SOCIAL NETWORK VIS

Lea Maria Joseffa Koinig

GEWÄHLTE PAPER

- Countering Security Analyst and Network Administrator Overload Through Alert and Packet Visualization, G. Conti, K. Abdullah, J. Grizzard, J. Stasko, J. Copeland, M. Ahamad, H. Owen and C. Lee, IEEE Computer Graphics and Applications (CG&A), March 2006.
- Mapping and Visualizing the Internet, Bill Cheswick, Hal Burch, and Steve Branigan, USENIX, San Diego, CA, June 2000.
- OverFlow: An Overview Visualization for Network Analysis, J. Glanfield, S. Brooks, T. Taylor, D. Paterson, C Smith, C. Gates, J. McHugh, VizSec 2009.

GEWÄHLTE PAPER

- Mapping and Visualizing the Internet, Bill Cheswick, Hal Burch, and Steve Branigan, USENIX, San Diego, CA, June 2000.
- OverFlow: An Overview Visualization for Network Analysis, J. Glanfield, S. Brooks, T. Taylor, D. Paterson, C Smith, C. Gates, J. McHugh, VizSec 2009.

OVERFLOW – WHAT?

- High Level Visualisierung von Netzwerken und Events in Netzwerken
- Visualisierung, die den Kontext für andere Visualisierungen bietet
- Soll innerhalb des FloVis Frameworks den Zusammenhang zeigen
  - Fokus + Kontext Ansatz

OVERFLOW – WHY?

- Bietet im Gegensatz zu bisherigen Ansätzen einen Ausgangspunkt für die Netzwerkvisualisierung
- Reduziert die kognitive Belastung des Nutzers
- Effektivität der automatisierten Analyse lässt nach

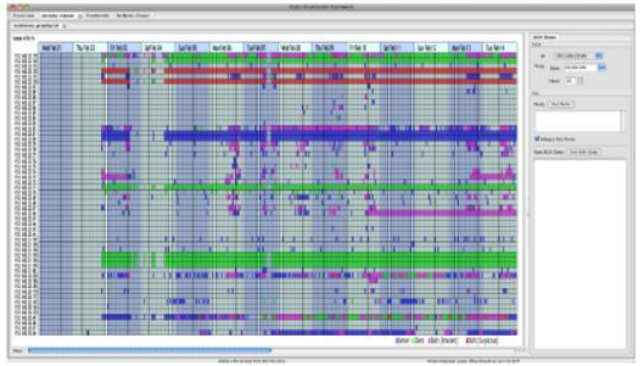
OVERFLOW – WHO?

- Sicherheitsanalytiker

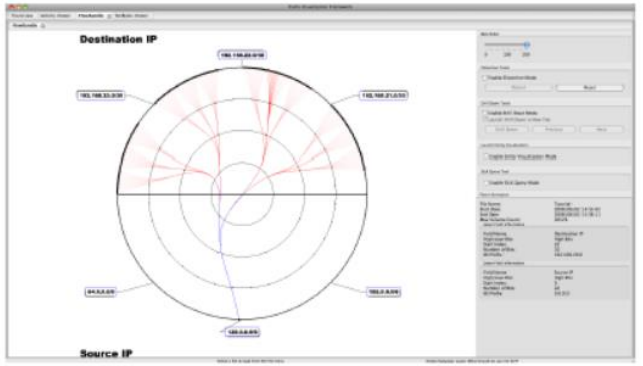
OVERFLOW – HOW?

- Fokus liegt auf den Interaktionen in und zwischen Subnetzen
- Verwendung von OverFlow im Kontext des FloVis Frameworks
- Organisatorischer Ansatz (Einteilen in Gruppen) → Überblick über die Situation und den Zusammenhang
- OverFlow bietet verschiedene Visualisierungen des gleichen Szenarios

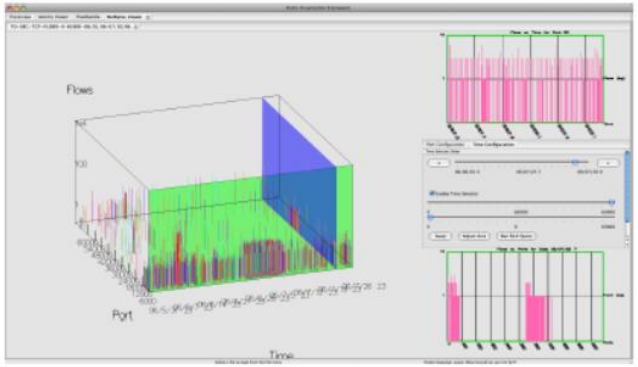
DAS FLOVIS FRAMEWORK



(a) Activity Viewer.

