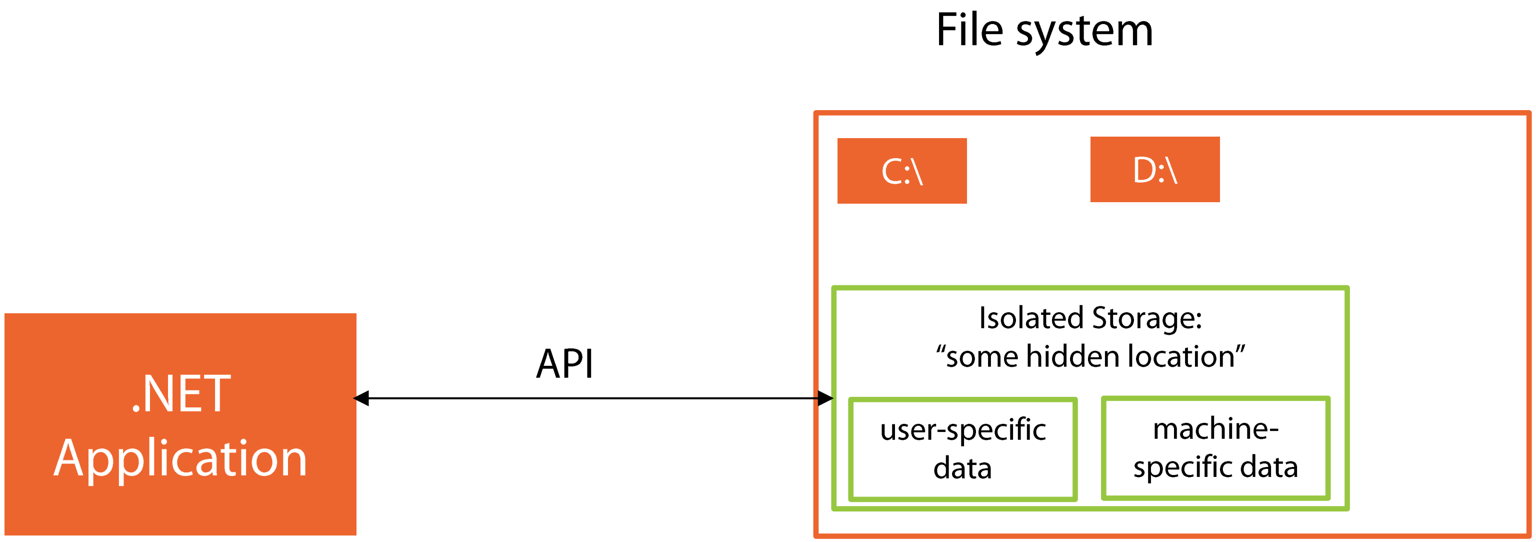
Restricted File Access With IsolatedStorageFileStream

Mohamad Halabi
Microsoft Integration MVP
@mohamadhalabi

pluralsight
hardcore dev and IT training

Isolated Storage



- **Example:** ***C:\Users\[user name]\AppData\Local\IsolatedStorage***

Usage Scenarios

- **Isolated storage locations would be useful in various cases:**
  - Restricted-access applications, such as Silverlight and ClickOnce
  - Storing temporary user or machine-specific data
  - Wanting a guaranteed application-unique location

Security

- **Isolated storage data is not secured against unwanted access, even though it's stored in "some" complex location**
- **User browsing the file system can dig out the data**
- **For applications:**
  - Restricted file-access applications cannot access secured data through the isolated storage API
  - Applications that are not restricted can dig out the data
- **In short: do not rely on isolated storage to 'hide' secure data**
  - It's a place to store user and machine-specific data
    - For partially trusted applications
    - For applications that do not care about the physical path of data

