Rebecca N. Wright

Rutgers University
www.cs.rutgers.edu/~rebecca.wright

Research interests: computer and communications security, particularly in the areas of privacy, accountability, cryptographic protocols, and fault-tolerant distributed computing.

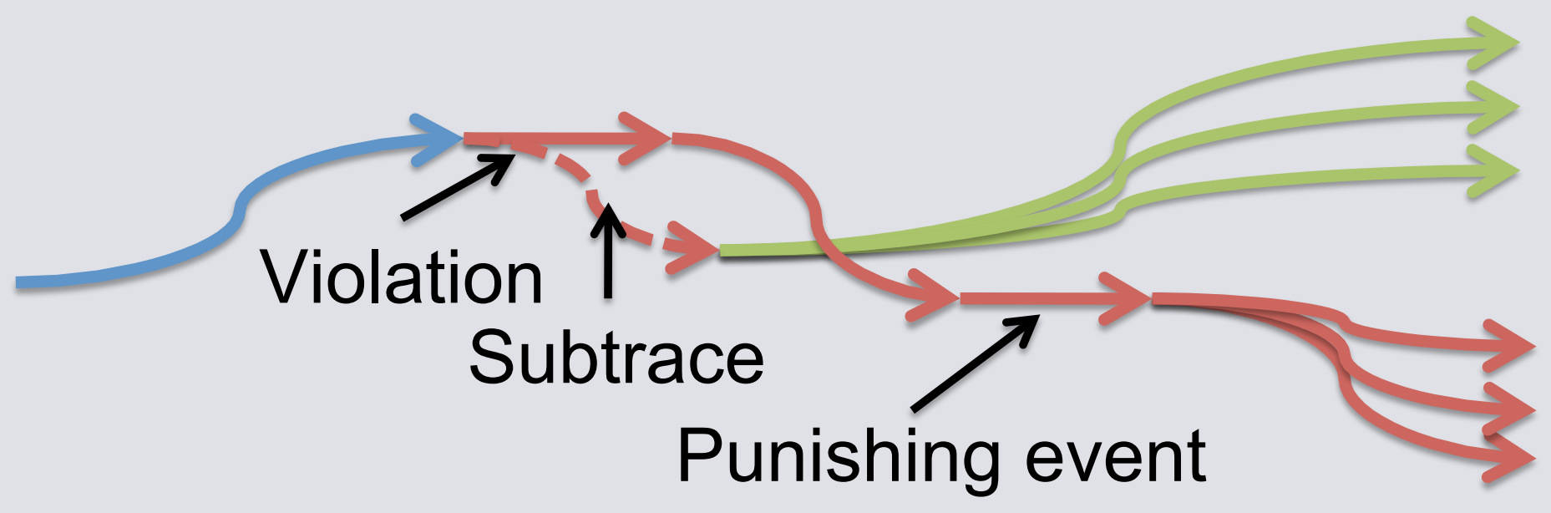
Privacy

- Means different things to different people, to different cultures, and in different contexts.
- Our work seeks to provide mathematical, rigorous privacy guarantees for definitions of privacy appropriate for different settings.
- Secure multiparty computation: multiple parties communicate to compute a function of their combined data, but without requiring the data to be combined or revealing anything else about the data to each other. Some of our work: private clustering [KDD'05, SDM'06], Bayesian networks [TKDE'06], reinforcement learning [ICML'08], approximations [ICALP'01], sampling [ICALP'07], imputation [PADM'06].
- Differential privacy: responses based on data should not depend substantially on any individual's data. Some of our work: differentially private random decision tree classification [PADM'09], pan-private algorithms in the streaming model [PODS'11].

Accountability

- Traditional focus in computer security is on preventive security. We want to complement this with accountability [WebSci'11, NSPW'11].
- Agents are held accountable for violations of security policy if they are, or could be, punished.
- Towards a formal model of accountability, we consider mediated and automated punishment.
- Example: mediated punishment:

Utility ends up worse after violation than without it.



- Formalization allows exploration of questions such as whether accountability can be separated from identifiability, tradeoffs between accountability and other properties.

Distributed Computing & Game Theory

- We consider asynchronous dynamics in distributed systems in which computational nodes repeatedly make decisions in response to others' behavior.
- We study when simple and unsophisticated rules of behavior (such as "best reply" and "regret minimization") guarantee convergence in asynchronous computational environments.
- [ICS'11]: In an asynchronous setting, if each node's reaction function has bounded recall and is self-independent, then the existence of multiple stable states implies that the system cannot guarantee convergence to a stable state.
- Applies to a broad range of settings including BGP Internet routing, TCP congestion control, stabilization of asynchronous Boolean circuits, technology diffusion in social networks, and convergence of game dynamics to pure Nash equilibria.

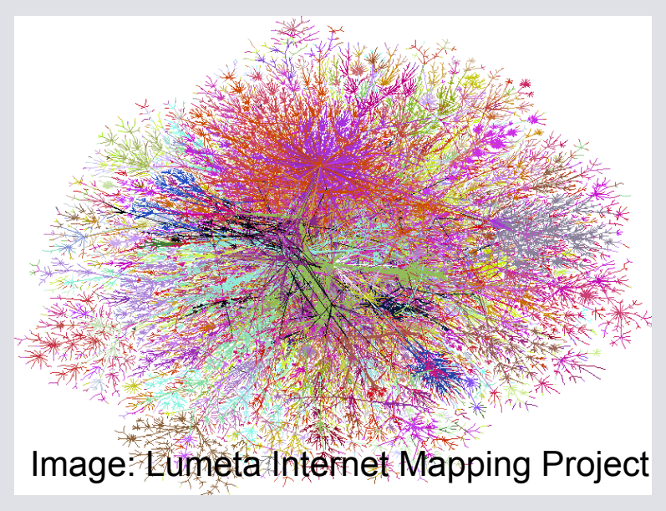


Image: Lumeta Internet Mapping Project

DIMACS

Center for Discrete Mathematics & Theoretical Computer Science
Founded as a National Science Foundation Science and Technology Center

DIMACS (Rebecca Wright, Director)

- Facilitates research, education, and outreach in discrete mathematics, theoretical computer science, and related areas, including their applications to other areas of computer science, other sciences, and beyond the sciences. Examples:
- Special Focus programs: foundations of the Internet, cybersecurity, algorithmic decision theory, energy, sustainability
- Education and outreach programs: computational thinking modules, bio-math connection, high school teacher training
- Integrative research and education programs: research experiences for undergraduates, tutorials, Reconnect program
- International programs: China, Africa, Czech Republic

中美软件研讨会 -- China-US Software Workshop
软件开发的双边合作 -- Bilateral Collaboration for Software Development

China-US Software Workshop
September 27-29, 2011
Beijing, China

RUTGERS