Usabilità e sicurezza informatica: TrACE, un tool per la visualizzazione del controllo degli accessi in Windows

Bernardo Palazzi
palazzi@dia.uniroma3.it
DIA – Università Roma Tre, IT
ISCOM – Ministero dello Sviluppo Economico - Comunicazioni, IT
CSI – Brown University, RI, USA

SMAU
18 ottobre 2008
Sponsors: U.S. National Science Foundation.

Cos'è l'Usabilità?

"L'usabilità rappresenta il grado di efficacia,efficienza e soddisfazione con cui un sistema può essere utilizzato da particolari utenti per raggiungere certi obiettivi in uno specifico contesto d'uso!" (**ISO 9241**)

Una sicurezza usabile significa: utenti che seguono agevolmente le regole di sicurezza

Come si valuta l'usabilità?

1. Indagine (Usability inquiry)
   - interviste per conoscere necessità degli utenti, aspetti graditi e sgraditi, conoscenza del sistema
2. Esame (Usability inspection)
   - esame dell'interfaccia e del comportamento da parte di esperti
3. Test (Usability test)
   - utenti campione partecipano ad uno user study

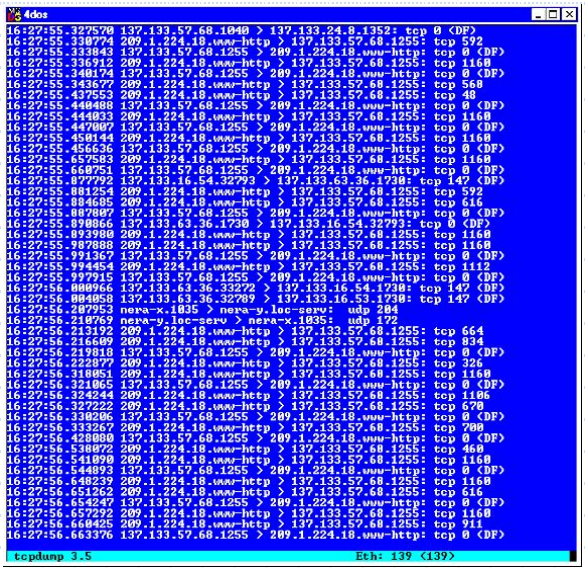
Usability Methods Toolbox: http://jthom.best.vwh.net/usability/

Usabilità e Visualizzazione

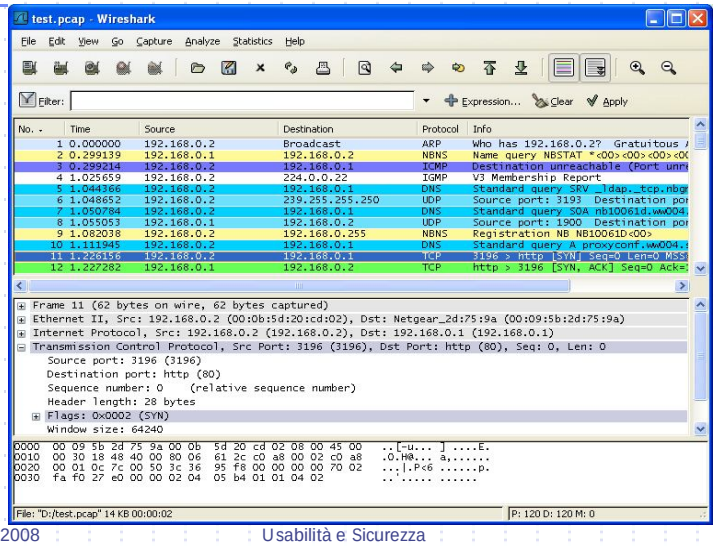
- La visualizzazione delle informazioni viene utilizzata per migliorare la comprensione dei dati astratti da parte dell'utente
- L'usabilità è quindi migliorata grazie alla superiore capacità di percezione umana delle informazioni visuali rispetto a quelle testuali
- In un sistema è possibile riconoscere a "colpo d'occhio" anomalie, eccezioni, casi limite, similitudini, differenze, modelli ecc.

Un'immagine vale 100 parole!