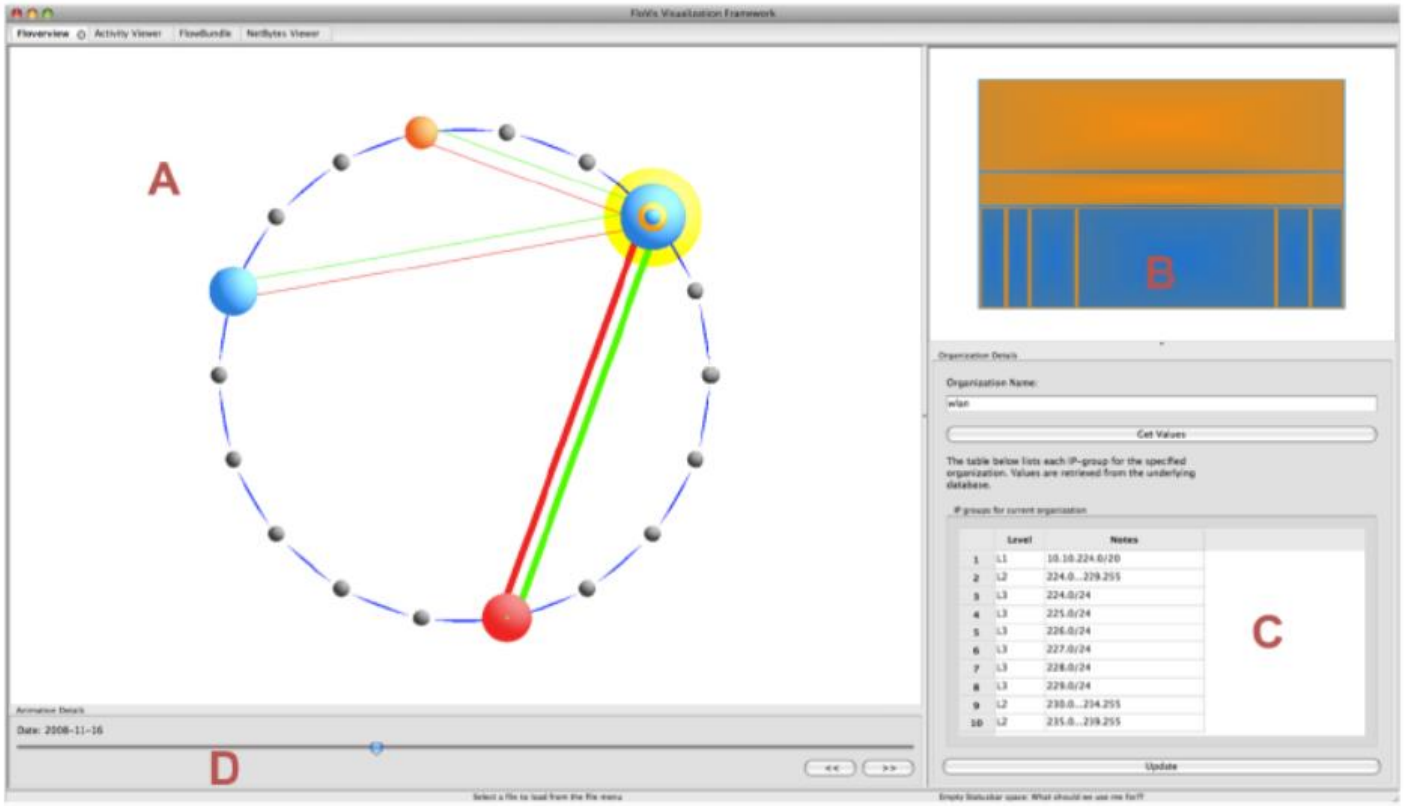


(b) FlowBundle.

