Improving Intrusion Detection Systems
Through Heuristic Evaluation

A. Zhou, J. Blustein, N. Zincir-Heywood

Computer Science, Dalhousie U.

The State of Network Security

- Bad!
  - Very few sysadmins check in real-time
  - High false alarm rates/Low detection rates
  - Does not differ by network or team size
- Sysadmins feel poorly about current tools
  - Including tools they have created themselves

What are we doing?

- Overall Goal:
  - Improve IDS through better technology…
  - and more suitable user interfaces
- HCI Sub-goal
  - Develop and assess new UI

Recent HCI Activities

- Ongoing survey and interviews
  focused on user and task profile
- Identified some UI flaws in Snort and Snortsnarf
- Developed a new UI to Snort
- Developed early draft of heuristics
- Evaluated those heuristics

Usability

- Many definitions but always includes
  - Types of users
  - The tasks those users need to perform with systems to achieve external goals
- Gates & Whalen personality assessment
- Our prediction:

  Thrive on diversity & challenge

Heuristics

- Discount (non-user) evaluation technique
- Method to focus evaluation to increase thoroughness
- Based on analysis of problems found in typical UIs

General & Special Heuristics

- Heuristics for specific areas can differ
- Controversy over security evaluation

Heuristics Development: General Method

- Combine results from multiple reviewers:
  - Identify all problems using a fixed vocabulary
  - Assess severity of each problem
- Finds maximal number of problems
- UE Experts are recommended
  - Understand vocabulary of evaluation
  - Familiar with common problems
  - No Hawthorne bias

Heuristic Development: Ours

- Based on surveys, interviews, and use of IDS
- Made a list of *all* UI-related problems
- Determined which were part of general ones
- Added & removed heuristics to made IDS set
- Next, evaluated performance …

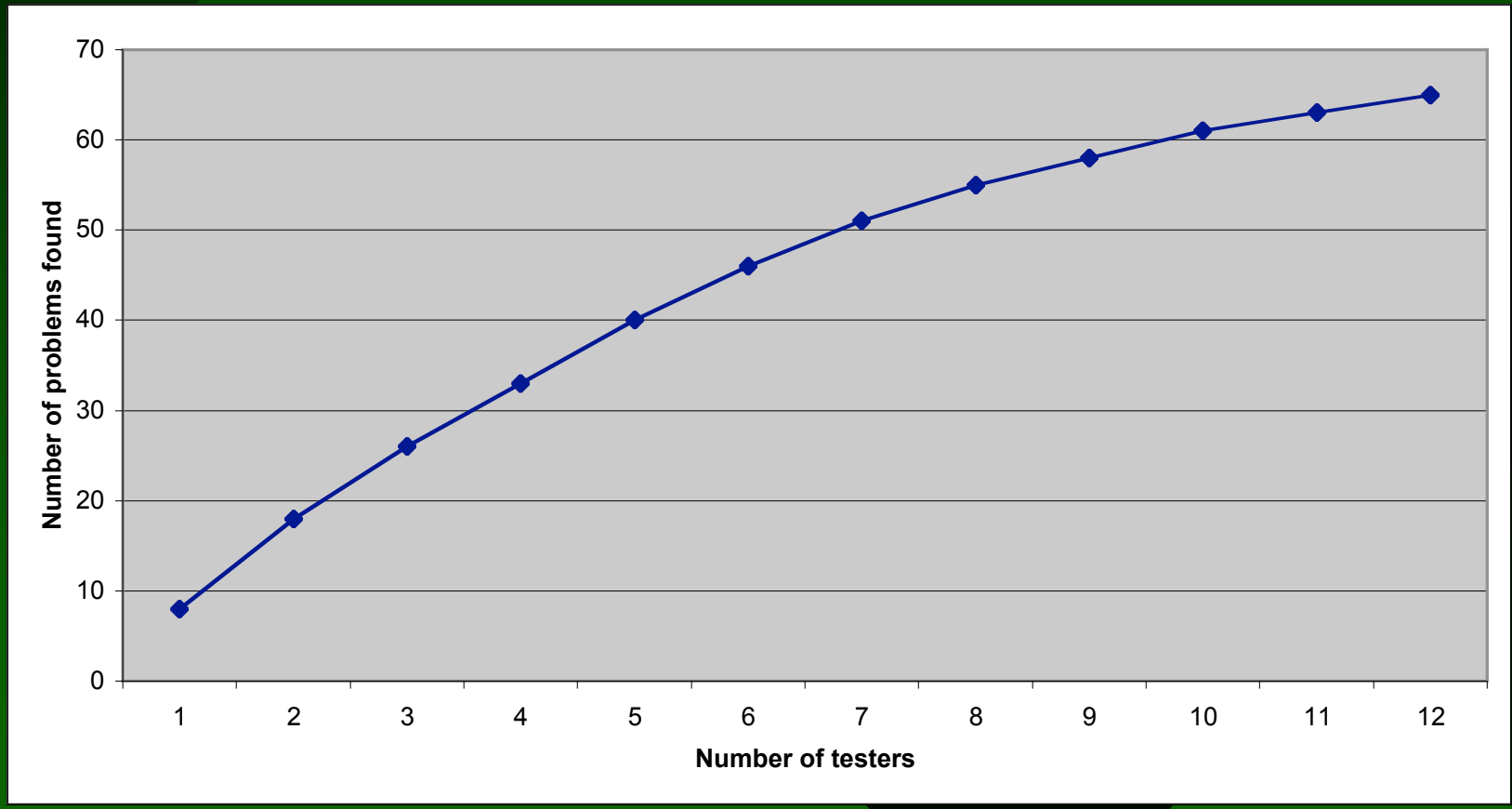
Experimental Parameters

- *N* = 12
  - 5 primarily UE experts
  - 7 primarily security experts
- Used Nielsen's general heuristics & ours
- Assessed
  - Our system (Snort Alert)
  - Snortsnarf