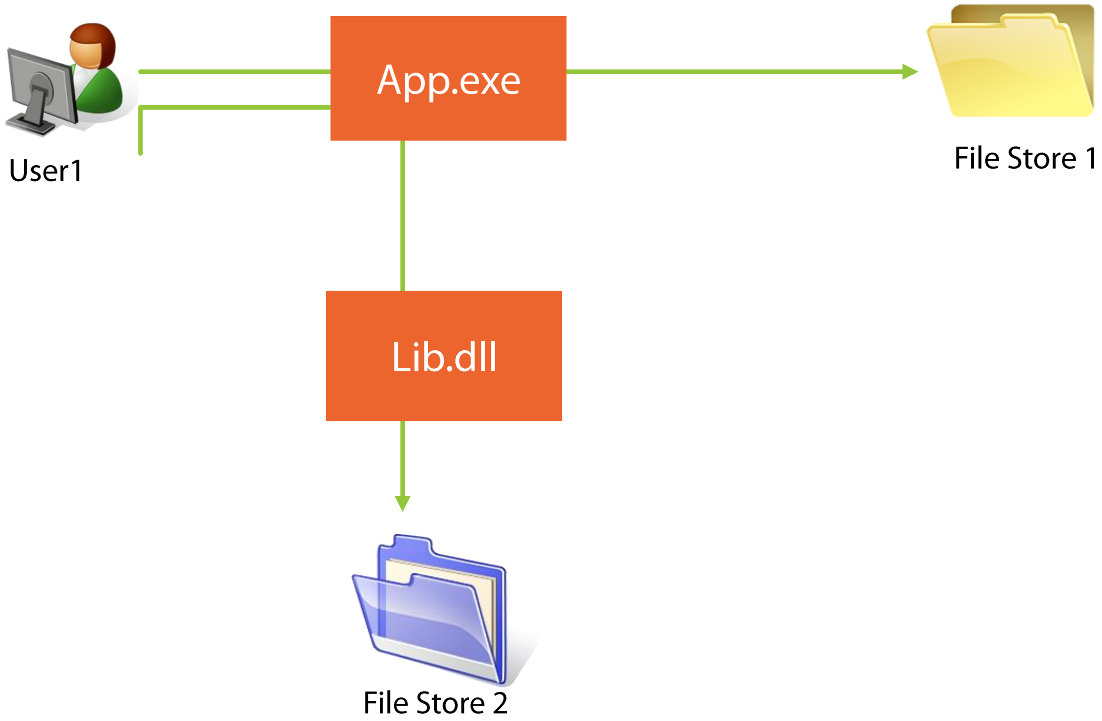
Isolated Storage Types

- What are these “special” isolated storage locations?
- System.IO.IsolatedStorage.IsolatedStorageFile exposes different storage locations

