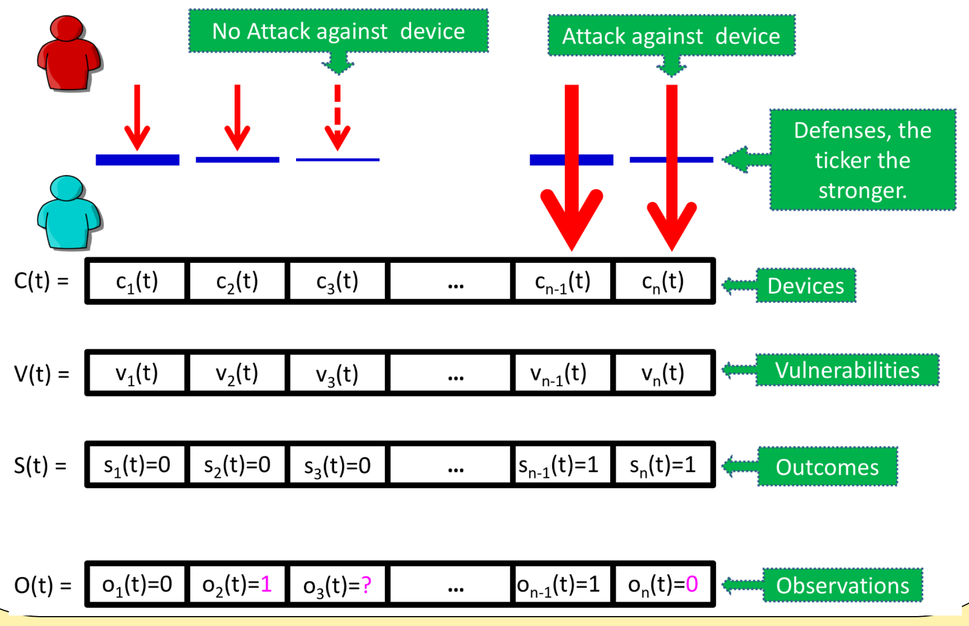
Security Metrics: Systematization and Road Ahead

Shouhuai Xu (University of Texas at San Antonio)
http://www.cs.utsa.edu/~shxu/socs/
[NSF #1111925]

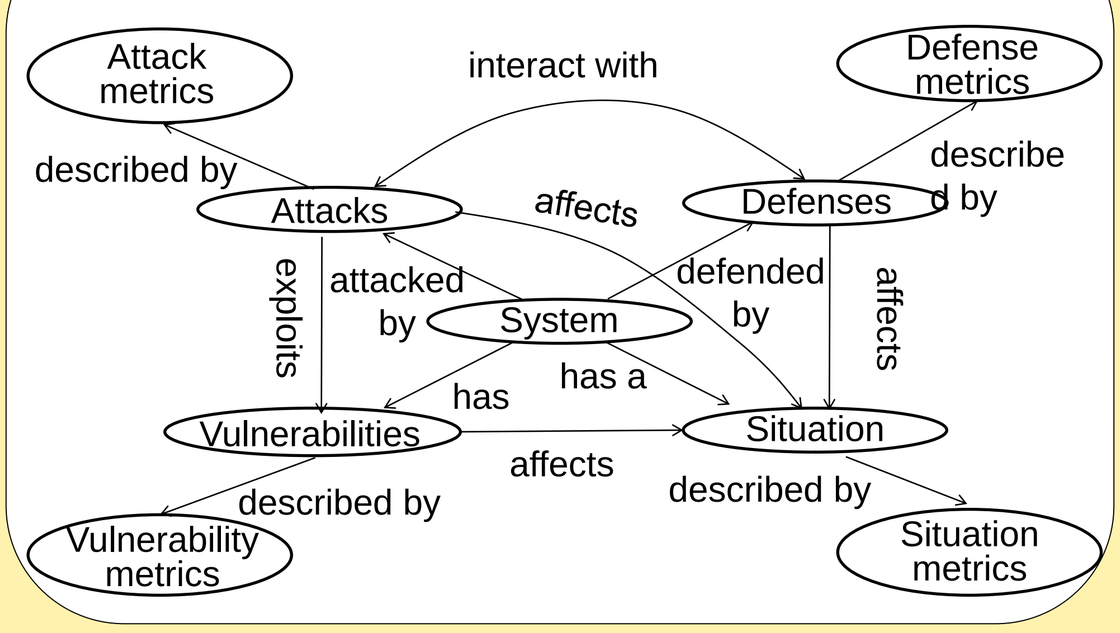
Motivation: Is it possible to tackle the security metrics problem?

