

## 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

```

tcpdump 3.5
16:27:55.327570 137.133.57.68.1848 > 137.133.24.8.1255: tcp 0 (DF)
16:27:55.330774 209.1.224.18.www-http > 137.133.57.68.1255: tcp 592
16:27:55.333843 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.336712 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1168
16:27:55.340174 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.343577 209.1.224.18.www-http > 137.133.57.68.1255: tcp 568
16:27:55.437953 209.1.224.18.www-http > 137.133.57.68.1255: tcp 48
16:27:55.459488 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.444833 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1168
16:27:55.447007 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.459144 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1168
16:27:55.456636 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.457583 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1168
16:27:55.460721 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.877792 137.133.16.54.32793 > 137.133.63.36.1730: tcp 147 (DF)
16:27:55.881254 209.1.224.18.www-http > 137.133.57.68.1255: tcp 592
16:27:55.884685 209.1.224.18.www-http > 137.133.57.68.1255: tcp 616
16:27:55.887807 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.890866 137.133.63.36.1730 > 137.133.16.54.32793: tcp 0 (DF)
16:27:55.893980 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1168
16:27:55.897888 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1168
16:27:55.991367 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:55.994454 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1112
16:27:55.997915 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.000966 137.133.63.36.33272 > 137.133.16.54.1730: tcp 147 (DF)
16:27:56.004088 137.133.63.36.32709 > 137.133.16.54.1730: tcp 147 (DF)
16:27:56.207953 nera-x.1035 > nera-y.lac-serv: udp 204
16:27:56.210769 nera-y.lac-serv > nera-x.1035: udp 172
16:27:56.215191 209.1.224.18.www-http > 137.133.57.68.1255: tcp 834
16:27:56.216609 209.1.224.18.www-http > 137.133.57.68.1255: tcp 834
16:27:56.219818 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.222977 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1168
16:27:56.318051 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1168
16:27:56.321065 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.324244 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1168
16:27:56.327222 209.1.224.18.www-http > 137.133.57.68.1255: tcp 670
16:27:56.330266 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.333267 209.1.224.18.www-http > 137.133.57.68.1255: tcp 700 (DF)
16:27:56.428800 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.538072 209.1.224.18.www-http > 137.133.57.68.1255: tcp 460
16:27:56.541090 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1168
16:27:56.544893 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.648239 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1168
16:27:56.654247 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
16:27:56.657292 209.1.224.18.www-http > 137.133.57.68.1255: tcp 1168
16:27:56.660405 209.1.224.18.www-http > 137.133.57.68.1255: tcp 911
16:27:56.663376 137.133.57.68.1255 > 209.1.224.18.www-http: tcp 0 (DF)
tcpdump 3.5
Ech: 139 (139)

```

# Analisi del traffico di rete: Wireshark

test.pcap - Wireshark

Filter:  Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.2	Broadcast	ARP	Who has 192.168.0.2? Gratuitous /
2	0.299139	192.168.0.1	192.168.0.2	NBNS	Name query NBSTAT *00<00>00<00>
3	0.299214	192.168.0.2	192.168.0.1	ICMP	Destination unreachable (Port unri
4	1.025659	192.168.0.2	224.0.0.22	IGMP	V3 Membership Report
5	1.044366	192.168.0.2	192.168.0.1	DNS	Standard query SRV _ldap._tcp.nbr
6	1.048652	192.168.0.2	239.255.255.250	UDP	Source port: 3193 Destination por
7	1.050784	192.168.0.2	192.168.0.1	DNS	Standard query SOA nb1006id.w004
8	1.055053	192.168.0.1	192.168.0.2	UDP	Source port: 1900 Destination por
9	1.082038	192.168.0.2	192.168.0.255	NBNS	Registration NB NB1006ID<00>
10	1.111945	192.168.0.2	192.168.0.1	DNS	Standard query A proxyconf.w004
11	1.222131	192.168.0.2	192.168.0.1	TCP	3196->3196 [SYN, ACK] Seq=0 ack=
12	1.222282	192.168.0.1	192.168.0.2	TCP	http->3196 [SYN, ACK] Seq=0 ack=

