System-centric Solutions to Micro-architectural and System-level Side Channels

Yinqian Zhang, Ph.D.
The Ohio State University

Micro-architectural and System-level Side Channels

- Micro-architectural side channels
  - CPU Cache
  - Branch prediction units / function units
  - Translation lookaside buffers
- System-level side channels
  - Operating system statistics
    - Procfs on Linux OS
    - System call return values
  - Resource access pattern
    - Memory page access patterns of SGX enclave programs
    - File access patterns of searchable symmetric encryption
    - Keystroke patterns
  - Timing channels
    - Shared kernel data structure

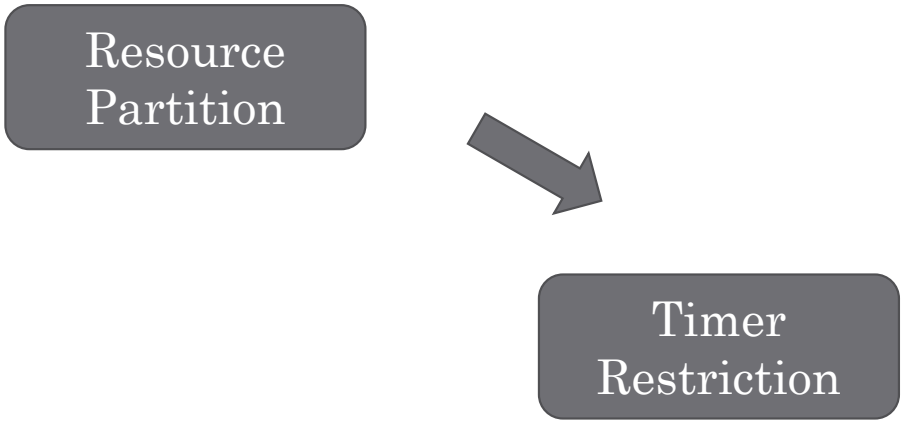
Side channels are broad in scope, but may share common solutions.

Taxonomy of System-centric Side-channel Defenses

Resource Partition

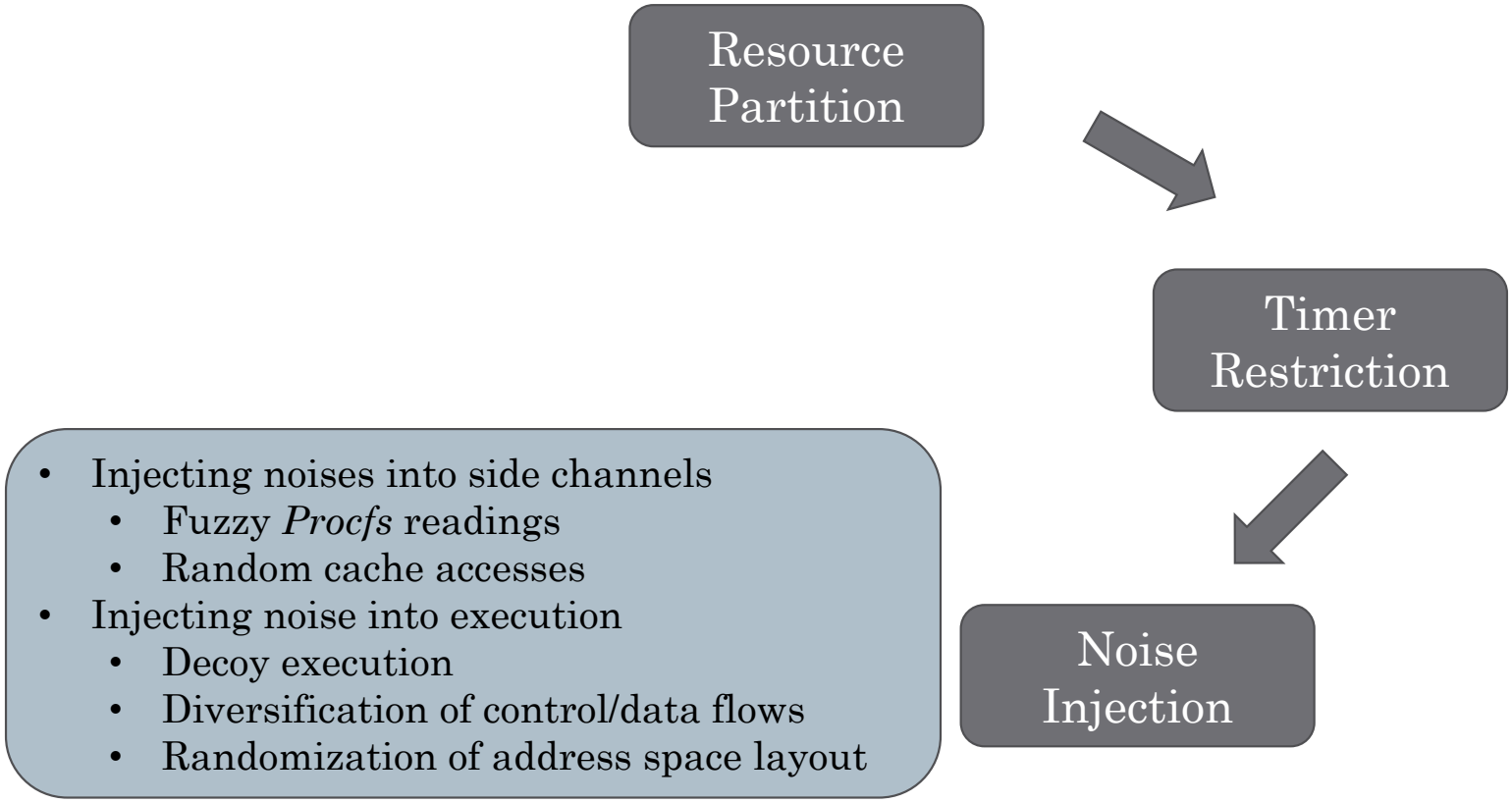
- Spatial partition: e.g., last level cache
  - Partition by set / line
- Temporal partition: e.g., private caches
  - Cleansing at context switch

