جامعة نيويورك أبوظبي
NYU ABU DHABI

MoMA LAB

ICSQuartz: Scan Cycle-Aware and Vendor-Agnostic Fuzzing for Industrial Control Systems

Corban Villa
NYU Abu Dhabi

Constantine Doumanidis
NYU Abu Dhabi

Hithem Lamri
NYU Abu Dhabi

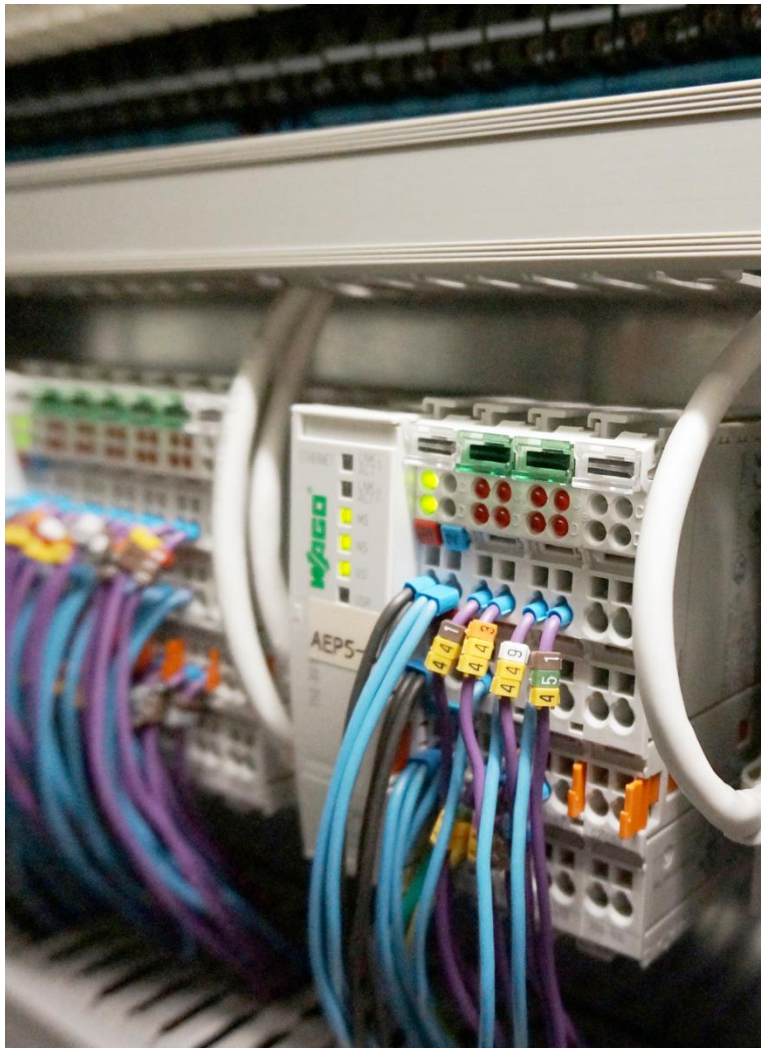
Prashant Rajput
InterSystems

Michail Maniatakos
NYU Abu Dhabi

NDSS 2025

02/26/2025

Critical Infrastructure & Industrial Control Systems (ICS)



ICS Under Attack

ICS Under Attack

Obama Order Sped Up Wave of Cyberattacks Against Iran

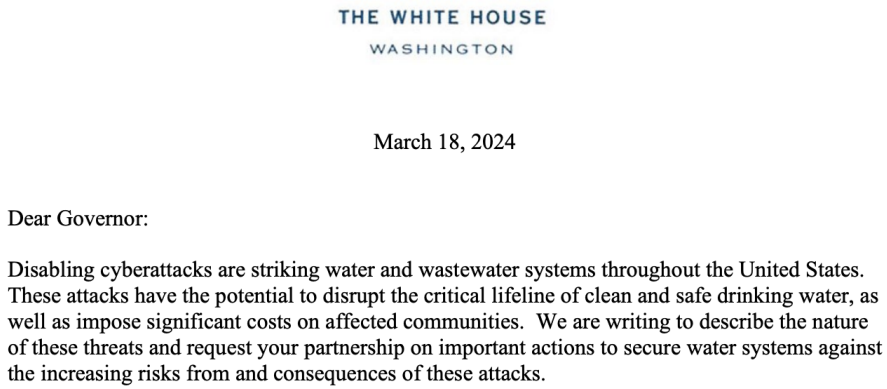
Share full article 360

By David E. Sanger

June 1, 2012

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

ICS Under Attack



THE WHITE HOUSE
WASHINGTON

March 18, 2024

Dear Governor:

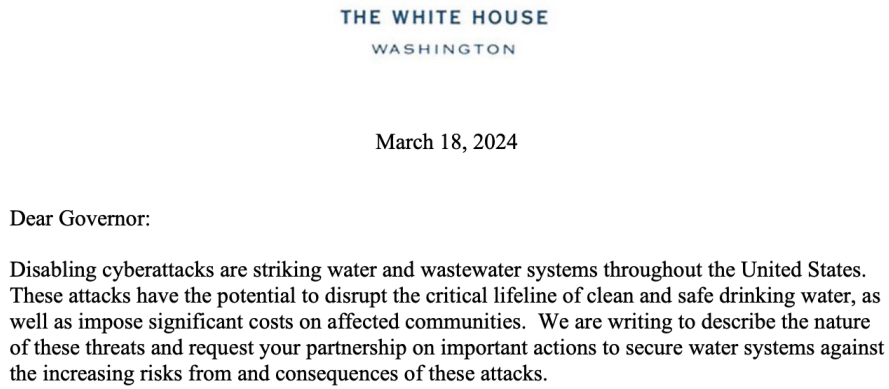
Disabling cyberattacks are striking water and wastewater systems throughout the United States. These attacks have the potential to disrupt the critical lifeline of clean and safe drinking water, as well as impose significant costs on affected communities. We are writing to describe the nature of these threats and request your partnership on important actions to secure water systems against the increasing risks from and consequences of these attacks.