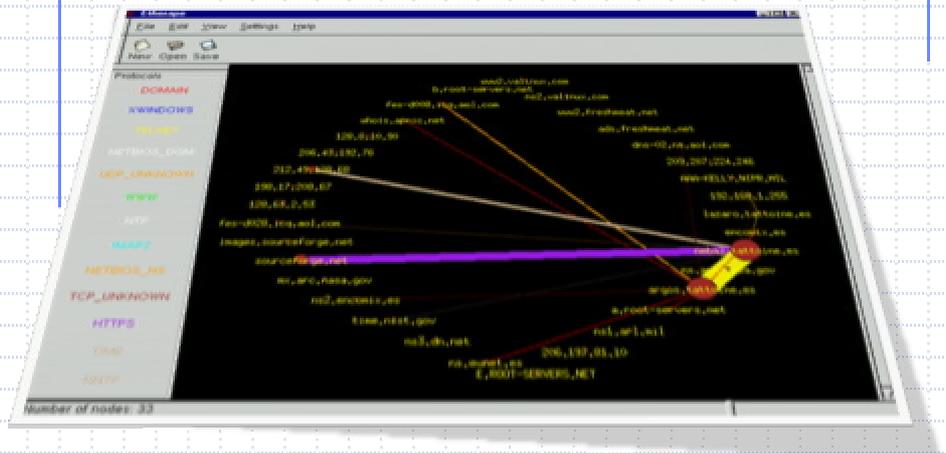
Frame 11 (62 bytes on wire, 62 bytes captured)

- Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear-2d:75:9a (00:09:5b:2d:75:9a)
- Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
- Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: Http (80), Seq: 0, Len: 0
  - Source port: 3196 (3196)
  - Destination port: http (80)
  - Sequence number: 0 (relative sequence number)
  - Header length: 28 bytes
  - Flags: 0x0002 (SYN)
  - Window size: 64240

0000 00 05 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00 ..[u... ]....E.  
 0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 .0.H... a....  
 0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 70 02 ...!P<6 .....p.  
 0030 fa f0 27 e0 00 00 02 04 05 b4 d1 01 04 02 ..!.....

File: "D:/test.pcap" 14 KB 00:00:02 P: 120 D: 120 M: 0

## Traffico di rete: EtherApe



SMAU 2008

Usabilità e Sicurezza by Juan Toledo can be found at <http://etherape.sourceforge.net/screenshot> <http://www.solaris4you.dk/snifersSS.html>

## Mantra dell'Information Visualization

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

Ben Shneiderman

<http://www.cs.umd.edu/~ben/>

SMAU 2008

Usabilità e Sicurezza

8

# Overview First... Prima una Panoramica...

No. Time Source Destination Protocol Info  
 1 0.000000 10.1.1.3.1 10.1.100.3 FTP Response: 530 Login  
 2 57.899660 10.1.1.3.1 10.1.100.3 FTP Response: 530 Login  
 3 107.449126 10.1.1.3.1 10.1.100.3 FTP Response: 530 Login  
 4 620.537217 10.1.1.3.1 10.1.100.3 FTP Response: 530 Login  
 5 1416.995338 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 6 1417.022553 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 7 1417.032157 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 8 1417.073243 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 9 1417.144019 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 10 1417.163352 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 11 1417.177927 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 12 1417.214781 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 13 1417.308656 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 14 1417.333711 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 15 1417.425149 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 16 1417.443194 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 17 1417.485418 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 18 1417.534217 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 19 1417.608517 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 20 1417.687446 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp  
 21 1417.745307 10.6.1.251 10.1.4.4 TCP [TCP ZeroWindow] ftp

Frame 11 (60 bytes on wire, 60 bytes captured)  
 Ethernet II, Src: 00:06:5b:04:20:14, Dst: 00:05:9a:50:70:09  
 Internet Protocol, Src Addr: 10.6.1.251 (10.6.1.251), Dst Addr: 10.1.4.4 (10.1.4.4)  
 Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: echo (7), Seq: 0, Ack: 0,

Filter:  Reset  Apply File: tcpdump.log

SMAU 2008

Usabilità e Sicurezza

9

No. Time Source Destination Protocol Info  
 2 57.899660 10.1.1.3.1 10.1.100.3 FTP Response: 530 Login

Frame 2 (88 bytes on wire, 88 bytes captured)  
 Ethernet II, Src: 00:05:9a:50:70:09, Dst: 00:06:5b:04:20:14  
 Internet Protocol, Src Addr: 10.1.3.1 (10.1.3.1), Dst Addr: 10.1.100.3 (10.1.100.3)  
 Transmission Control Protocol, Src Port: ftp (21), Dst Port: 33337 (33337), Seq: 0, Ack: 0,  
 File Transfer Protocol (FTP)

Filter:  Reset  Apply File: tcpdump.log

Zoom and  
Filter...

Zoom e  
Selezione...

