prospettiva applicativa
- Come realizzare Cross Cell authentication
- Servizi kerberizzati

Servizi WEB
Autenticazione in sendmail via GSSAPI

FASE 6: Valutazioni
SESSIONE di LAVORO di GRUPPO guidato e orientato ad un itinerario pratico per la kerberizzazione del proprio ambiente

==========

INFORMAZIONI GENERALI

Organizzatore Responsabile: Enrico M. V. Fasanelli
Docenti: Enrico M. V. Fasanelli, Fulvio Ricciardi, Silvia Arezzini
Durata: 3 giorni (primo e secondo giorno: intera giornata; terzo giorno: prima mattina ora di pranzo)
Sede: Lecce

OBIETTIVI E TARGET

Kerberos è un protocollo di autenticazione per sistemi in rete.
E' stato disegnato per fornite autenticazione "forte" per applicazioni di tipo client/server mediante l'uso di crittografia a chiave privata.
La necessità di autenticazione "forte" deriva dal fatto che i protocolli di comunicazione usati, in quello che oggi comunemente chiamiamo Internet, sono tutt'altro che sicuri.
E' infatti molto semplice "fiutare" una trasmissione di dati sulla rete, e carpire le parole-chiave o impersonare un utente o servizio sulla rete e far sì che clienti ignari contattino l'utente o il servizio falsificato invece dell'originale.
Il protocollo Kerberos, disegnato al Massachusetts Institute of Technology (MIT) prevede l'uso di crittografia "forte" attraverso la quale ogni attore (client o server) può provare la propria identità all'omologo, pur utilizzando un sistema di comunicazione intrinsecamente insicuro (Internet) e quindi proteggere la comunicazione, attraverso l'uso di crittografia.
La prima versione del protocollo disponibile al di fuori dell'MIT negli anni 80 (kerberos4) è stata adesso resa obsoleta dalla nuova versione, Kerberos5, disponibile al di fuori degli USA a partire dalla fine del 2000.
Nell'INFN si usano sistemi basati su autenticazioni Kerberos (versione 4) già dal 1995, anno in cui l"INFN ha adottato AFS (Andrew File System) come file system distribuito, la cui autenticazione è basata sulla versione 4 del protocollo Kerberos.
Nel 1996 il gruppo di valutazione di DCE/DFS ha iniziato a sperimentare l'autenticazione basata sul protocollo Kerberos5 (ed alcune delle sue funzionalità interessanti come la autenticazione incrociata)

A partire dall'inizio del 2001, presso la Sezione INFN di Lecce, si è iniziato ad usare a nuova versione del protocollo Kerberos non solo per la correzione di alcuni errori di disegno della versione precedente (che la rendevano vulnerabile in situazioni particolari), ma anche e soprattutto per le nuove funzionalità grazie alla possibilità di accedere alle distribuzioni del software prodotto negli USA.
Si e' così costituito un gruppo di lavoro che ha presentato alla Commissione Calcolo e Reti dell'INFN un progetto di implementazione di autenticazione basata sul protocollo Kerberos5 per tutto l'INFN. Il progetto è ora in avanzato stato di realizzazione, e questo richiede che le conoscenze sul protocollo, sulle sue implementazioni e sull'operatività debbano essere diffuse all'interno della comunità degli amministratori di sistema dell'INFN ed eventualmente anche degli utenti, che comunque dovranno usare Kerberos5 nelle operazioni quotidiane (come leggere la posta, o accedere a filesystems remoti).

Interessati: System manager appartenenti ai Servizi Calcolo di Sezioni e sedi distaccate. Utenti evoluti di Servizi di Calcolo e Reti