Order Sped Up Wave of
acks Against Iran

360

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

ICS Under Attack



THE WHITE HOUSE
WASHINGTON

March 18, 2024

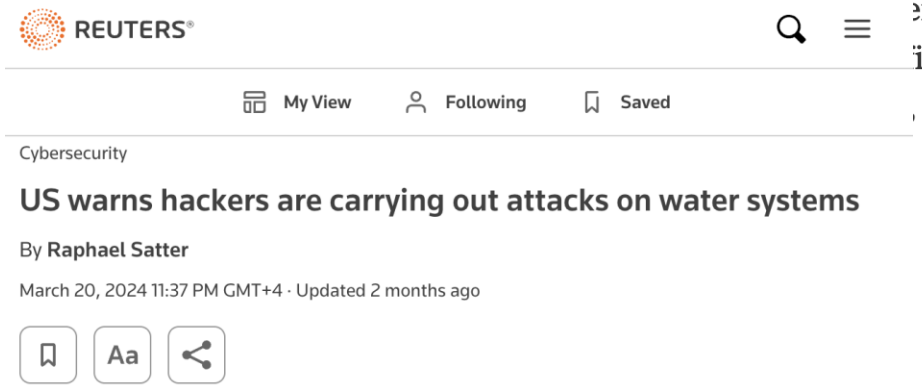
Dear Governor:

Disabling cyberattacks are striking water and wastewater systems throughout the United States. These attacks have the potential to disrupt the critical lifeline of clean and safe drinking water, as well as impose significant costs on affected communities. We are writing to describe the nature of these threats and request your partnership on important actions to secure water systems against the increasing risks from and consequences of these attacks.

Order Sped Up Wave of
acks Against Iran

360

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the ems that run Iran's main nuclear enrichment icantly expanding America's first sustained use of , according to participants in the program.



REUTERS

My View Following Saved

Cybersecurity

US warns hackers are carrying out attacks on water systems

By **Raphael Satter**

March 20, 2024 11:37 PM GMT+4 · Updated 2 months ago

Aa

ICS Under Attack

THE WHITE HOUSE
WASHINGTON

March 18, 2024

Dear Governor:

Disabling cyberattacks are striking water and wastewater systems throughout the United States. These attacks have the potential to disrupt the critical lifeline of clean and safe drinking water, as well as impose significant costs on affected communities. We are writing to describe the nature of these threats and request your partnership on important actions to secure water systems against the increasing risks from and consequences of these attacks.

Order Sped Up Wave of
Attacks Against Iran

360

WASHINGTON — From his first months in office, Pres
Obama secretly ordered increasingly sophisticated atta
ems that run Iran's main nuclear enrichr
icantly expanding America's first sustai
according to participants in the progra

REUTERS®

My View Following Saved

Cybersecurity

US warns hackers are carrying out attacks on water systems

By **Raphael Satter**

March 20, 2024 11:37 PM GMT+4 · Updated 2 months ago

Aa

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR Product ID: AA24-038A

February 7, 2024

Australian Government Australian Signals Directorate
ASD AUSTRALIAN SIGNALS DIRECTORATE ACSC
Communications Security Establishment Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications Centre canadien pour la cybersécurité
National Cyber Security Centre PART OF THE GCSB
National Cyber Security Centre a part of GCHQ

ICS Under Attack

THE WHITE HOUSE
WASHINGTON

March 18, 2024

Dear Governor:

Disabling cyberattacks are strik
These attacks have the potentia
well as impose significant cost
of these threats and request you
the increasing risks from and c

Order Sped Up Wave of
acks Against Iran

Menu 360

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

< Cybersecurity Advisories SHARE:

his first months in office, Pres
increasingly sophisticated atta
un Iran's main nuclear enrichr
panding America's first sustai
g to participants in the progra

REUTERS

Cybersecurity

US warns hackers a

By Raphael Satter

March 20, 2024 11:37 PM GMT+4

Aa

ALERT

Exploitation of Unitronics PLCs used in Water and Wastewater Systems

Release Date: November 28, 2023

RELATED TOPICS: CYBERSECURITY BEST PRACTICES

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR Product ID: AA24-038A

February 7, 2024

ASD AUSTRALIAN SIGNALS DIRECTORATE ACSC

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

ICS Under Attack

THE WHITE HOUSE
WASHINGTON

March 18, 2024

Dear Governor:

Disabling cyberattacks are strik
These attacks have the potentia
well as impose significant cost
of these threats and request you
the increasing risks from and c

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

< Cybersecurity Advisories

REUTERS

Cybersecurity

US warns hackers a

By Raphael Satter

March 20, 2024 11:37 PM GMT+4

Aa

Order Sped Up Wave of
Attacks Against Iran

Menu 360

ALERT

Exploitation of Unitronic
Water and Wastewater S

Release Date: November 28, 2023

RELATED TOPICS: CYBERSECURITY BEST PR

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:CLEAR Product ID: AA24-038A

February 7, 2024

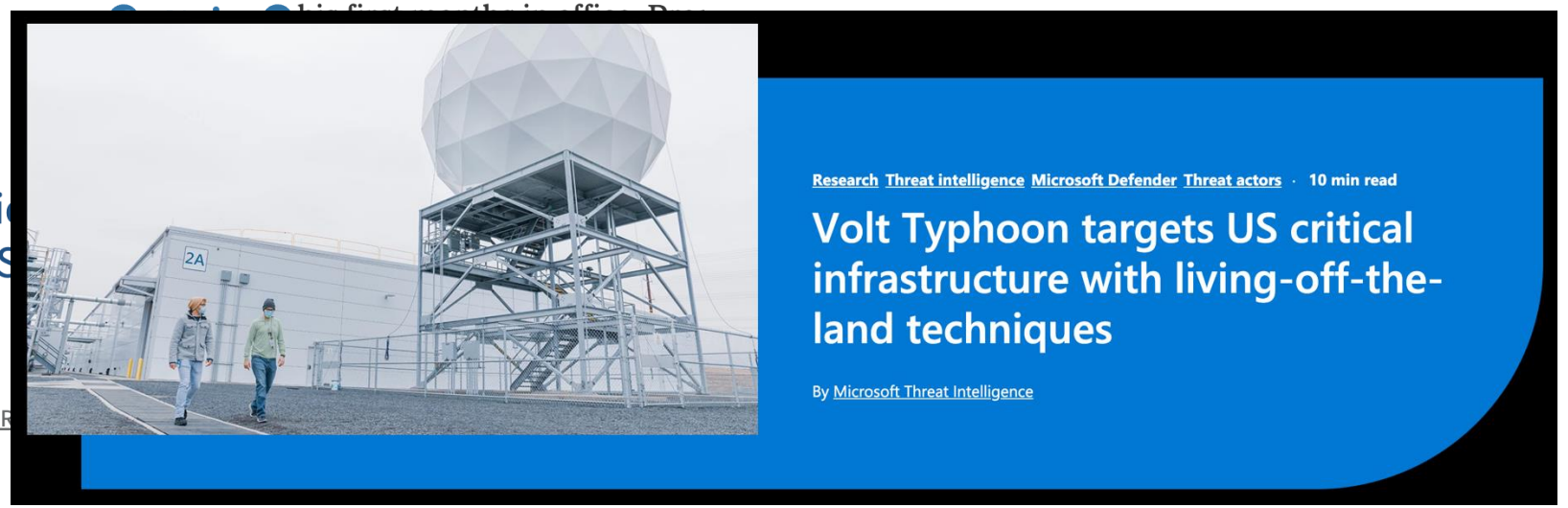
ASD AUSTRALIAN SIGNALS DIRECTORATE ACSC

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ



ICS Under Attack

ICS Under Attack

ICS Security

Why are these systems vulnerable?