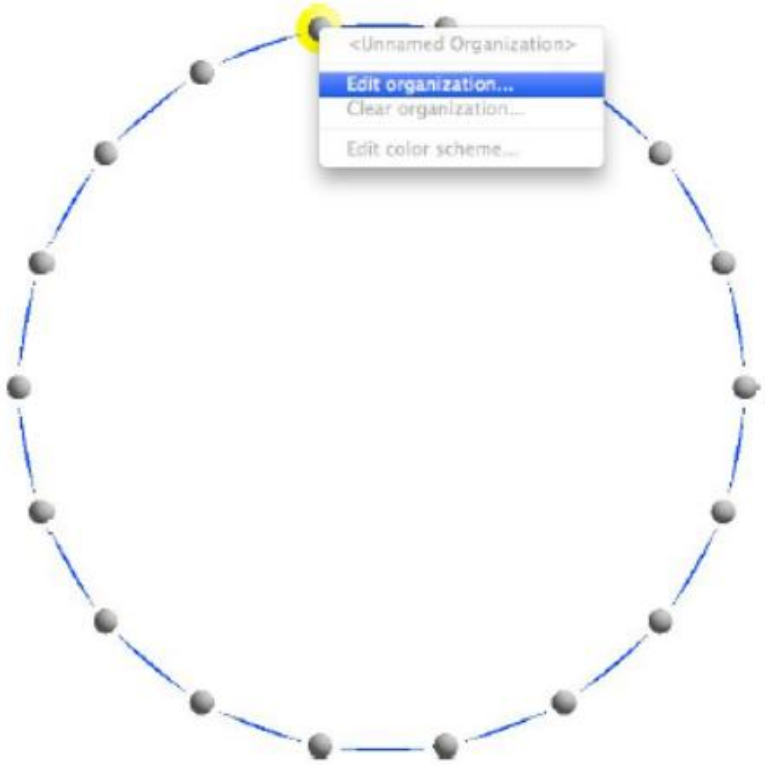


(c) NetBytes Viewer.

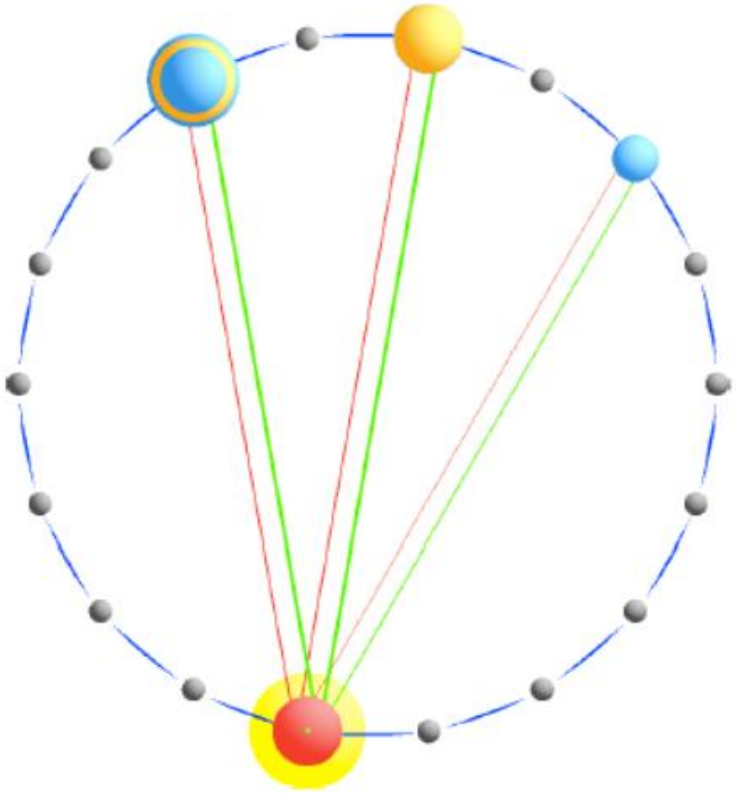
OVERFLOW – HOW?