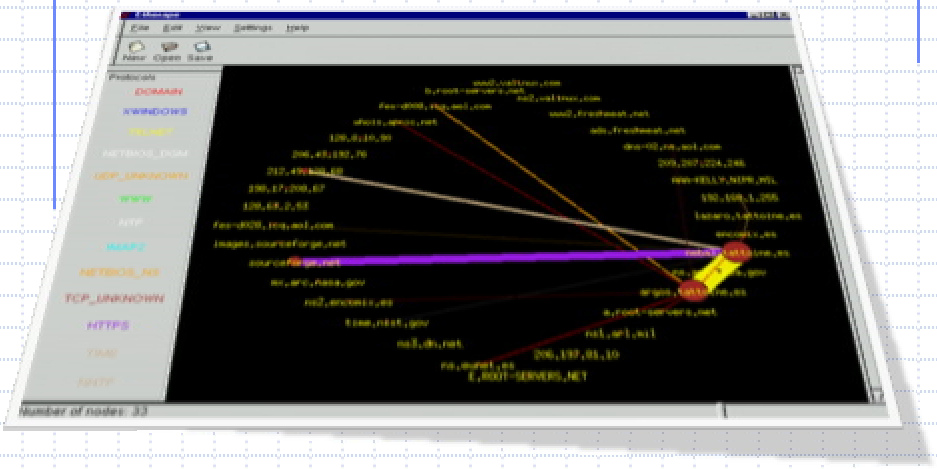
Analisi del traffico di Rete: TCPDump



Analisi del traffico di rete: Wireshark



Traffico di rete: EtherApe



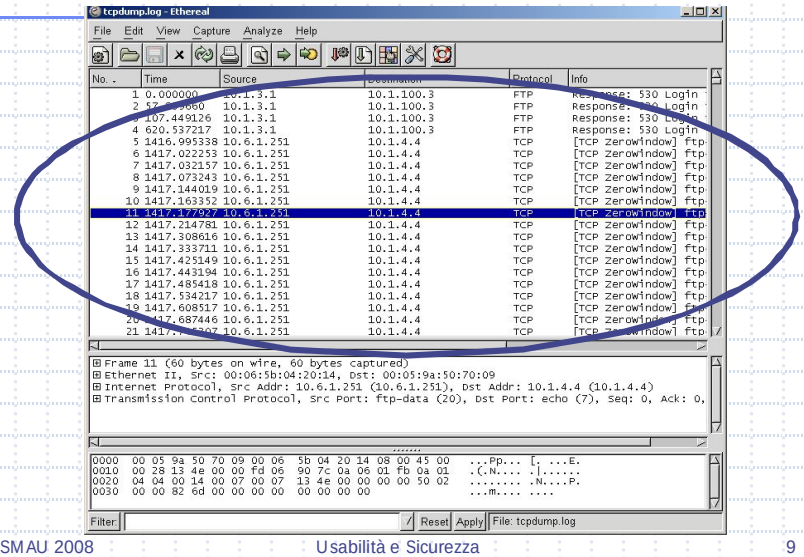
EtherApe by Juan Toledo can be found at http://etherape.sourceforge.net/
screenshot http://www.solaris4you.dk/sniffersSS.html

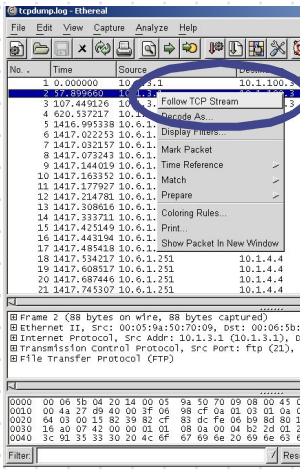
Mantra dell'Information Visualization

- **Overview, zoom & filter, details-on-demand**
- **Overview, zoom & filter, details-on-demand**
- **Overview, zoom & filter, details-on-demand**
- **Overview, zoom & filter, details-on-demand**
- **Overview, zoom & filter, details-on-demand**
- **Overview, zoom & filter, details-on-demand**
- **Overview, zoom & filter, details-on-demand**
- **Overview, zoom & filter, details-on-demand**
- **Overview, zoom & filter, details-on-demand**

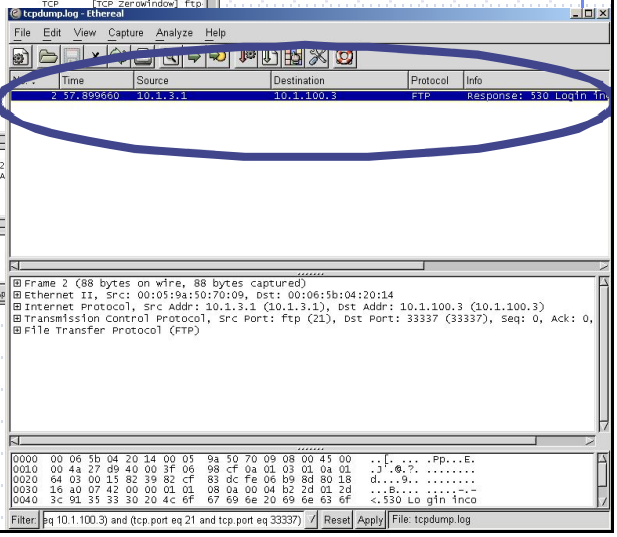
Ben Shneiderman
http://www.cs.umd.edu/~ben/

Overview First...
Prima una Panoramica...

