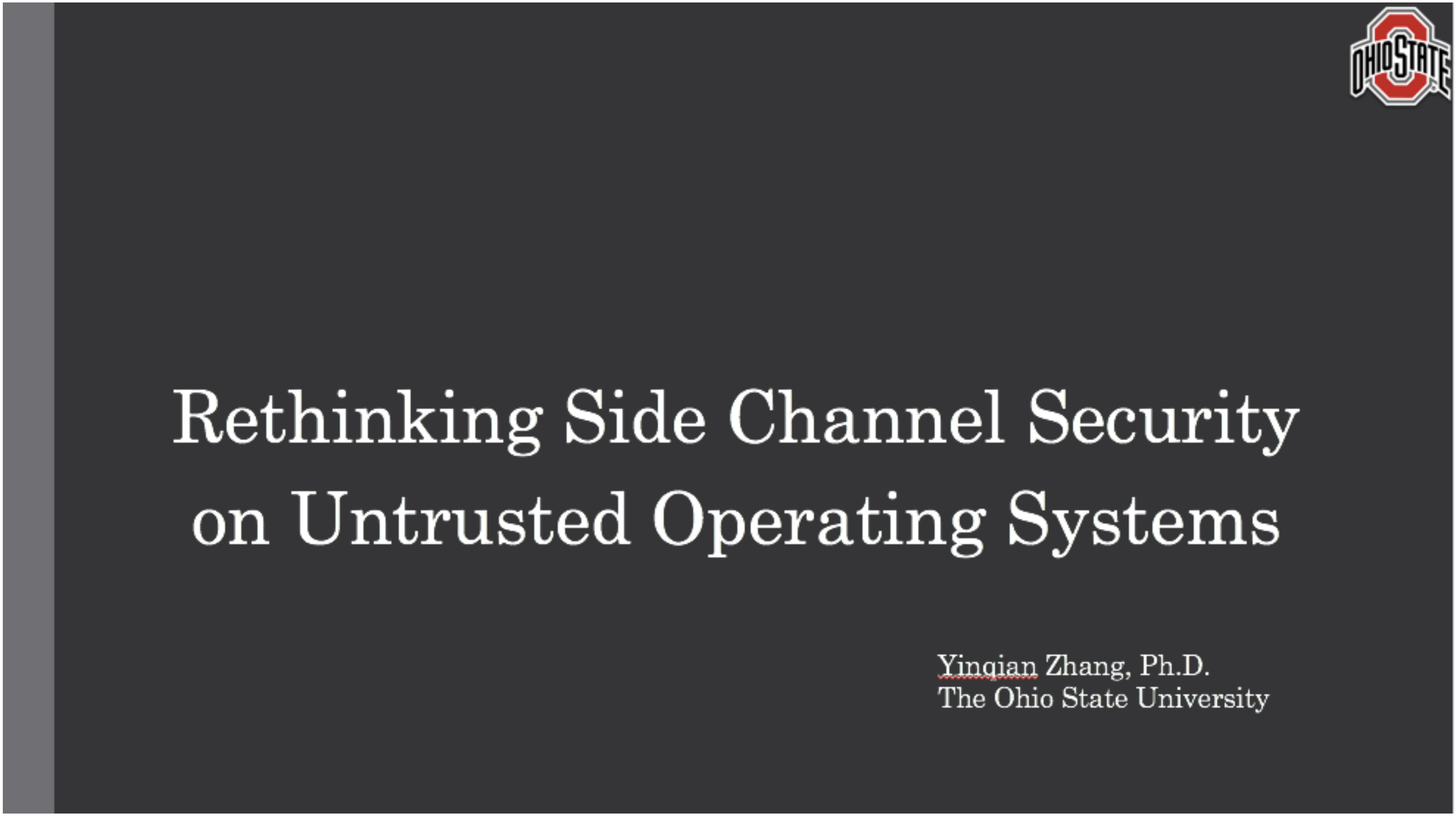
Rethinking Side Channel Security on Untrusted Operating Systems

