Effective Visualization of File System Access-Control

Alex Heitzmann
Charalampos Papamanthou
Roberto Tamassia

CSI – Brown University, RI, USA

Bernardo Palazzi

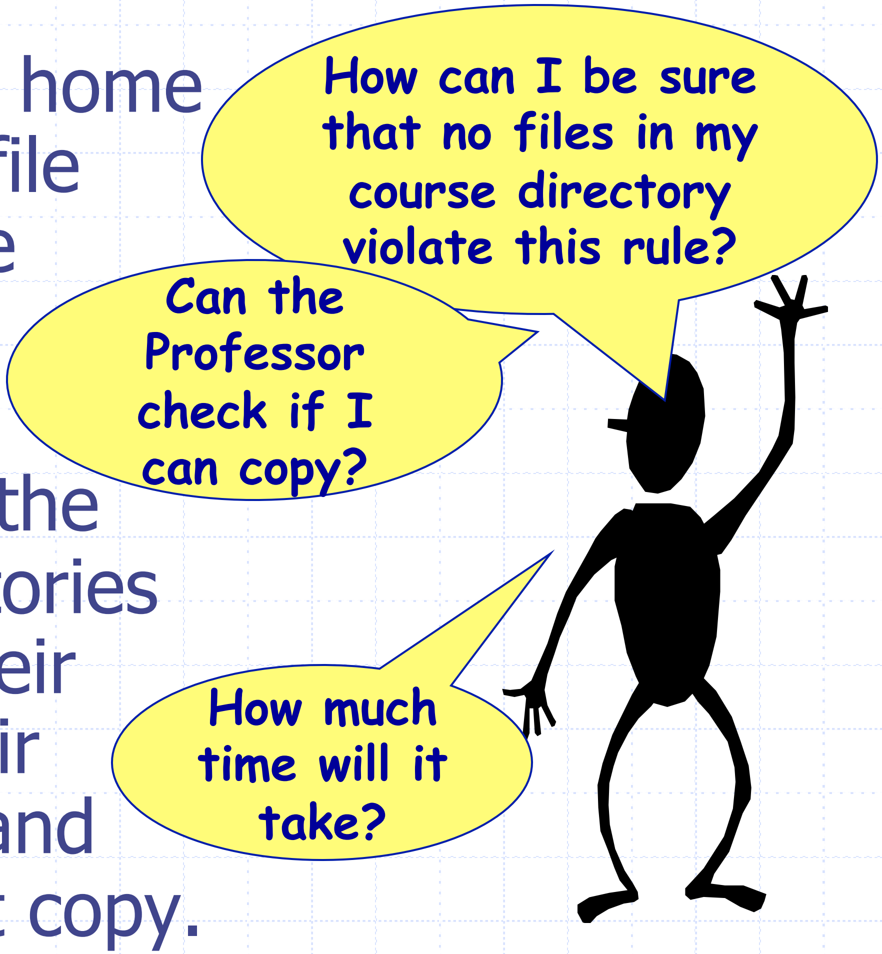
DIA – Roma Tre University, IT
ISCOM – Ministry of Communications, IT
CSI – Brown University, RI, USA