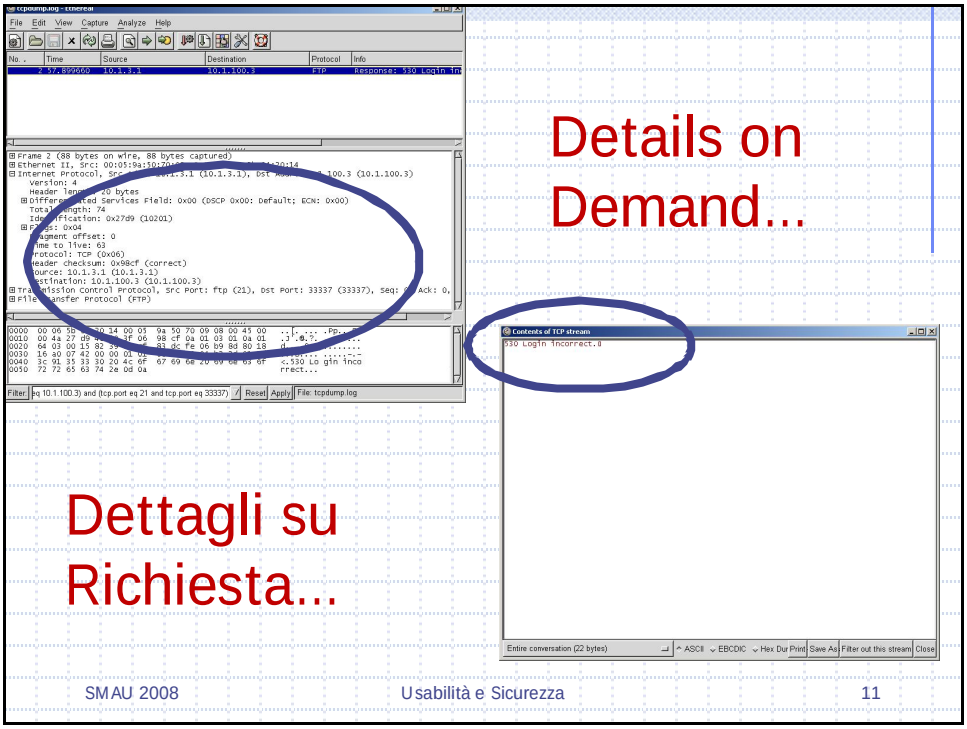




Zoom and Filter...



Zoom e Selezione...

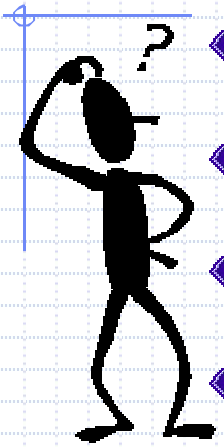


Principali elementi visuali

- Colore
- Dimensione
- Forma
- Interattività
- Direzione
- Scale
- Sequenza
- Filtraggio
- Punto di vista

http://www.siggraph.org/education/materials/HyperVis/concepts/matrx_lo.htm
http://www1.cs.columbia.edu/~zhou/project/CHI98Title.html

Usabilità, Visualizzazione e Sicurezza



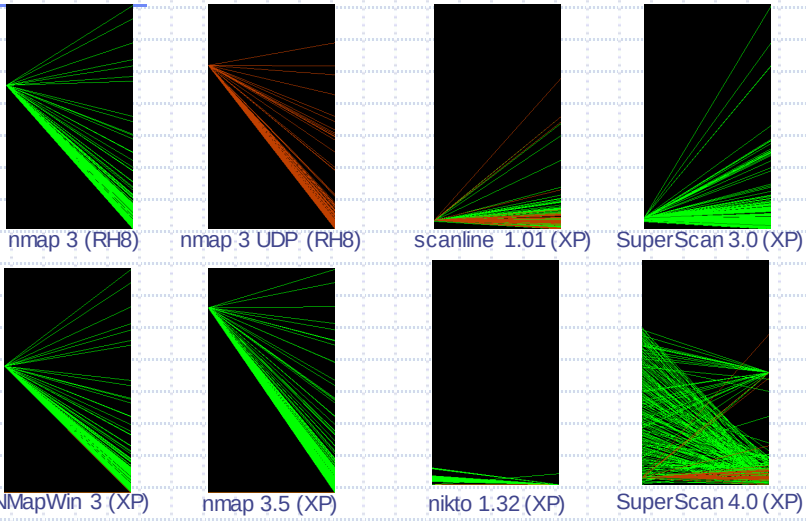
- Non considerare solo l'algoritmo ma inserire il fattore umano
- Aiutare ad individuare e comprendere nuovi attacchi
- Aiutare ad individuare minacce interne
- Creare tracce visuali degli attacchi

Da dove partire?

Visualizzazione delle Scansioni

- Comprendere il traffico di rete per valutare performance e scoprire condizioni anomale
- Gli strumenti che raccolgono traffico di rete "raw", calssificano i pacchetti secondo il proprio protocollo e forniscono filtri, ad es. TCPDump e Wireshark
- Necessità di strumenti di visualizzazione che associno modelli di traffico con forme geometriche e che aiutino ad individuare modelli di attacco, come gli *smart books* utilizzati nella difesa per identificare le armi nemiche.

