Effective Visualization of File System Access-Control

Alex Heitzmann
Charalampos Papamanthou
Roberto Tamassia
CSI – Brown University, RI, USA

Bernardo Palazzi
DIA – Roma Tre University, IT
ISCOM – Ministry of Communications, IT
CSI – Brown University, RI, USA

CS 167/9 Guest Lecture

Sponsors: U.S. National Science Foundation, Kanellakis Fellowship at Brown University, and Italian Ministry of Research.

Discretionary Access Control

- Users can protect what they own.
- The owner may grant access to others.
- The owner may define the type of access (read/write/execute) given to others.
- This is the standard model used in many operating systems
- Alternative model (not covered): Mandatory Access Control (MAC)

Closed Policy

- Give Tom read access to “foo”
- Give Bob r/w access to “bar”
  - Tom: I would like to read “foo”
    - Access allowed
  - Tom: I would like to read “bar”
    - Access denied
- This policy is also called “default secure”

Open Policy

- Deny Tom read access to “foo”
- Deny Bob r/w access to “bar”
  - Tom: I would like to read “foo”
    - Access denied
  - Tom: I would like to read “bar”
    - Access allowed
- Windows uses also this kind of policy

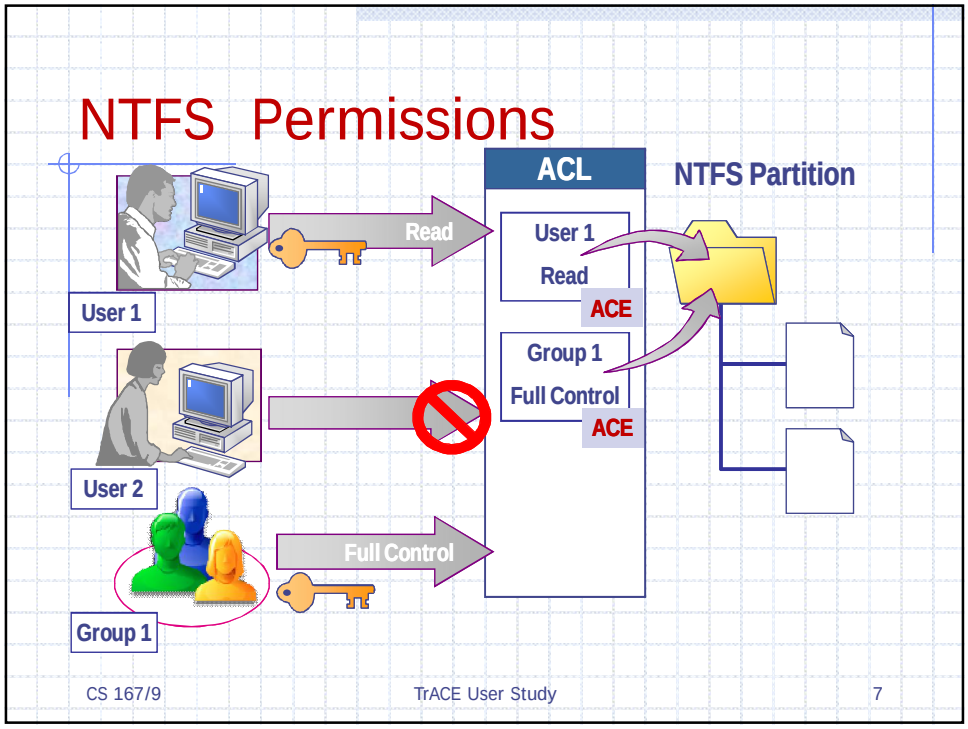
Closed Policy with Negative Authorizations and Deny Priority

