SGXELIDE: Enabling Enclave Code Secrecy via Self-Modification

#### **Erick Bauman**<sup>1</sup>, Huibo Wang<sup>1</sup>, Mingwei Zhang<sup>2</sup>, Zhiqiang Lin<sup>1,3</sup>

<sup>1</sup>University of Texas at Dallas <sup>2</sup>Intel Labs <sup>3</sup>The Ohio State University

CGO 2018

《曰》 《聞》 《臣》 《臣》 三臣 …

Introduction 000000	Background and Overview	Design and Implementation	Evaluation	Conclusion
Intel SG>	K			



0000	00

Background and Overview

esign and Implementation

Evaluation

Conclusion

# Intel SGX



#### Intel SGX

• Provides secure enclaves

0000	00

Background and Overview

Design and Implementation

Evaluation

Conclusion

# Intel SGX



#### Intel SGX

- Provides secure enclaves
- Memory regions isolated from all other code

0000	00

Background and Overview

Design and Implementation

Evaluation

Conclusion

# Intel SGX



#### Intel SGX

- Provides secure enclaves
- Memory regions isolated from all other code
- Cannot be accessed by OS or hypervisor

Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion
Intel SC	ĴΧ			



Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion
Intel SG	Х			



Introduction 000000	Background and Overview	Design and I	mplementation	Evaluation 0000	Conclusion 000
Intel SG	<				
			Client Applicatior	1	

Disk	
Enclave	
Code	Data

	Background and Overview	Design and Implementation	Evaluation	Conclusion 000
Intel SC	ΞX			



Client			
Application	on		
Enclave			
Code	Data		
Diak			
DISK			
Enclave			
Code	Data		

Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion
Intel SG	×			
	Attest	Client Application Enclave Code	Data	

Introduction 000000	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion 000
Intel SG	×			
	Attest Attest	Client Applicatio Enclave Code	n Data	

Introduction 000000	Background and Overview	Design and Imple	ementation	Evaluation 0000	Conclusion
Intel SG>	<				
	Attest		lient Application Enclave Code	ata 🔒	
Da Co	ata Integrity ode Integrity		Disk Enclave Code Da	ata	

Introduction 000000	Background and Overview	Design and	mplementation	Evaluation	Conclusion
Intel SG>	<				



Introduction 000000	Background and Overview	Design and Ir	nplementation	Evaluation 0000	Conclusion
Intel SG2	X				
	Attest Secret Data		Client Application Enclave	ata 🎧 Secre Data	t

Data Integrity Code Integrity Data Confidentiality

Enclave				
Code	Data Gecret			
	•			
Disk				
Enclave				
Code	Data			

Intel SGX	Introduction	Background and Overview	Design and I	mplementation	Evaluation 0000	Conclusion
	Intel SG	<				
Attest Client Application Enclave		Attest	2	Client Application Enclave		

Code

Data Integrity Code Integrity Data Confidentiality

	Code 🤒	Data	a 🔒	Secret Data	
	Disk				
	Enclave				
	Code	Data	a		

Introduction	Background and Overview	Design and Ir	nplementation	Evaluation 0000	Conclusion 000
Intel SC	GX				
	Attest	?	Client Application Enclave Code	ta P Seci Data	ret
4	Data Integrity Code Integrity Data Confidentiality		Disk Enclave Code Da	ta	

Code Confidentiality

Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion
Intel SG	X			

"The enclave file can be disassembled, so the algorithms used by the enclave developer will not remain secret." -SGX SDK Manual

Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion
SGXELIC	)E			

#### Definition

Elide: To leave out or omit

Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion
Challeng	es			

#### • Enclaves must be signed and unmodified until initialization

Introduction	Background and Overview ●00000	Design and Implementation	Evaluation 0000	Conclusion
Challeng	ges			

- Enclaves must be signed and unmodified until initialization
- The entire enclave cannot be encrypted

Introduction	Background and Overview ●0000	Design and Implementation	Evaluation	Conclusion
Challend	pes			

- Enclaves must be signed and unmodified until initialization
- The entire enclave cannot be encrypted
- Any secrets cannot be stored in the enclave

000000	●0000	0000	0000	000
Challen	nes			

- Enclaves must be signed and unmodified until initialization
- The entire enclave cannot be encrypted
- Any secrets cannot be stored in the enclave
- There should be minimal toolchain changes

Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion
Main Ide	ea			

#### Redact (or sanitize) secrets and restore at runtime

Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion
Blacklist	vs. Whitelist			

Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion
Blacklist	vs. Whitelist			

• User specifies secrets (e.g. annotations)

Introduction	Background and Overview oo●oo	Design and Implementation	Evaluation 0000	Conclusion
Blacklis	t vs. Whitelist			

- User specifies secrets (e.g. annotations)
- Minimizes code that must be encrypted

Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion
Blacklist	vs. Whitelist			

- User specifies secrets (e.g. annotations)
- Minimizes code that must be encrypted
- Burden of annotating secrets on developer

Introduction	Background and Overview oo●oo	Design and Implementation	Evaluation 0000	Conclusion

- User specifies secrets (e.g. annotations)
- Minimizes code that must be encrypted
- Burden of annotating secrets on developer
- Risk of mistakes

Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion

#### Blacklist

- User specifies secrets (e.g. annotations)
- Minimizes code that must be encrypted
- Burden of annotating secrets on developer
- Risk of mistakes

Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion

#### Blacklist

- User specifies secrets (e.g. annotations)
- Minimizes code that must be encrypted
- Burden of annotating secrets on developer
- Risk of mistakes

#### Whitelist

Only specify code that must not be redacted

Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion

#### Blacklist

- User specifies secrets (e.g. annotations)
- Minimizes code that must be encrypted
- Burden of annotating secrets on developer
- Risk of mistakes

- Only specify code that must not be redacted
- Applicable to any enclave

Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion
<b>DI</b> 111 1				

#### Blacklist

- User specifies secrets (e.g. annotations)
- Minimizes code that must be encrypted
- Burden of annotating secrets on developer
- Risk of mistakes

- Only specify code that must not be redacted
- Applicable to any enclave
- No need for developer to mark secrets

Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion
<b>DI</b> 111 1				

#### Blacklist

- User specifies secrets (e.g. annotations)
- Minimizes code that must be encrypted
- Burden of annotating secrets on developer
- Risk of mistakes

- Only specify code that must not be redacted
- Applicable to any enclave
- No need for developer to mark secrets
- More code must be encrypted

Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion	
Our Solution					

#### • Sign sanitized enclave and restore secrets after initializing

Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion			
Our Solution							

- Sign sanitized enclave and restore secrets after initializing
- Encrypt all nonessential functions

000000			evaluation 0000	000			
Our Solution							

- Sign sanitized enclave and restore secrets after initializing
- Encrypt all nonessential functions
- Use remote attestation
| Introduction<br>000000 | Background and Overview | Design and Implementation | Evaluation<br>0000 | Conclusion<br>000 |
|------------------------|-------------------------|---------------------------|--------------------|-------------------|
| Our Sol                | ution                   |                           |                    |                   |

- Sign sanitized enclave and restore secrets after initializing
- Encrypt all nonessential functions
- Use remote attestation
- Use both local and remote storage

SovEu				
Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion



Introduction	Background and Overview	Design and Implementation ●000	Evaluation 0000

# Remote vs. Local Data





< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □

Introduction
000000

Background and Overview

Design and Implementation

Evaluation

Conclusion



Introduction
000000

Background and Overview

Design and Implementation

Evaluation

Conclusion







Introduction

Background and Overview

Design and Implementation

Evaluatior

Conclusion





Introduction

Background and Overview

Design and Implementation

Evaluation

Conclusion



Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion



Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion
<u> </u>				



Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion
<u> </u>				



Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion
		_		



Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion
		_		



Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion
		_		



Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion



Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion



Introduction Background and Overview Design and Implementation Evaluation Conclusion

# SGXELIDE Design - Local Data



◆ロ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

## SGXELIDE Design - Local Data



◆ロ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

# SGXELIDE Design - Local Data



## SGXELIDE Design - Local Data



# SGXELIDE Design - Local Data



## SGXELIDE Design - Local Data



<ロト < 団 ト < 巨 ト < 巨 ト 三 の Q () 16/23

## SGXELIDE Design - Local Data



# SGXELIDE Design - Local Data



Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion
Benchma	arks			

	Original	LOC w	// SGX	LOC w	/ SgxElide	TC	TC	Sanitized	Sanitized
Benchmarks	LOC	UC	TC	UC	TC	Functions	Bytes	Functions	Bytes
AES	802	472	427	522	540	185	75999	15	3840
DES	473	463	372	513	485	179	75455	9	3296
Sha1	315	423	251	473	364	179	73791	9	1632
Shas	2417	1529	1240	1579	1353	224	80127	54	7968
2048	413	551	192	601	305	208	76351	38	4448
Biniax	3523	3582	193	3632	306	208	76351	38	4448
Crackme	48	316	93	366	206	182	73711	12	1536

