Network Situational Displays from Network Flow Data

Timothy J. Shimeall
CERT/NetSA

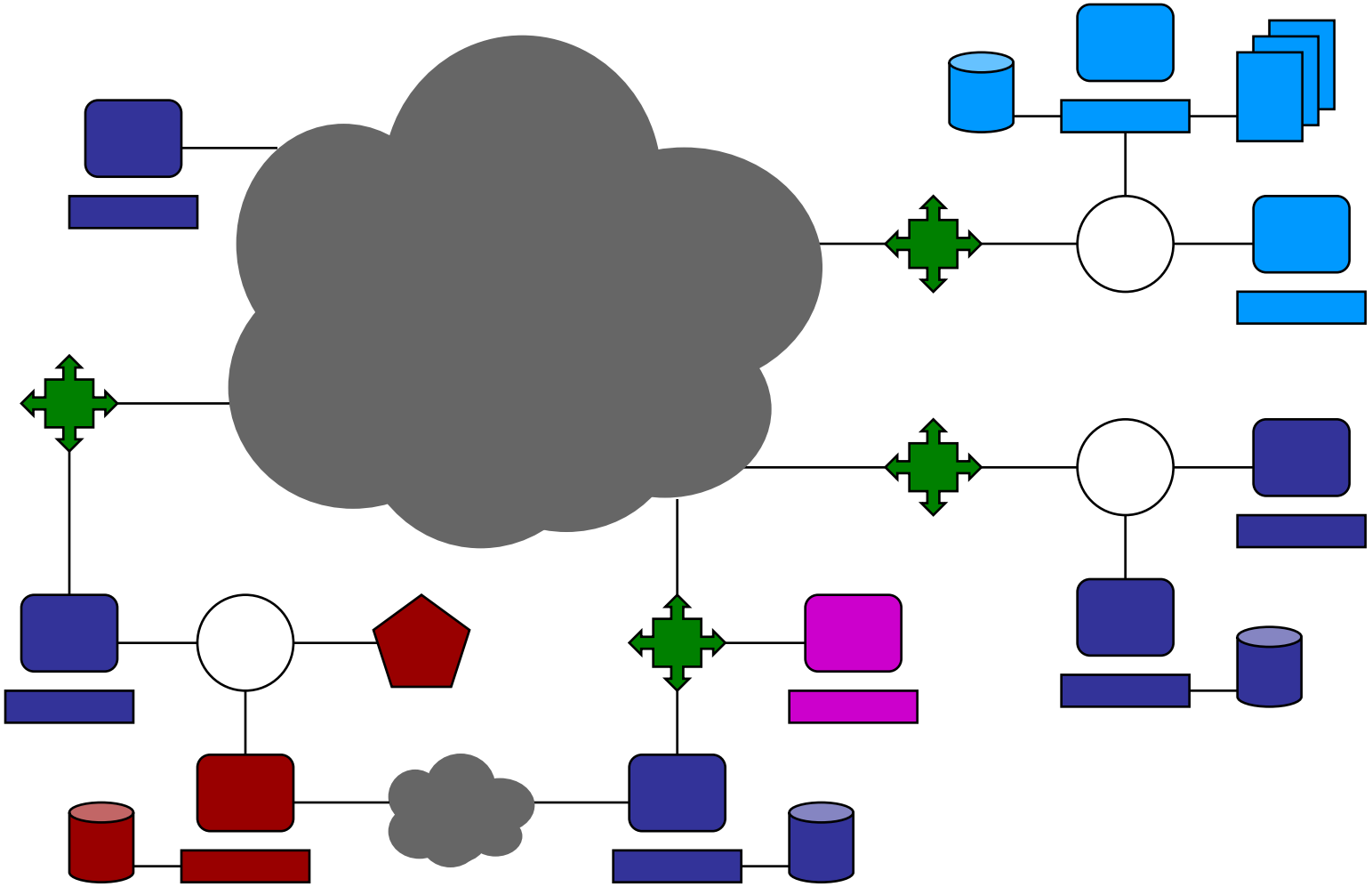
NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