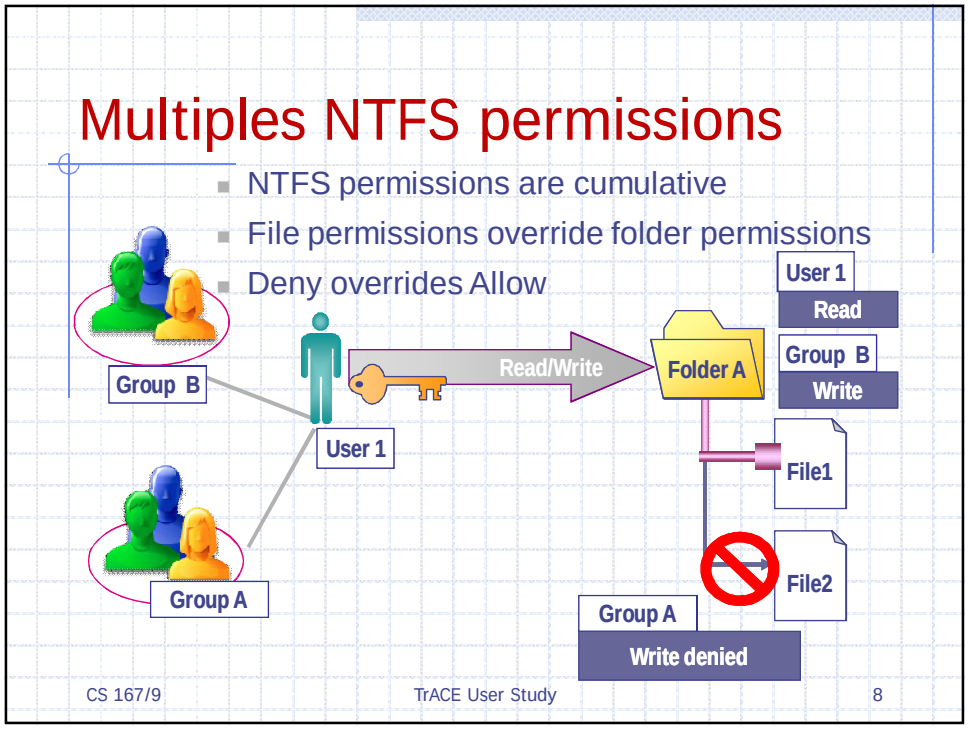
- Give Tom r/w access to “bar”
- Deny Tom write access to “bar”

  Tom: I would like to read “bar”
  - Access allowed
  - Tom: I would like to write “bar”
    - Access denied
- This policy is used by Windows to manage access control

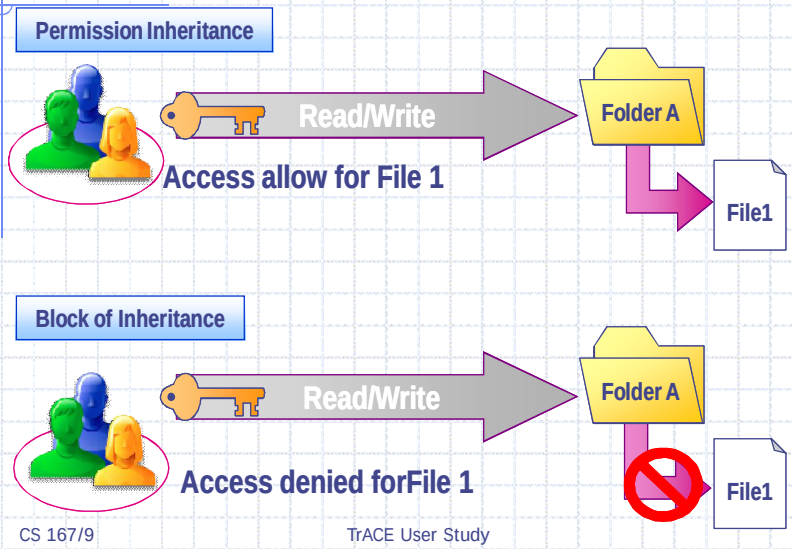
Access Control Entries and Lists

- A Discretionary Access Control List (DACL) for a resource (e.g., a file or folder) is a sorted list of zero or more Access Control Entries (ACEs)
- An ACE refers specifies that a certain set of accesses (e.g., read, execute and write) to the resources is allowed or denied for a user or group
- Examples of ACEs for folder “Bob’s CS167 Grades”
  - Bob; Read; Allow
  - TAs; Read; Allow
  - TWD; Read, Write; Allow
  - Bob; Write; Deny
  - TAs; Write; Allow


