

# TWC: Small: Understanding Network Level Malicious Activities: Classification, Community Detection and Inference of Security Interdependence

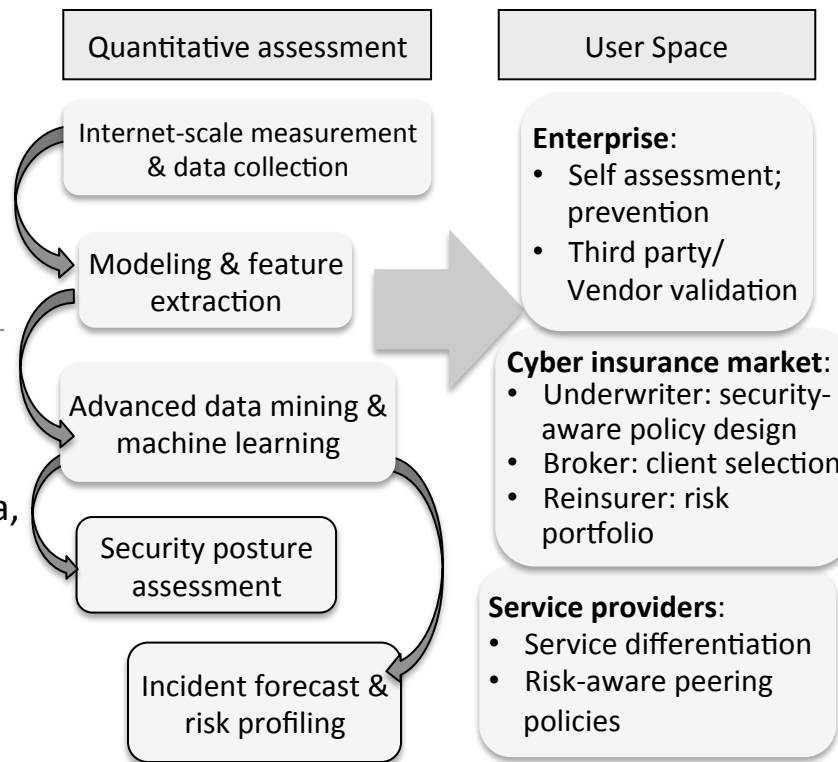


## Challenge:

- How to define metrics to quantitatively assess the security posture of a network entity rather than individual hosts.

## Solution:

- Using a diverse set of Internet measurement and demographical data, and a large set of data breach incidents.
- Applying supervised learning to perform breach prediction at an org level.



## Scientific Impact:

Directly relevant to the design and implementation of security policies

- can only be meaningfully applied at a network organizational level
- under severe resource limitation

## Broader Impact:

- Potential paradigm shift in introducing new ways of thinking about cyber security at a higher level and in a more holistic manner.
- Research finds direct use in the cyber insurance industry.
- Successful tech transfer.

CNS-1422211  
 University of Michigan, Ann Arbor  
 Contact/PI: Mingyan Liu  
 ([mingyan@umich.edu](mailto:mingyan@umich.edu))