YINQIAN ZHANG, OHIO STATE UNIVERSITY

Cybersecurity Research Acceleration Workshop and Showcase, Indianapolis, IN
October 11, 2017



Rethinking Side Channel Security on Untrusted Operating Systems

Yinqian Zhang, Ph.D.
The Ohio State University

CRII: SaTC: Rethinking Side Channel Security on Untrusted Operating Systems

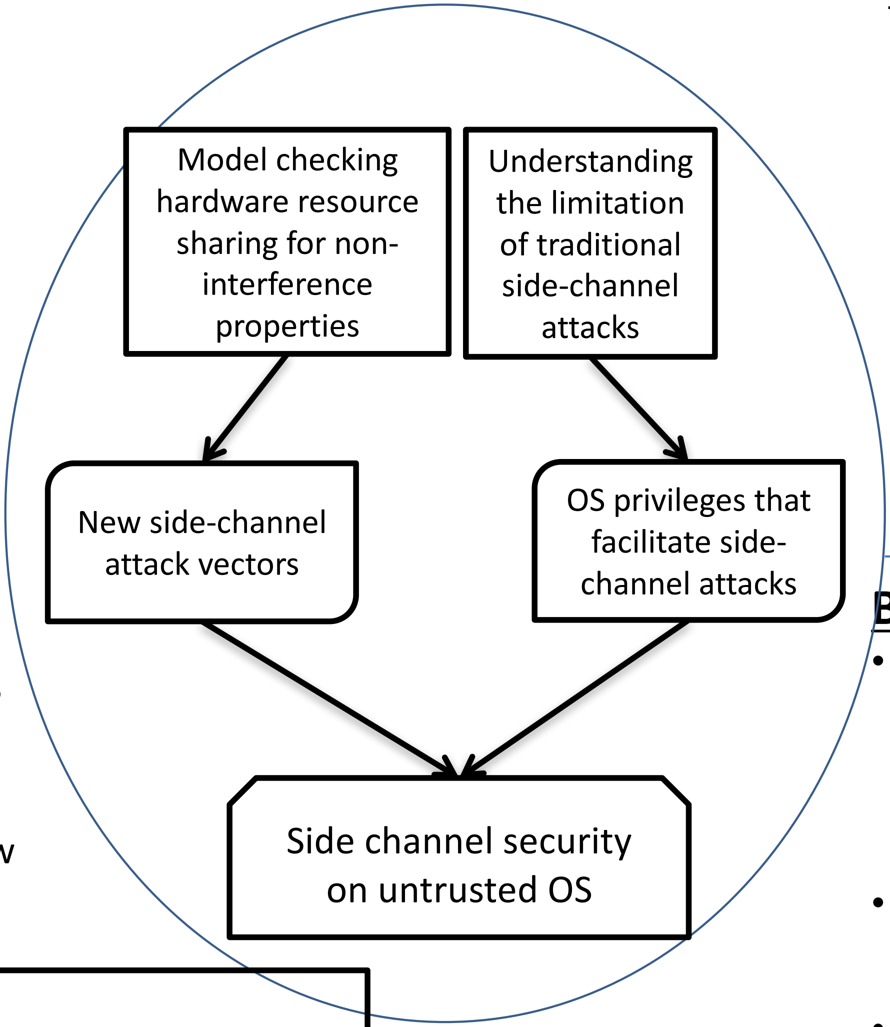
The Ohio State University

Challenge:

- Intel Software Guard eXtension (SGX) promises the confidentiality of software programs shielded in enclaves even when the operating system is untrusted
- Unfortunately, no systematic study of side-channel threats against the shielded execution on untrusted operating systems

Solution:

- Systematically investigating OS privileges that facilitate side-channel attacks
- Model checking to identify new side-channel attack vectors