- A systematization of security metrics from the perspective of attack-defense interactions
- An ontology of security metrics describing the relationships between them
- What we need to do in order to tackle the problem and future research directions

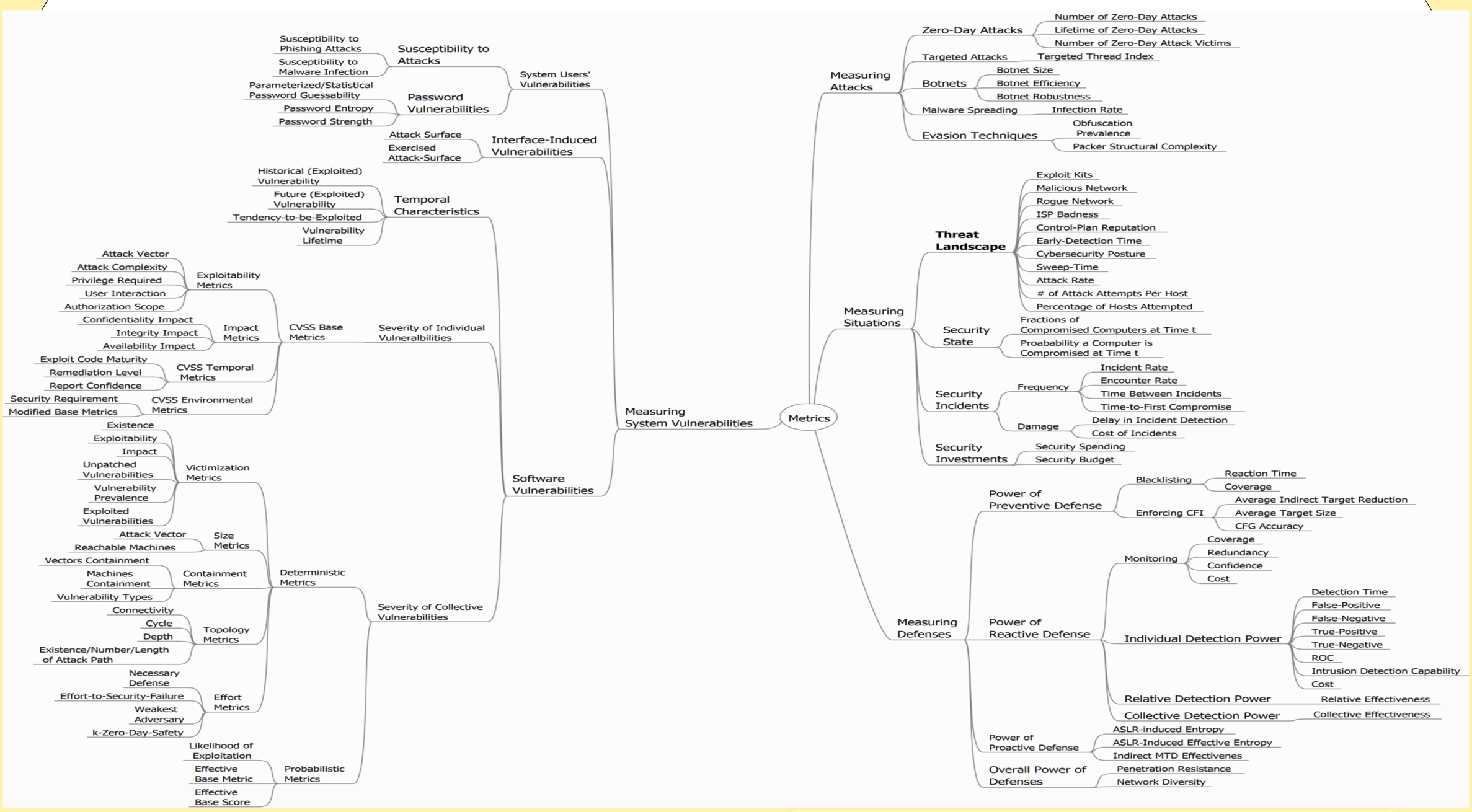
Illustration of attack-defense interactions



A high-level ontology of security metrics



A taxonomy of security metrics



Suggestions for future research

- Understanding desirable properties of security metrics
- Defining and measuring metrics that matter more
- Explicitly defining security metrics in publications.
- Developing security metrics curriculum.
- Government agencies playing a bigger role in bridging industry (with real data) and academia.

References

- M. Pendleton, R. Garcia-Lebron, J. Cho, and S. Xu. *A Survey on Systems Security Metrics*, ACM Computing Survey, to appear (available from the above website).

Ongoing research

- Defining security / resilience / agility metrics
- Designing measurement methodologies
- Conducting case studies with repeatable experiments

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

UTSA