ICS Security

Why are these systems vulnerable?

- 4th Industrial Revolution: Operational Technology (OT) merges with IT.

ICS Security

Why are these systems vulnerable?

- 4th Industrial Revolution: Operational Technology (OT) merges with IT.

- Full-fledged operating systems with IT vulnerabilities.

ICS Security

Why are these systems vulnerable?

- 4th Industrial Revolution: Operational Technology (OT) merges with IT.
- Full-fledged operating systems with IT vulnerabilities.
- Remote monitoring requires network-connected devices.

ICS Security

Why are these systems vulnerable?

- 4th Industrial Revolution: Operational Technology (OT) merges with IT.
- Full-fledged operating systems with IT vulnerabilities.
- Remote monitoring requires network-connected devices.
- ICS software is imperfect, often containing bugs and vulnerabilities.

ICS Software Testing

How can we detect vulnerabilities before they are deployed?

ICS Software Testing

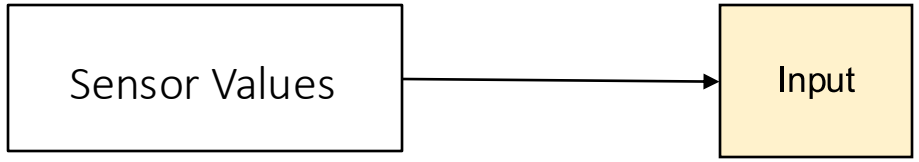
How can we detect vulnerabilities before they are deployed?

Software Fuzzing

ICS Software Testing

How can we detect vulnerabilities before they are deployed?

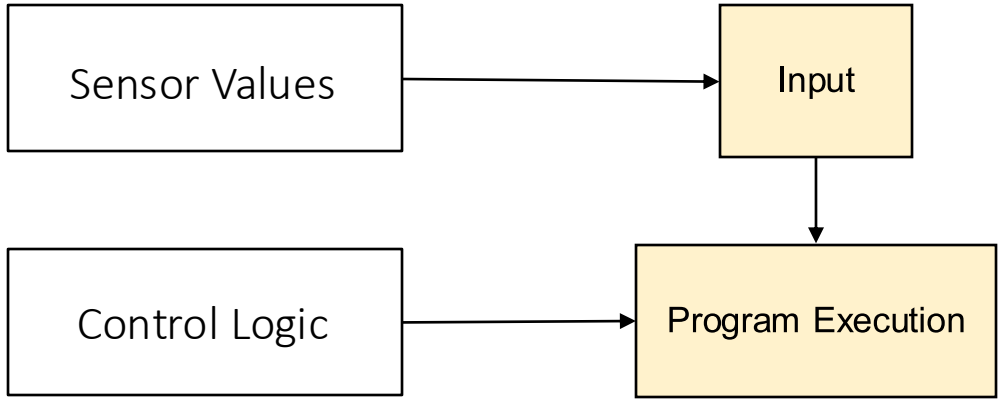
Software Fuzzing



ICS Software Testing

How can we detect vulnerabilities before they are deployed?

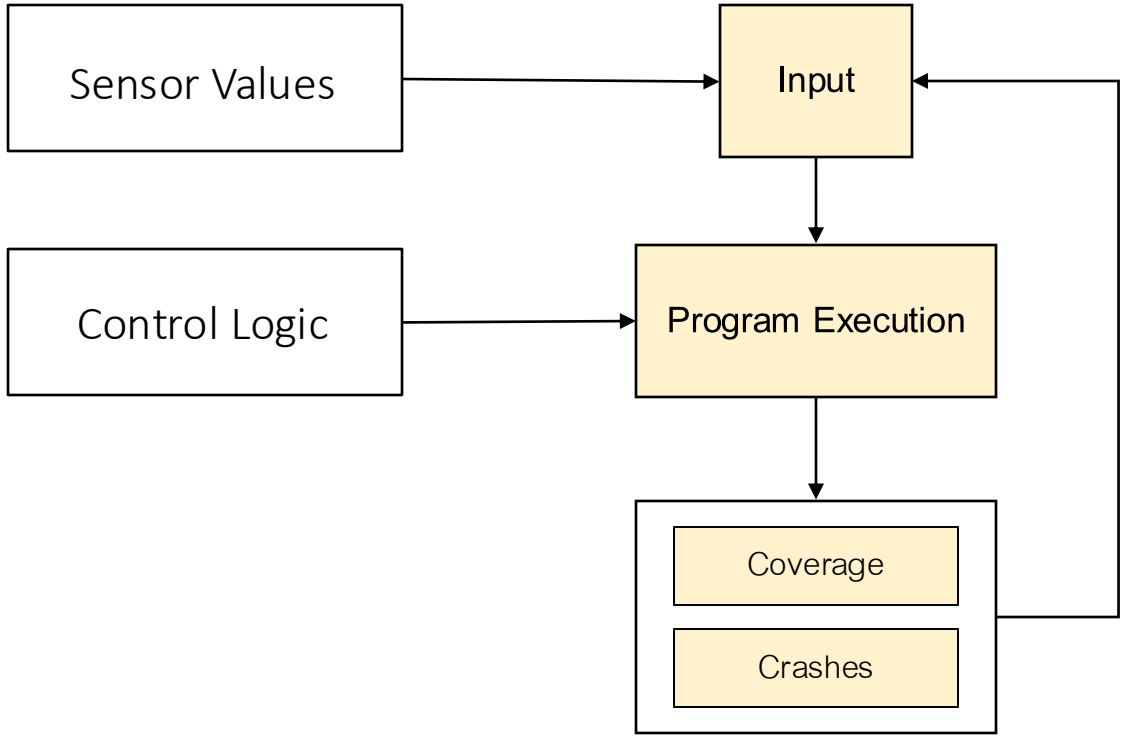
Software Fuzzing



ICS Software Testing

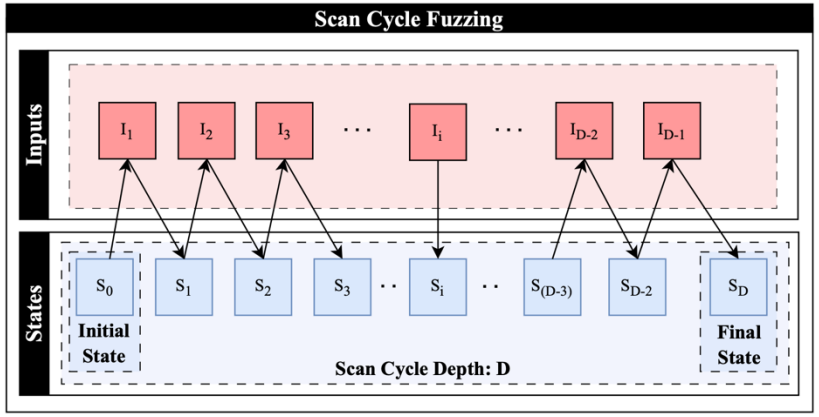
How can we detect vulnerabilities before they are deployed?

