Cybersecurity Dynamics

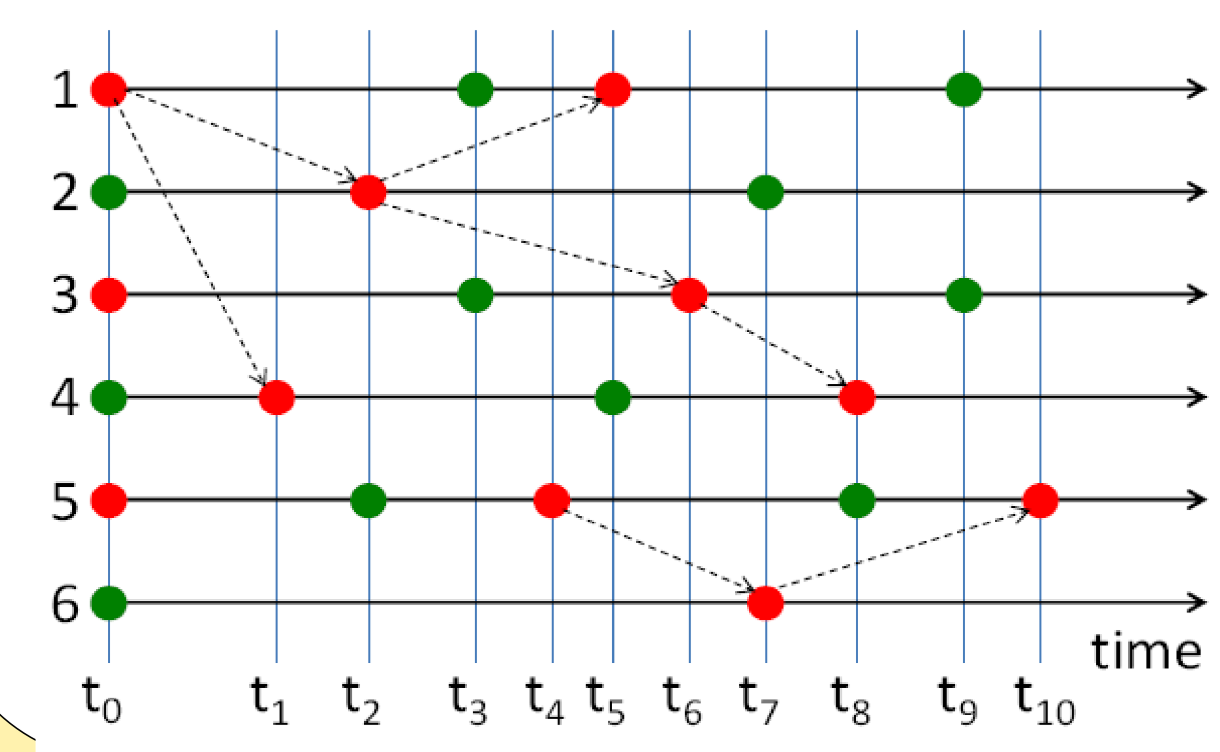
Shouhuai Xu (University of Texas at San Antonio)

http://www.cs.utsa.edu/~shxu/socs/ [NSF #1111925]

Motivation: Can we model cybersecurity from a holistic perspective?