Modelli di scansione con RumInt

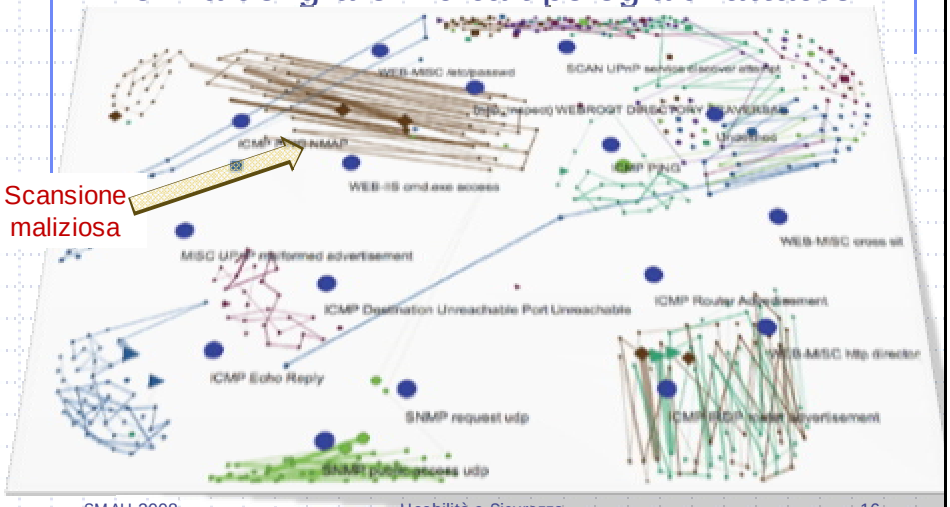


nmap 3 (RH8) | nmap 3 UDP (RH8) | scanline 1.01 (XP) | SuperScan 3.0 (XP)

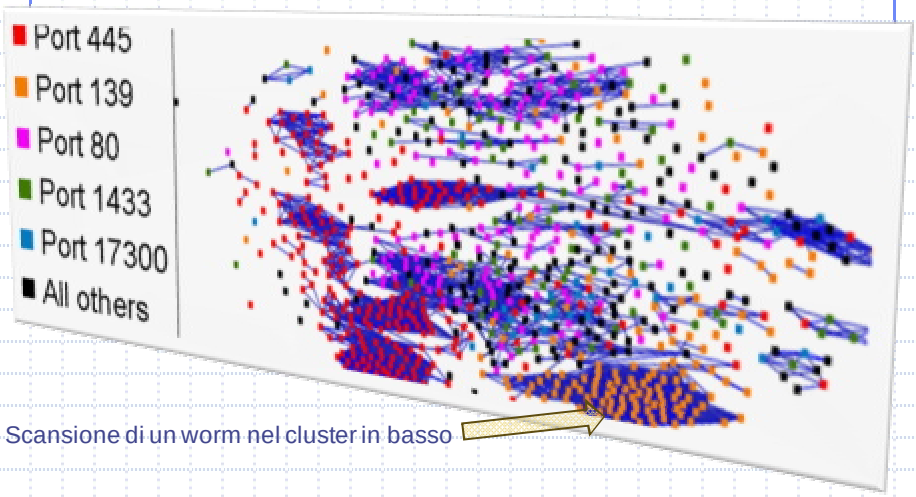
NMapWin 3 (XP) | nmap 3.5 (XP) | nikto 1.32 (XP) | SuperScan 4.0 (XP)

Visualizzazione delle Scansioni

- Forma del grafo indica tipologia di attacco



Visualizzazione delle Scansioni



Scansione di un worm nel cluster in basso

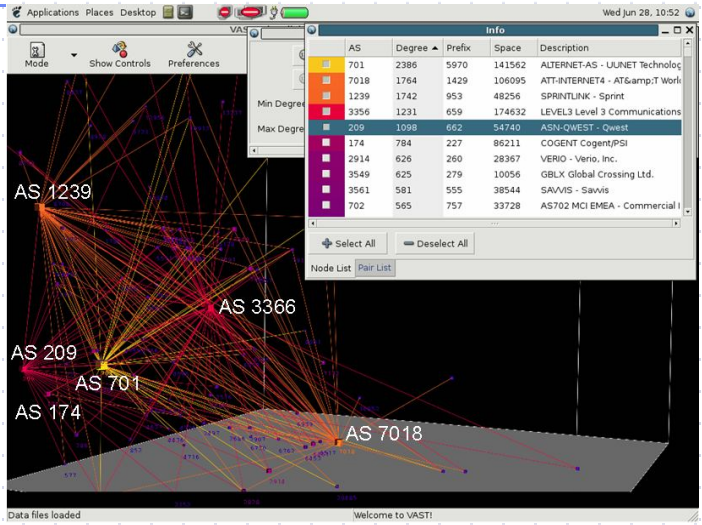
BGP Visualization

- Il border gateway protocol (BGP) controlla la raggiungibilità tra host in differenti autonomous systems (AS), ad es. reti gestite Internet Service Providers
- BGP lavora amministrando una tabella di routing di coppie (prefisso , AS-path)
- I path sono determinati da accordi commerciali tra ISP
- La tabella di routing di Internet contiene circa 200K prefissi
- I router BGP ricevono quotidianamente circa un milione di aggiornamenti (annunci)

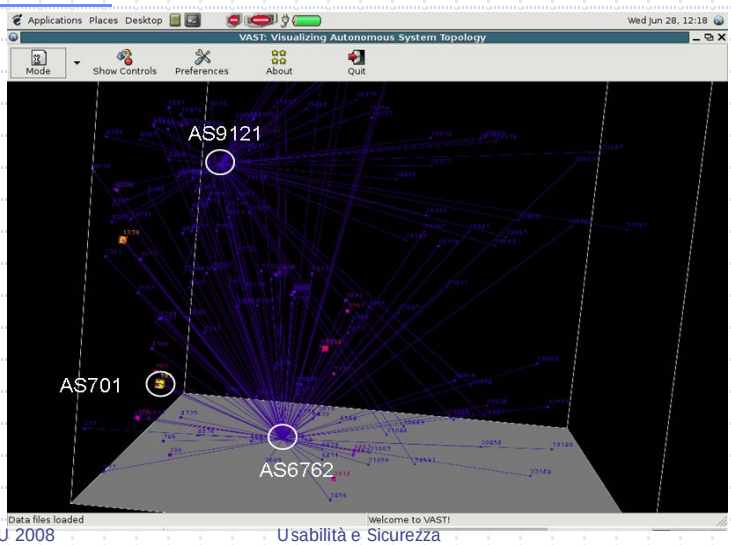
VAST

- Oberheide et al.,*VAST: visualizing autonomous system topology*, VizSec 2006
- Differenti visualizzazioni 3D, compreso lo schema 3D di connettività tra autonomous systems
- Utilizzo
  - Analisi Forense
  - Identificazione di infrastrutture critiche su internet