Model checking hardware resource sharing for non-interference properties

Understanding the limitation of traditional side-channel attacks

New side-channel attack vectors

OS privileges that facilitate side-channel attacks

Side channel security on untrusted OS

Award # 1566444
The Ohio State University
Contact: Prof. Yinqian Zhang
(yinqian@cse.ohio-state.edu)

Scientific Impact:

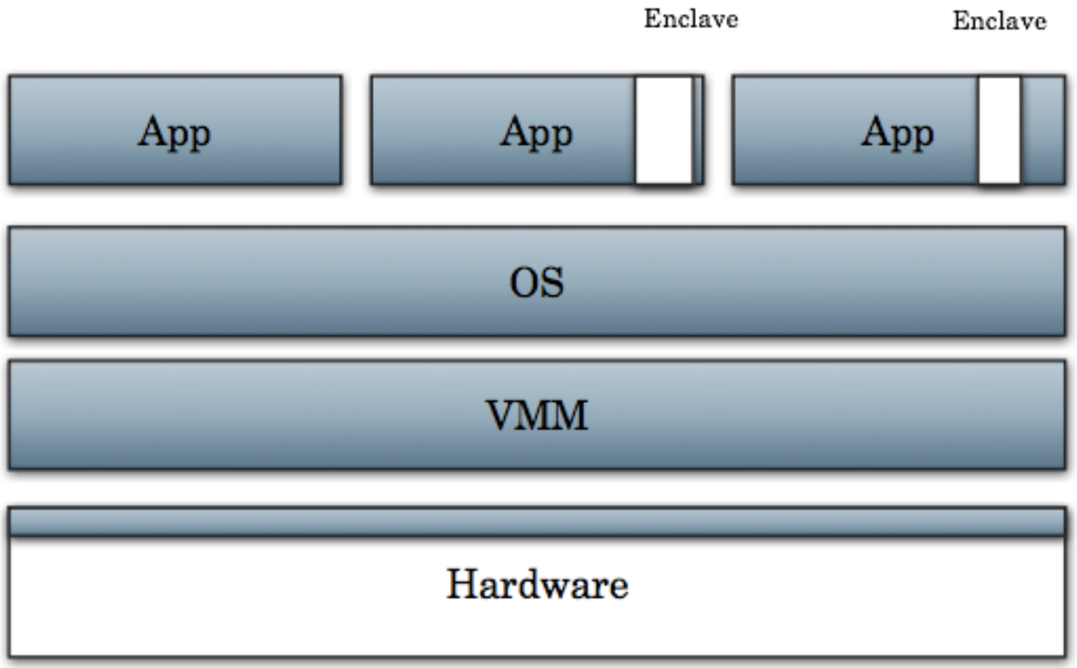
- Advancing the state-of-the-art of side channel studies by exploiting model-checking techniques to automatically identify information leakage through shared hardware resources
- Systematic understanding of side-channel security against shielded execution on untrusted operating systems

Broader Impact:

- Knowledge of side-channel threats will be disseminated to industry vendors, including both SGX hardware manufacturers and software developers
- Introduction of side channel security into undergraduate security courses
- Involvement of underrepresented minority students in security research