Taxonomy of System-centric Side-channel Defenses

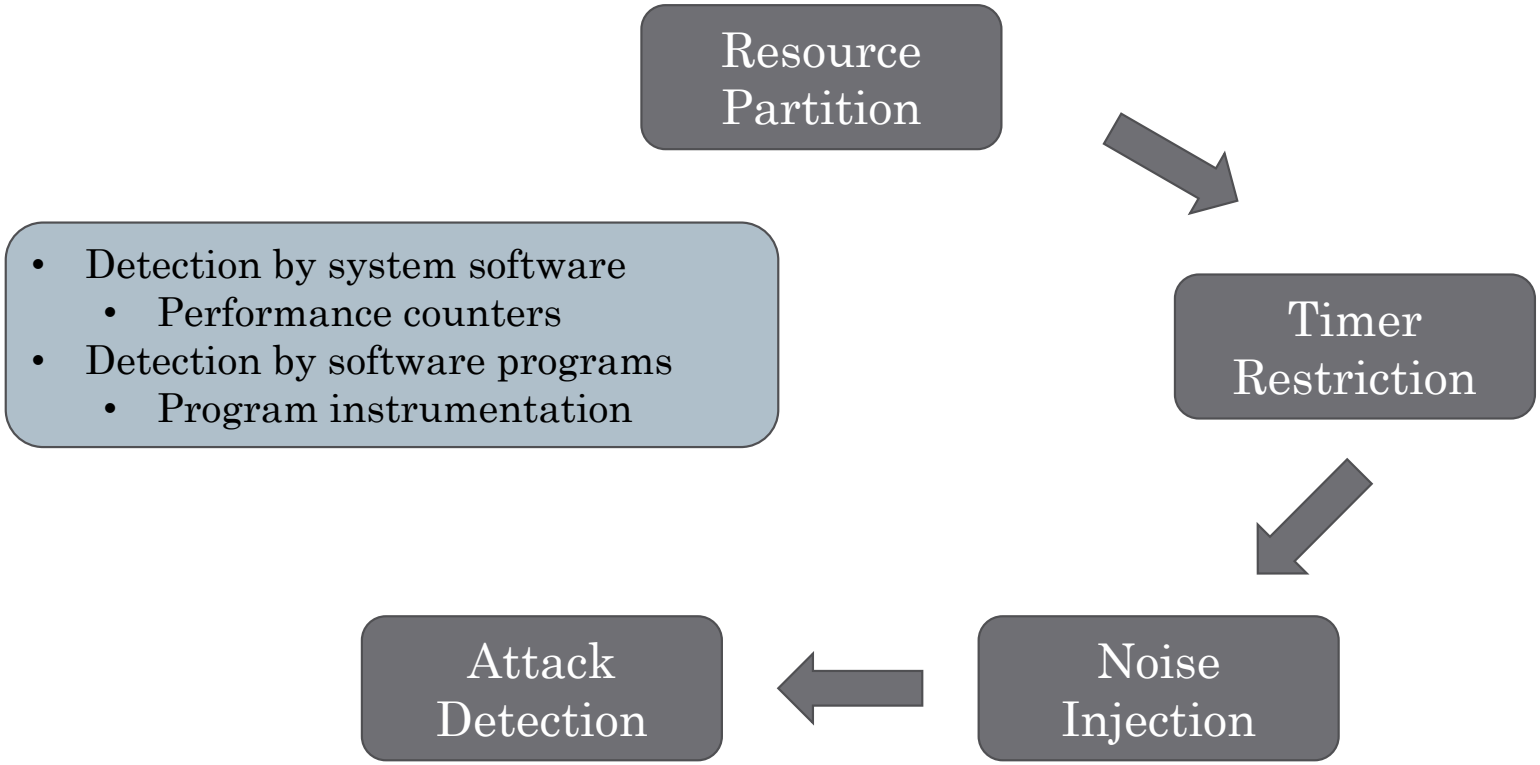


- Public compute clouds and web browsers