vizSEC '08

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

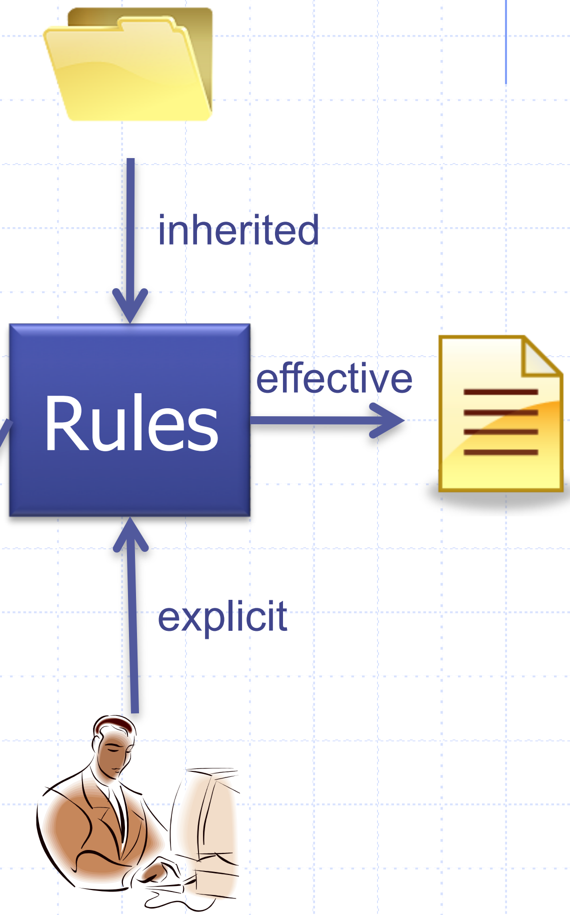
A Problem in our Department

- Each CS student has a home directory on a shared file system for their course work.
- The department has recently required that the students' course directories are not readable by their classmates so that their work remains private and other students can not copy.


How can I be sure that no files in my course directory violate this rule?
Can the Professor check if I can copy?
How much time will it take?

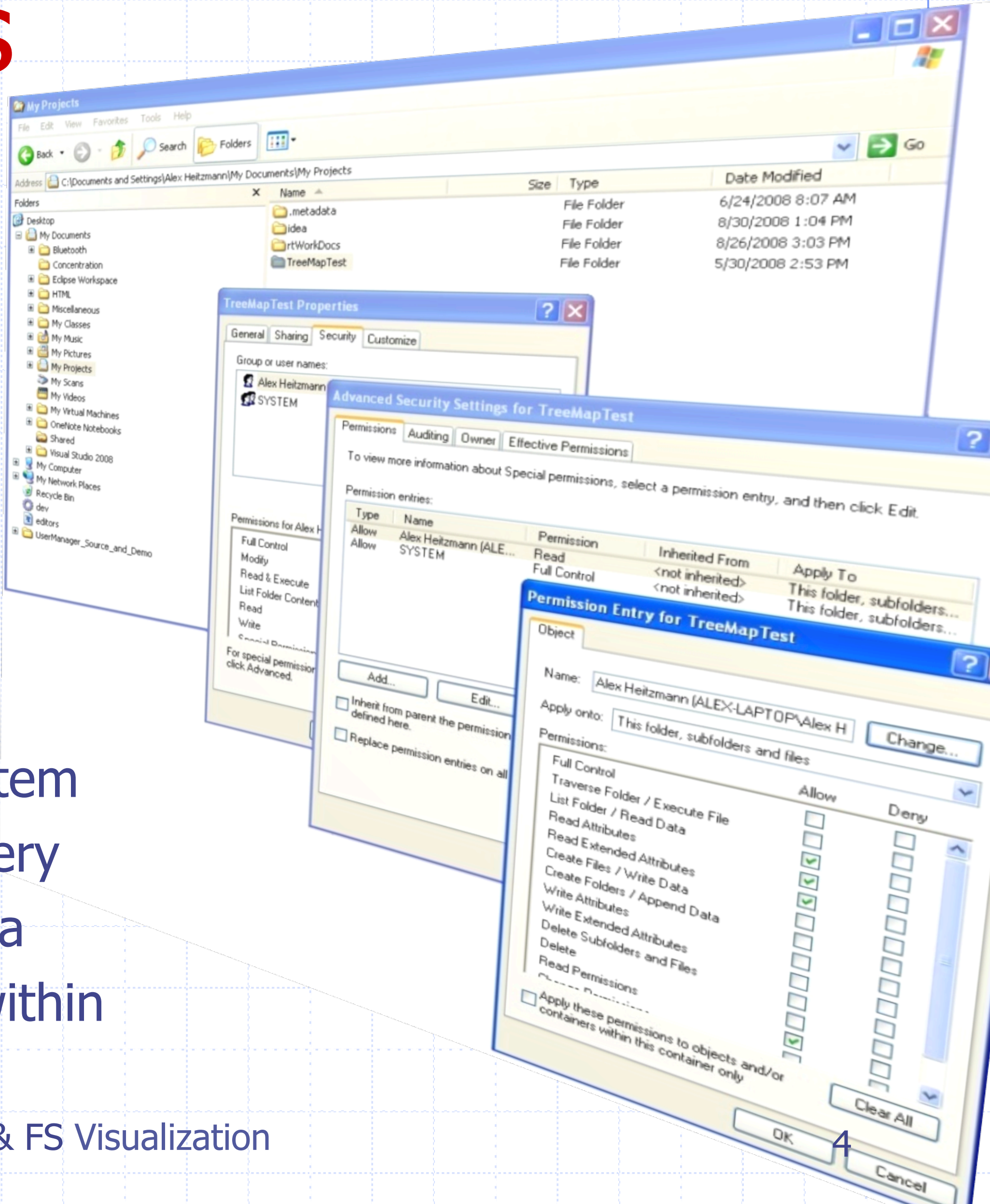
NTFS file permissions

- **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.