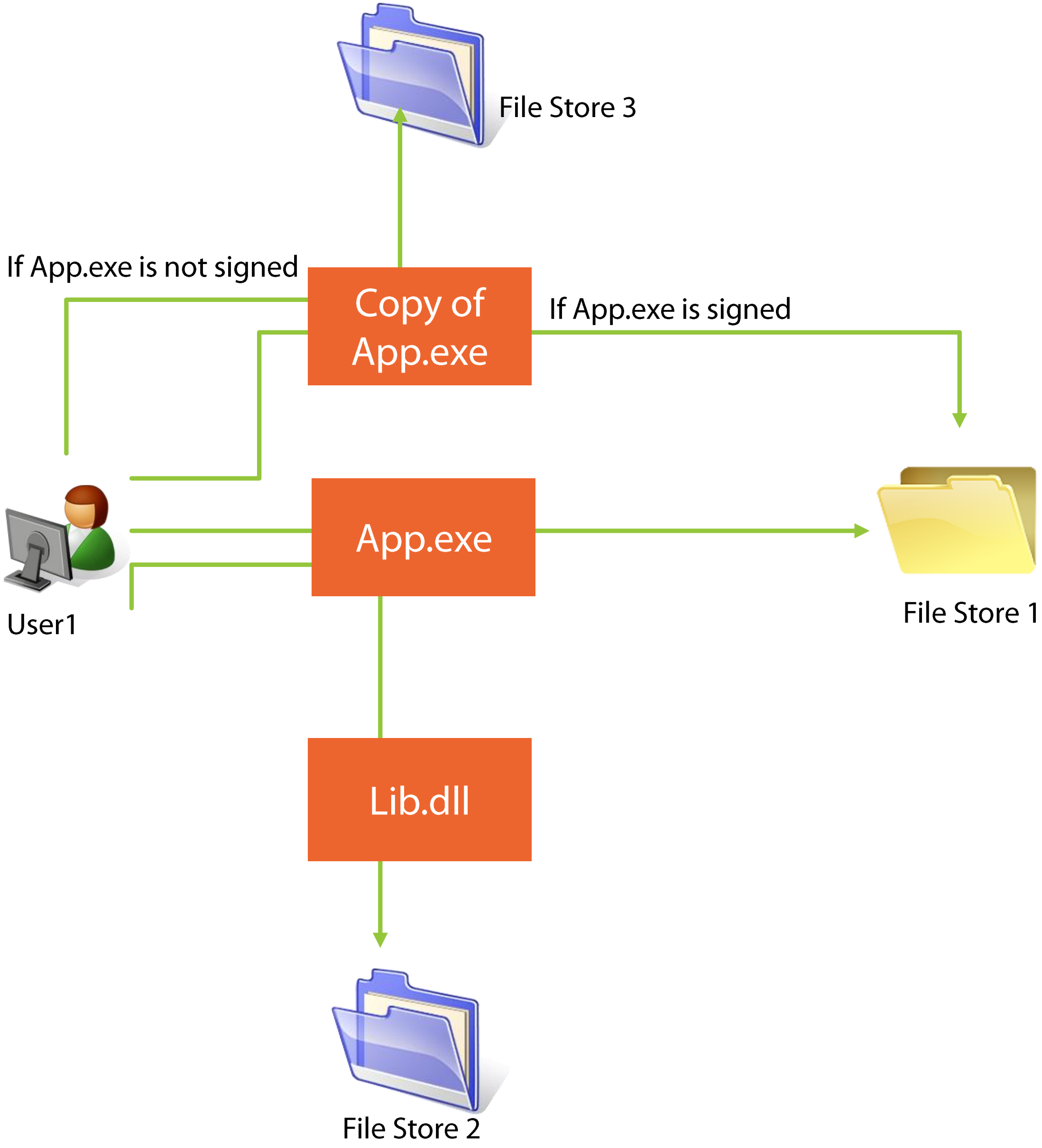
User-specific	Machine-specific
GetUserStoreForAssembly GetUserStoreForDomain GetUserStoreForApplication GetUserStoreForSite	GetMachineStoreForAssembly GetMachineStoreForDomain GetMachineStoreForApplication