SMAU 2008

**Details on Demand...**

**Dettagli su Richiesta...**

SMAU 2008      Usabilità e Sicurezza      11

## Principali elementi visuali

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

[http://www.siggraph.org/education/materials/HyperVis/concepts/matr\\_x\\_lo.htm](http://www.siggraph.org/education/materials/HyperVis/concepts/matr_x_lo.htm)  
<http://www1.cs.columbia.edu/~zhou/project/CHI98Title.html>

SMAU 2008      Usabilità e Sicurezza      12

## Usabilità, Visualizzazione e Sicurezza



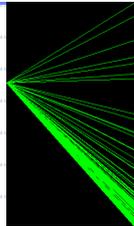
- ◆ Non considerare solo l'algoritmo ma inserire il fattore umano
- ◆ Aiutare ad individuare e comprendere nuovi attacchi
- ◆ Aiutare ad individuare minacce interne
- ◆ Creare tracce visuali degli attacchi

**Da dove partire?**

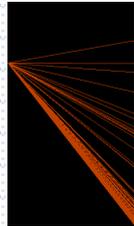
## Visualizzazione delle Scansioni

- ◆ Comprendere il traffico di rete per valutare performance e scoprire condizioni anomale
- ◆ Gli strumenti che raccolgono traffico di rete "raw", classificano 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.

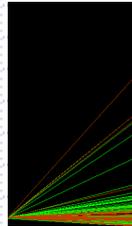
## Modelli di scansione con RumInt



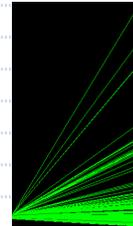
nmap 3 (RH8)



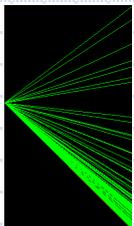
nmap 3 UDP (RH8)



scanline 1.01 (XP)

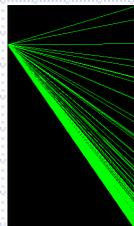


SuperScan 3.0 (XP)



NMapWin 3 (XP)

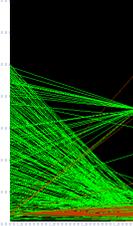
SMAU 2008



nmap 3.5 (XP)



niko 1.32 (XP)



SuperScan 4.0 (XP)