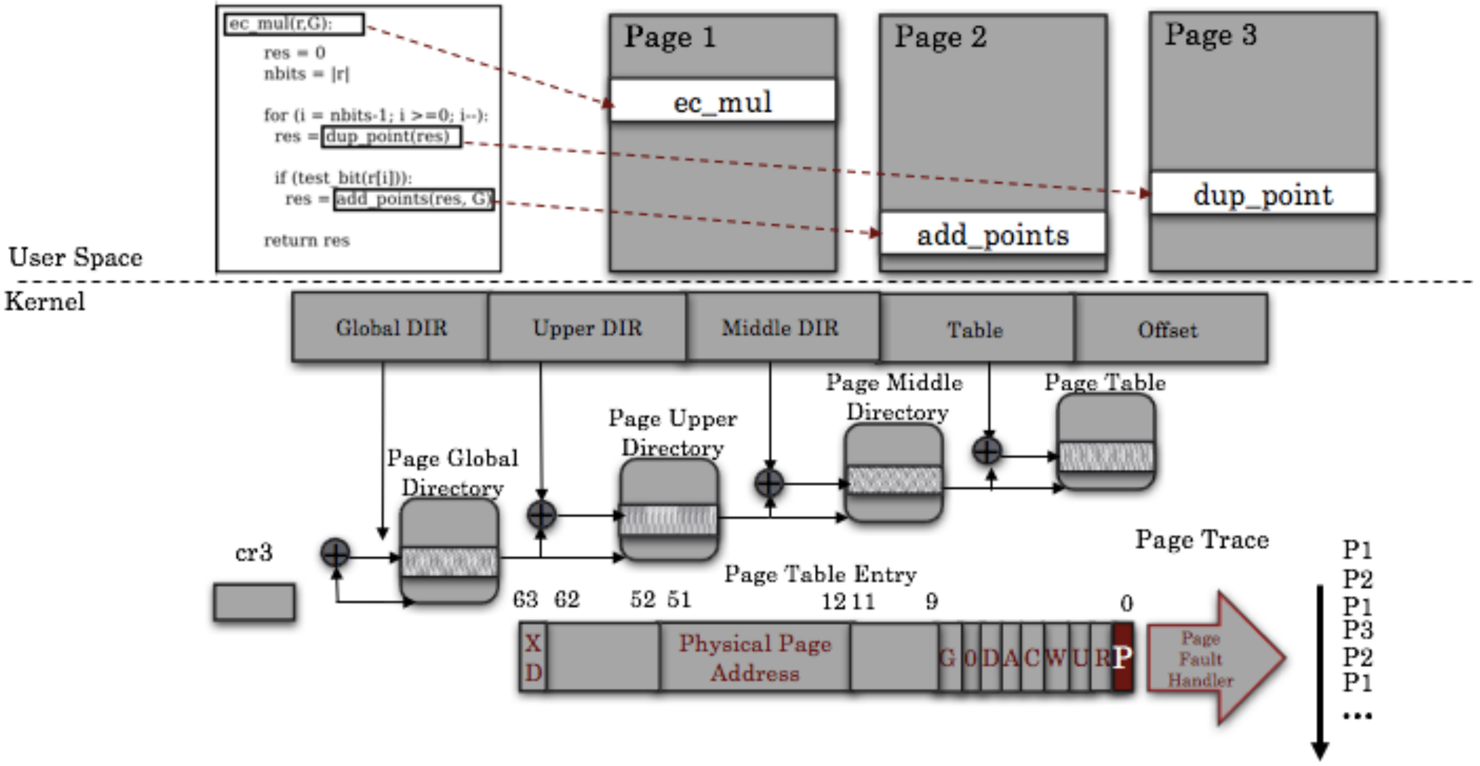
Intel Software Guard Extensions (SGX)

- Intel SGX provides shielded execution environments to security-critical applications
- Secret data and code can be protected even though the operating system is untrusted/compromised



SGX Threat Model

Side-Channel Attacks against SGX Enclaves



```
ec_mul(r,G):
    res = 0
    nbits = |r|

    for (i = nbits-1; i >=0; i--):
      res = dup_point(res)

      if (test_bit(r[i])):
        res = add_points(res, G)

    return res
```

Research Goals

- Advance the state-of-the-art research on side channel security: automatically identify information leakage through shared resources.
- Evaluate the severity of side-channel attacks by privileged attackers: higher fidelity, efficiency, and robustness.
- Conduct a preliminary exploration of potential research directions towards effective mitigation of privileged side channel attacks.