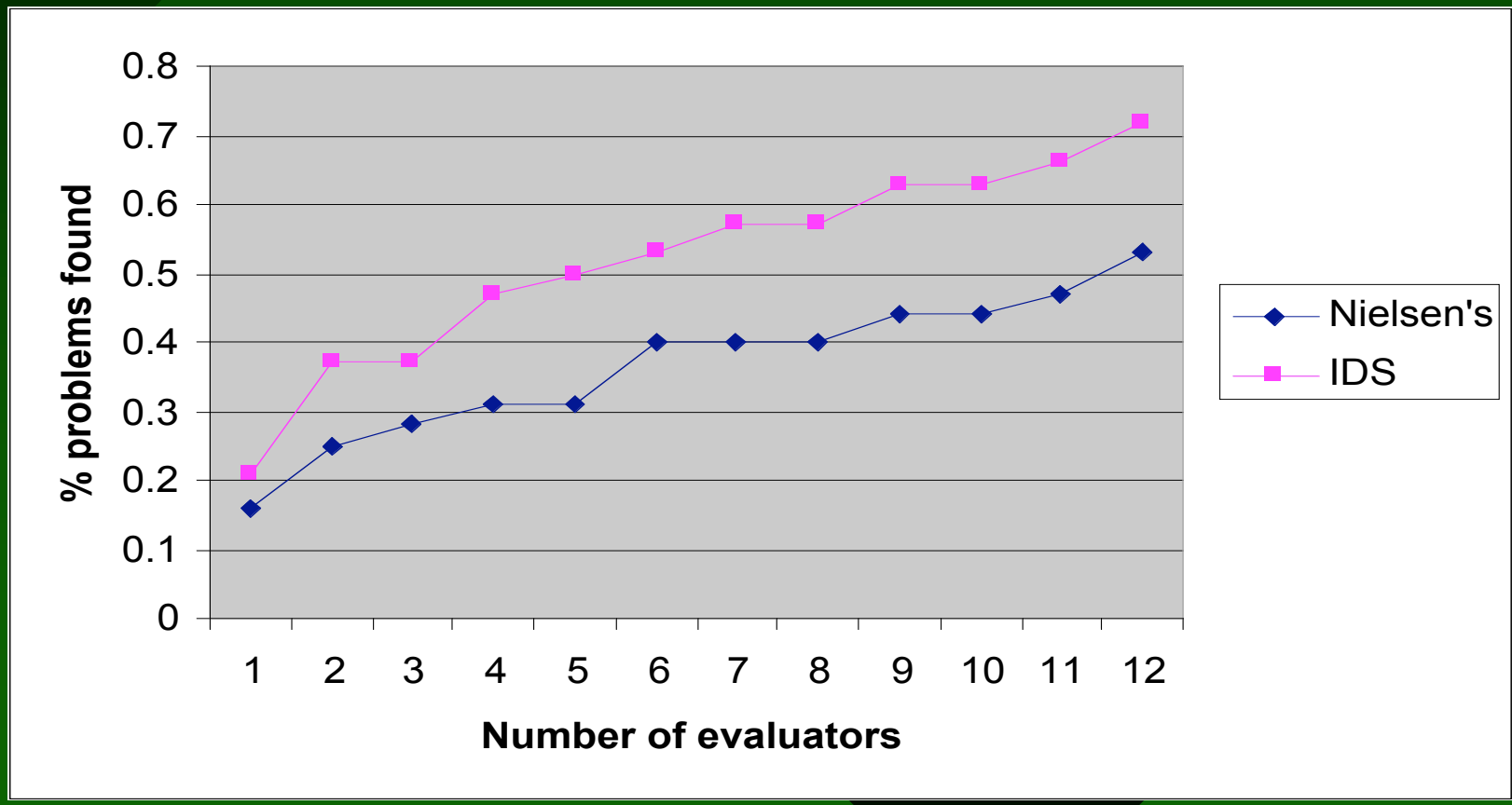
Results

- Twelve testers found more problems than one expert
- The IDS set outperformed the general set
- But there was extensive overlap

Five Is *Not* Enough



IDS Heuristics Outperform General Heuristics



Conclusion

- Heuristics *can* apply to security systems
- Five UE expert testers is *not* enough
- Do we need a special IDS set?
  - Substantial overlap
  - Some novel problems found with IDS set
  - Not 100% agreement between sets
  - Statistical investigation is ongoing

Future Directions

- Ongoing survey

  `http://www.cs.dal.ca/~secsurv/`

- Detailed statistical analysis of overlap
- Heuristics to be refined

Contact Addresses

1. http://www.cs.dal.ca/~secsurv/

2. Dr. Jamie Blustein

   Dalhousie U. Faculty of Computer Science

   http://www.cs.dal.ca/~jamie/