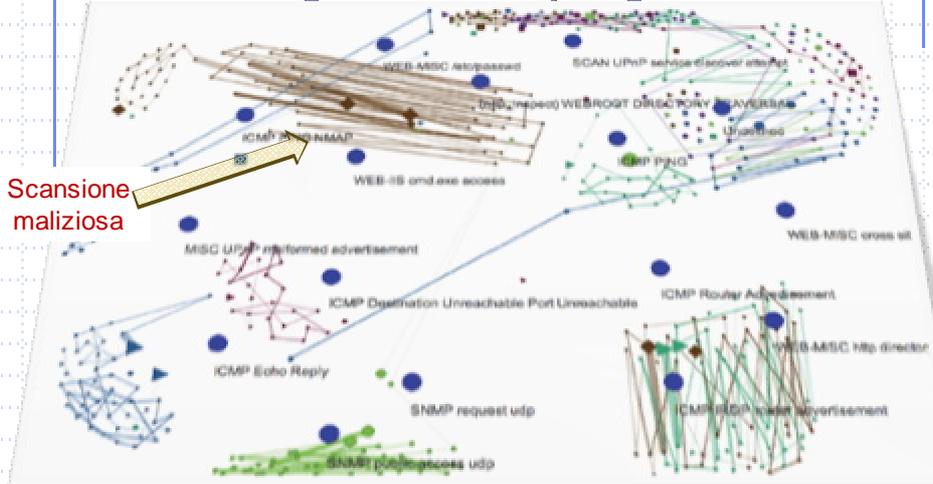
Usabilità e Sicurezza

<http://www.rumint.org/>

15

## Visualizzazione delle Scansioni

◆ Forma del grafo indica tipologia di attacco

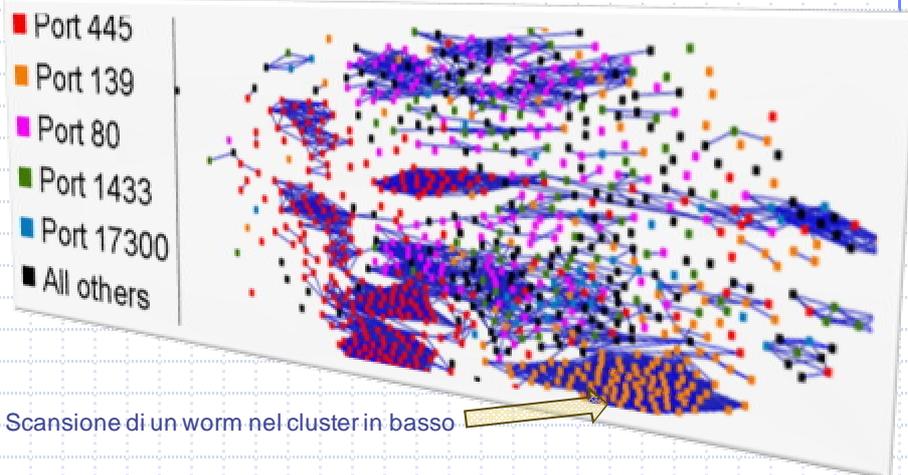


SMAU 2008

Usabilità e Sicurezza

16

## Visualizzazione delle Scansioni



SMAU 2008

Usabilità e Sicurezza

18

## 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)

SMAU 2008