  - Fuzzy timers
  - Deterministic execution

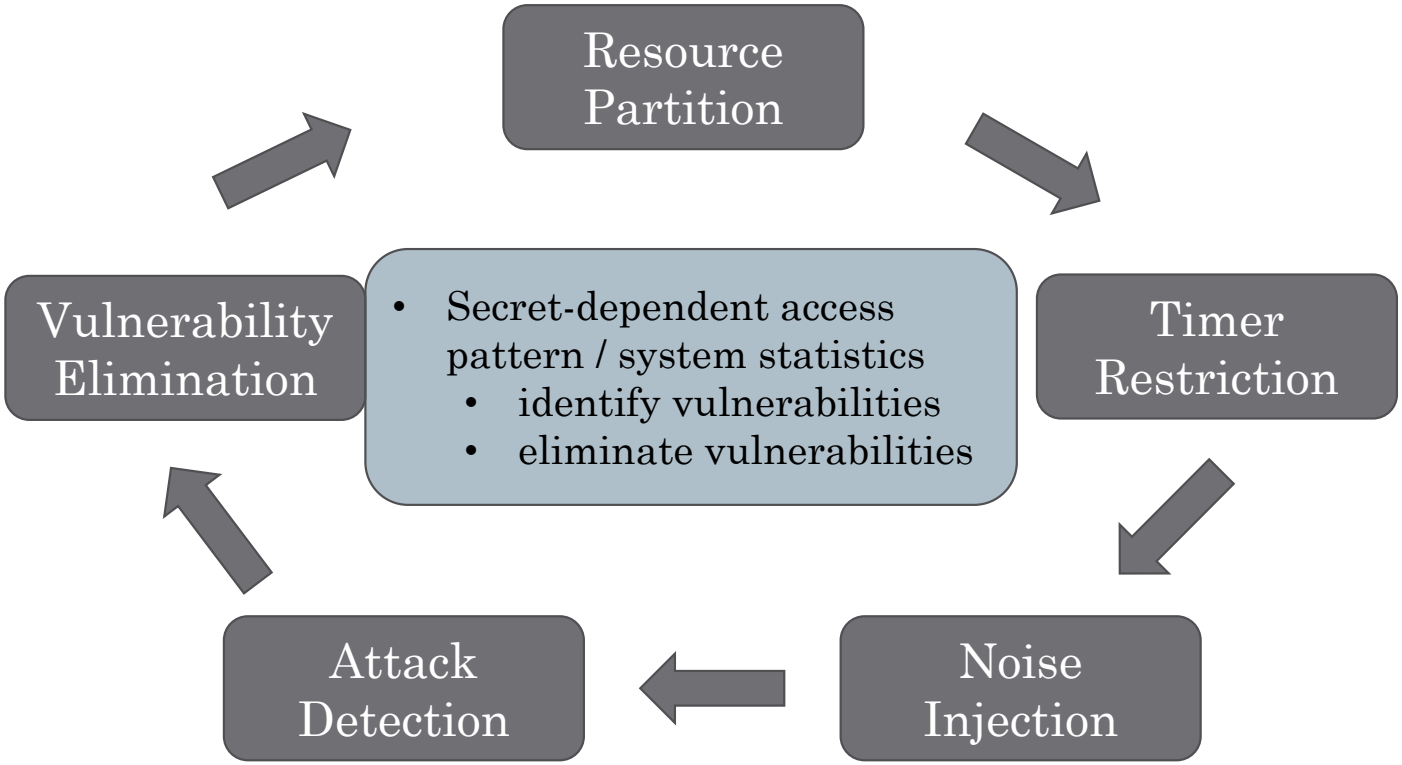
Taxonomy of System-centric Side-channel Defenses