Software Fuzzing



Limitations of State-of-the-Art ICS Fuzzing

- Proprietary compilers, executables
- Vendor-locked solutions
- Imprecise (e.g., address sanitizer)
- Require specific hardware/software
- No scan cycle awareness



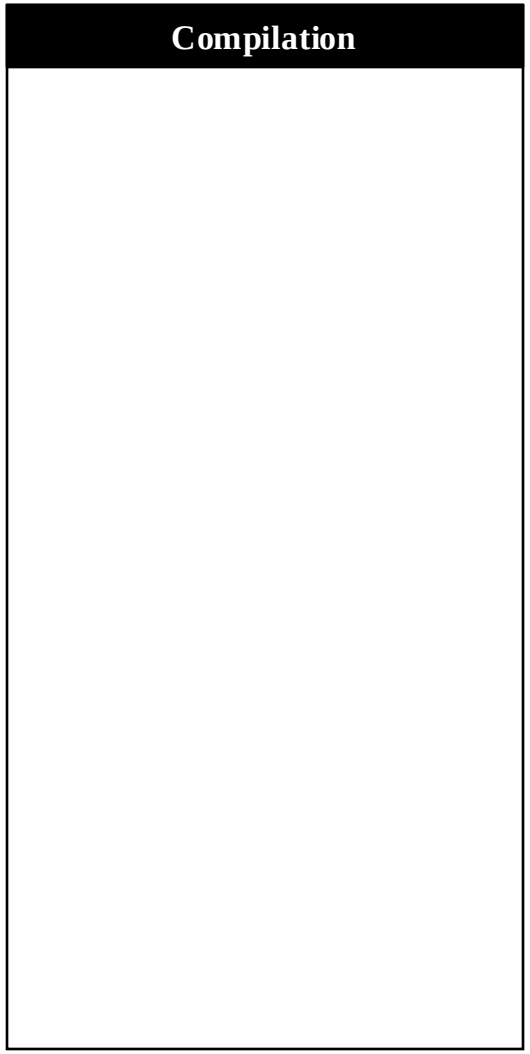