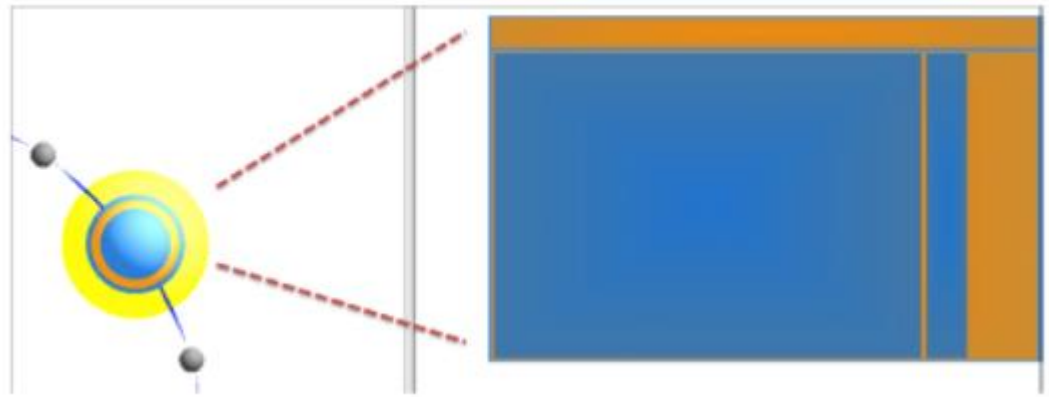


OVERFLOW – HOW?

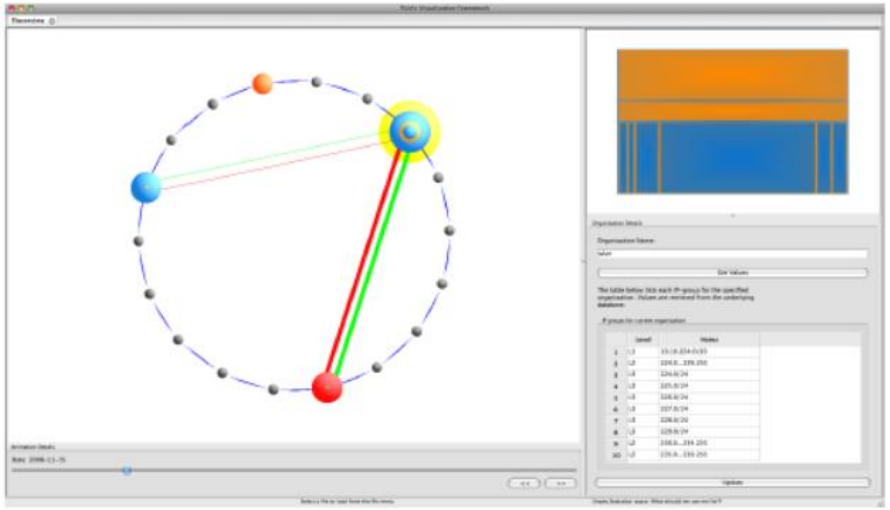


OVERFLOW – HOW?

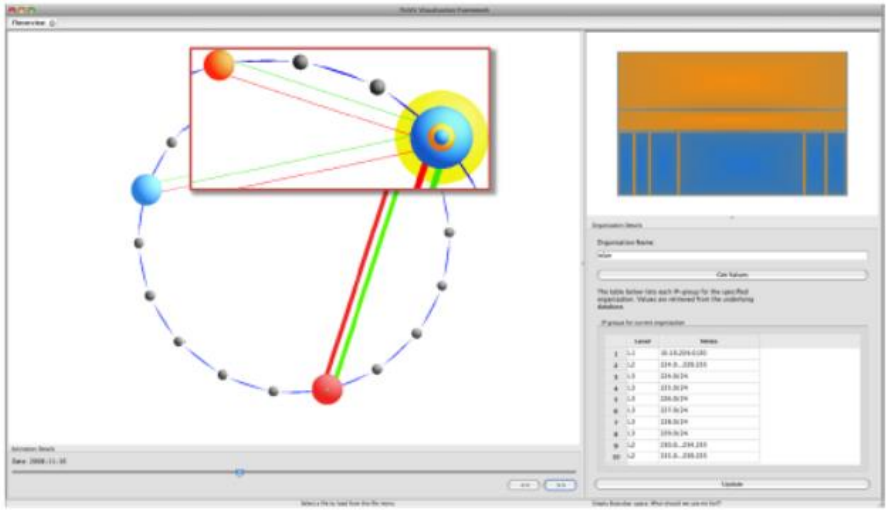




OVERFLOW – HOW?