NTFS Permissions
ACL
NTFS Partition
Read
User 1
Read
ACE
Group 1
Full Control
ACE
User 1
User 2
Full Control
Group 1
CS 167/9
TrACE User Study
7


Multiples NTFS permissions
NTFS permissions are cumulative
File permissions override folder permissions
Deny overrides Allow
User 1
Read
Group B
Write
Read/Write
Folder A
Group B
User 1
File1
File2
Group A
Group A
Write denied
CS 167/9
TrACE User Study
8

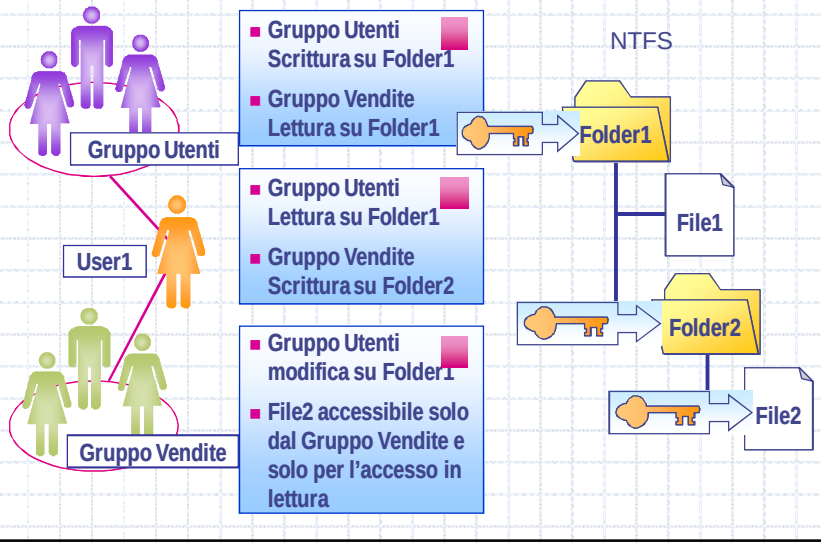
NTFS: permission inheritance



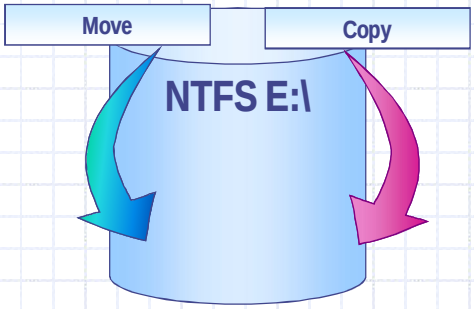
Access Control Algorithm

- The DACL of a file or folder is a sorted list of ACEs
  - Local ACEs precede inherited ACEs
  - ACEs inherited from folder F precede those inherited from parent of F
  - Among those with same source, Deny ACEs precede Allow ACEs
- Algorithm for granting access request (e.g., read and execute):
  - ACEs in the DACL are examined in order
  - Does the ACE refer to the user or a group containing the user?
  - If so, do any of the accesses in the ACE match those of the request?
  - If so, what type of ACE is it?
    - **Deny**: return ACCESS_DENIED
    - **Allow**: grant the specified accesses and if there are no remaining accesses to grant, return ACCESS_ALLOWED
  - If we reach the end of the DACL and there are remaining requested accesses that have not been granted yet, return ACCESS_DENIED

