



RACF password synchronization proof of concept

Project Number	
Project Title	
Contractor	Internal
Contract number	
Title of Deliverable	
Contractual Date of Delivery	

Internal Project Number	IN/POC-RACF
Author(s)	Enrico Badella
Team id	
Status of deliverable	



1	INTRODUZIONE	3
2	OBIETTIVI	3
3	ARCHITETTURA	4
4	MODALITÀ DI INSTALLAZIONE	5
4.1	z/OS	5
4.2	Unix	5
4.3	Windows 2000	6
5	RISULTATI	6
6	TUDO	6

1 Introduzione

Questo documento descrive l'architettura ed il software sviluppato per il *proof of concept* che realizza la propagazione delle password da ambiente host verso ambienti Unix o Windows.

La necessità di un componente in grado di sincronizzare le password degli ambienti legacy si evidenzia principalmente quando un'azienda inizia ad affrontare il problema del *life-cycle* delle userid. Questo problema nasce quando il numero degli ambienti informatici si moltiplica; ciascuno con i propri sistemi d'autenticazione e d'autorizzazione degli utenti e *security policies*. Si assiste quindi ad una proliferazione di userid e password, spesso di bassa qualità da un punto di vista della sicurezza. Con l'aumento delle userid emesse aumenta anche il rischio delle cosiddette '*userid tramandate*' ossia quelle userid passate da un utente all'altro ad esempio quando cessa un rapporto di lavoro.

Negli ultimi anni, con l'aumentare della sensibilità verso i rischi di sicurezza, si è iniziato ad affrontare il problema utilizzando le tecnologie **LDAP** e **Meta Directory**. Quest'ultima tecnologia è indirizzata principalmente alle aziende di grandi dimensioni con almeno 10000 userid; da questo si comprende come mai le offerte sul mercato siano così limitate. Sino a metà del 2003 i vendor in grado di offrire una soluzione di Meta Directory sono stati cinque.

Il proof of concept qui descritto nasce come *skunk work* durante uno studio di fattibilità, effettuato per un'azienda del settore automotive. Lo studio di fattibilità doveva valutare la possibilità di realizzare un sistema di Meta Directory, effettuare un'*assessment* degli ambienti da integrare e valutare in modo approfondito le soluzioni software disponibili sul mercato. In questo progetto sono stati contattati ed analizzati i cinque fornitori di soluzioni di Meta Directory. Uno dei requisiti fondamentali per il potenziale fornitore era la capacità di integrare la sincronizzazione delle password da e verso **RACF**. Solamente uno dei fornitori è stato in grado di mostrare su campo questa funzionalità, anche se con alcuni problemi e limitazioni.

2 Obiettivi

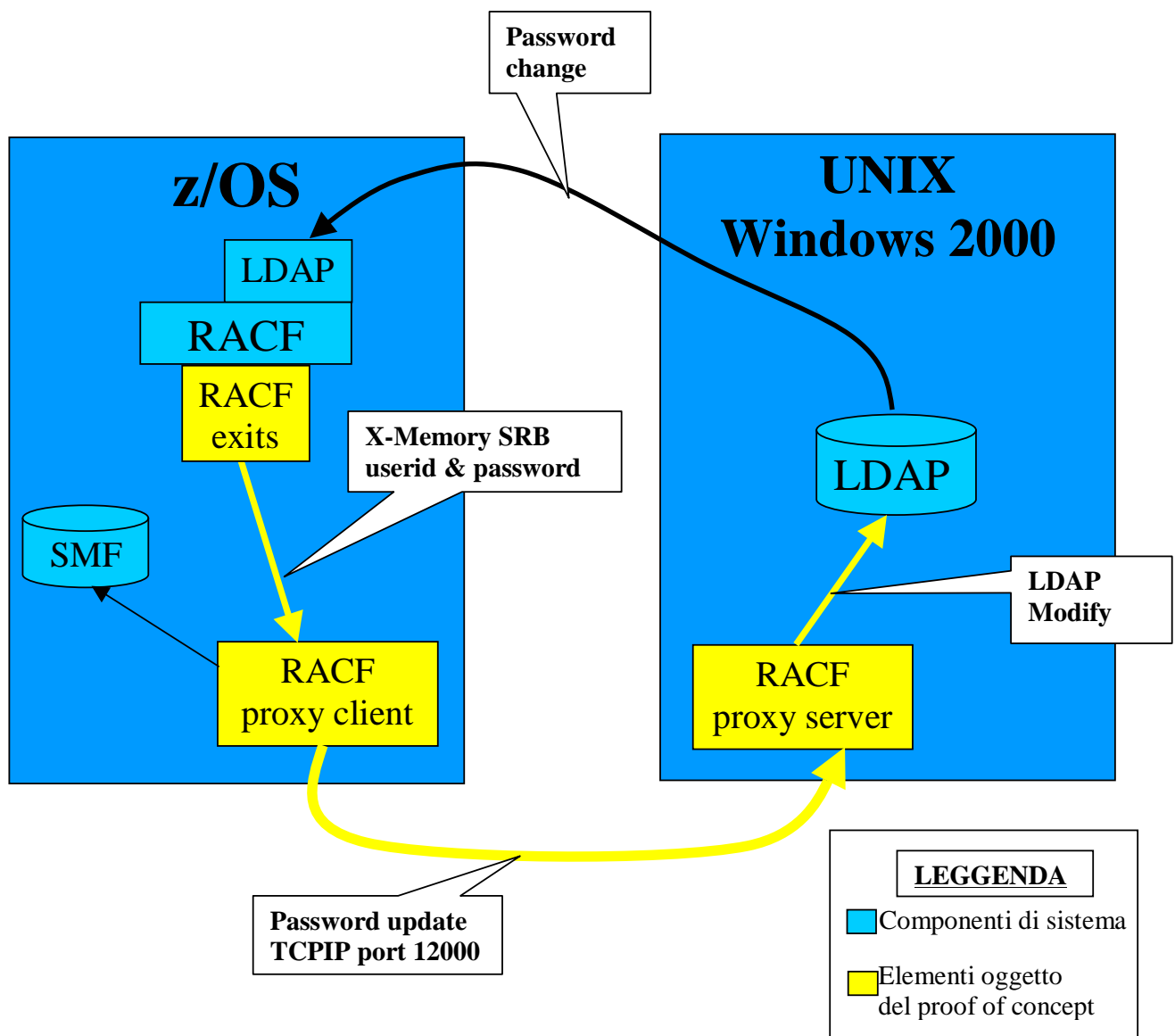
I principali obiettivi del proof of concept possono così essere riassunti:

- Definire un'architettura modulare e facilmente migrabile su piattaforme hardware e software diverse.
- Individuare le componenti necessarie in ambiente legacy per interfacciarsi con RACF.

- Facilità d'installazione specialmente nel mondo legacy.
- Compatibilità con versioni non aggiornate di sistemi operativi, in particolare su host.
- Implementare le funzionalità minime per effettuare delle prove di cambio password bidirezionale.

3 Architettura

L'architettura realizzata è mostrata nella seguente figura. Si possono individuare due



componenti principali; una client, residente su host ed una server su Unix o piattaforma Microsoft. Gli elementi oggetto dello sviluppo sono quelli mostrati in giallo nella figura.

Sulle piattaforme Unix o Microsoft non si presentano particolari problemi per lo sviluppo. Il RACF proxy server è un'applicazione socket ed LDAP standard. Molta più attenzione deve essere posta nella parte client su host. La principale limitazione è imputabile al contesto in cui sono invocate le **User Exits RACF**. Infatti, oltre agli ovvi problemi di interagire con la componente base della sicurezza mainframe, si hanno vincoli di addressing dell'architettura MVS/370, MVS/XA ed MVS/ESA, pre-emption e di load autorizzato. Per questi motivi è stato necessario separare in più moduli la gestione della cattura e propagazione della password. I moduli comunicano fra di loro mediante **Cross Memory SRB**.

Per semplicità di implementazione e per tempi ristretti, la comunicazione tra la componente server e quella client avviene senza l'uso di un canale crittografato, a scapito della sicurezza.

La propagazione delle password da mondo Unix o Windows non è stata realizzata mediante User Exit RACF ma utilizzando la componente LDAP presente con RACF a partire dalla versione 2.8 di OS/390. Anche questa scelta è stata presa per ridurre i tempi di realizzazione. E' ovvio che in una possibile implementazione sarebbe conveniente utilizzare il canale crittografato già attivo per propagare le password da RACF verso gli altri ambiente.

4 Modalità di installazione

Le componenti sviluppate non presentano particolari problemi di installazione. Nel seguito sono delineate le principali operazioni da svolgere

4.1 z/OS

- Caricare le Exit RACF in **SYS1.LPA**
- Aggiungere il modulo di comunicazione alle librerie **APF-authorized in SYS1.LINKLIB**
- Aggiungere il Client Proxy alle librerie APF-authorized in **SYS1.LINKLIB**
- Installare il Client Proxy come started task in **SYS1.PROCLIB**
- Aggiungere il JCL per lo started task in **SYS1.PROCLIB IPL**
- Eseguire **IPL**

4.2 Unix

- Installare il Server Proxy in una directory privata
- A seconda della piattaforma Unix configurare **LD_LIBRARY_PATH** o **LD_RUN** con la directory contenente le librerie LDAP.
- Configurare il file **/etc/racfsrver** con i parametri richiesti

4.3 Windows 2000

- Installare il Server Proxy in una directory privata oppure in `%SystemROOT%\system32`
- Configurare il Registry
- Lanciare `racfserver -u` per registrare il servizio

5 Risultati

Gli obiettivi prefissati per il proof of concept sono stati raggiunti completamente.

E' stato infatti possibile propagare la password cambiata da **TSO** (comando **ALU userid password(password)**) verso gli altri ambienti che effettuano autenticazione LDAP. Analogamente il cambio password effettuato da **Active Directory**, per il quale è stato realizzato un'analogo componente di cattura password, è stato propagato correttamente verso l'ambiente host.

Per limitazioni di tempo e risorse investibili sono state introdotte ed accettate le seguenti limitazioni:

- Canale non crittografato tra client e server del RACF Proxy.
- Non è effettuato logging su **SMF**
- Il cambio password da LDAP verso RACF avviene utilizzando il server LDAP disponibile con RACF.

Nonostante queste limitazioni descritte, si è potuto verificare la correttezza e flessibilità dell'architettura proposta.

6 TODO

Le principali aree d'intervento per portare il proof of concept a diventare un prodotto sono le seguenti:

- Logging su SMF e gestione della configurazione lato mainframe.
- Canale crittografato
- Cambio password verso mainframe senza uso di LDAP
- Procedure d'installazioni automatizzate per mondo Microsoft
- Script REXX per l'estrazione degli utenti da RACF