Usabilità e Sicurezza

19

# 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

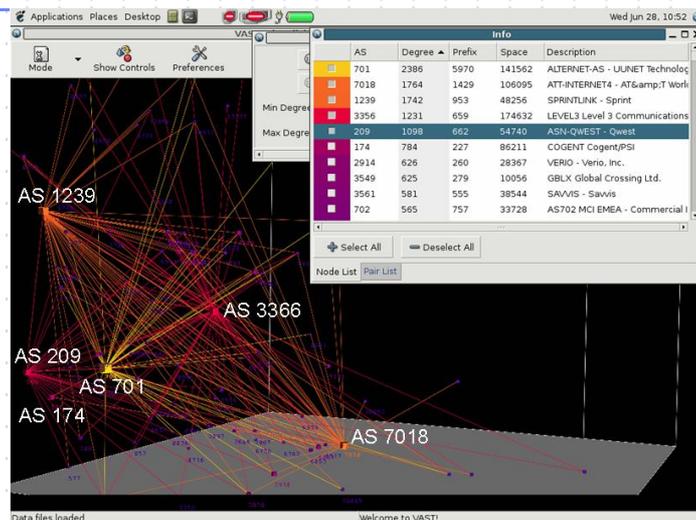


SMAU 2008

Usabilità e Sicurezza

20

# Top 5 Autonomous Systems

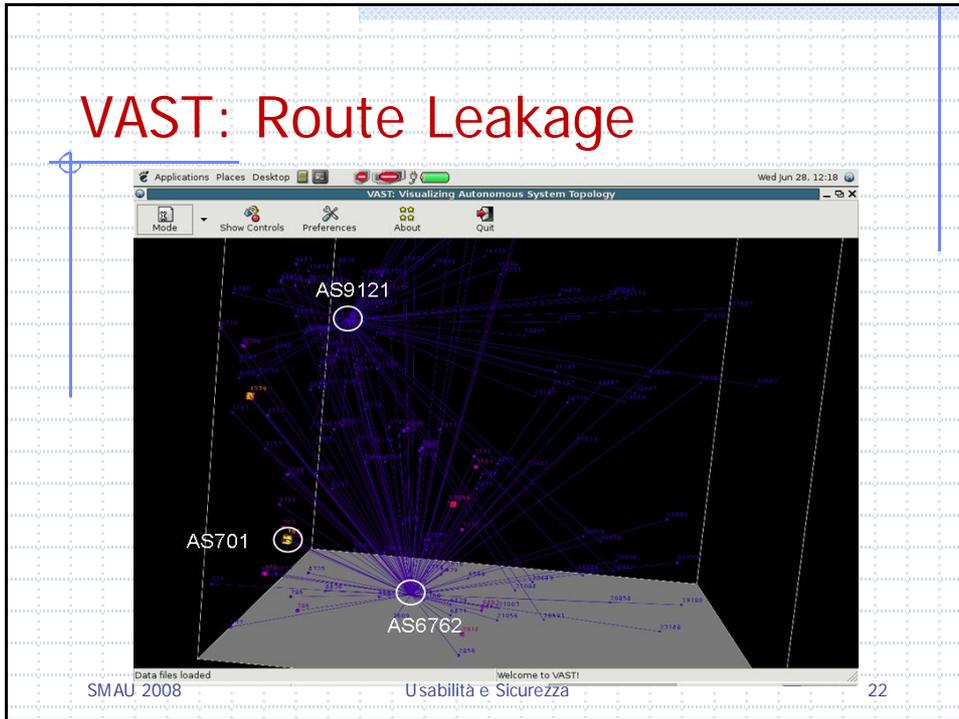


SMAU 2008

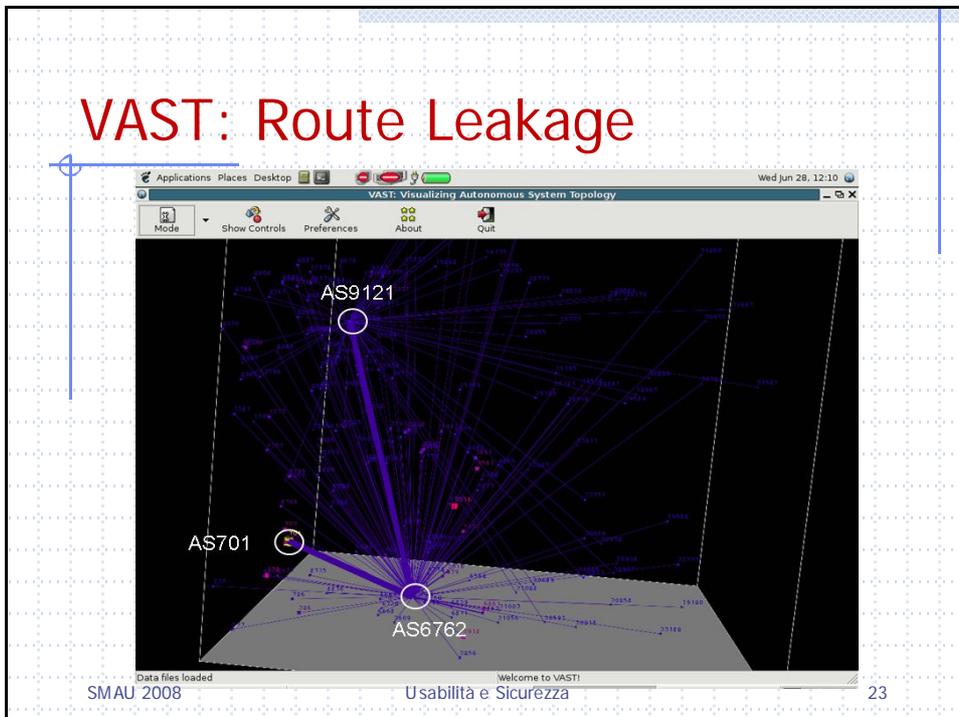
Usabilità e Sicurezza

21

# VAST: Route Leakage

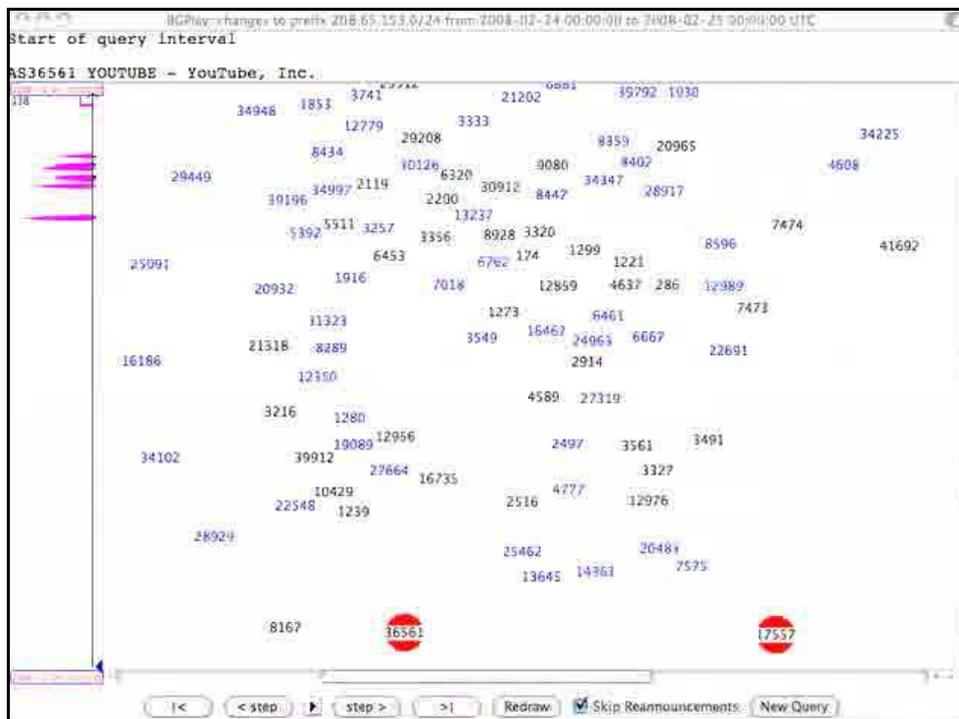
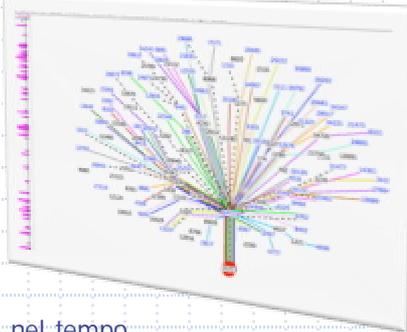