Introduction
000000

Background and Overview

Design and Implementation

Evaluation

Conclusion

### Sanitization/Restoration Time

		Remote Data			Local Data			
	Sanitize	Stand.	Restore	Stand.	Sanitize	Stand.	Restore	Stand.
Benchmarks	Time	Dev.	Time	Dev.	Time	Dev.	Time	Dev.
AES	0.09	0.01	4.06	0.54	0.15	0.01	3.76	0.20
DES	0.09	0.01	3.99	0.52	0.14	0.01	3.97	0.75
Sha1	0.09	0.01	3.67	0.35	0.14	0.01	3.97	0.98
Shas	0.09	0.00	4.06	0.53	0.15	0.01	4.26	0.97
2048	0.09	0.01	3.78	0.52	0.15	0.01	3.73	0.28
Biniax	0.09	0.00	4.44	0.61	0.15	0.01	4.32	0.92
Crackme	0.09	0.01	3.53	0.28	0.15	0.00	3.54	0.78

Introduction	Background and Overview	Design and Implementation		Conclusion
			0000	

# SGXELIDE Overhead - Remote Data



Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion

# SGXELIDE Overhead - Local Data



Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion
Discus	sions			

Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion •oo
Discussi	ons			

• How do we defend against malicious enclaves?

000000	00000	0000	0000	•00				
	Discussions							

- How do we defend against malicious enclaves?
- How do we protect vulnerable enclaves?

	000000	00000	0000	0000	000
Design and implementation Evaluation Outputs of	000000	00000	0000	0000	000

- How do we defend against malicious enclaves?
- How do we protect vulnerable enclaves?
- How does this influence side-channel attacks?

Discussio	ane			
Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion ●○○

- How do we defend against malicious enclaves?
- How do we protect vulnerable enclaves?
- How does this influence side-channel attacks?

### Limitations and future work

Discuss	ione			
Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion

- How do we defend against malicious enclaves?
- How do we protect vulnerable enclaves?
- How does this influence side-channel attacks?

#### Limitations and future work

Framework not completely transparent

Dicouco	iono			
Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion

- How do we defend against malicious enclaves?
- How do we protect vulnerable enclaves?
- How does this influence side-channel attacks?

#### Limitations and future work

- Framework not completely transparent
- Would be useful to test SGXELIDE with large-scale software

Dicouco	iono			
Introduction	Background and Overview	Design and Implementation	Evaluation	Conclusion

- How do we defend against malicious enclaves?
- How do we protect vulnerable enclaves?
- How does this influence side-channel attacks?

#### Limitations and future work

- Framework not completely transparent
- Would be useful to test SGXELIDE with large-scale software
- Framework is proof-of-concept and not production ready

000000	00000	0000	0000	000	
Conclusion					

### SGXELIDE

- Presented framework for SGX that ensures code confidentiality
- Sanitize enclave and dynamically restore code at runtime
- Evaluated SGXELIDE's performance with SGX benchmarks we developed
- Showed SGXELIDE has very little overhead with no performance penalty after restoration
| Conclusi     | on                      |                           |            |            |
|--------------|-------------------------|---------------------------|------------|------------|
| Introduction | Background and Overview | Design and Implementation | Evaluation | Conclusion |

## SGXELIDE

- Presented framework for SGX that ensures code confidentiality
- Sanitize enclave and dynamically restore code at runtime
- Evaluated SGXELIDE's performance with SGX benchmarks we developed
- Showed SGXELIDE has very little overhead with no performance penalty after restoration

## SGXELIDE Source

github.com/utds3lab/sgxelide

Introduction	Background and Overview	Design and Implementation	Evaluation 0000	Conclusion
Thank Ye	ou			



Normal Enclave Code Generation



## erick.bauman@utdallas.edu

github.com/utds3lab/sgxelide

(a)

23/23