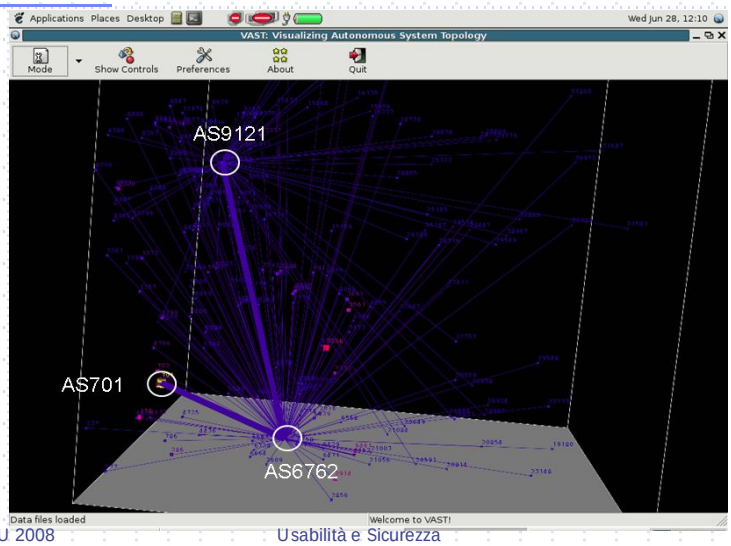
Top 5 Autonomous Systems



VAST: Route Leakage

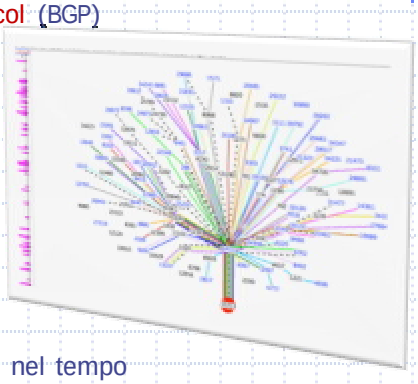


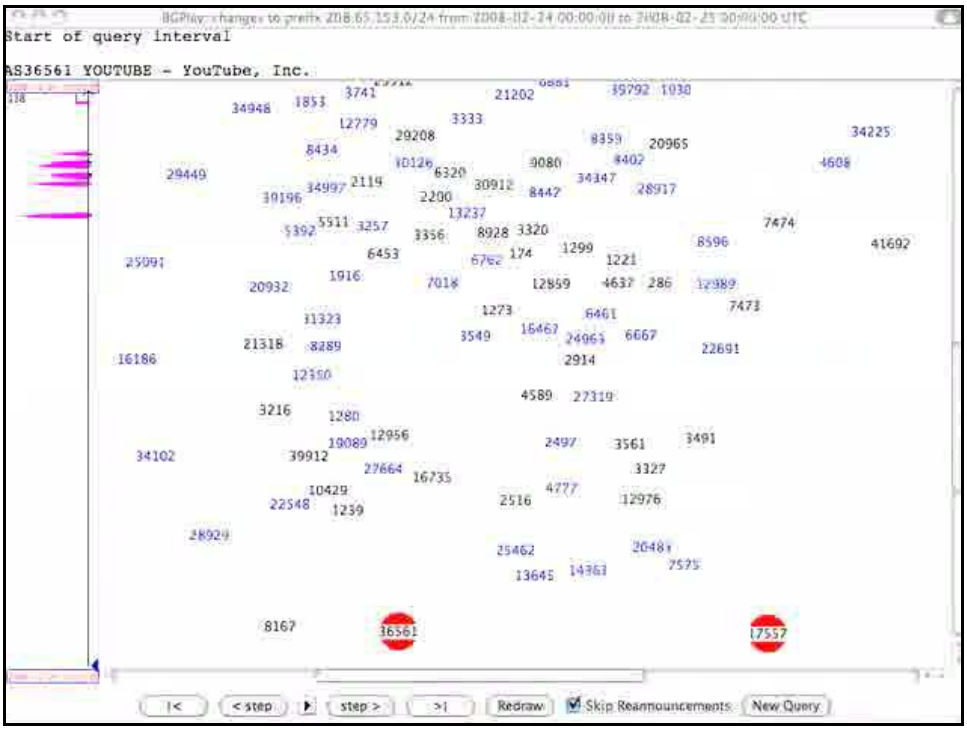
VAST: Route Leakage



BGPlay and iBGPlay

- Di Battista+, BGPlay e iBGPlay, www.ris.ripe.net/bgplay, www.ibgplay.org
- Visualizza il border gateway protocol (BGP)
- Grafi animati degli annunci BGP per un certo prefisso all'interno di uno specifico intervallo temporale
- Nodi: AS
- Path: sequenza di AS da attraversare per raggiungere la propria destinazione
- Visualizzazione mediante spring embedder con punti fissi
- Animazione di path che cambiano nel tempo