Fuzzing Framework

Existing Projects

Our Contributions

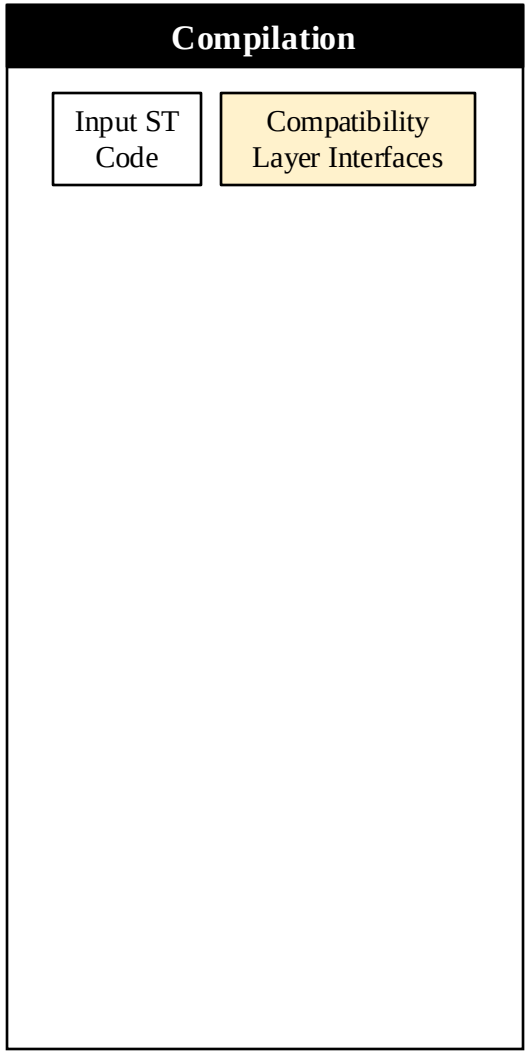
Fuzzing Framework

Existing Projects | Our Contributions



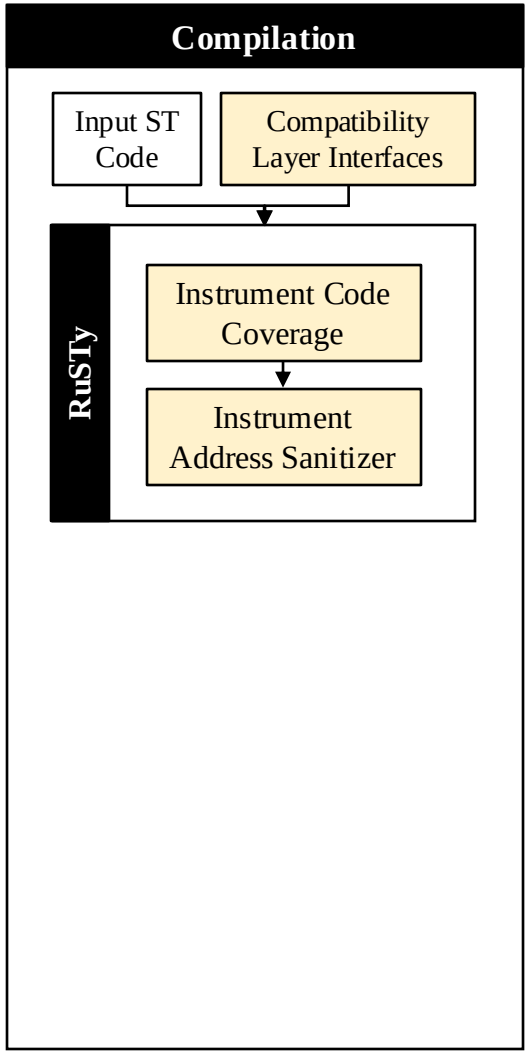
Fuzzing Framework

Existing Projects | Our Contributions