Address C:\Documents and Settings\Alex Heitzmann\My Documents\My Projects

Name	Size	Type	Date Modified
.metadata		File Folder	6/24/2008 8:07 AM
idea		File Folder	8/30/2008 1:04 PM
rtWorkDocs		File Folder	8/26/2008 3:03 PM
TreeMapTest		File Folder	5/30/2008 2:53 PM

TreeMapTest Properties

Group or user names:

Alex Heitzmann
SYSTEM

Permissions for Alex H

Full Control
Modify
Read & Execute
List Folder Content
Read
Write

For special permission click Advanced.

Advanced Security Settings for TreeMapTest

To view more information about Special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Alex Heitzmann (ALE...	Read	<not inherited>	This folder, subfolders...
Allow	SYSTEM	Full Control	<not inherited>	This folder, subfolders...

□ Inherit from parent the permission defined here.

□ Replace permission entries on all

Permission Entry for TreeMapTest

Name: Alex Heitzmann (ALEX-LAPTOP\Alex H

Apply onto: This folder, subfolders and files

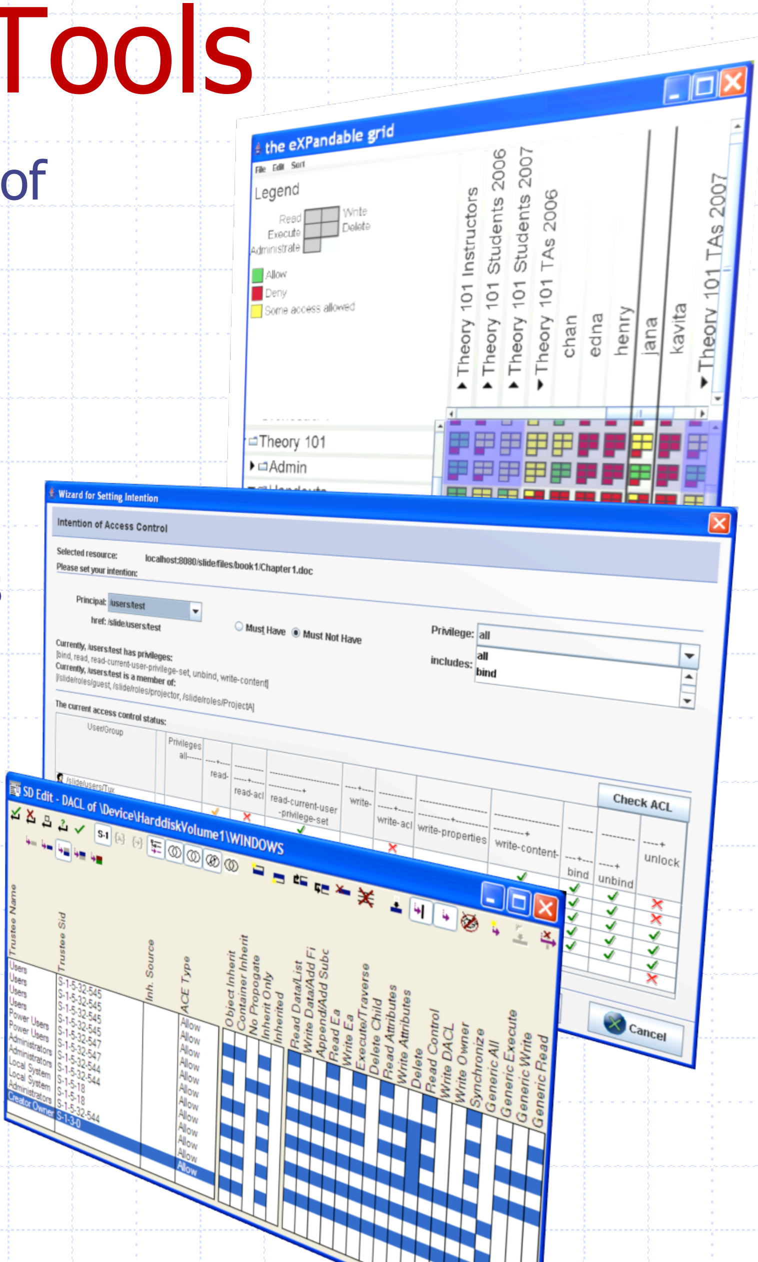
Permissions:

	Allow	Deny
Full Control	□	□
Traverse Folder / Execute File	□	□
List Folder / Read Data	☑	□
Read Attributes	☑	□
Read Extended Attributes	☑	□
Create Files / Write Data	□	□
Create Folders / Append Data	□	□
Write Attributes	□	□
Write Extended Attributes	□	□
Delete Subfolders and Files	□	□
Delete	□	□
Read Permissions	☑	□

□ Apply these permissions to objects and/or containers within this container only

Existing 3rd Party Tools

- Matrix-based, allowing consolidation of information into a single window.
- Reeder et al.; “Expandable Grids for Visualizing and Authoring Computer Security Policies”; SIGCHI 2008
- Cao and Iverson; “Intentional Access Management: Making Access Control Usable for End-Users”; SOUPS 2006
- Smith; SdEDIT, 2006
    - http://czwsoft.dyndns.org/sdedit.html



the eXPandable grid

Legend

Read, Write, Execute, Delete, Administrate

🟩 Allow

🟥 Deny

🟨 Some access allowed

Theory 101 Instructors, Theory 101 Students 2006, Theory 101 Students 2007, Theory 101 TAs 2006, chan, edna, henry, jana, kavita, Theory 101 TAs 2007

Theory 101

Admin

Handouts

Wizard for Setting Intention

Intention of Access Control

Selected resource: localhost:8080/slide/files/book1/Chapter1.doc

Please set your intention:

Principal: /users/test

href: /slide/users/test

○ Must Have ● Must Not Have

Privilege: all

includes: all, bind

Currently, /users/test has privileges:
[bind, read, read-current-user-privilege-set, unbind, write-content]

Currently, /users/test is a member of:
[/slide/roles/guest, /slide/roles/projector, /slide/roles/ProjectA]

The current access control status:

User/Group: /slide/users/Tux

Privileges: all, read, read-acl, read-current-user-privilege-set, write, write-acl, write-properties, write-content, bind, unbind, unlock

Check ACL

Cancel

SD Edit - DACL of \Device\HarddiskVolume1\WINDOWS

Trustee Name: Users, Users, Users, Users, Power Users, Power Users, Administrators, Administrators, Local System, Local System, Administrators, Creator Owner