(b) The second day.



(c) The third day.

OVERFLOW – PROBLEME?

- Große Abhängigkeit von den SiLK Tools
- „Bessere“ (andere) Darstellungen?

MAPPING AND VISUALIZING THE INTERNET – WHAT?

- Routing Pfade seit August 1998 gesammelt
- Sammlung von Intranet Daten
- Darstellung der Knoten und Kanten

MAPPING AND VISUALIZING THE INTERNET – WHY?

- Übersicht über das Internet und sein „Zentrum“
- Übersicht über das Intranet – mögliche Security Leaks, Trends, etc. werden aufgedeckt

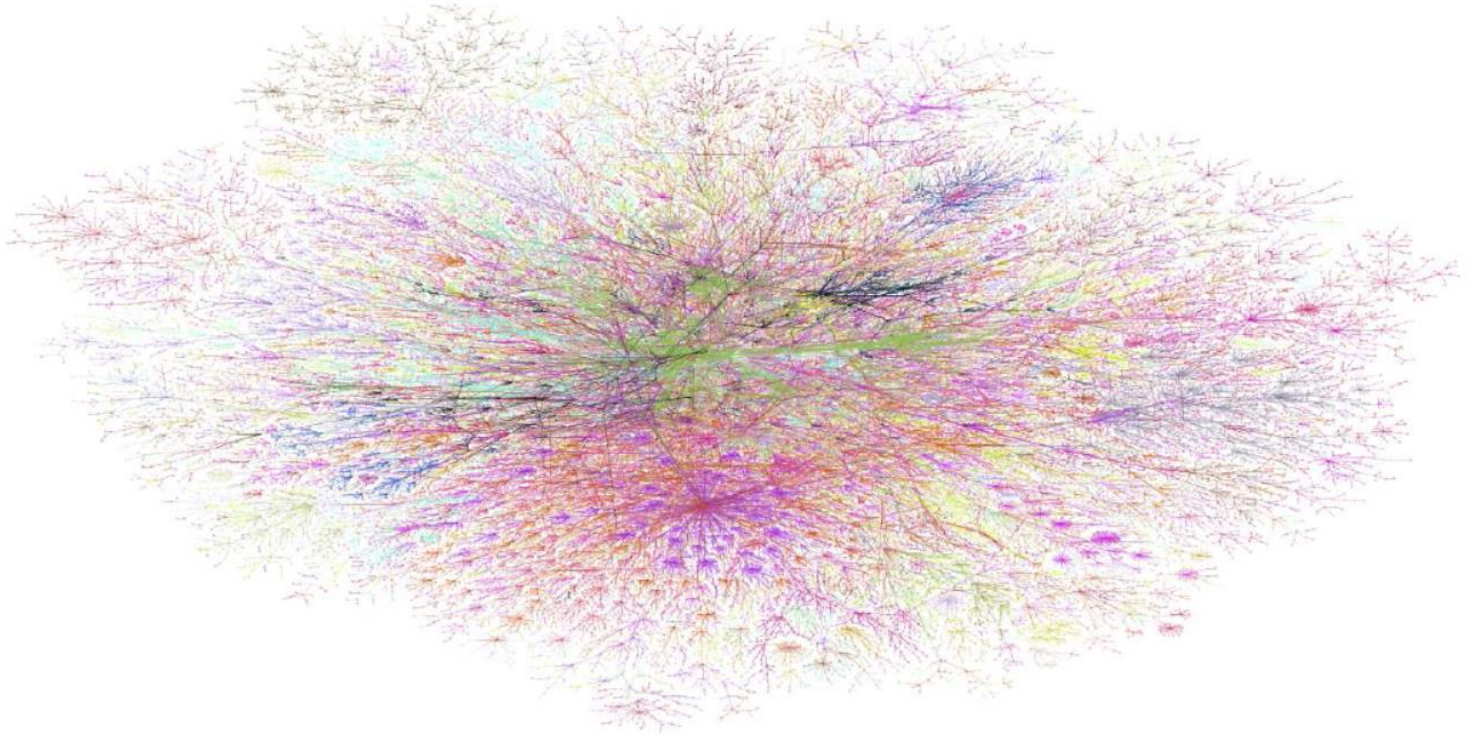
MAPPING AND VISUALIZING THE INTERNET – WHO?