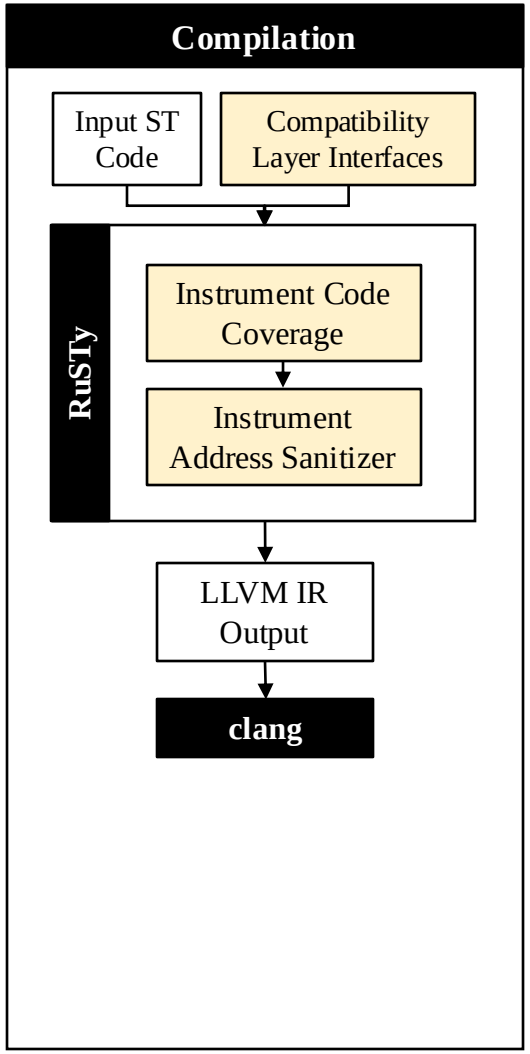
Fuzzing Framework

Existing Projects | Our Contributions



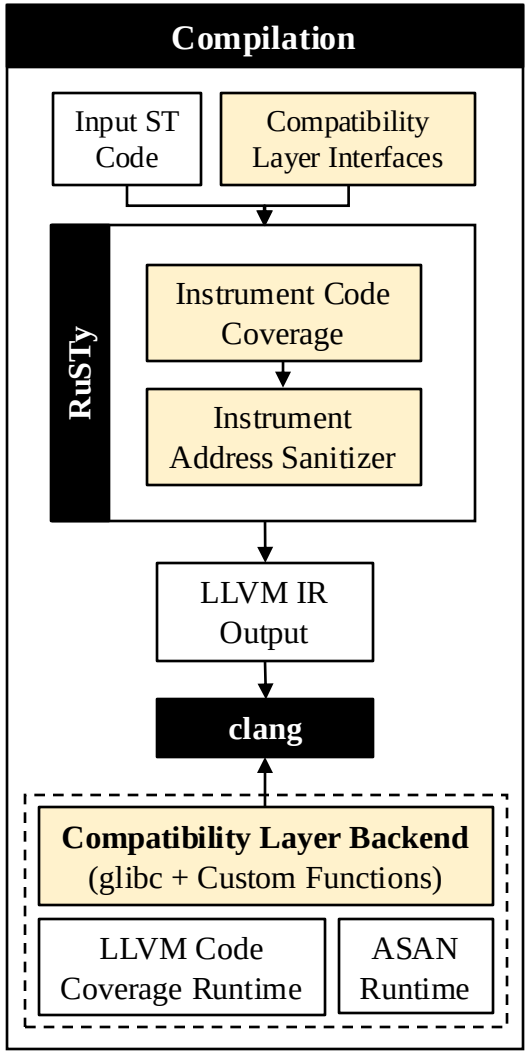
Fuzzing Framework

Existing Projects | Our Contributions



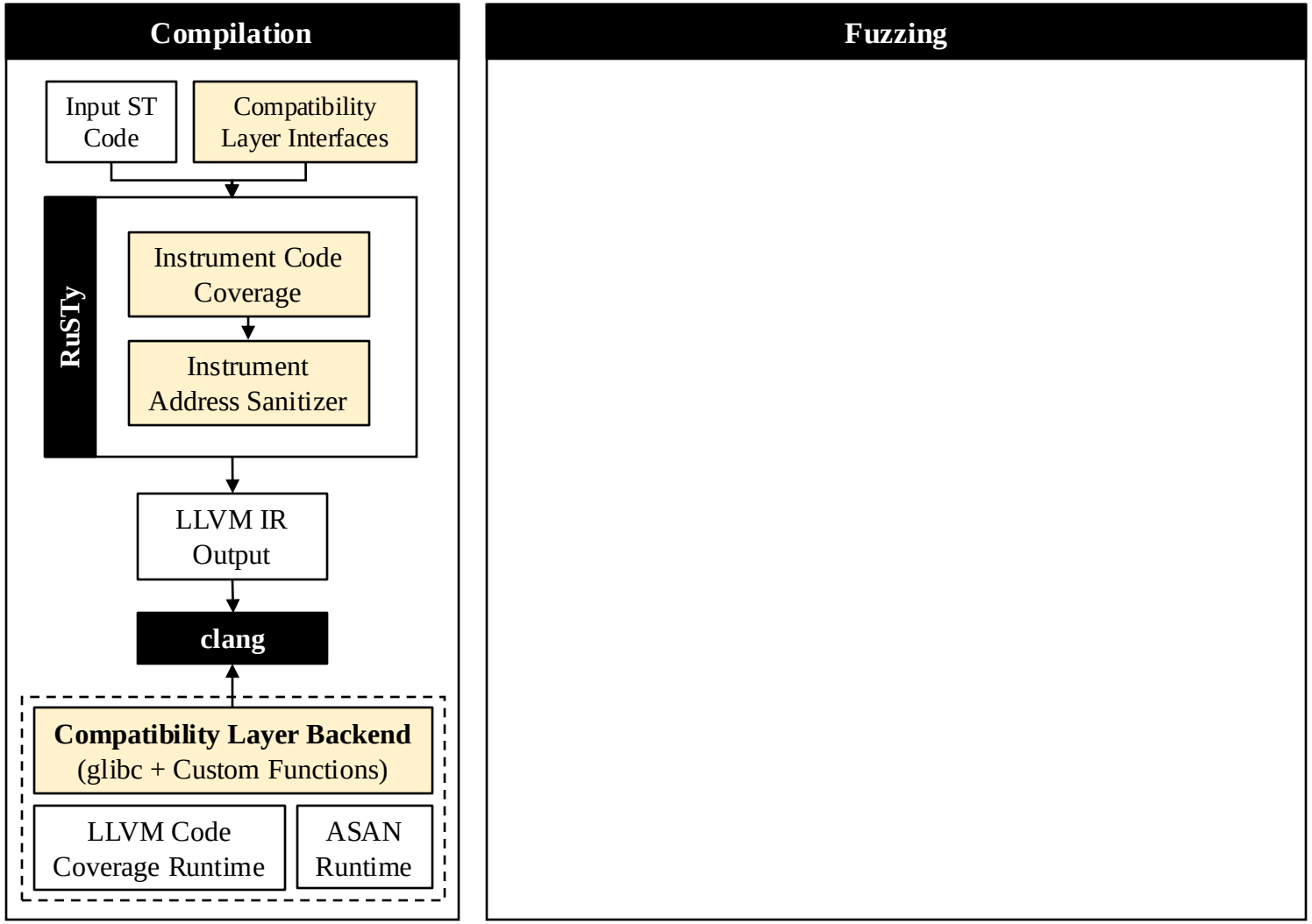
Fuzzing Framework