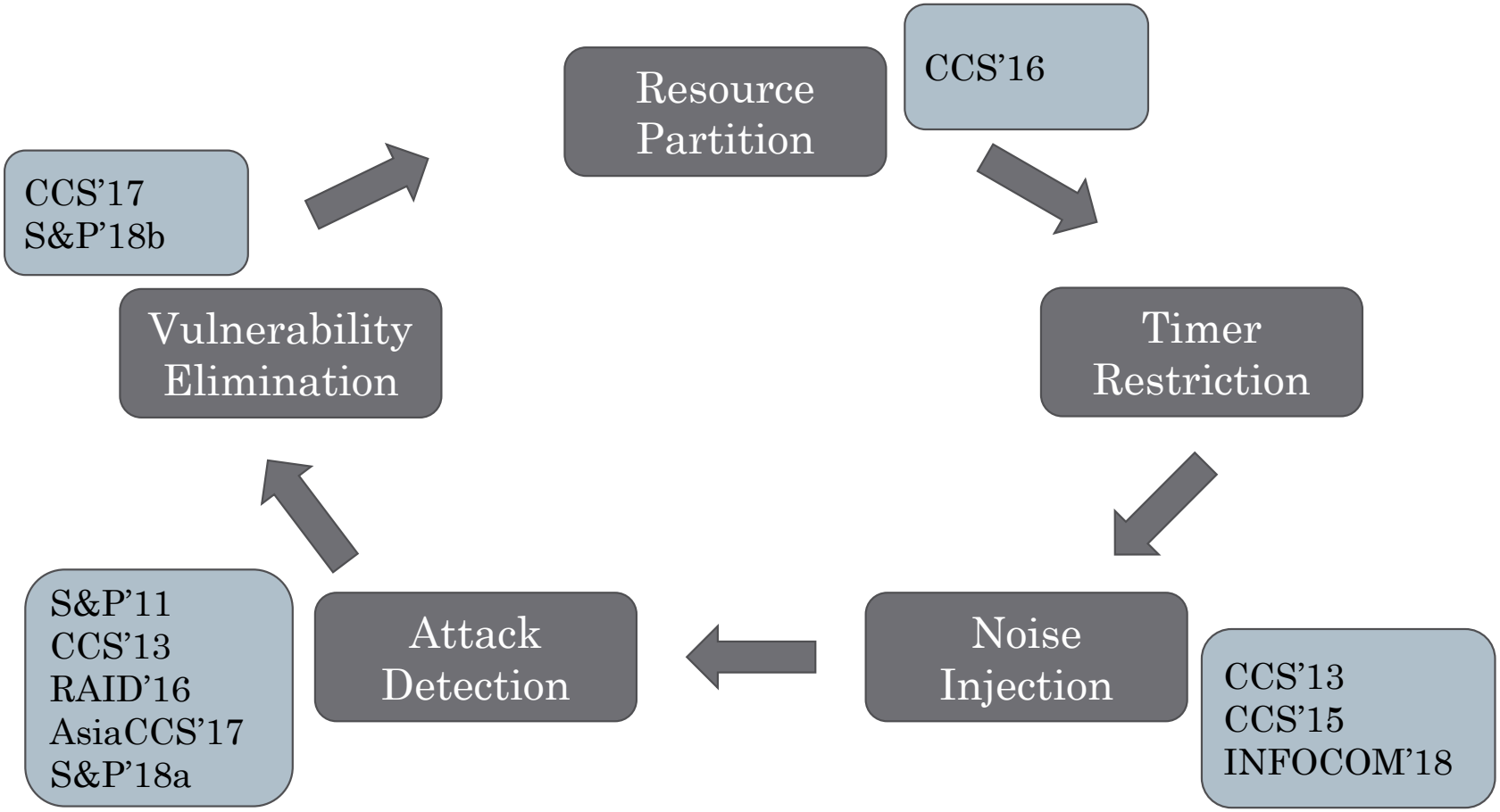
Taxonomy of System-centric Side-channel Defenses