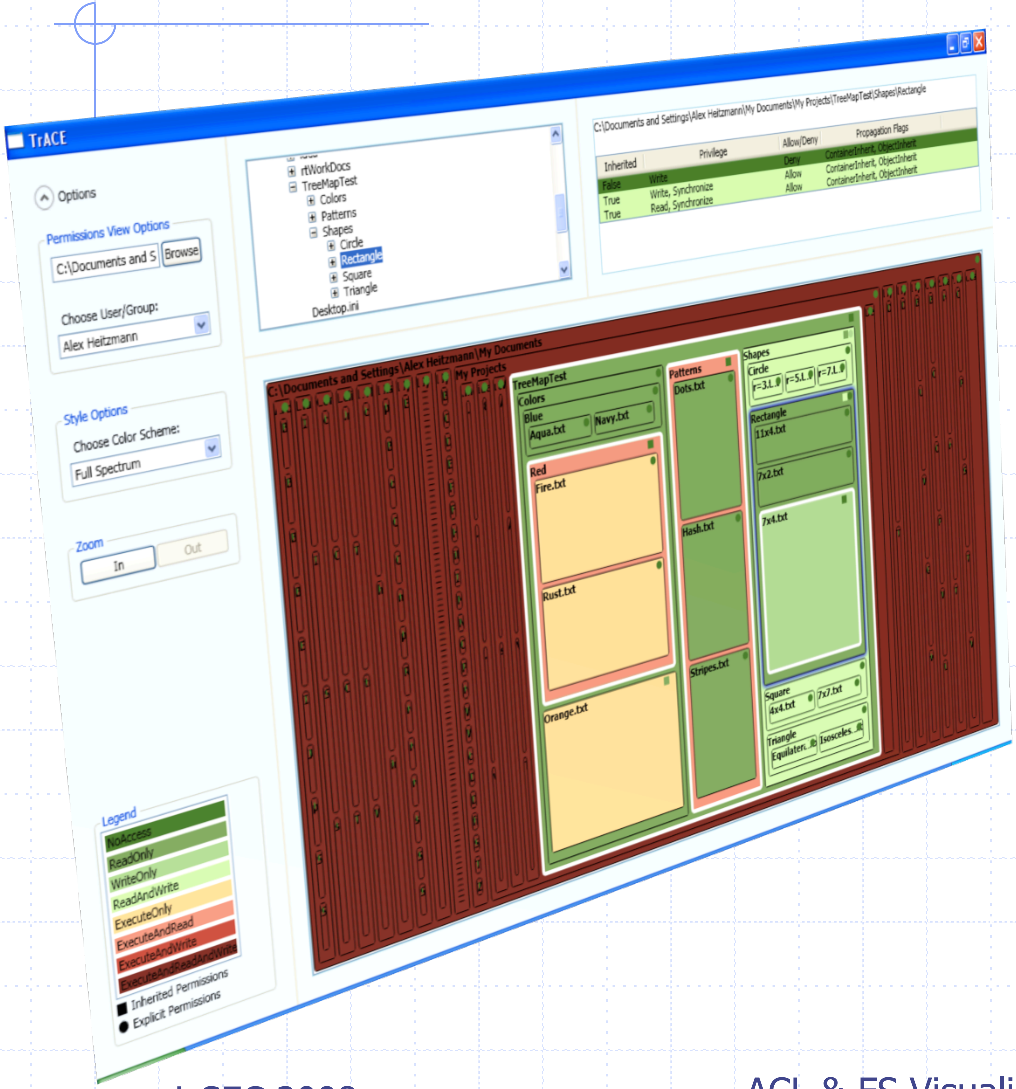
Trustee Sid: S-1-5-32-545, S-1-5-32-545, S-1-5-32-545, S-1-5-32-545, S-1-5-32-545, S-1-5-32-547, S-1-5-32-547, S-1-5-32-544, S-1-5-32-544, S-1-5-18, S-1-5-18, S-1-5-32-544, S-1-3-0

Inh. Source

ACE Type: Allow, Allow, Allow, Allow, Allow, Allow, Allow, Allow, Allow, Allow, Allow, Allow, Allow

Object Inherit, Container Inherit, No Propogate, Inherit Only, Inherited, Read Data/List, Write Data/Add Fi, Append/Add Subc, Read Ea, Write Ea, Execute/Traverse, Delete Child, Read Attributes, Write Attributes, Delete, Read Control, Write DACL, Write Owner, Synchronize, Generic All, Generic Execute, Generic Write, Generic Read