# VAST: Route Leakage



# BGPlay and iBGPlay

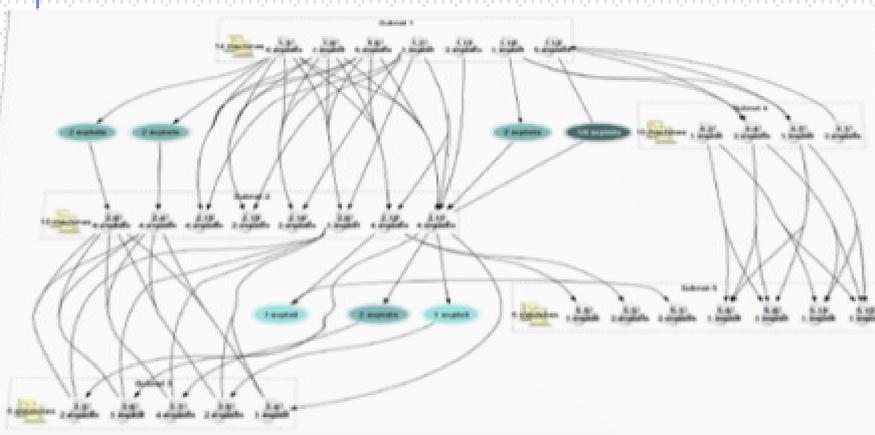
- Di Battista+, BGPlay e iBGPlay, [www.ris.ripe.net/bgplay](http://www.ris.ripe.net/bgplay), [www.ibgplay.org](http://www.ibgplay.org)
- Visualizza il **border gateway protocol** (BGP)
- Grafi animati degli annunci BGP per un certo prefisso all'interno di uno specifico intervallo temporale
- **Nodi**: 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 obiettivo 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



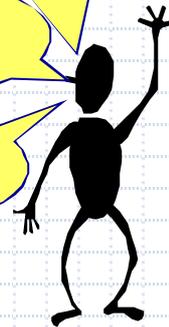
## Un Problema in Dipartimento

- ◆ 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 ...

Come posso essere sicuro che nessun file nella mia cartella di corso violi questa regola?

Il professore può controllare se copio ?

Quanto tempo ci vuole?

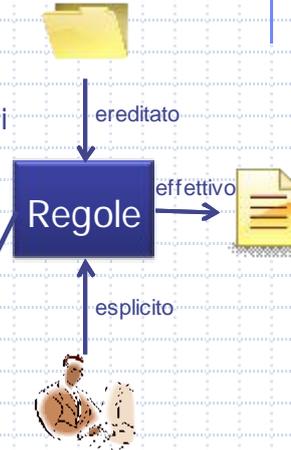


## Controllo degli accessi

- ◆ **Controllo degli accessi**: approccio per permettere o negare l'uso di risorse da parte di specifiche entità
- ◆ **Politica**: collezione strutturata 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, permessi/nega)
- ◆ Negli attuali sistemi operativi, le politiche per il controllo degli accessi 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**: ereditati esplicitamente dai permessi delle cartelle di livello superiore.
- ◆ **Effettivo**: ottenuto dalla combinazione dei permessi espliciti 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