Existing Projects | Our Contributions



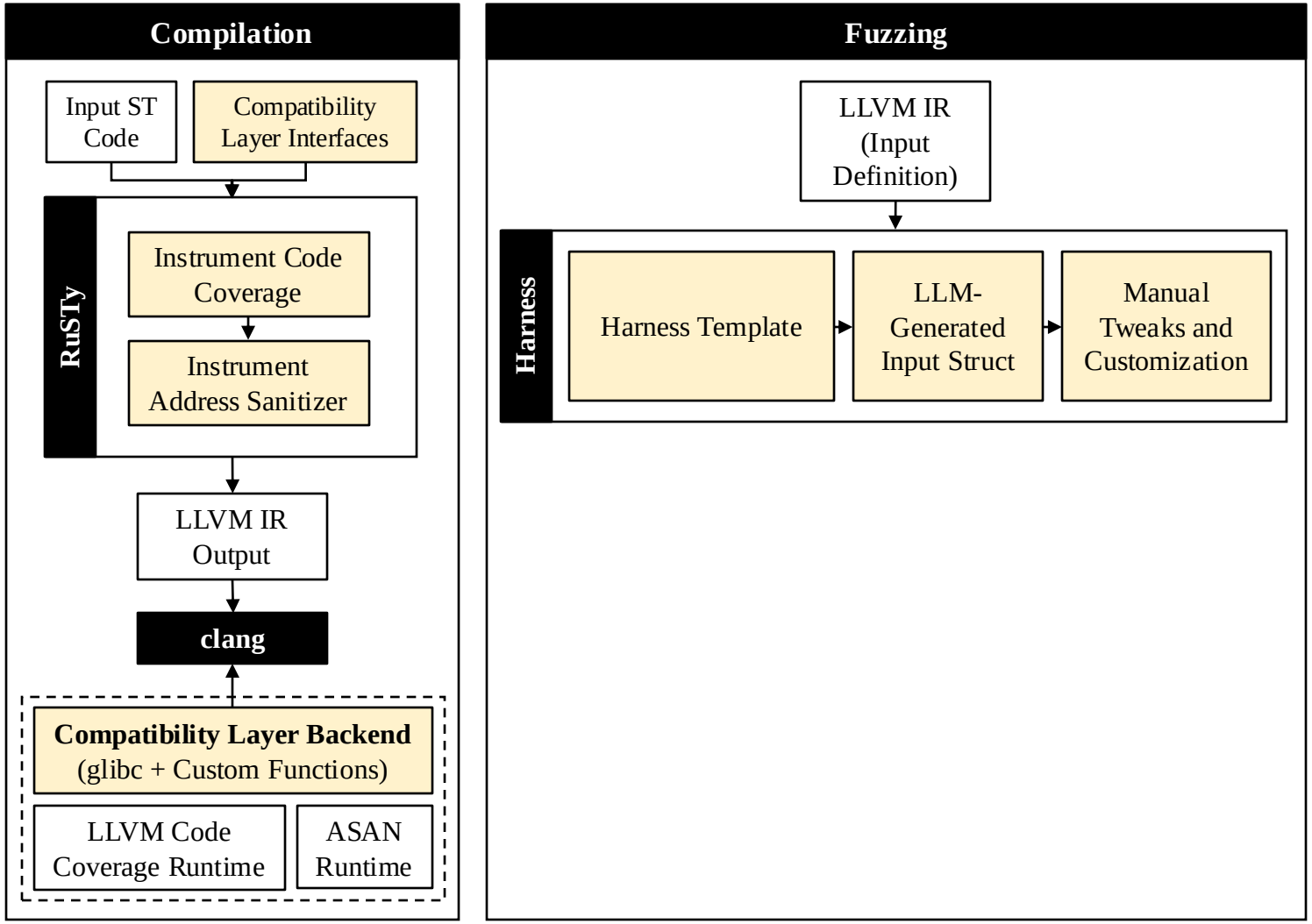
Fuzzing Framework

Existing Projects | Our Contributions



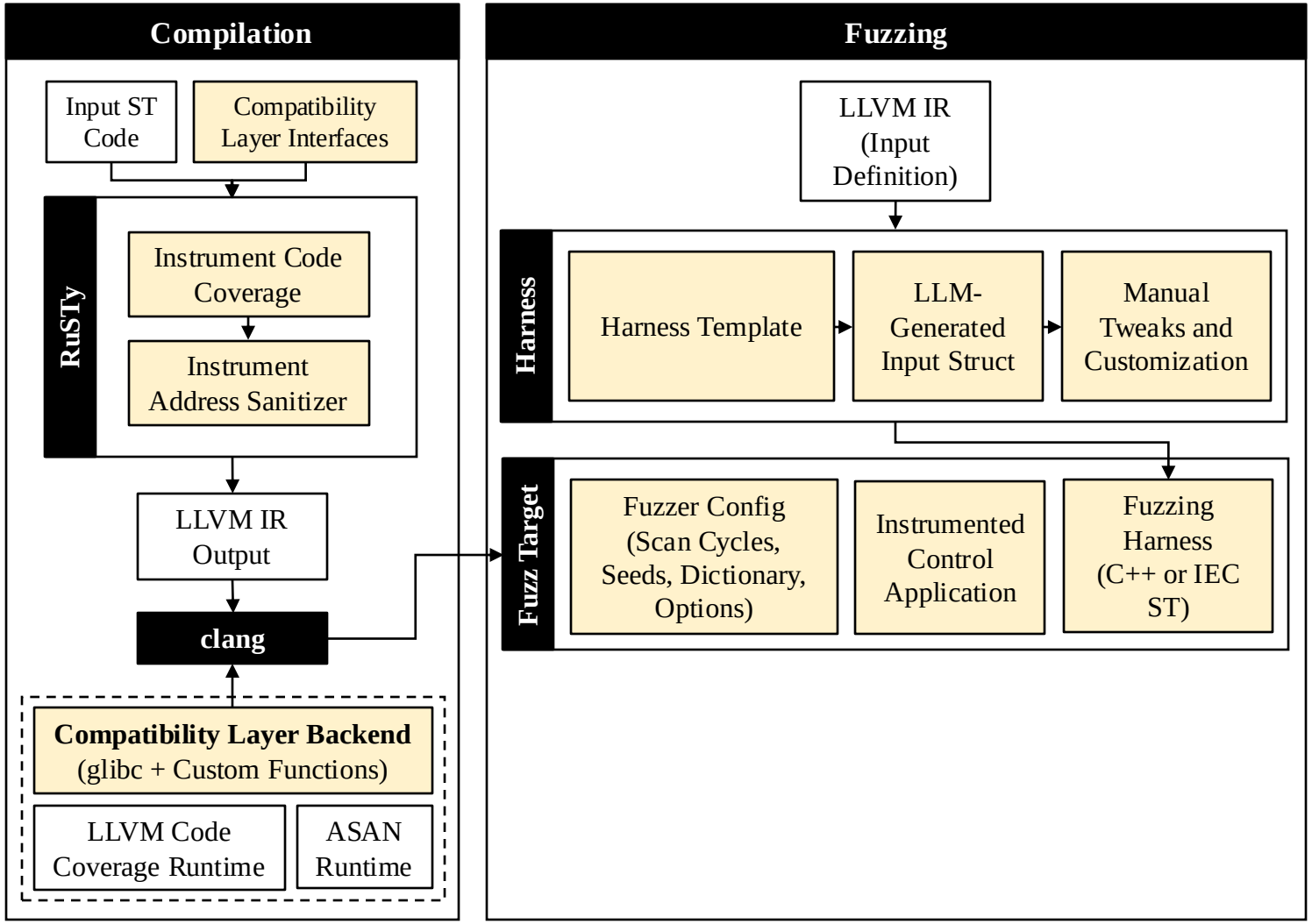
Fuzzing Framework

Existing Projects | Our Contributions



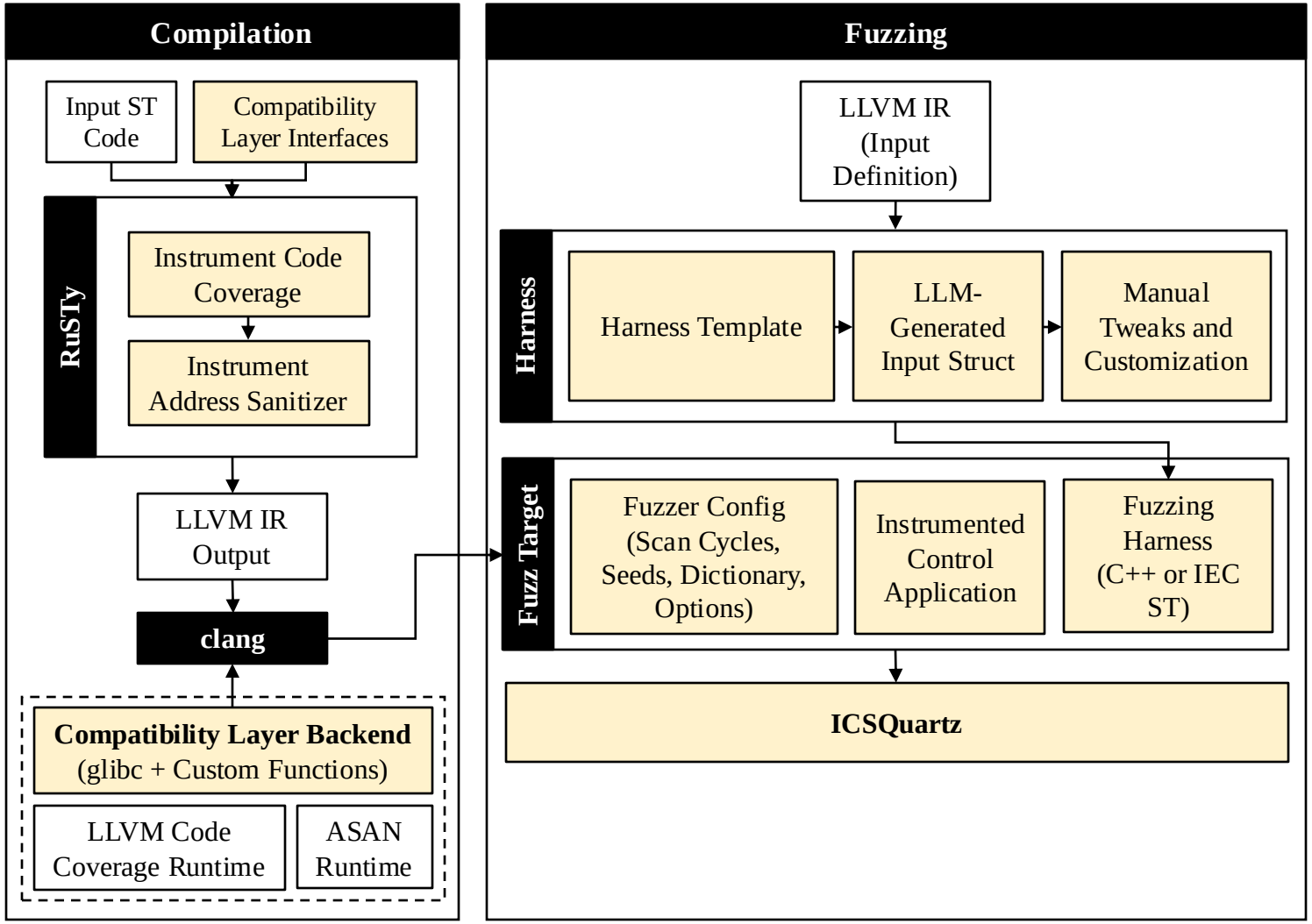