- Forscher
- Firmeninterne Personen

MAPPING AND VISUALIZING THE INTERNET – HOW?

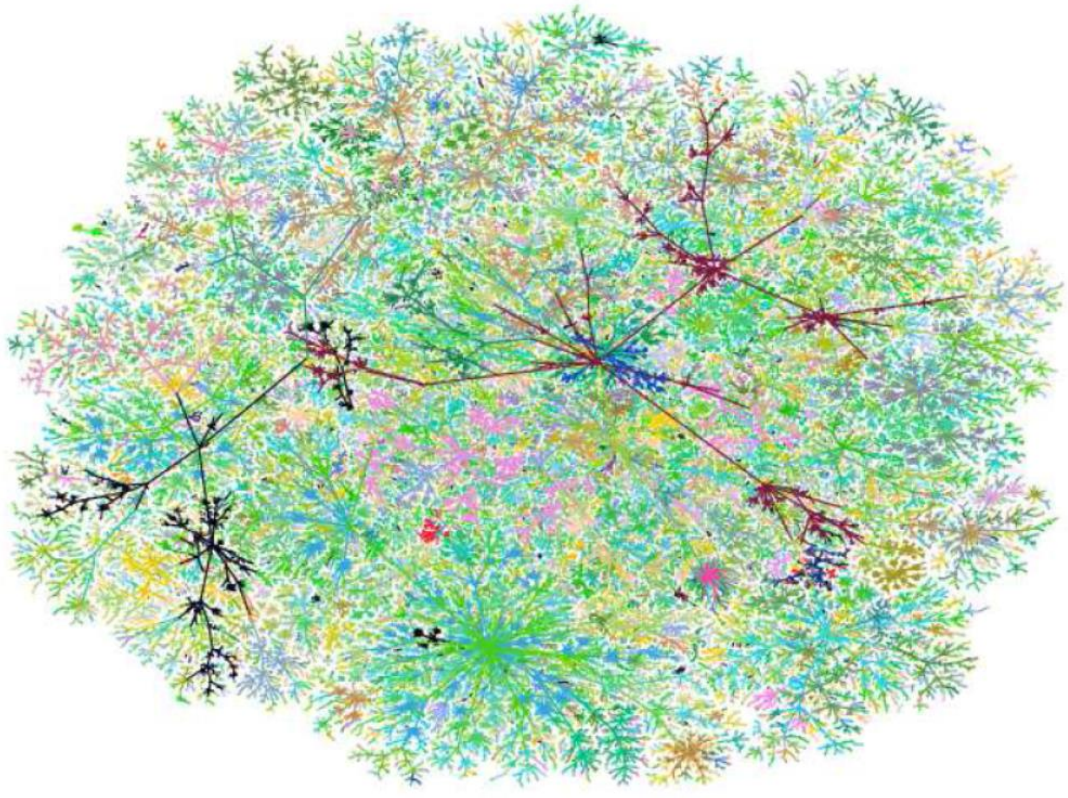
- Suche eines antwortenden Hosts
- Verfolgen des Pfades eines ausgehenden Paketes
- Der Pfad wir „Hop“-weise entdeckt
- Mapping der Knoten und Kanten

MAPPING AND VISUALIZING THE INTERNET – HOW?