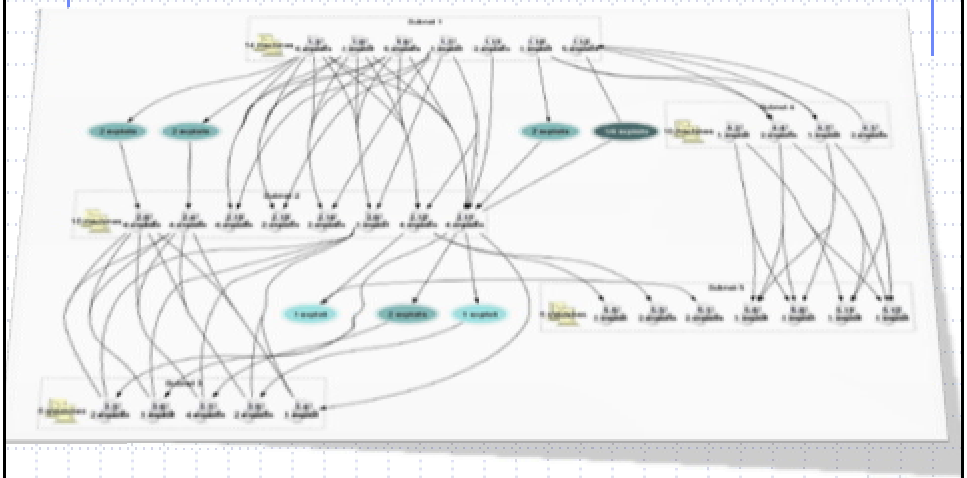




Albero degli Attacchi

- Un albero degli attacchi modella le vulnerabilità di un sistema e tutte le sequenze di exploit che possono essere utilizzate per ottenere un obbiettivo specifico
- I primi lavori sugli alberi degli attacchi (Schneier) mostrano come vettori di attacchi multipli possono compromettere un singolo obiettivo
- Una grande quantità di sorgenti supera di molto l'abilità umana di visualizzare, comprendere e analizzare alberi degli attacchi
- Tecniche di Graph drawing possono aiutare a raggruppare e visualizzare grafi di grandi dimensioni

Grafo degli Attacchi



Un Problema in Dipartimento

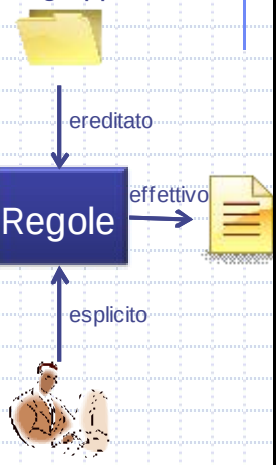
- Ogni studente ha un *home directory* su un file system condiviso per le prove intermedie per un esame .
- Il dipartimento ha recentemente richiesto che le cartelle degli studenti di un corso non siano leggibili dai propri colleghi in modo tale che gli altri studenti non possano copiare troppo facilmente …

Controllo degli accessi

- Controllo degli accessi: approccio per permettere o negare l'uso di risorse da parte di specifiche entità
- Politica: collezione struttrata di regole (permessi) per esprimere gli obiettivi per il controllo degli accessi
- Una access control entries (ACE) è una politica di base per una risorsa contraddistinta da una tripla (entità, privilegio, permetti/nega)
- Negli attuali sistemi operativi, le politiche per il controllo degli accesi a file o a cartelle è espresso tramite una access control list (ACL), che consiste di una lista di ACE
- Strumenti standard mostrano le ACL come tabelle con checkbox
- Tecniche di visualizzazione possono aiutare ad individuare configurazioni errate

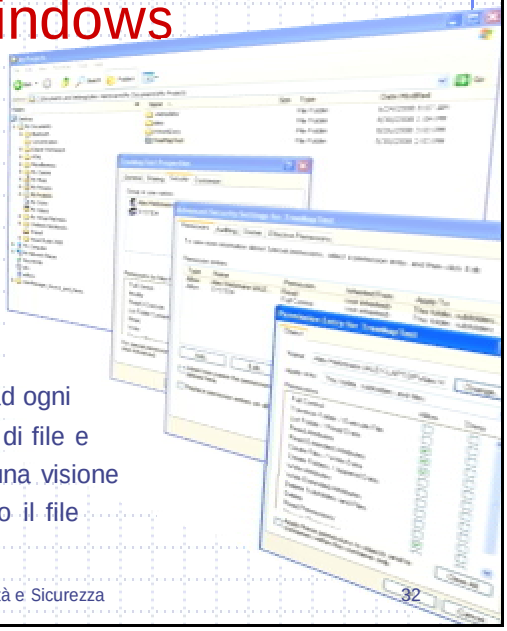
Permessi NTFS

- **Espliciti**: impostati da *owner* per ogni utente /gruppo.
- **Ereditati**: erditati esplicitamente dai permessi delle cartelle di livello superiore.
- **Effettivo**: ottenuto dalla combinazione dei permessi espiciti ed ereditati
- Determinare i permessi effettivi:
  - Di default, un utente/gruppo non ha privilegi
  - I permessi espliciti revocano i permessi ereditati in conflitto
  - Le negazioni esplicite revocano i permessi diretti