Enter TrACE: Treemap Access Control Evaluator



Permissions View Options: C:\Documents and S

Choose User/Group: Alex Heitzmann

Choose Color Scheme: Full Spectrum

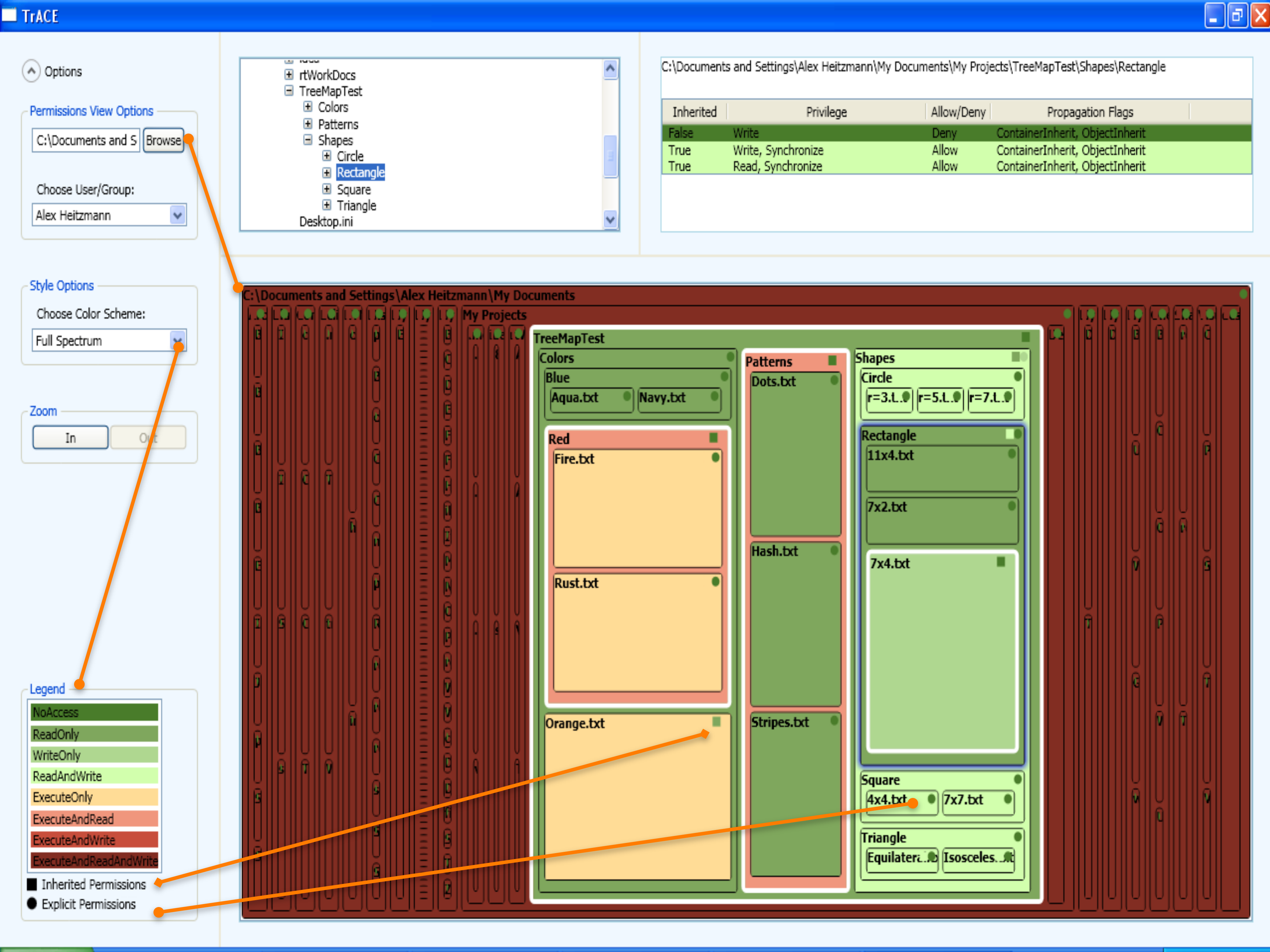
C:\Documents and Settings\Alex Heitzmann\My Documents\My Projects\TreeMapTest\Shapes\Rectangle

Inherited	Privilege	Allow/Deny	Propagation Flags
False	Write	Deny	ContainerInherit, ObjectInherit
True	Write, Synchronize	Allow	ContainerInherit, ObjectInherit
True	Read, Synchronize	Allow	ContainerInherit, ObjectInherit

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, introduced by Ben Shneiderman in “Tree visualization with tree-maps: 2-d space-filling approach”; TOG 1991.