Taxonomy of System-centric Side-channel Defenses



Taxonomy of System-centric Side-channel Defenses



An Exploration of Two Research Ideas

Embedding side-channel attack detection capabilities into program execution

Injecting noise into program execution with statistical privacy guarantees

Embedding Attack Detection Capabilities into Guest Virtual Machines

- *Motivation*:
  - Lack of hypervisor-level protection in public multi-tenant clouds
  - To detect side-channel attack activities from within guest VMs
- Modify guest OS kernels to perform side-channel analysis to detect third-party VM activities

  *(*S&P'11*) HomeAlone: Co-Residency Detection in the Cloud via Side-Channel Analysis.*
  Joint work with Drs. Ari Juels, Alina Oprea, Michael K. Reiter

- Monitor hypervisor context switch to detect L1-cache side-channel attacks

  *(*CCS'13*) Düppel: Retrofitting Commodity Operating Systems to Mitigate Cache Side Channels in the Cloud*
  Joint work with Dr. Michael K. Reiter

Embedding Attack Detection Capabilities into SGX Enclave Programs

- Motivation:
  - In the threat model of Intel SGX, OS is outside of the TCB
  - To detect side-channel attacks conducted by malicious OS
- Methods:
  - Compiler-assisted approach to automatically instrument enclave programs
  - Detect Asynchronous Enclave eXit and Hyper-Thread usage at runtime

(S&P'18) *Racing in Hyperspace: Closing Hyper-Threading Side Channels on SGX with Contrived Data Races*
Joint work between Ohio State University and Indiana University

(AsiaCCS'17) *Detecting Privileged Side-Channel Attacks in Shielded Execution with DEJA VU*
Joint work between Ohio State University and UNC Chapel Hill

Towards Execution Privacy

- Noise injection to mitigate side-channel threats
  - Injecting noise into program execution
  - Injecting noise into side channels
- An execution privacy framework to provably eliminate side channels
  - A side channel is modeled as a sequence of observations *x[1], x[2], …, x[n]*, each of which can be a tuple of multiple pieces of information
  - A randomized mechanism *A(x)* to achieve differential privacy
  - Examples: Linux/Android procfs and symmetric searchable encryption

(CCS'15) *Mitigating Storage Side Channels Using Statistical Privacy Mechanisms*
Joint work between Ohio State University and UNC Chapel Hill

(INFOCOM'18) *Differentially Private Access Patterns for Searchable Symmetric Encryption*
Joint work between Ohio State University and UNC Chapel Hill

