appropriate autorizzazioni all'interno del codice. Quando il codice richiede autorizzazioni utilizzando il metodo Demand, CLR verifica che tutti i moduli che chiamano il codice in questione dispongano delle autorizzazioni appropriate. Senza queste autorizzazioni, la richiesta non riesce. La verifica delle autorizzazioni viene determinata eseguendo uno stack-walk. È importante dal punto di vista dell'usabilità e della sicurezza che il codice riceva le autorizzazioni minime necessarie per l'esecuzione.
Nell'esempio di codice riportato di seguito viene illustrata una richiesta di autorizzazione di base:

```
[assembly:FileIOPermissionAttribute(SecurityAction.RequestMinimum,Write="C:\\test.tmp")]
[assembly:PermissionSet(SecurityAction.RequestOptional,Unrestricted=false)]
```

Questo esempio indica al sistema di protezione del Framework .NET che il codice non dovrebbe essere eseguito a meno che, non riceva l'autorizzazione a scrivere a C: \ test.tmp. Se il codice incontra sempre criteri di protezione che non concedono quest'autorizzazione, viene generata una PolicyException e il codice non viene eseguito. Utilizzando questa richiesta, si può essere certi che il codice verrà eseguito solo se verrà concessa tale autorizzazione.
Questo esempio indica anche al sistema che non è richiesta alcuna autorizzazione aggiuntiva. Le autorizzazioni di esecuzione non necessarie al codice possono portare a problemi di sicurezza.
Un altro modo per limitare le autorizzazioni che il codice riceve, in base al criterio dei minimi privilegi, è quello di elencare le autorizzazioni specifiche che si desidera rifiutare.

7.6.10.4 Protezione dell'accesso ai metodi

.NET Framework fornisce un meccanismo denominato Code Access Security (CAS), che consente di applicare vari livelli di attendibilità a codice diverso in esecuzione nella stessa applicazione.
Alcuni metodi potrebbero non essere adatti per consentire le chiamate da parte di codice arbitrario non attendibile. Potrebbero, infatti, fornire informazioni limitate; potrebbero non eseguire il controllo degli errori sui parametri; non verificare la correttezza dei parametri; potrebbero funzionare in modo non corretto o causare qualche problema. L'utente dovrebbe essere informato di questi casi e adottare le misure appropriate per proteggerli.
In alcuni casi, potrebbe essere necessario limitare i metodi che non sono destinati all'uso generalizzato da parte del pubblico, ma che devono comunque essere esposti pubblicamente. Ad esempio, nel caso di un'interfaccia che deve essere chiamata attraverso le proprie DLL e pertanto deve essere pubblica, ma che non si vuole esporre pubblicamente, per evitare che il suo punto d'ingresso possa essere sfruttato da codice dannoso. Un altro motivo comune per limitare un metodo non destinato all'uso pubblico (ma che deve essere pubblico) consiste nell'evitare di dover documentare e supportare quella che potrebbe essere un'interfaccia molto interna.
Il codice gestito (managed code) offre diverse possibilità per essere adeguatamente protetto:
Limitare l'ambito di accessibilità alla classe, all'assembly o alle classi derivate, se queste sono affidabili. Questo è il modo più semplice per limitare l'accesso al metodo. Si noti che, in generale, le classi derivate possono essere meno affidabili della classe da cui derivano, sebbene in alcuni casi condividano l'identità della classe genitore. In particolare, non dedurre il grado di sicuerzza dalla parola chiave protected, che viene utilizzata in un contesto non necessariamente relativo alla sicurezza.
Limitare l'accesso del metodo a determinati chiamanti. Il criterio di selezione può essere il nome sicuro (strong name), l'identità di chi lo pubblica, la zona, ecc.
Limitare l'accesso del metodo ai chiamanti che dispongono di specifiche autorizzazioni.
Analogamente la sicurezza delle dichiarazioni consente di controllare l'ereditarietà delle classi. È possibile utilizzare InheritanceDemand per eseguire le seguenti operazioni:

- Imporre che le classi derivate abbiano un'identità o un'autorizzazione specificate.
- Imporre alle classi derivate di sostituire metodi specifici per avere un'identità o un'autorizzazione specifici.

L'esempio seguente illustra come proteggere una classe pubblica, limitando l'accesso, con la richiesta che i chiamanti si firmino con un nome sicuro specifico.