Esempi: permessi NTFS

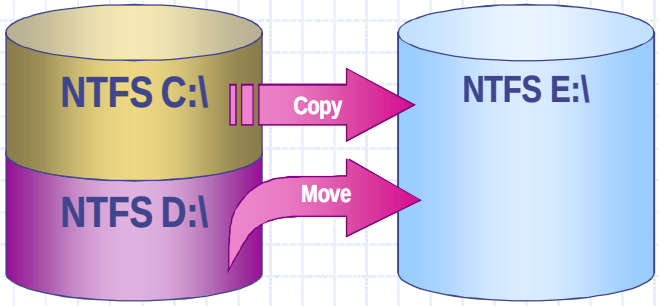


NTFS: move or copy a file within the same volume



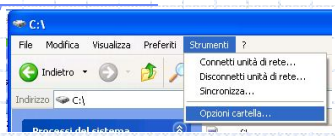
- If you **move** a file or a folder inside the same volume your permission will be the same of the **source** folder
- If you **copy** a file or a folder inside the same volume your permission will be the same of the **destination** folder

NTFS: move or copy a file across different volumes



- If you **copy** or **move** a file or a folder on different volumes your permission will be the same of the **destination** folder

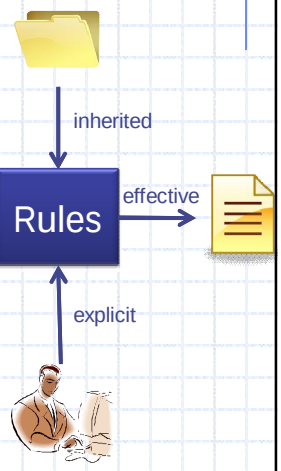
How activate NTFS permissions in Windows XP Pro



- NTFS permissions in Windows XP Pro are disabled by default.
- Using **Folder Options…** from **Tools** menu inside **Windows Explorer** is possible to activate NTFS permission in windows by unchecking **Use simple file sharing**

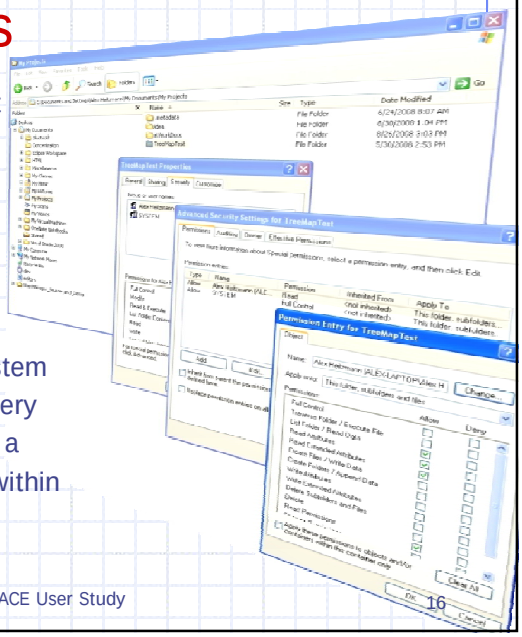
NTFS file permissions

- **Explicit**: set by the *owner* for each user/group.
- **Inherited**: dynamically inherited from the explicit permissions of ancestor folders.
- **Effective**: obtained by combining the explicit and inherited permission.
- Determining effective permissions:
  - By default, a user/group has no privileges.
  - Explicit permissions override conflicting inherited permissions.
  - Denied permissions override conflicting allowed permissions.

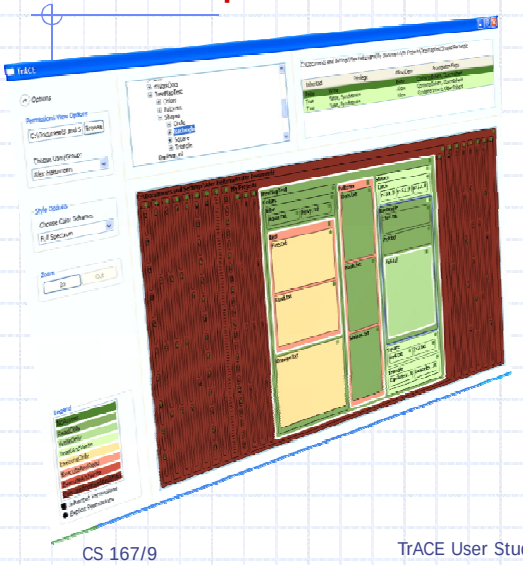


Windows Tools

- Access control management tools provide detailed information and controls, across multiple dialogs.
- Focus on single file/folders.
- It is challenging for an inexperienced user, or a system administrator dealing with very large file structures, to gain a global view of permissions within the file system .