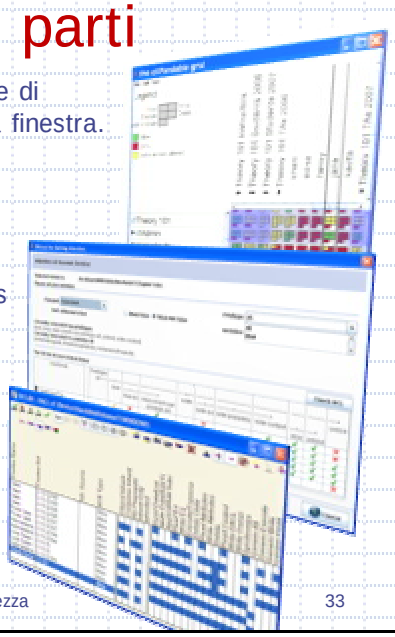
Strumenti di Windows

- Gli strumenti standard per il controllo degli accessi forniscono informazioni dettagliate e controlli, attraverso finestre di dialogo multiple.
- Il focus è su singoli file o cartelle.
- E' impegnativo per gli utenti ad ogni livello gestire grandi strutture di file e soprattutto riuscire ad avere una visione di insieme dei permessi in tutto il file system.

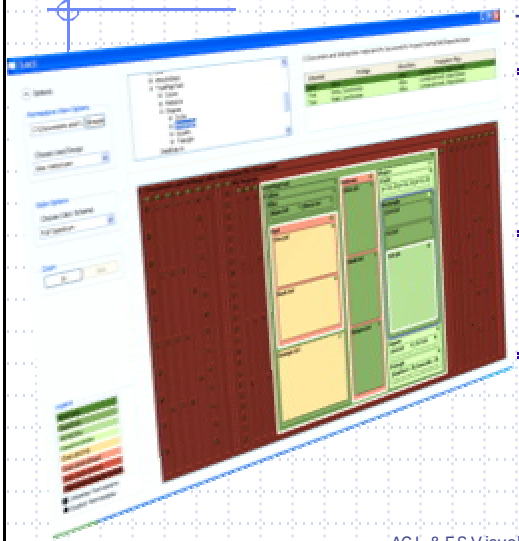


Strumenti di terze parti

- La visualizzazione a matrice permette di vedere le informazioni in una singola finestra.
- 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