Current Results (2016.05 – 2017.10)

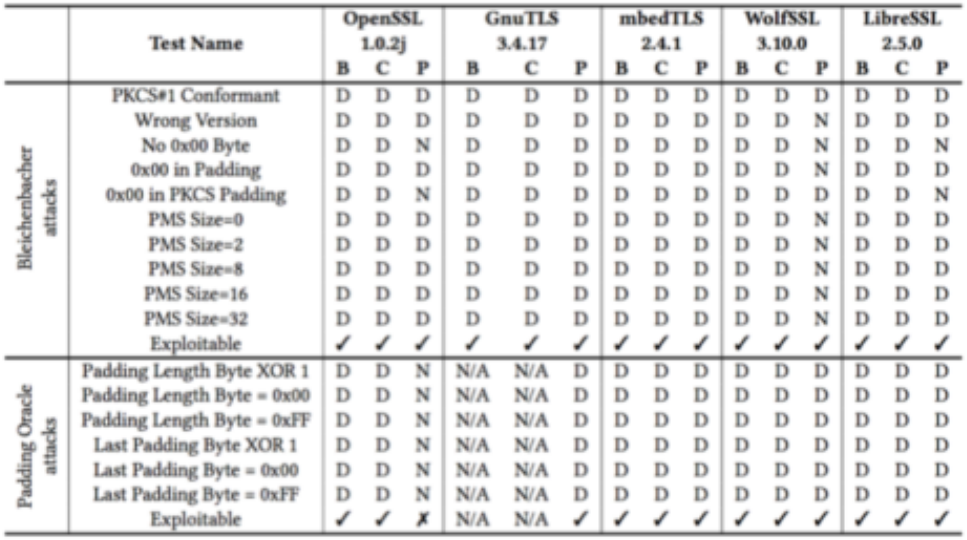
- Understanding side-channel hazards of Intel SGX
  - Memory side-channel attack surfaces (CCS'17)
- Detecting side-channel vulnerabilities in enclave programs
  - Sensitive control-flow vulnerabilities in SSL/TLS (CCS'17)
- Compiler-assisted runtime defenses
  - Timed execution for detecting side-channel attacks at runtime (AsiaCCS'17)

Memory Side-Channel Attack Surfaces

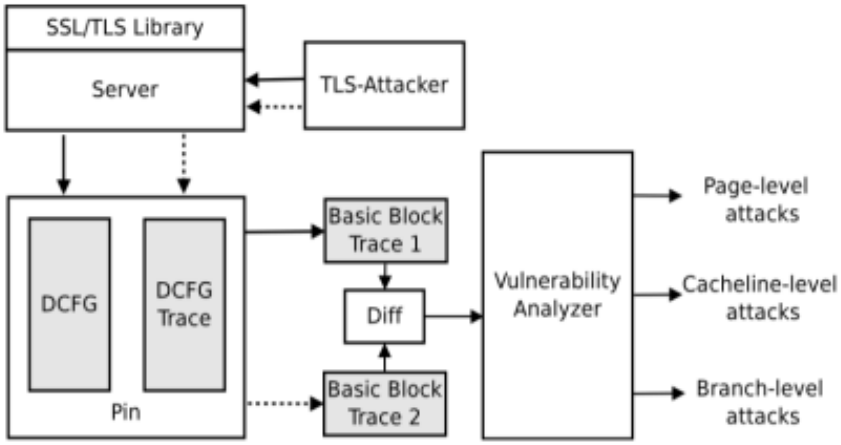
- Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX (CCS'17)
  - Collaboration among Indiana University, OSU, & UIUC
- A systematic study of memory side channels on SGX
  - Address translation caches
  - Page tables
  - Cache & memory hierarchy
- New attacks:
  - Sneaky page monitoring (SPM) attacks
  - Cache-DRAM attacks

Detecting Vulnerabilities in Enclave Programs

- Stacco: Differentially Analyzing Side-Channel Traces for Detecting SSL/TLS Vulnerabilities in Secure Enclaves (CCS'17)
- SSL/TLS libraries inside SGX enclaves are subject to man-in-the-kernel attacks
  - CBC padding oracle
  - Bleichenbacher attack