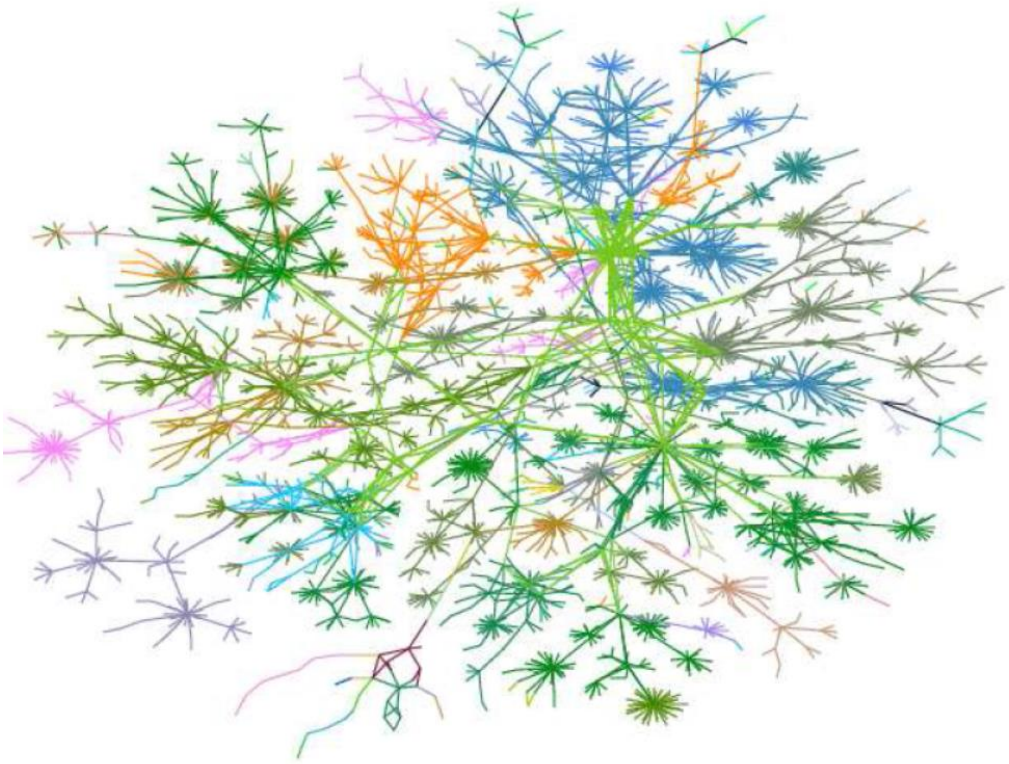


„smashed peacock on a windshield“

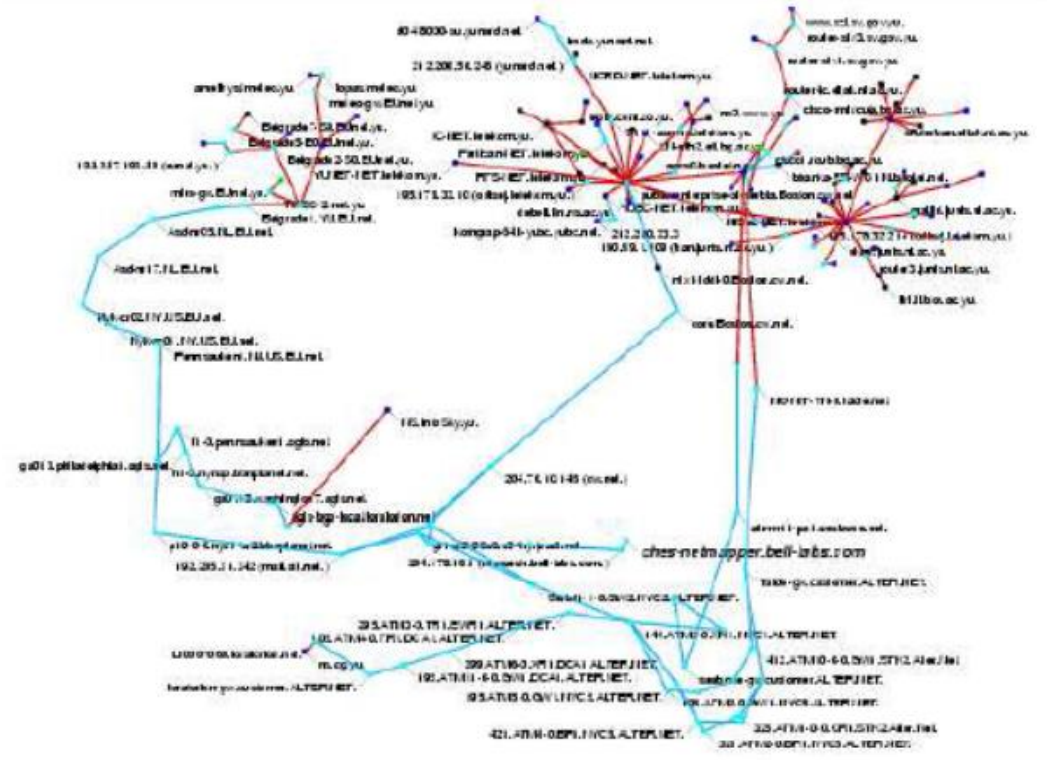
MAPPING AND VISUALIZING THE INTERNET – HOW?