Enter TrACE:
Treemap Access Control Evaluator



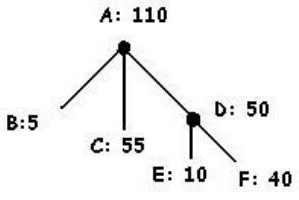
TrACE allows the user to:

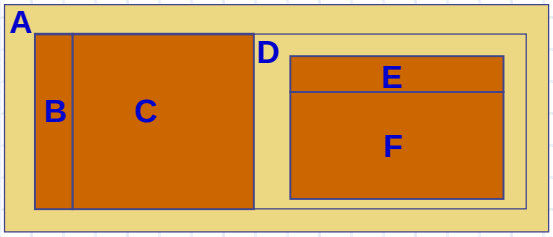
- At a glance, determine the explicit, inherited, and effective permissions of files and folders.
- Understand access control relationships between files and their ancestors.
- Quickly evaluate large directory structures and find problem areas.

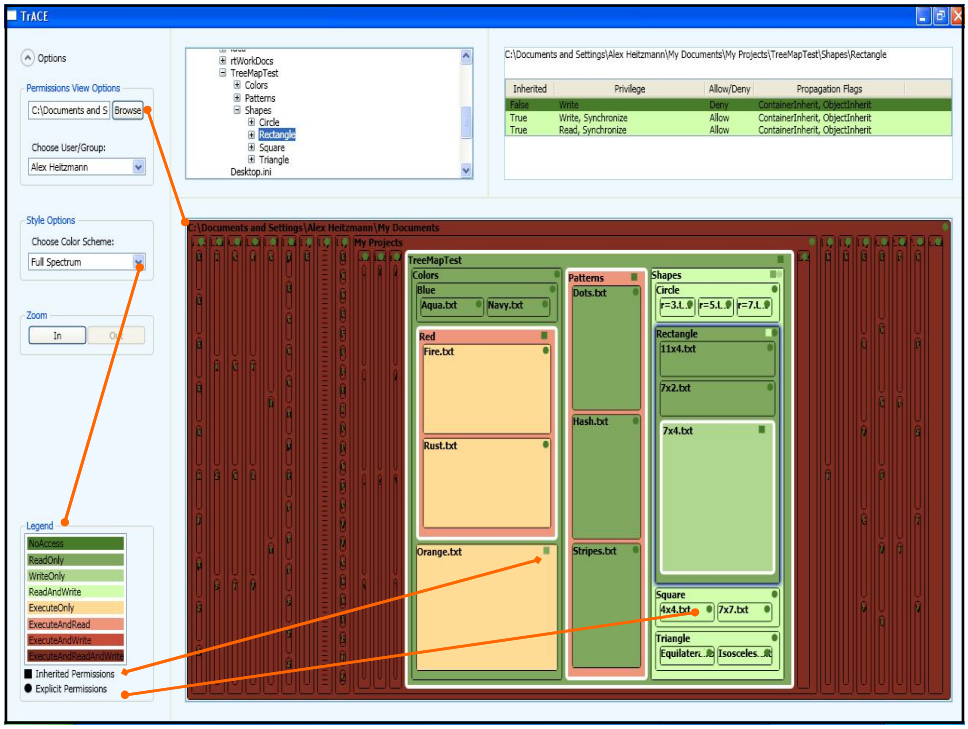
TrACE uses treemaps.