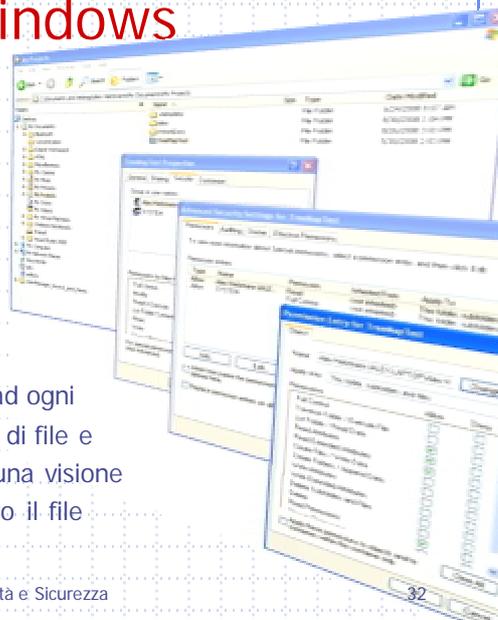
SMAU 2008

Usabilità e Sicurezza

31

## 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.



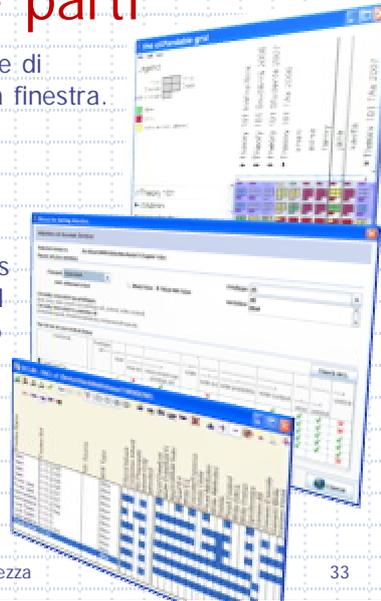
SMAU 2008

Usabilità e Sicurezza

32

## 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://czwssoft.dyndns.org/sdedit.html>

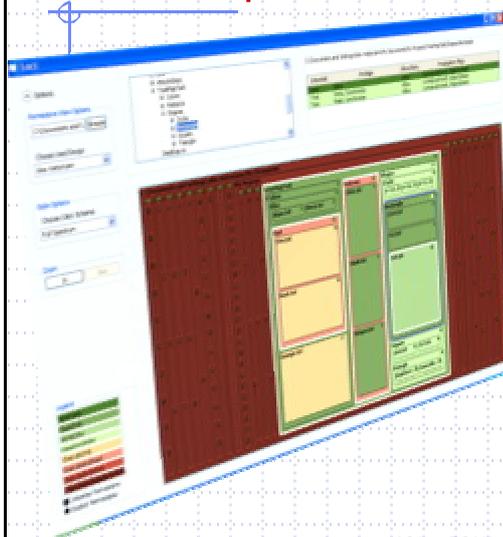


SMAU 2008

Usabilità e Sicurezza

33

## Introduzione a TrACE: Treemap Access Control Evaluator



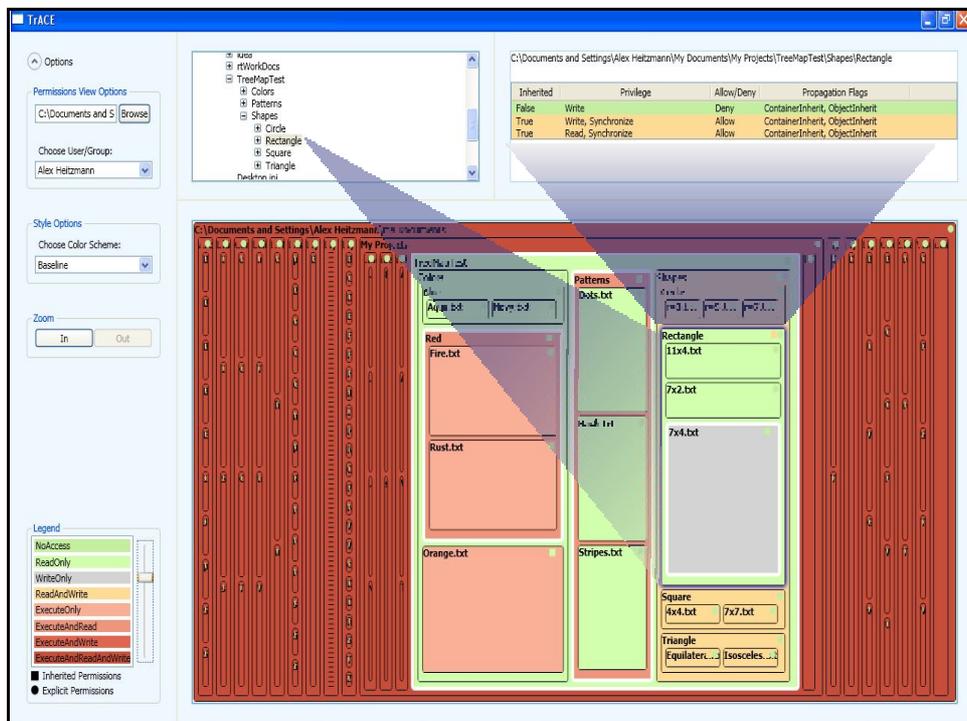
