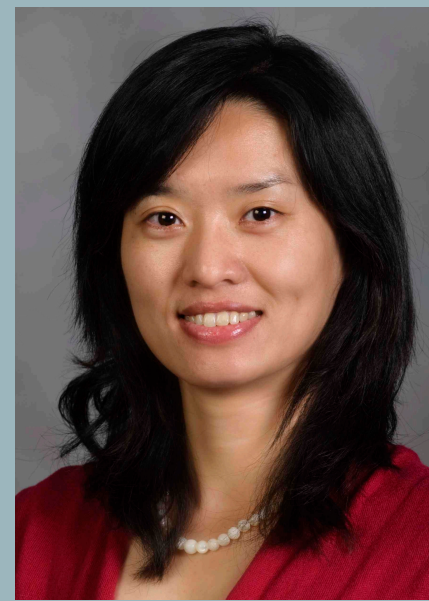


Storytelling Security: Semantic and Structural Causal Analysis

PI: Danfeng (Daphne) Yao, Virginia Tech, Department of Computer Science



Causal analysis of system events and triggering user events for general anomaly detection

Objective: to design a novel host anomaly detection approach for system assurance through analyzing how a system responds to user requests, specifically enforcing causal relations of authenticated events at runtime.

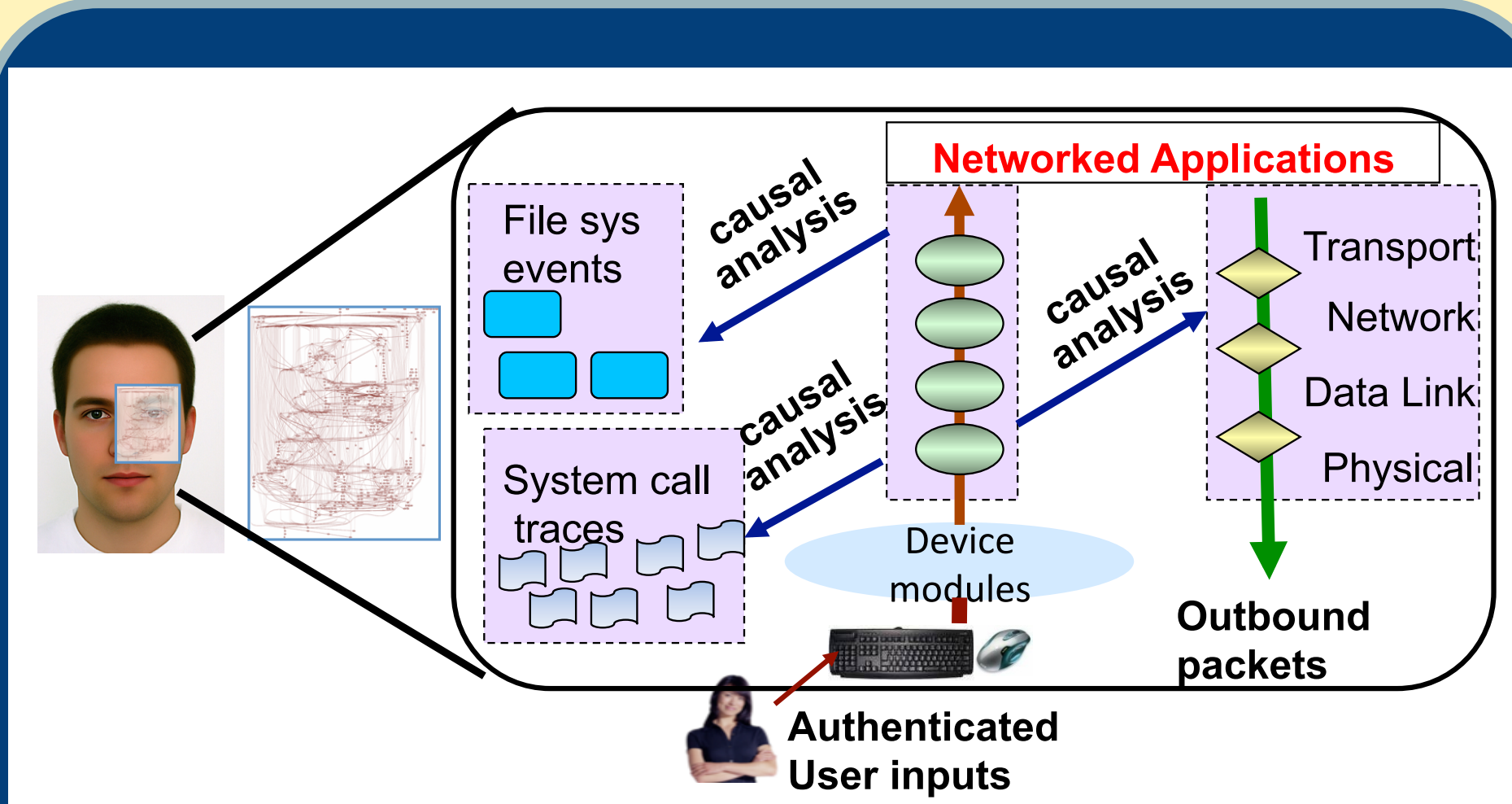
... How to define normality in systems?