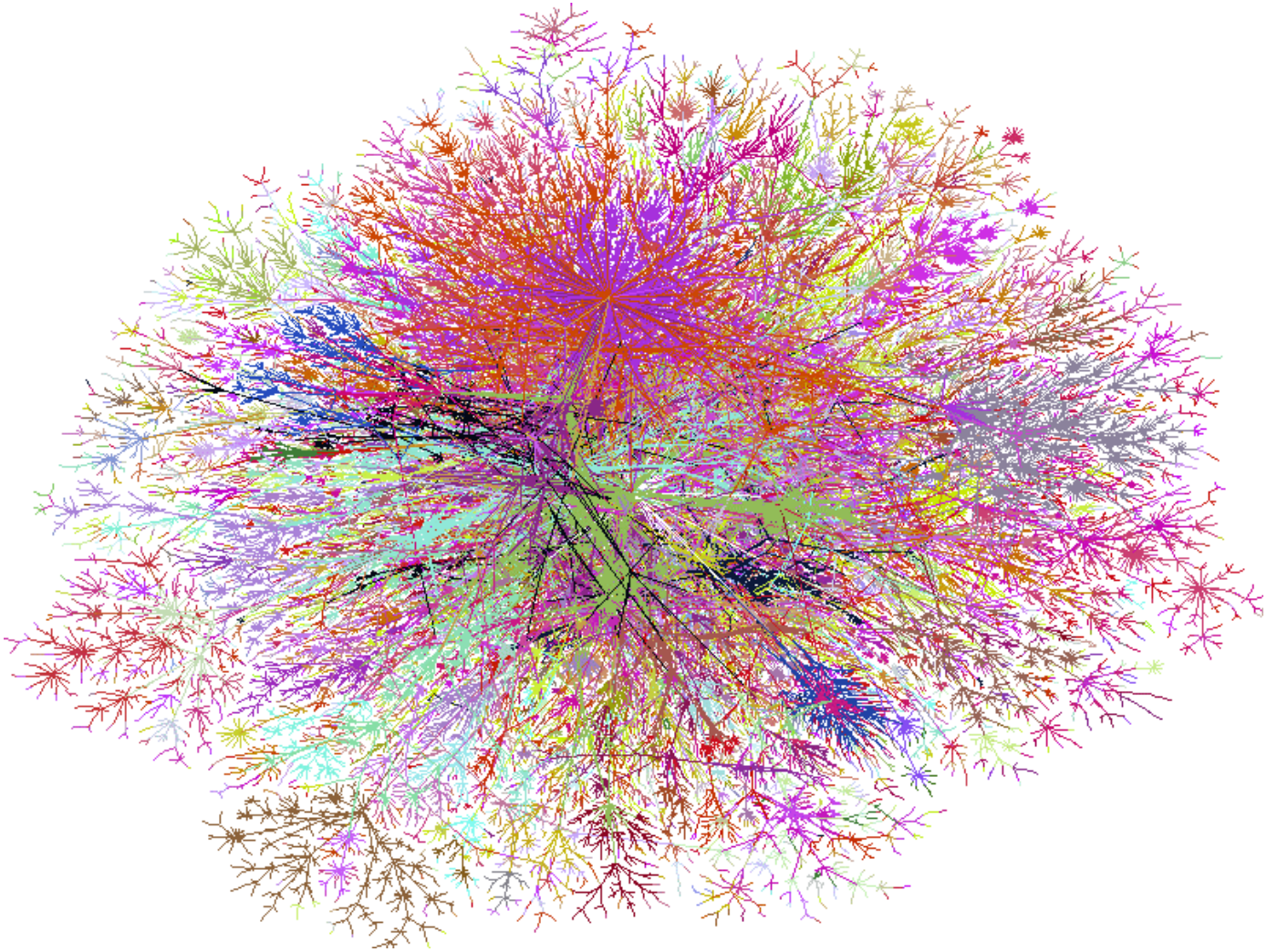
Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