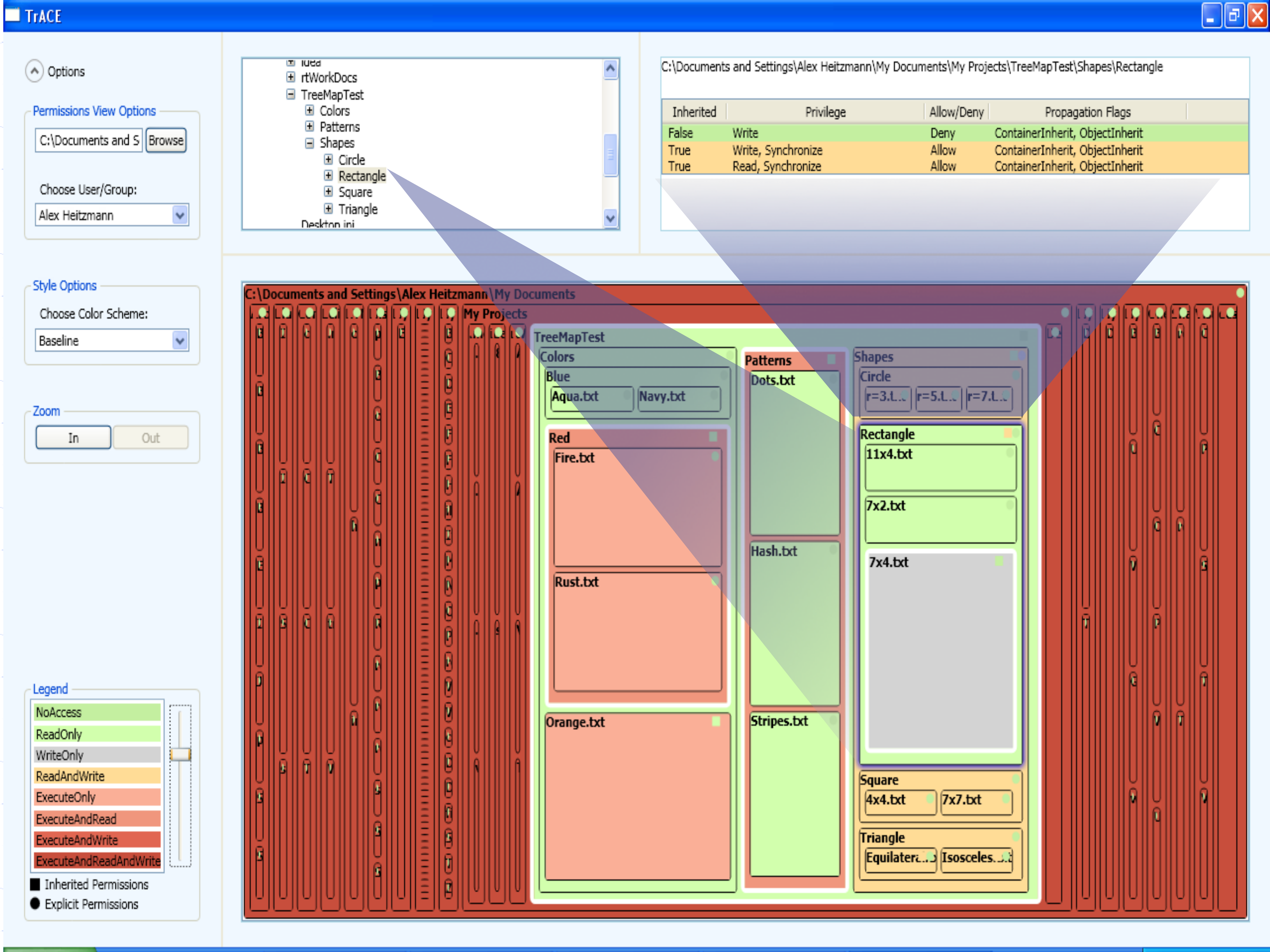
C:\Documents and S

Choose User/Group: Alex Heitzmann

Choose Color Scheme: Full Spectrum

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
True	Read, Synchronize	Allow	ContainerInherit, ObjectInherit



C:\Documents and S

Choose User/Group: Alex Heitzmann

Choose Color Scheme: Baseline

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
True	Read, Synchronize	Allow	ContainerInherit, ObjectInherit