Related Work

Category	Publication
Resource partition	Raj, Nathuji, Singh, England. *Resource management for isolation enhanced cloud services*. ACM CCSW'09.
	Kim, Peinado, Mainar-Ruiz. *STEALTHMEM: system-level protection against cache-based side channel attacks in the cloud*, USENIX Security'12
	Varadarajan, Ristenpart, Swift. *Scheduler-based defenses against cross-VM side-channels*. USENIX Security'14.
	Liu, Ge, Yarom, Mckeen, Rozas, Heiser, Lee. *CATalyst: Defeating last- level cache side channel attacks in cloud computing*, HPCA'16. (*)
	Zhou, Reiter, Zhang. *A software approach to defeating side channels in last-level caches*, ACM CCS'16
Noise injection	Zhang and Reiter. *Duppel: retrofitting commodity operating systems to mitigate cache side channels in the cloud*, ACM CCS'13.
	Liu, Harris, Maas, Hicks, Tiwari, Shi. *Ghostrider: A hardware-software system for memory trace oblivious computation*, ASPLOS'15 (*)
	Crane, Homescu, Brunthaler, Larsen, Franz. *Thwarting cache side-channel attacks through dynamic software diversity*, NDSS'15

(*) Hardware-software hybird solutions

Related Work (Con't)

Category	Publication
Noise injection	Rane, Lin, Tiwari. *Raccoon: Closing digital side-channels through obfuscated execution*, USENIX Security'15. Xiao, Reiter, Zhang, *Mitigating Storage Side Channels Using Statistical Privacy Mechanisms,* ACM CCS'15. Chen, Lai, Reiter, Zhang, *Differentially Private Access Patterns for Searchable Symmetric Encryption*, INFOCOM'18
Timer restriction	Aviram, Hu, Ford, Gummadi, *Determinating timing channels in compute clouds*, ACM CCSW'10. Vattikonda, Das, Shacham. *Eliminating fine grained timers in Xen*. ACM CCSW'11. Li, Gao, Reiter. *Stopwatch: A cloud architecture for timing channel mitigation*. ACM TIFS 2014. Kohlbrenner and Shacham, *Trusted browsers for uncertain times*, USENIX Security'16 Cao, Chen, Li, Wu, *Deterministic Browser*, ACM CCS'17.
Attack detection	Demme, Maycock, Schmitz, Tang, Waksman, Sethumadhavan, Stolfo. *On the feasibility of online malware detection with performance counters*, ISCA'13.

Related Work (Con't)

Category	Publication
Attack detection	Zhang, Zhang, Lee. *Cloudradar: A real-time side-channel attack detection system in clouds*, RAID'16.
	Shih, Lee, Kim, Peinado. *T-sgx: Eradicating controlled-channel attacks against enclave programs,* NDSS'17.
	Gruss, Schuster, Ohrimenko, Haller, Lettner, Costa. Strong and efficient cache side-channel protection using hardware transactional memory, USENIX Security'17
	Chen, Zhang, Reiter, Zhang. *Detecting privileged side-channel attacks in shielded execution with deja vu*, AsiaCCS'17
	Chen, Wang, Chen, Chen, Zhang, Wang, Lai, Lin, *Racing in Hyperspace: Closing Hyper-Threading Side Channels on SGX with Contrived Data Races*, IEEE S&P'18.
Vulnerability elimination	Molnar, Piotrowski, Schultz, Wagner. The program counter security model: automatic detection and removal of control-flow side channel attacks, ICISC'05.
	Coppens, Verbauwhede, Bosschere, Sutter. *Practical mitigations for timing-based side-channel attacks on modern x86 processors*. IEEE S&P'09.
	Doychev, Feld, Köpf, Mauborgne. CacheAudit: A tool for the static analysis of cache side channels, USENIX Security'13.

Related Work (Con't)

Category	Publication
Vulnerability elimination	Wang, Wang, Liu, Zhang, Wu. *Cached: Identifying cache-based timing channels in production software*, USENIX Security'17 Xiao, Li, Chen, Zhang. *Stacco: Differentially analyzing side-channel traces for detecting SSL/TLS vulnerabilities in secure enclaves*, ACM CCS'17 Zhou, Qian, Reiter, Zhang, *Static Evaluation of Noninterference Using Approximate Model Counting,* IEEE S&P'18

Questions?

yinqian@cse.ohio-state.edu