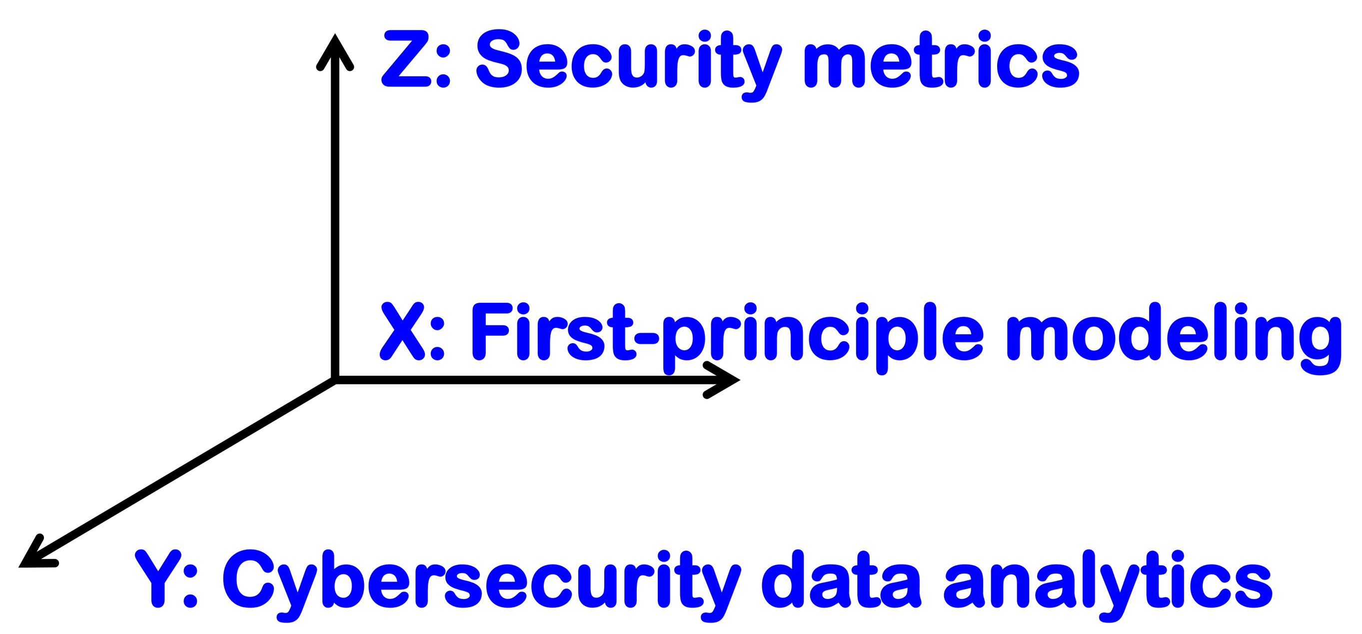
- Understand and quantify the global effectiveness of defense architectures / mechanisms
- Achieve quantitative cybersecurity risk management and principled decision-making
- Predict and dictate the evolution of the global security state to benefit the defender