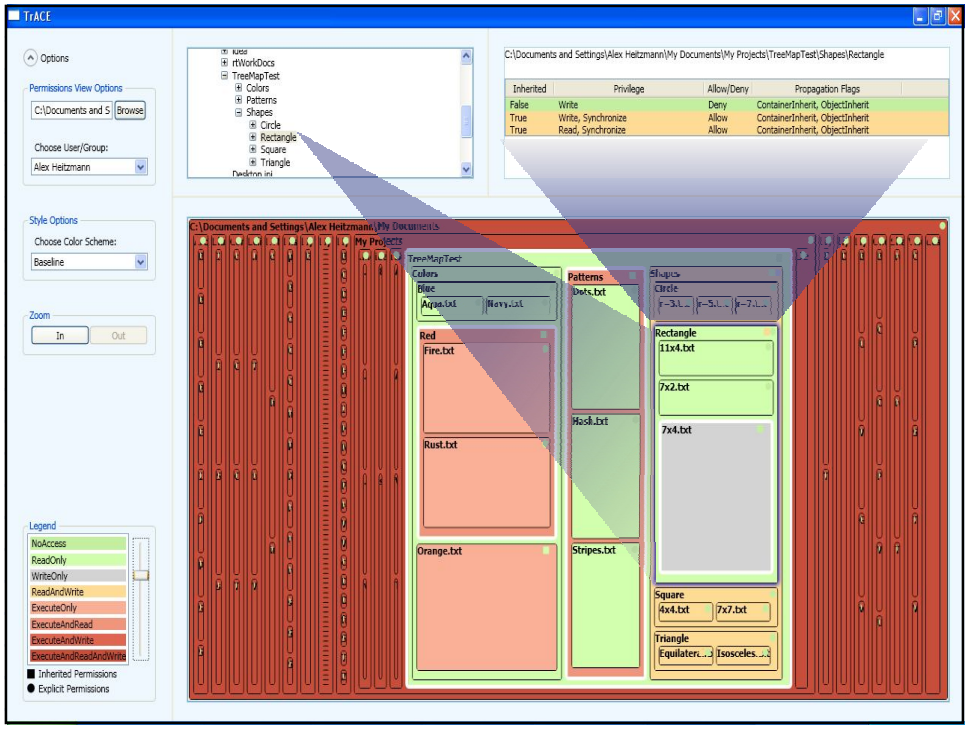
What is a Treemap?

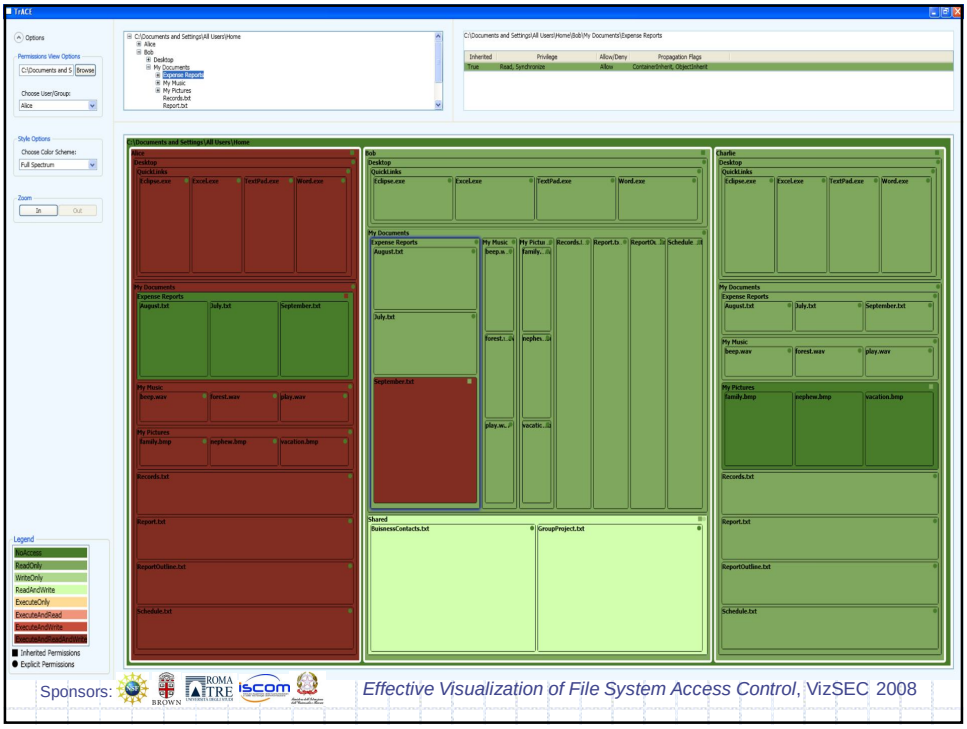
- A visualization method to display large hierarchical data structures (trees)
- Layout based on nested rectangles.
- Treemaps were introduced by Ben Shneiderman in "Tree visualization with tree-maps: 2-d space-filling approach"; TOG 1991