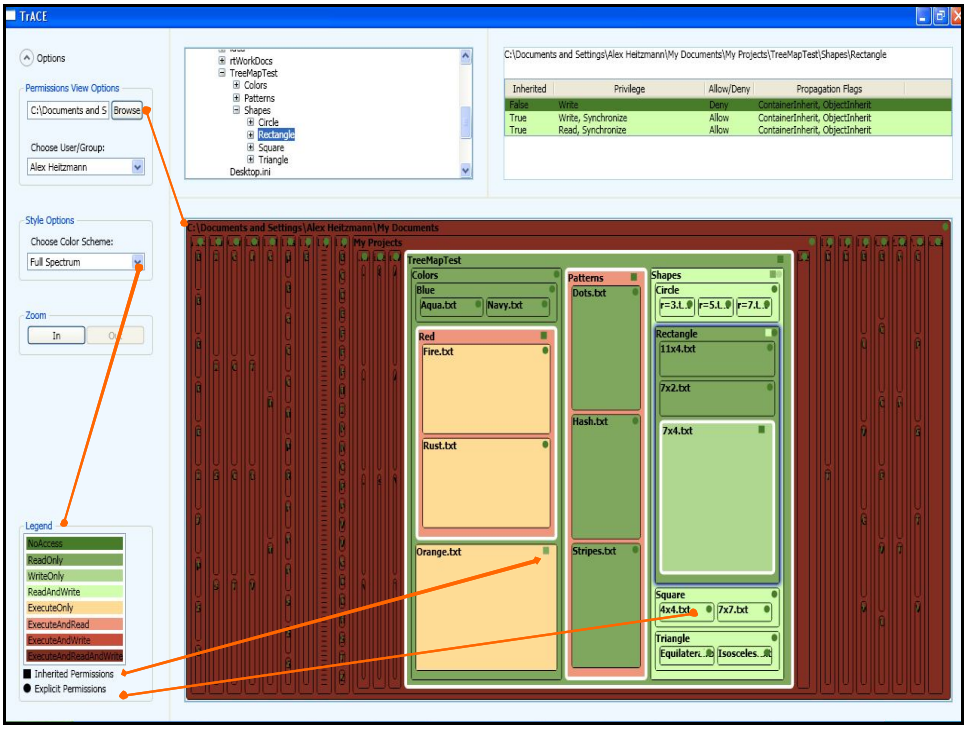


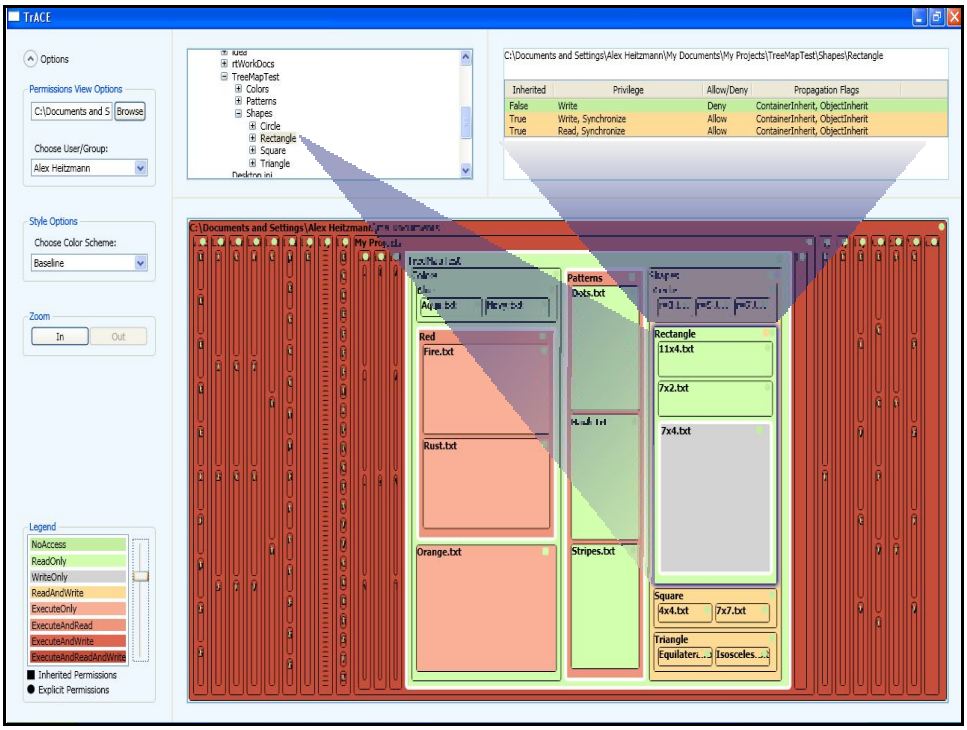
Introduzione a TrACE: Treemap Access Control Evaluator



TrACE permette all'utente di:

- determinare a colpo d'occhio i permessi espliciti, ereditati, ed effettivi di file e cartelle.
- comprendere le relazioni per il controllo degli accessi tra i file e i propri "antenati"
- Valutare rapidamente la struttura di grandi cartelle e individuare rapidamente le aree con problemi.


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
True
Read, Synchronize
Allow
ContainerInherit, ObjectInherit
C:\Documents and Settings\Alex Heitzmann\My Documents
My Projects
TreeMapTest
Colors
Blue
Aqua.txt
Navy.txt
Red
Fire.txt
Rust.txt
Orange.txt
Patterns
Dots.txt
Hash.txt
Stripes.txt
Shapes
Circle
Rectangle
11x4.txt
7x2.txt
7x4.txt
Square
4x4.txt
7x7.txt
Triangle


TrACE
Options
Permissions View Options
Choose User/Group:
Style Options
Choose Color Scheme:
Baseline
Zoom
In
Out
Legend
Inherited Permissions
Explicit Permissions

TrACE — Treemap Access Control Evaluator

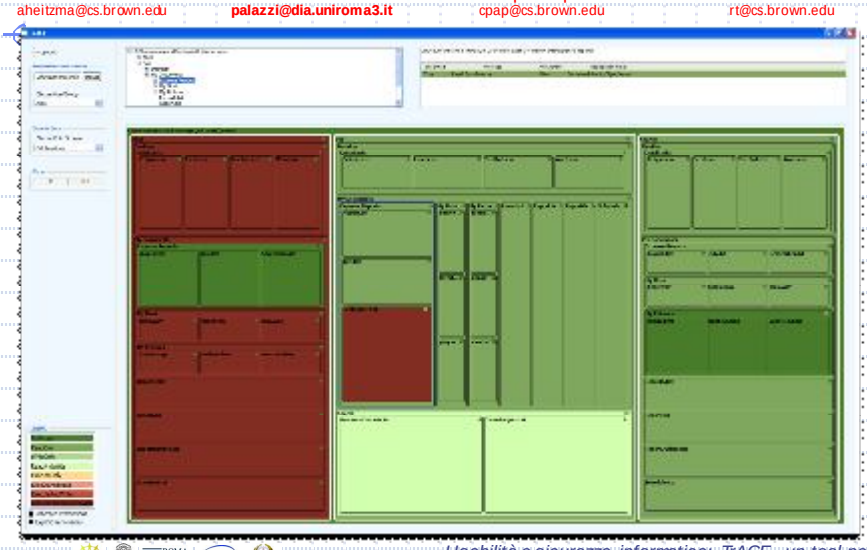
A visualization tool to aid in the analysis and management of file system permissions.

Alexander Heitzmann
aheitzma@cs.brown.edu

Bernardo Palazzi
palazzi@dia.uniroma3.it

Charalampos Papamanthou
cpap@cs.brown.edu

Roberto Tamassia
rt@cs.brown.edu



Sponsors:

Usabilità e sicurezza informatica: TrACE, un tool per la visualizzazione del controllo degli accessi in Windows, SMAU 2008