Esecuzione di programmi con autorizzazioni di accesso limitate

Prof. Alessandro Pinto
Prof. Franco Ricci

Istituto di Istruzione Superiore

“Benvenuto Cellini”

Firenze

Corso di formazione tecnica 2008/2009

Considerazioni sulle autorizzazioni di accesso

In un contesto multi-utente, il singolo utente di norma ha autorizzazioni limitate allo scopo di:

- Assicurare la riservatezza dei dati/documenti prodotti da altri utenti.
- Evitare la distruzione accidentale o volontaria di documenti di altri utenti.
- Evitare l'installazione arbitraria di pacchetti software non testati che
  - possono rendere instabile la macchina
  - possono entrare in conflitto con altre applicazioni
  - possono violare licenze e copyright
- Evitare la disinstallazione arbitraria, fortuita o volontaria di applicazioni legittimamente installate.
- Limitare il rischio di attacco di alcuni tipi di virus.

Le applicazioni correttamente progettate per operare in ambiente multiutente non presentano particolari difficoltà di installazione.

Questo purtroppo non è generalmente vero per applicazioni obsolete (Win9x/Me) o per applicazioni previste per lavorare solo in contesto personale.

In generale, per effettuare l'installazione di un software, conviene procedere come segue:

1. Installare l'applicazione come amministratore (o utente appartenente al gruppo Administrators)
2. Eseguire una prima volta l'applicazione come amministratore per verificarne la funzionalità ed escludere altri problemi di compatibilità (N.B. spesso questa operazione è necessaria se il programma deve creare durante il primo avvio alcuni file necessari al funzionamento)
3. Disconnettere l'amministratore ed accedere come utente con autorizzazioni limitate.
4. Verificare la funzionalità dell'applicazione

Problemi tipici successivi all'installazione

1. Nel menù avvio dell'utente manca il collegamento all'applicazione

Il programma di installazione ha creato il collegamento solo nel profilo dell'utente corrente (quindi dell'amministratore).

Il problema è di banale soluzione, basta accedere come amministratore e se si desidera renderlo visibile a tutti gli utenti, **copiare** il collegamento mancante dal profilo:

C:\Documents and Settings**Administrator**\Menu Avvio\Programmi

al profilo:

C:\Documents and Settings**All Users**\Menu Avvio\Programmi

infine eliminare il collegamento dal profilo dell'utente amministratore.

In alternativa, **copiare** il collegamento nel profilo dei singoli utenti specifici:

C:\Documents and Settings**<nome utente>**\Menu Avvio\Programmi

- **Ricordarsi di copiare e non spostare** (vedi regole sui permessi NTFS)
- L'utente appartenente al gruppo "Power Users" ha autorizzazioni sufficienti per cancellare il collegamento dal profilo "All Users".

2. L’applicazione richiede le autorizzazioni di modifica nella cartella (sottocartelle) in cui è installato

Possibili sintomi: accesso negato a qualche file, in avvio, esecuzione, uscita o salvataggio dati.

Può dipendere dalla necessità dell’applicazione di:

- Modificare file di configurazione (personalizzazione del programma)
- Creare file temporanei di lavoro
- Aprire in modalità esclusiva con permessi R/W certi file (es. database)
- Salvare il lavoro dell’utente

In ordine di preferenza si può attuare una delle seguenti soluzioni:

1. Configurare l’applicazione (se lo prevede) per salvare i file di configurazione, lavoro o temporanei nel profilo dell’utente o in altra cartella ad accesso user.
2. Attribuire le autorizzazioni di modifica all’utente per i file che lo richiedono
3. Attribuire le autorizzazioni di modifica all’utente per le (eventuali) sottocartelle
4. Attribuire le autorizzazioni di modifica all’utente per la cartella del programma

3. L’applicazione richiede le autorizzazioni di modifica nella cartella Windows (e/o altre sottocartelle di sistema)

Possibili sintomi: accesso negato a qualche file, in avvio, esecuzione, uscita o salvataggio dati.