... How to detect deviations from normalcy in systems?

Need: structural/semantic-aware data analysis

Insight: a trustworthy system should have predictable responses to user requests

- Challenges:** indirect causality; scalability
Summary of new/general methodologies:
- Cryptographic data authenticity in OS [TDSC'12, ACNS '10, CODASPY'12]
 - Bayesian-based causality learning, rule-based system causality analysis [WSCS'12, NSS'11],
 - User-centric program analysis [MoST'12]



Storytelling security: a security monitoring methodology that provides context, structure, and semantics to interpret events and their causal relations for enforcing normal patterns on a host or a network.

Theory and Practice of User-Centric Anomaly Detection

Data Authenticity in Operating System

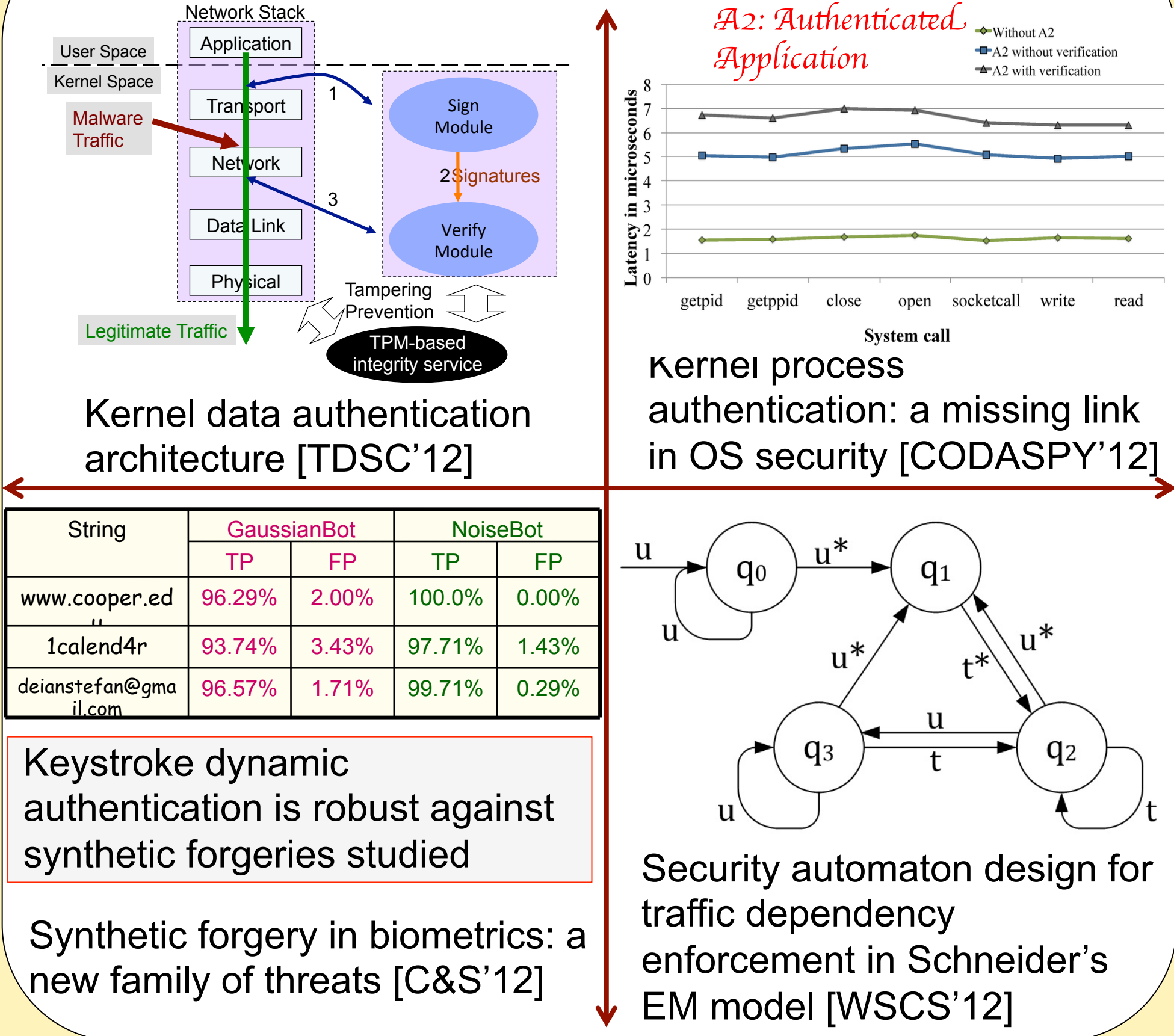
- ✓ Kernel enhancement with crypto mechanisms for kernel data authenticity
- ✓ OS design principles, e.g., cryptographic process authentication, provenance verification