TrACE
Options
Permissions View Options
C:\Documents and S
Browse
Choose User/Group:
Alex Heitzmann
Style Options
Choose Color Scheme:
Full Spectrum
Zoom
In
Legend
NoAccess
ReadOnly
WriteOnly
ReadAndWrite
ExecuteOnly
ExecuteAndRead
ExecuteAndWrite
ExecuteAndReadAndWrite
Inherited Permissions
Explicit Permissions
rtWorkDocs
TreeMapTest
Colors
Patterns
Shapes
Circle
Rectangle
Square
Triangle
Desktop.ini
C:\Documents and Settings\Alex Heitzmann\My Documents\My Projects\TreeMapTest\Shapes\Rectangle
Inherited
Privilege
Allow/Deny
Propagation Flags
False
Write
Deny
ContainerInherit, ObjectInherit
True
Write, Synchronize
Allow
ContainerInherit, ObjectInherit
Read, Synchronize
C:\Documents and Settings\Alex Heitzmann\My Documents
My Projects
TreeMapTest
Blue
Aqua.txt
Navy.txt
Red
Fire.txt
Rust.txt
Orange.txt
Dots.txt
Hash.txt
Stripes.txt
r=3.L
r=5.L
r=7.L
11x4.txt
7x2.txt
7x4.txt
4x4.txt
7x7.txt
Equilater...
Isosceles...


TrACE
Options
Permissions View Options
C:\Documents and S
Browse
Choose User/Group:
Alex Heitzmann
Style Options
Choose Color Scheme:
Baseline
Zoom
In
Out
Legend
NoAccess
ReadOnly
WriteOnly
ReadAndWrite
ExecuteOnly
ExecuteAndRead
ExecuteAndWrite
ExecuteAndReadAndWrite
Inherited Permissions
Explicit Permissions
rtWorkDocs
TreeMapTest
Colors
Patterns
Shapes
Circle
Rectangle
Square
Triangle
C:\Documents and Settings\Alex Heitzmann\My Documents\My Projects\TreeMapTest\Shapes\Rectangle
Inherited
Privilege
Allow/Deny
Propagation Flags
False
Write
Deny
ContainerInherit, ObjectInherit
True
Write, Synchronize
Allow
ContainerInherit, ObjectInherit
Read, Synchronize
Blue
Aqua.txt
Red
Fire.txt
Rust.txt
Orange.txt
Dots.txt
Hash.txt
Stripes.txt
11x4.txt
7x2.txt
7x4.txt
4x4.txt
7x7.txt


TrACE
Options
Permissions View Options
Choose User/Group:
Style Options
Choose Color Scheme:
Full Spectrum
Zoom
Legend
NoAccess
ReadOnly
WriteOnly
ReadAndWrite
ExecuteOnly
ExecuteAndRead
ExecuteAndWrite
Inherited Permissions
Explicit Permissions
Sponsors:
Effective Visualization of File System Access Control, VizSEC 2008