Physical-Centric



ISP-centric



Source: http://www.cheswick.com/ches/map/gallery/index.html

Difficulties

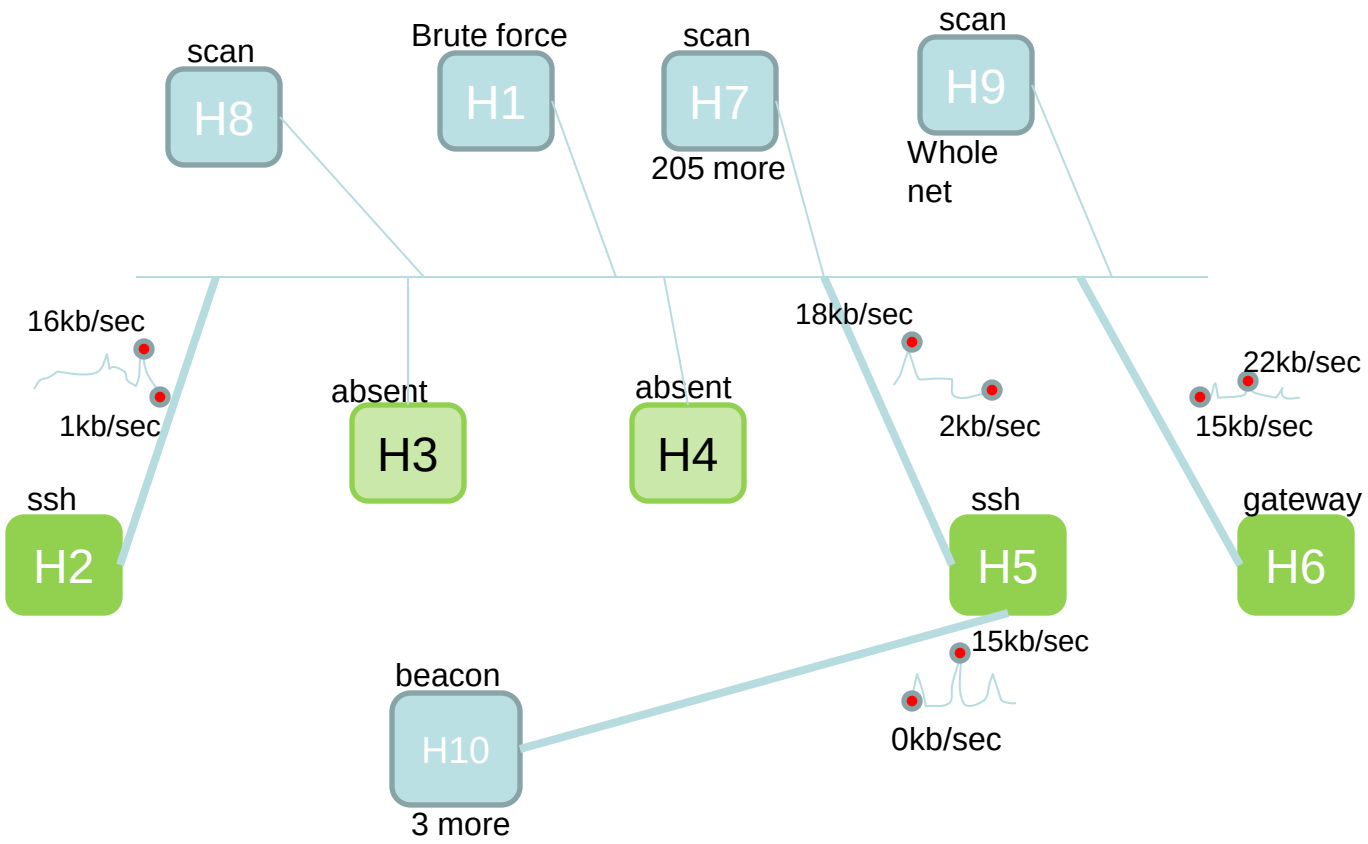
Generation from flow

Pertinence to current threat model

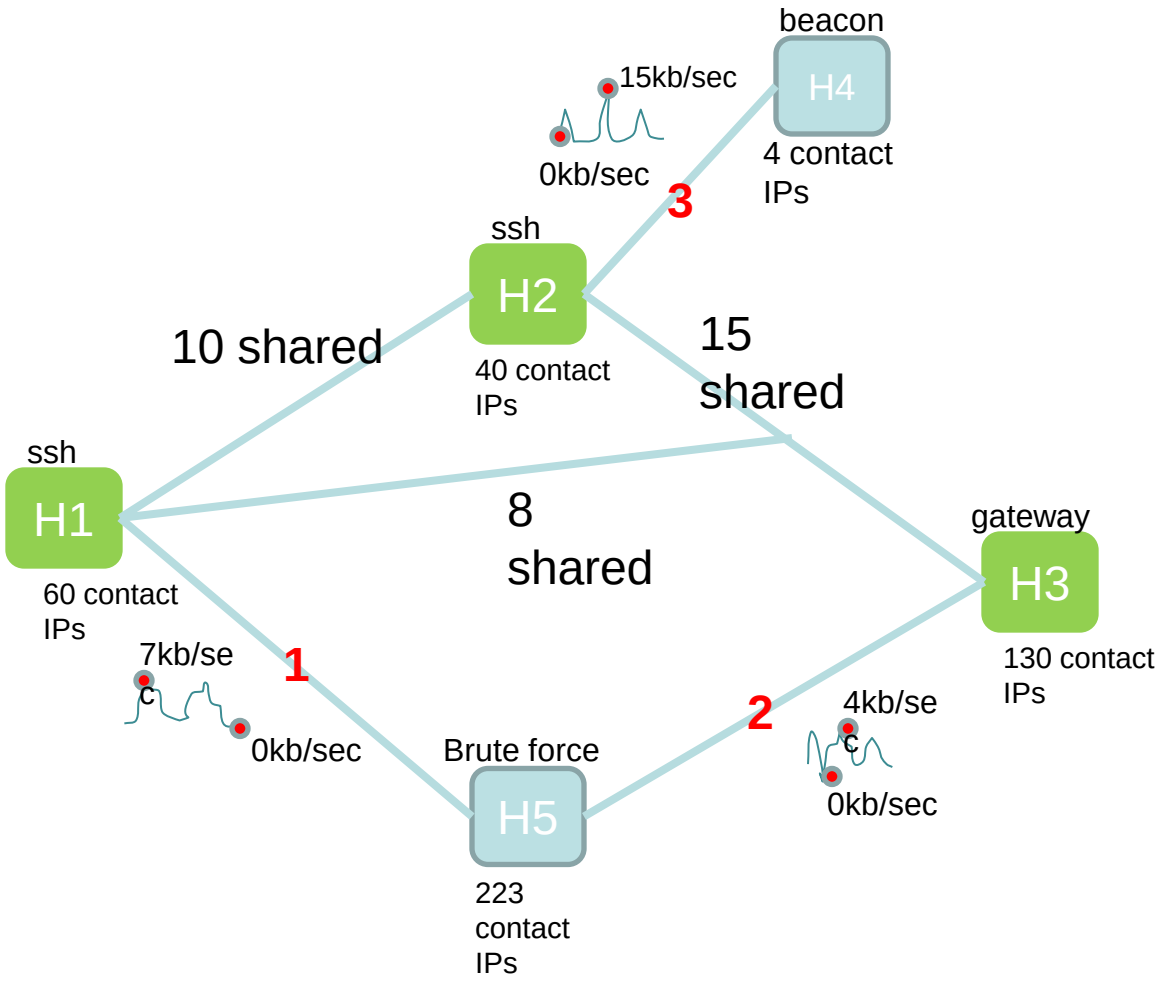
Ability to represent activity

Clarity to decision-makers

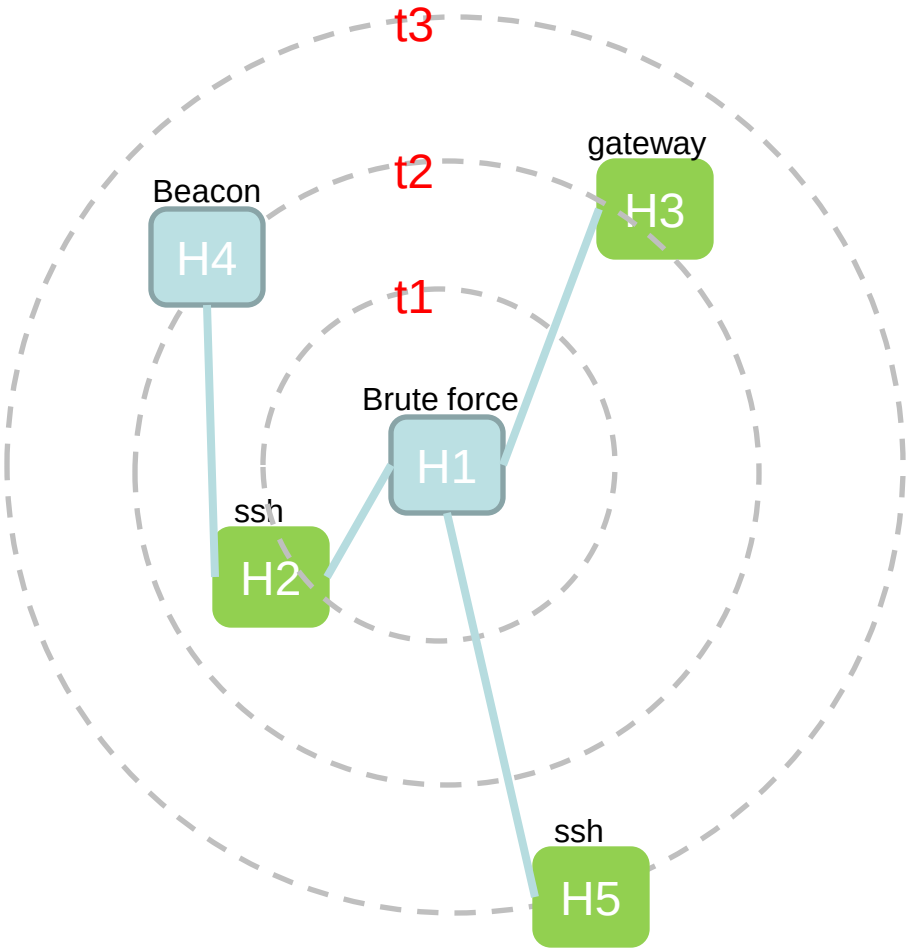
Connection-centric



Address-Centric



Time-Centric



Situation

Timeframe

Volume

Hosts

Services

Contacts

Display

Position

Color

Labeling

Juxtaposition

Clutter elimination

Goals

Questions

Flow-based generation

Multivariate

Awareness

Decisions

Summary

Supergraphics

Flexibility

Self-interpreting

Questions?