Scalable Causality Learning/Enforcement

- ✓ Causal analysis of system events, learning and enforcement
- ✓ Dependency computation of user, file sys, network, system call events
- ✓ Useful beyond computer security

SYSTEMS AND METHOD FOR MALWARE DETECTION. PCT PATENT FILED. MARCH 2010.

Highlights of Research Results



Selected Publications

- Data Provenance Verification for Secure Hosts. K. Xu, H. Xiong, C. Wu, D. Stefan, and D. Yao. *IEEE Transactions of Dependable and Secure Computing (TDSC)*. 9(2), 173-183. 2012.
- User Intention-Based Traffic Dependence Analysis For Anomaly Detection. H. Zhang, W. Banick, D. Yao and N. Ramakrishnan. In *Proceedings of Workshop on Semantics and Security (WSCS)*. 2012.
- Identifying Native Applications with High Assurance. H. Almohri, D. Yao, and D. Kafura. In *Proceedings of ACM Conference on Data and Application Security and Privacy (CODASPY)*. Feb. 2012.
- Detecting Infection Onset With Behavior-Based Policies. K. Xu, D. Yao, Q. Ma, and A. Crowell. In *Proceedings of the Fifth International Conference on Network and System Security (NSS)*. Sep. 2011.
- Robustness of Keystroke-Dynamics Based Biometrics Against Synthetic Forgeries. D. Stefan, X. Shu, and D. Yao. *Computers & Security*. 31. 109-121. 2012. **(Best Paper Award at CollaborateCom'10)**
- User-Centric Dependence Analysis for Identifying Malicious Mobile Apps. K. O. Elish, D. Yao, and B. G. Ryder. In *Proceedings of the Workshop on Mobile Security Technologies (MoST)*. May 2012.
- A Semantics Aware Approach to Automated Reverse Engineering Unknown Protocols. Y. Wang, X. Yun, M. Z. Shafiq, A. X. Liu, Z. Zhang, L. Wang, D. Yao, Y. Zhang, and L. Guo. In *IEEE International Conference on Network Protocols (ICNP)*. Oct. 2012. **(Best Paper Award)**

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

NSF CAREER: Human-Behavior Driven Malware Detection (03/2010-02/2015)



National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