illustration of the dynamics



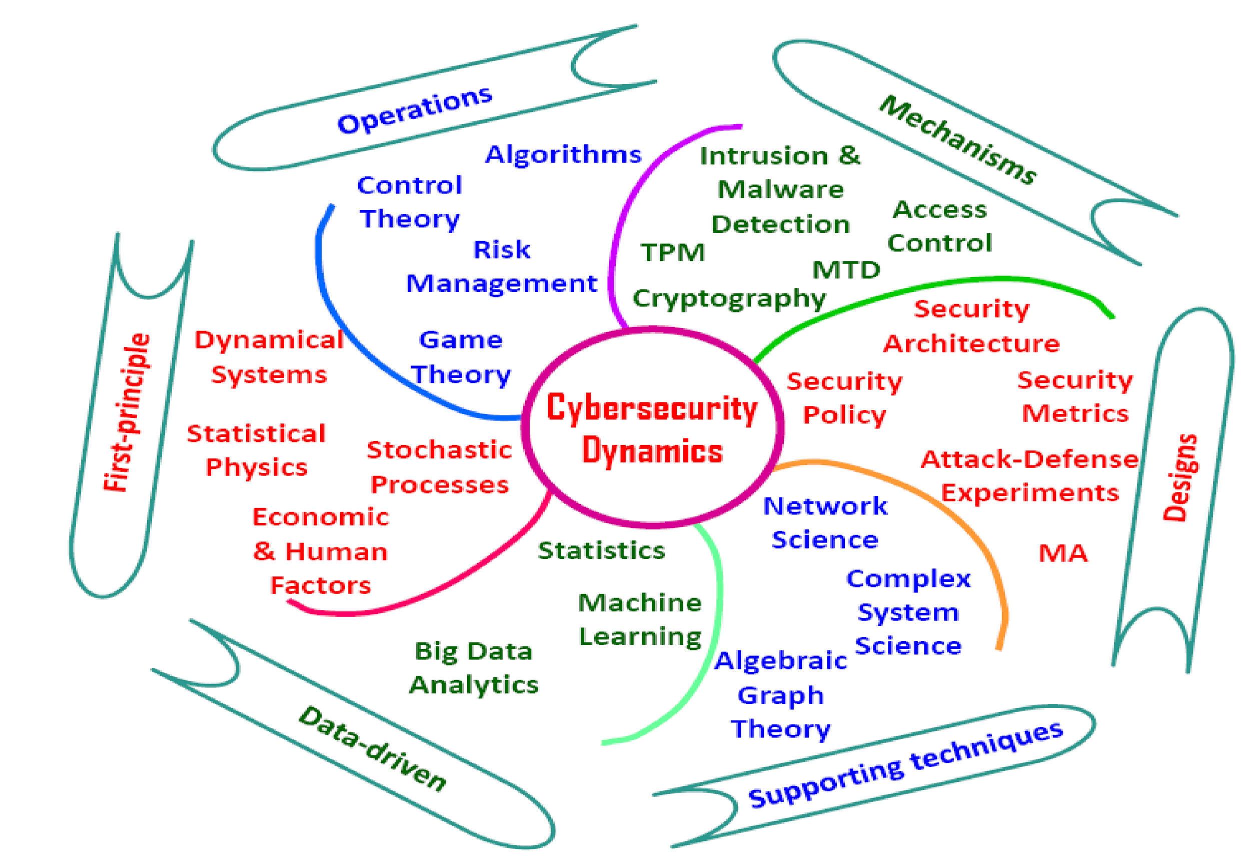
Cybersecurity Dynamics [1] describes the evolution of global cybersecurity state caused by cyber attack-defense interactions. In this toy cyber system that has six nodes, which can represent computers (but other resolutions are both possible and relevant), a node may be in one of two states, **secure** or **compromised**; a secure node may become compromised and a compromised node may become secure again, and so on. A red-colored node u pointing to a red-colored node v means u successfully attacked v. Even if node 5 is not attacked by any other node at time t_4, it still can become compromised because of (e.g.) an insider attack launched by an authorized user. An important abstraction is ***attack-defense structure***, (i.e., which computer can directly attack against and/or defend for which other computers).

Approach: X-Y-Z-T



- Models are centered at security metrics
- First-principle modeling leads to deep understanding about the dynamics (e.g., what can happen under what circumstances)
- Data analytics help validate models and obtain security parameters
- T (time) means everything can be dynamic

The concept and its power



Inherent technical barriers

- Scalability barrier: This state-space explosion problem.
- Nonlinearity barrier: Highly nonlinear.
- Dependence barrier: Modeling dependent/adaptive attacks.
- Structural dynamics barrier: Dynamic attack-defense structures.
- Non-equilibrium/transient behavior barrier: Harder than equilibrium.

Some highlights

- Under fairly general (or weak) assumptions, preventive and reactive cybersecurity dynamics always converge to some unique equilibrium [2].
- Active cyber defense dynamics can exhibit Bifurcation and Chaos [3].
- Cybersecurity exhibits emergent behaviors [4]

References (available from the above website)

1. S. Xu. Cybersecurity Dynamics. HotSoS'14.
2. R. Zheng, W. Lu, and S. Xu. Preventive and Reactive Cyber Defense Dynamics Is Globally Stable. manuscript, 2016.
3. R. Zheng, W. Lu, and S. Xu. Active Cyber Defense Dynamics Exhibiting Rich Phenomena. HotSoS'15.
4. S. Xu. Emergent Behavior in ybersecurity. HotSoS'14

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