GetUserStoreForAssembly

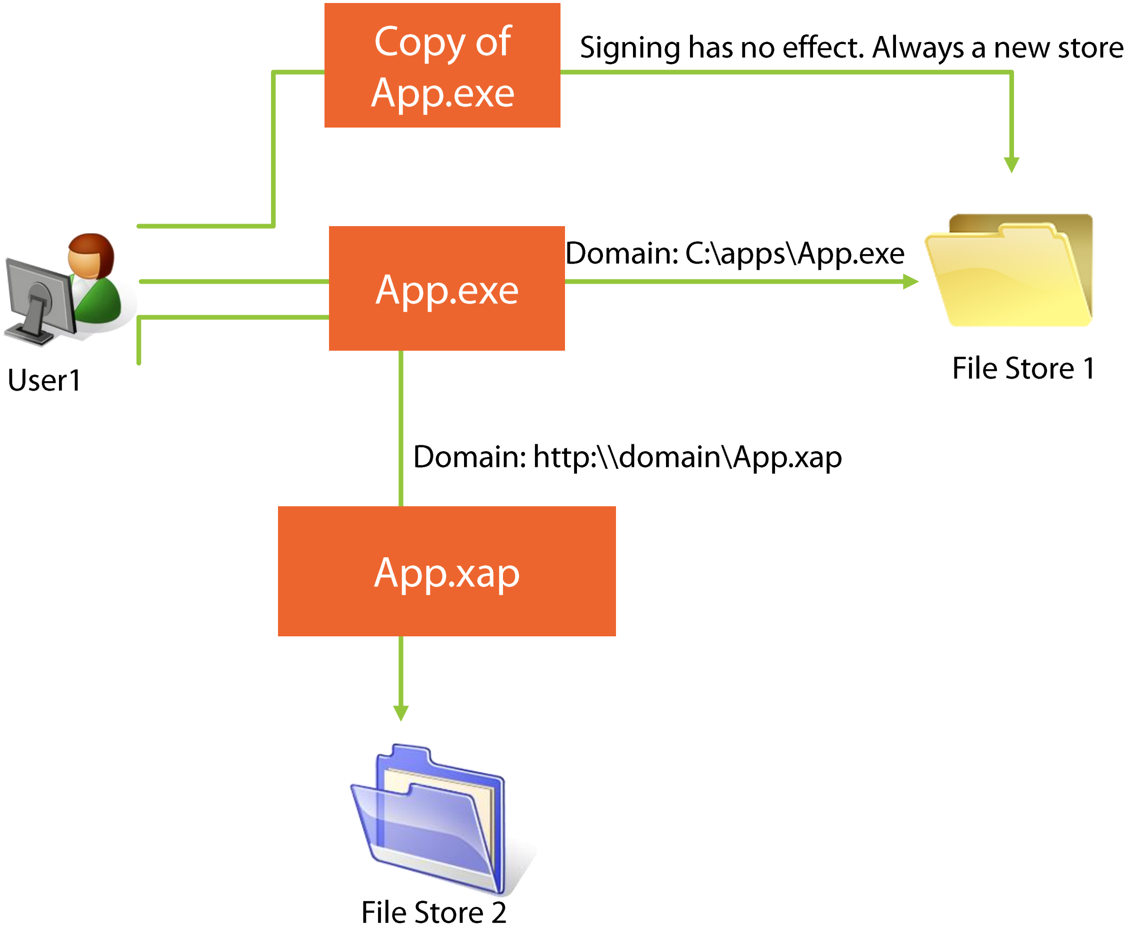
- **Store unique to:**
  - Specific user
  - Assembly running under this user's identity (logged-in user, app pool identity)



GetUserStoreForAssembly…Cont'd



GetUserStoreForDomain



Copy of App.exe

Signing has no effect. Always a new store

App.exe

Domain: C:\apps\App.exe

User1

File Store 1

Domain: http:\\domain\App.xap

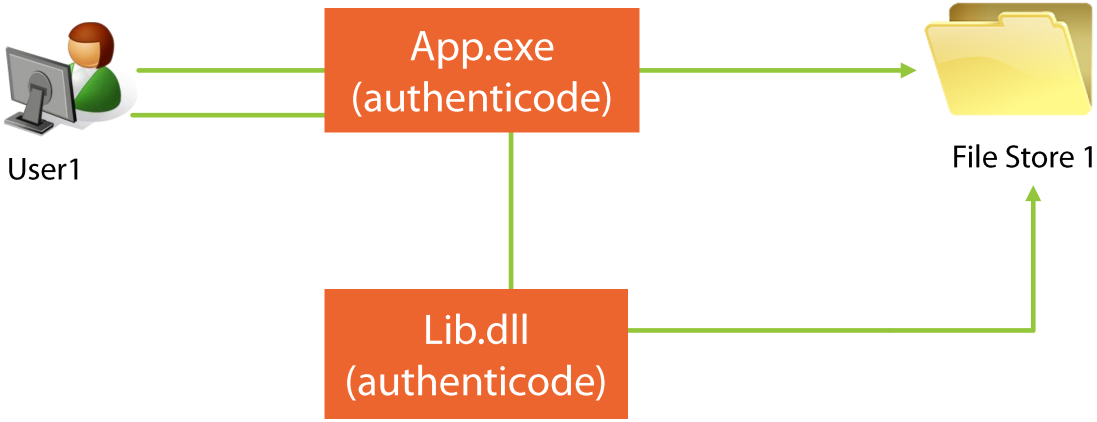
App.xap

File Store 2

Domain isolation == assembly isolation when application is copied and not signed

GetUserStoreForApplication

- **Requires Authenticode signature**
- **Authenticode verifies publisher or author of an assembly**
  - Strong name signature guarantee unique assembly identity