	Test Name	OpenSSL 1.0.2j			GnuTLS 3.4.17			mbedTLS 2.4.1			WolfSSL 3.10.0			LibreSSL 2.5.0		
		B	C	P	B	C	P	B	C	P	B	C	P	B	C	P
Bleichenbacher attacks	PKCS#1 Conformant	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D
	Wrong Version	D	D	D	D	D	D	D	D	D	D	D	N	D	D	D
	No 0x00 Byte	D	D	N	D	D	D	D	D	D	D	D	N	D	D	N
	0x00 in Padding	D	D	D	D	D	D	D	D	D	D	D	N	D	D	D
	0x00 in PKCS Padding	D	D	N	D	D	D	D	D	D	D	D	D	D	D	N
	PMS Size=0	D	D	D	D	D	D	D	D	D	D	D	N	D	D	D
	PMS Size=2	D	D	D	D	D	D	D	D	D	D	D	N	D	D	D
	PMS Size=8	D	D	D	D	D	D	D	D	D	D	D	N	D	D	D
	PMS Size=16	D	D	D	D	D	D	D	D	D	D	D	N	D	D	D
	PMS Size=32	D	D	D	D	D	D	D	D	D	D	D	N	D	D	D
	Exploitable	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Padding Oracle attacks	Padding Length Byte XOR 1	D	D	N	N/A	N/A	D	D	D	D	D	D	D	D	D	D
	Padding Length Byte = 0x00	D	D	N	N/A	N/A	D	D	D	D	D	D	D	D	D	D
	Padding Length Byte = 0xFF	D	D	N	N/A	N/A	D	D	D	D	D	D	D	D	D	D
	Last Padding Byte XOR 1	D	D	N	N/A	N/A	D	D	D	D	D	D	D	D	D	D
	Last Padding Byte = 0x00	D	D	N	N/A	N/A	D	D	D	D	D	D	D	D	D	D
	Last Padding Byte = 0xFF	D	D	N	N/A	N/A	D	D	D	D	D	D	D	D	D	D
	Exploitable	✓	✓	✗	N/A	N/A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓