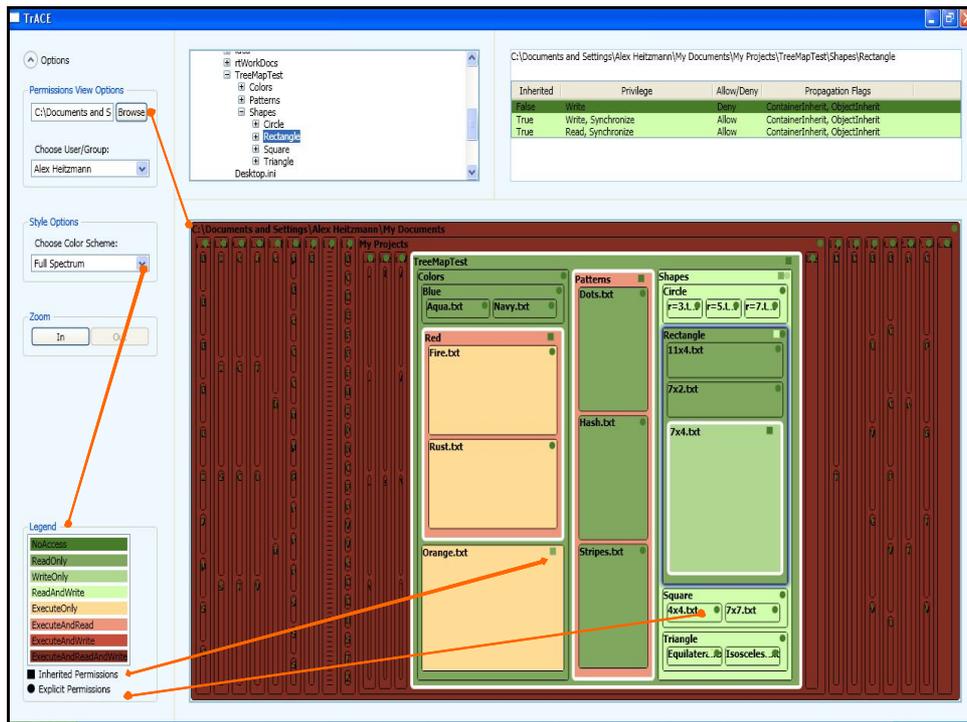
TrACE permette all'utente di:

- ◆ 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.

vizSEC 2008

ACL & FS Visualization

34



# TrACE — Treemap Access Control Evaluator

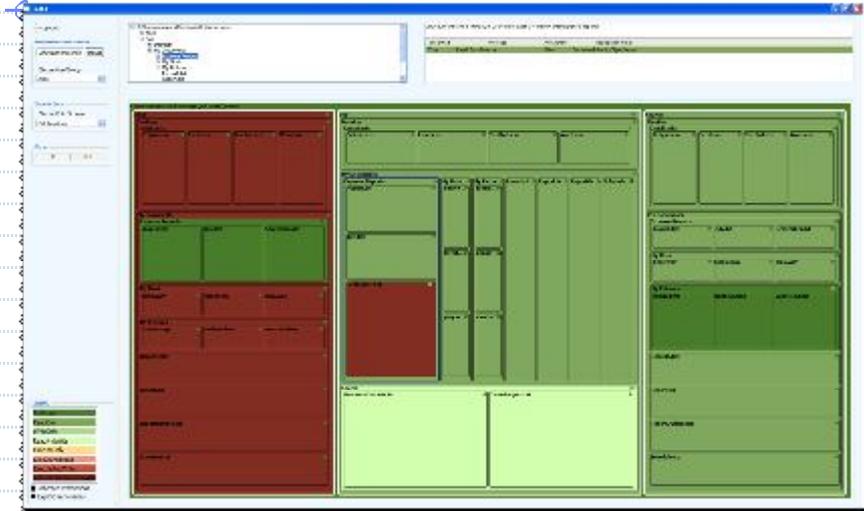
A visualization tool to aid in the analysis and management of file system permissions.

Alexander Heitzmam  
aheitzma@cs.brown.edu

Bernardo Palazzi  
palazzi@dia.uniroma3.it

Charalampos Papamantou  
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.