Vecchi programmi per win9x possono fare riferimento ad una cartella \windows\temp per i file temporanei. In altri casi l’applicazione può richiedere l’accesso in scrittura alla cartella *system32.*

Si sconsiglia vivamente di apportare modifiche alla configurazione che consentano all’utente di accedere con autorizzazioni di scrittura/modifica sulle cartelle di sistema:

Questo renderebbe infatti praticamente inutile qualsiasi accorgimento di sicurezza per l’ambiente multi-utente basato sulle autorizzazioni.

In altre parole una applicazione di questo tipo va considerata come **incompatibile.** Cercare una versione aggiornata dell’applicazione oppure sostituire con un’altra applicazione equivalente progettata specificatamente per 2k/XP

4. Accesso a chiavi di registro

L’applicazione richiede l’accesso a chiavi e sottochiavi dell’albero HKEY_Local_Machine (es. HKLM\Software\<produttore>\<programma>)

Possibili sintomi: l’applicazione non si avvia. L’applicazione non conserva le personalizzazioni dell’utente.

Tipicamente sono chiavi che conservano settaggi e riferimenti per l’esecuzione dell’applicazione.

Le chiavi in HKLM sono visibili a tutti gli utenti e protette dalla modifica da parte del singolo utente.

Una ricerca mirata può portare a determinare quale valore, insieme di valori o sottochiavi necessitano in maniera stringente permessi diversi dal sola lettura.

Il set minimo di autorizzazioni (non ereditate) di cui l’utente dovrebbe disporre, solitamente mancanti, sono:
“*impostazione valore*”, “*creazione sottochiave*”, “*elimina*”

N.B. **Limitarsi in ogni caso alle sottochiavi del programma in questione, non modificare i permessi a livello di root HKLM**
(se questo fosse indispensabile considerare il programma come **incompatibile**).

5. Chiavi di registro mancanti

L’applicazione, eseguita come utente, cerca delle chiavi di registro inesistenti

Possibili sintomi: l’applicazione non si avvia; l’applicazione manca di alcune parti fondamentali (es. menù, toolbar, pannelli…)

Questo avviene quando l’applicazione, in sede di installazione, crea le chiavi di registro (per le personalizzazioni) di cui ha bisogno solo nel percorso HKEY_Current_User (HKCU) e di conseguenza solo per l’utente che ha eseguito l’installazione (amministratore).

In questo caso occorre individuare le chiavi mancanti e clonarle nel profilo di ciascun utente.
Per questo scopo si può **esportare** le chiavi da regedit in un file .reg, **accedere come utente** e **importare** nel registro le chiavi esportate.
La procedura va ripetuta per ogni utente che deve fare utilizzare l’applicazione (Le chiavi utente nel registro sono presenti solo quando l’utente è connesso).

Eventualmente, con tutti i problemi di sicurezza connessi (vedi slide precedente), si può verificare se è sufficiente importare le chiavi in HKLM. (Non è detto, tuttavia, che sia previsto che l’applicazione le cerchi in quel percorso).

“Houston, abbiamo un problema…”

- Spesso la soluzione dei problemi più frequenti di installazione in ambiente multiutente si identifica con una attenta ricognizione dell’installato, sia per il file system, sia per il registro di sistema.
- Fare attenzione ai messaggi di errore che spesso (ma non sempre) danno una prima indicazione della fonte del problema. (Es. un accesso negato). Consultare anche il visualizzatore di eventi di Windows.
- Se l’applicazione non si avvia si può tentare di farla eseguire dall’utente come *amministratore* o *power user* (con *“esegui come…”* oppure inserendo l’utente **temporaneamente** nel gruppo *administrators*).
  Questo consente di discriminare tra permessi insufficienti e percorsi di installazione errati/mancanti.

Se l’applicazione sembra funzionare facendo accesso come utente con autorizzazioni limitate, **verificare, comunque, che sia funzionale in tutte le sue parti** in altre parole, eseguire un lavoro completo in tutte le sue fasi (salvataggio, stampa, etc come così come verrebbe eseguito dall’utente).

Verificare sul manuale dell’applicativo se sono previste personalizzazioni in merito a percorsi di installazione, file temporanei, librerie, output dati, etc

Ultima possibilità per individuare il problema: impiegare utility di monitoraggio del file system e del registro (es. **process monitor** http://www.sysinternals.com) alla ricerca dei file e chiavi interessate dall’esecuzione del programma.