TrACE — Treemap Access Control Evaluator

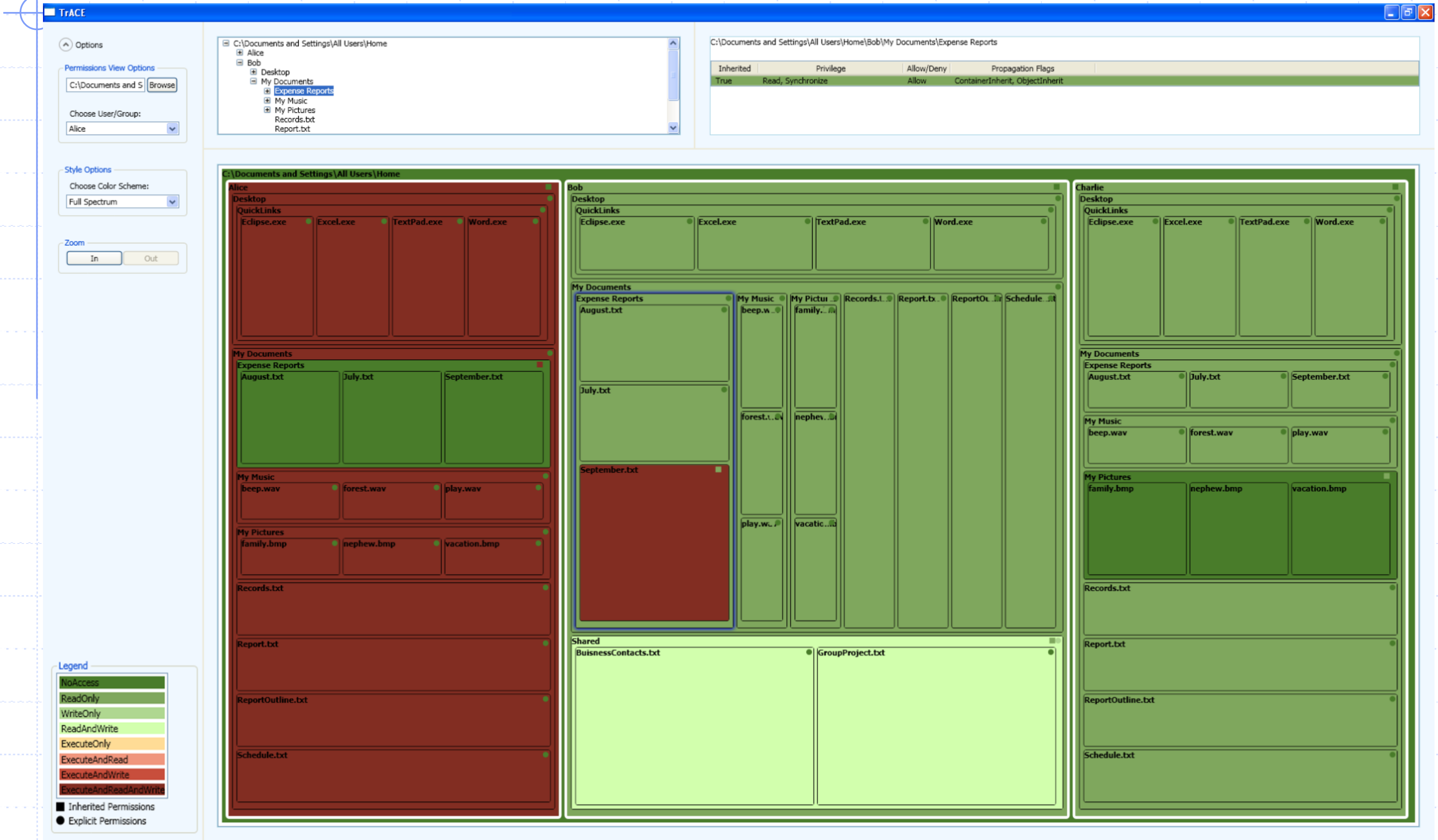
A visualization tool to aid in the analysis and management of file system permissions.

Alexander Heitzmann
aheitzma@cs.brown.edu

Bernardo Palazzi
palazzi@dia.uniroma3.it

Charalampos Papamanthou
cpap@cs.brown.edu

Roberto Tamassia
rt@cs.brown.edu



TrACE

Options

Permissions View Options

C:\Documents and S Browse

Choose User/Group: Alice

Style Options

Choose Color Scheme: Full Spectrum

Zoom: In | Out

```
⊟ C:\Documents and Settings\All Users\Home
  ⊞ Alice
  ⊟ Bob
    ⊞ Desktop
    ⊟ My Documents
      ⊞ Expense Reports
      ⊞ My Music
      ⊞ My Pictures
        Records.txt
        Report.txt
```

C:\Documents and Settings\All Users\Home\Bob\My Documents\Expense Reports

Inherited	Privilege	Allow/Deny	Propagation Flags
True	Read, Synchronize	Allow	ContainerInherit, ObjectInherit

Legend

- 🟩 NoAccess
- 🟩 ReadOnly
- 🟩 WriteOnly
- 🟩 ReadAndWrite
- 🟨 ExecuteOnly
- 🟥 ExecuteAndRead
- 🟥 ExecuteAndWrite
- 🟥 ExecuteAndReadAndWrite
- ■ Inherited Permissions
- ● Explicit Permissions

Sponsors:

Effective Visualization of File System Access Control, VizSEC 2008