GetUserStoreForSite

- **Also provides a unique storage location per user…**
  - But within scope of an entire web domain
- **A user will get the same store across all applications from same web domain**

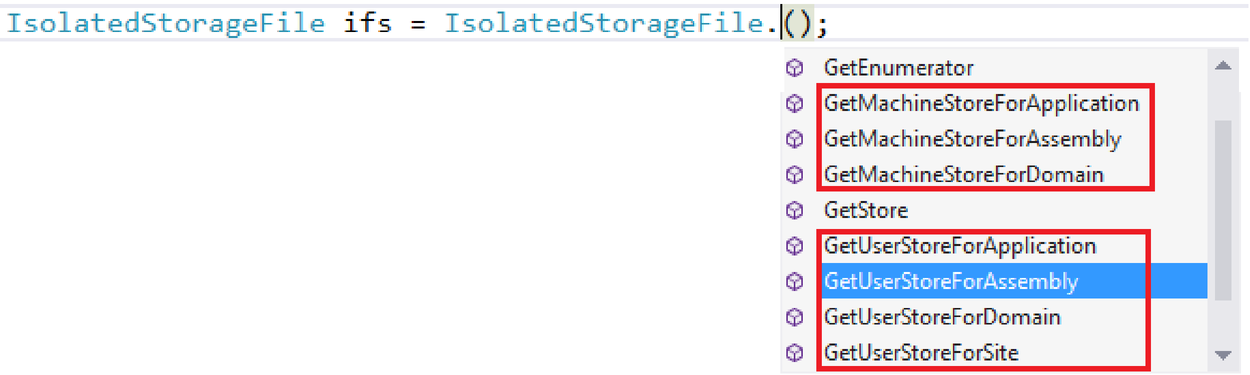
Machine Isolation

- **So far we have discussed isolation by users…**
- **There other type is isolation by machine**
  - Application data shared by all users in the system

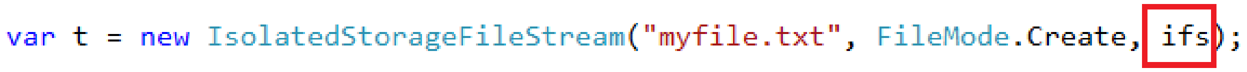
Machine Isolation Method	Equivalent User Isolation Method
GetMachineStoreForApplication	GetUserStoreForApplication
GetMachineStoreForDomain	GetUserStoreForDomain
GetMachineStoreForAssembly	GetUserStoreForAssembly

IsolatedStorageFileStream

- IsolatedStorageFileStream is used to read and write from isolated storage locations



```
IsolatedStorageFile ifs = IsolatedStorageFile.();
```



```
var t = new IsolatedStorageFileStream("myfile.txt", FileMode.Create, ifs);
```

IsolatedStorageFileStream

- **IsolatedStorageFileStream constructors accept same FileStream parameters (FileMode, FileAccess, FileShare, bufferSize)**
- **FileStream read/write techniques apply here also**
- **You can set quotas for max data that can be written to a store**
  - Important for partial trust applications
  - Default 1 MB
  - IsolatedStorageFile.Quota to query quota
  - IncreaseQuotaTo() to increase quota
    - Cannot be reduced anymore

Summary

- **Isolated storage: special file storage location for applications**
  - Stores user and machine-specific data
  - Actual physical location is hidden behind an API
- **IsolatedStorageFile class exposes different isolation locations**
  - Two categories: user and machine isolations
- **IsolatedStorageFileStream is used to read/write into isolated storage**
- **Cases of usage:**
  - Restricted file-access applications
  - Applications needing only temporary files
  - Applications wanting guaranteed unique file access