SSL/TLS Library

Server

TLS-Attacker

DCFG

DCFG Trace

Pin

Basic Block Trace 1

Diff

Basic Block Trace 2

Vulnerability Analyzer

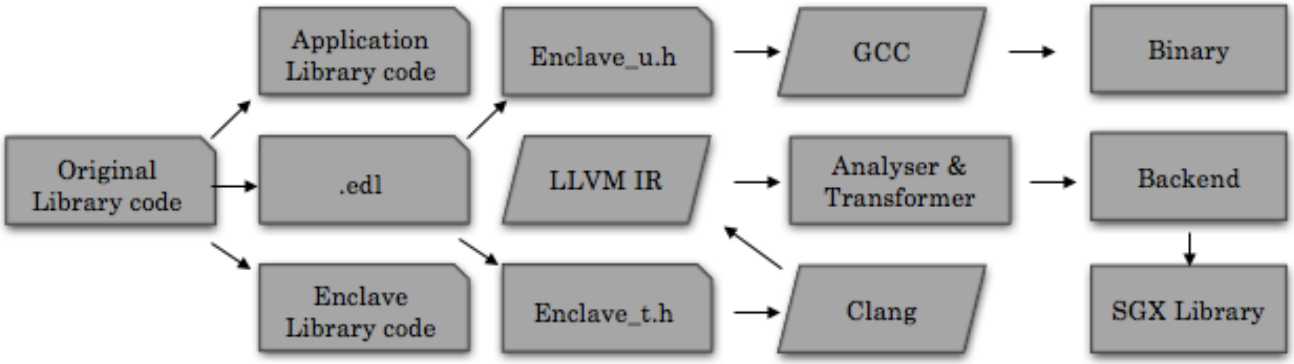
Page-level attacks

Cacheline-level attacks

Branch-level attacks

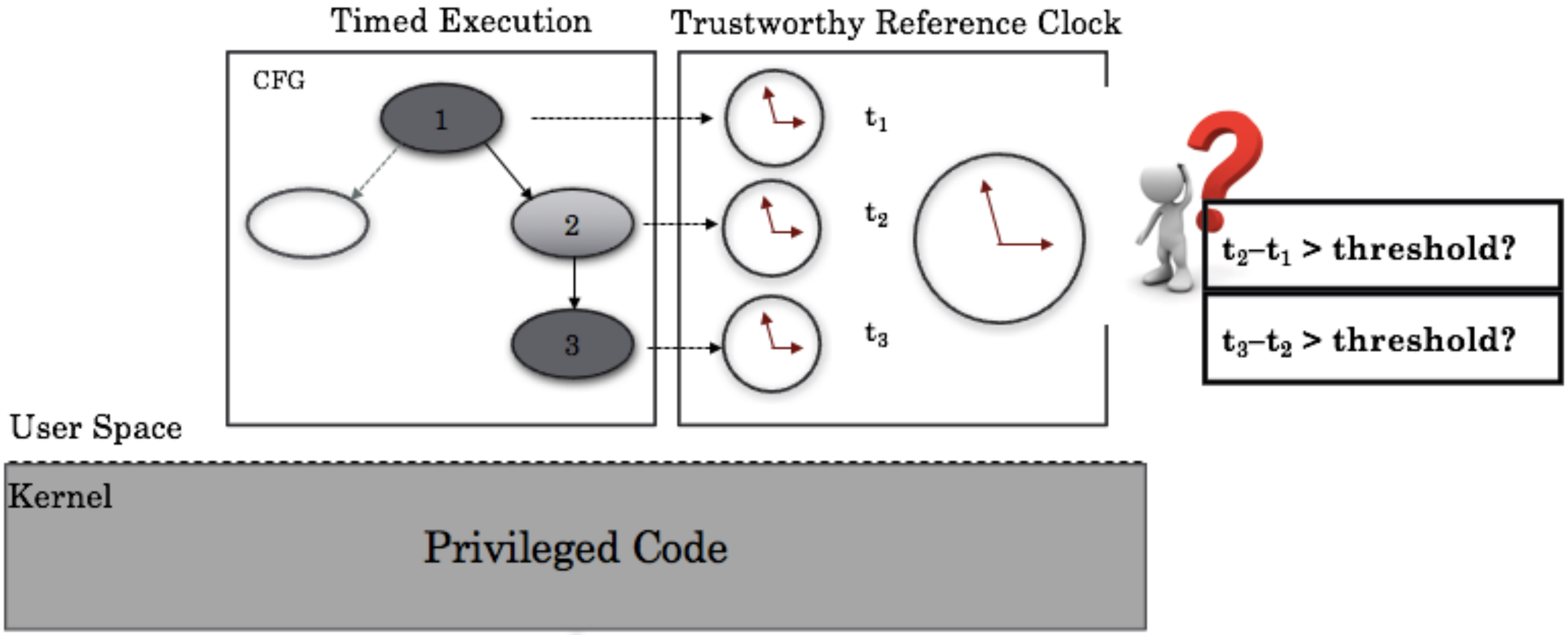
Attack Detection in SGX Enclaves

- Detecting Privileged Side-Channel Attacks in Shielded Execution with Déja Vu (AsiaCCS'17)
  - Collaboration between OSU and UNC
- Key insight
  - Exception-based attacks and interrupt-based attacks yield large number of AEXs
  - Shielded execution will be slowed down significantly when under attack
- Déjà Vu: a software framework to detect privileged side-channel attacks by measuring program execution time



Attack Detection in SGX Enclaves

- Detecting Privileged Side-Channel Attacks in Shielded Execution with Déja Vu (AsiaCCS'17)
  - Collaboration between OSU and UNC



Questions?

yinqian@cse.ohio-state.edu