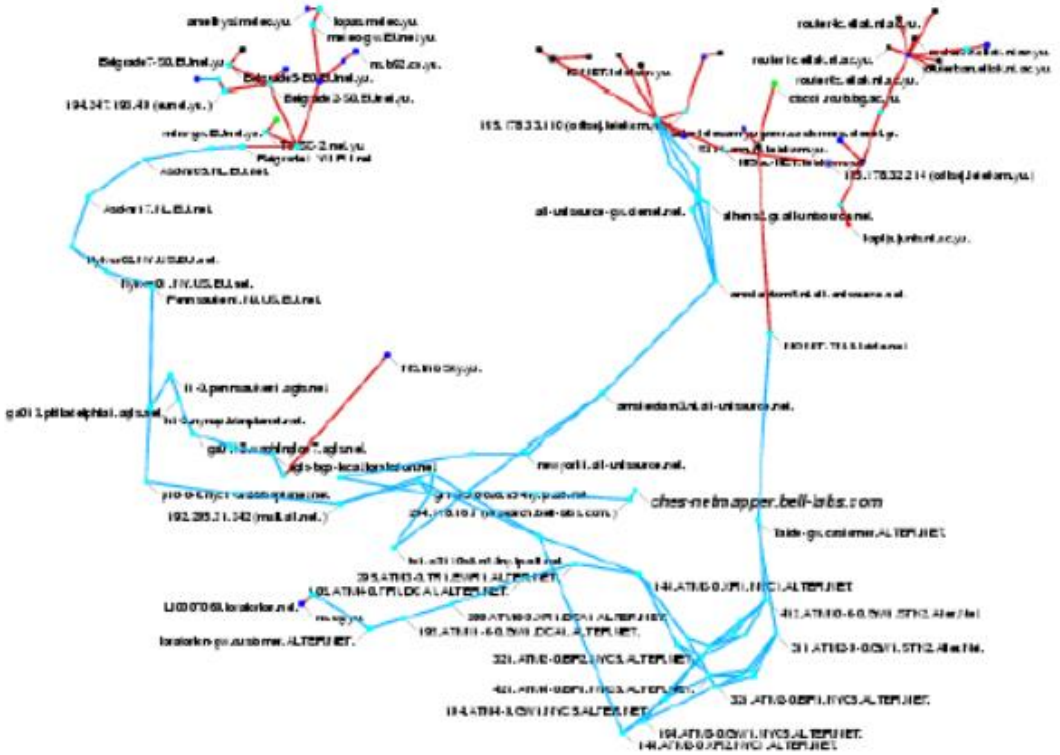


MAPPING AND VISUALIZING THE INTERNET – HOW?



MAPPING AND VISUALIZING THE INTERNET – HOW?





MAPPING AND VISUALIZING THE INTERNET – PROBLEME?

- Darstellung des „gesamten“ Internets sehr unübersichtlich
- Blockung der Testpakete
- Das Testen sollte nicht mit einem Hackerangriff verwechselt werden → Lösung?
- Es wird nur der Pfad eines ausgehenden Pakets verfolgt
- Wie visualisiert man die gewonnen Daten am besten, sodass man Nutzen daraus ziehen kann?
- Standardalgorithmen zu langsam

VERGLEICH DER PAPER

- OverFlow:
  - Zu Beginn ist nicht klar, was OverFlow überhaupt ist, und welche Daten zugrunde liegen.
  + Sehr gute Beschreibung von OverFlow inklusive Bildern
  + Sehr gute Differenzierung von anderen Ansätzen

- Mapping and Visualizing the Internet:
  - Differenzierung von anderen Ansätzen ist nicht klar
  - Zu wenig Gedanken über WHY? und WHO?
  + Es ist bereits zu Beginn ersichtlich, worum es geht und welche Daten visualisiert werden sollen.

FRAGEN?