Fuzzing Framework

Existing Projects | Our Contributions



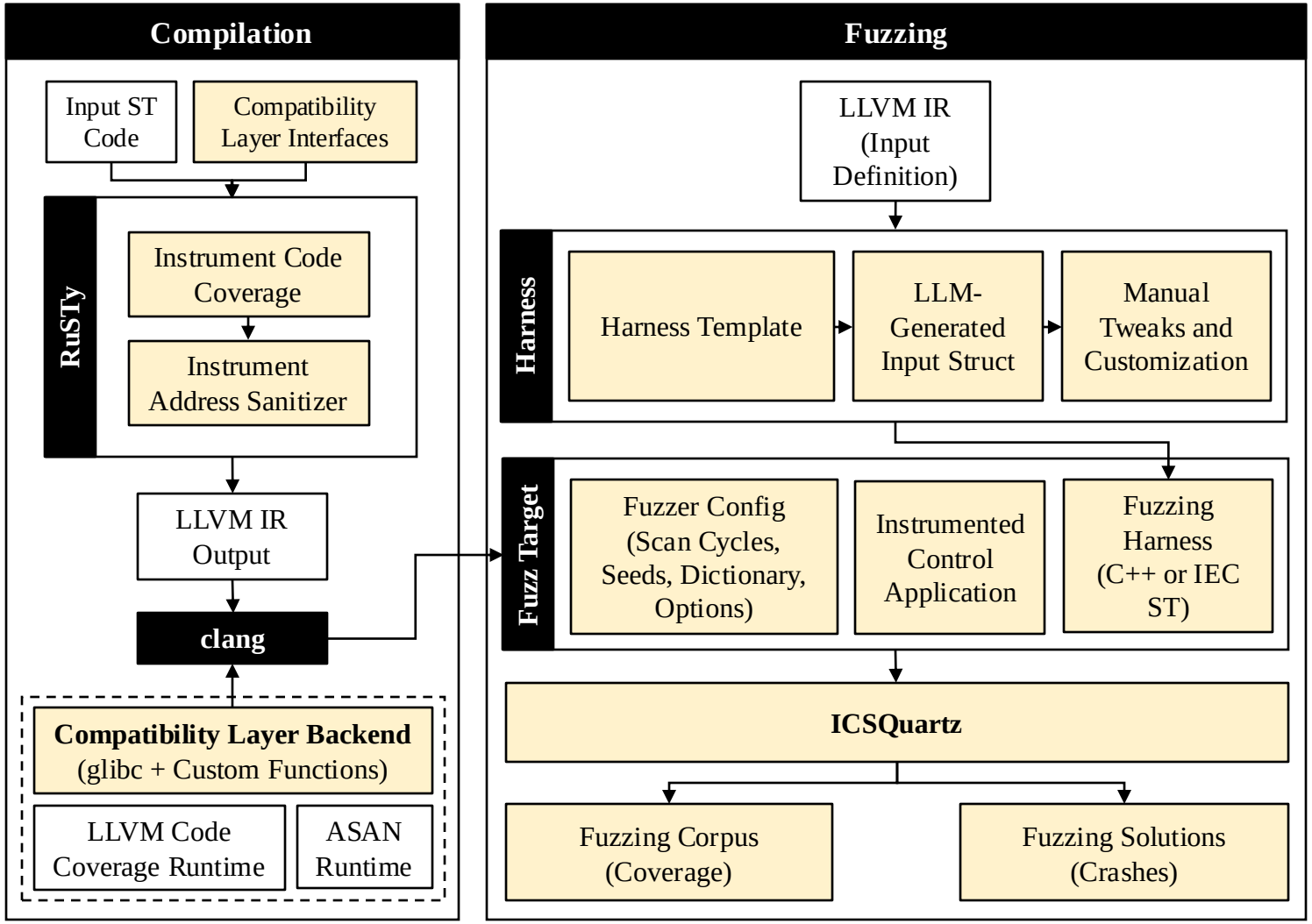
Fuzzing Framework

Existing Projects | Our Contributions



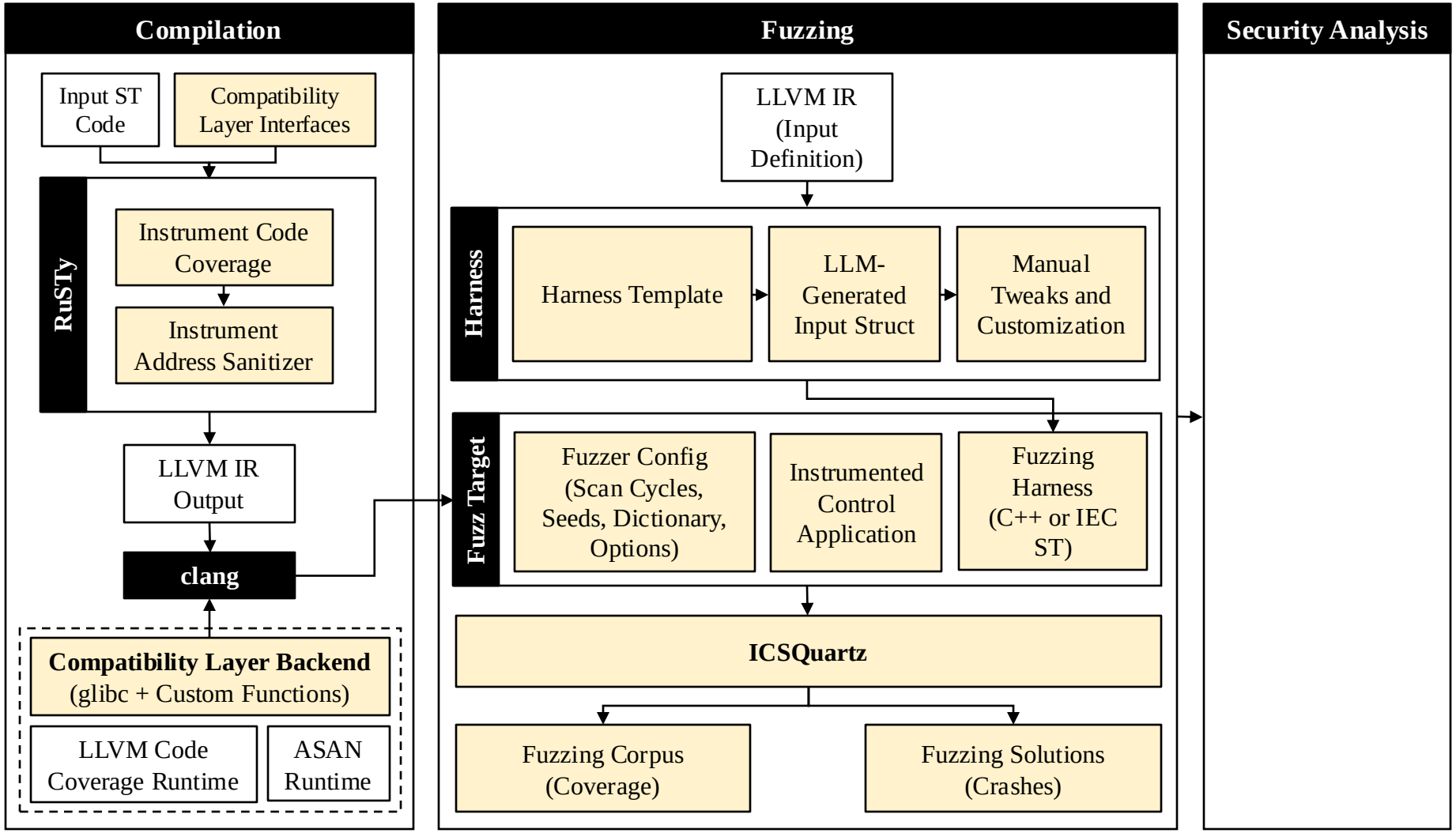
Fuzzing Framework

Existing Projects | Our Contributions

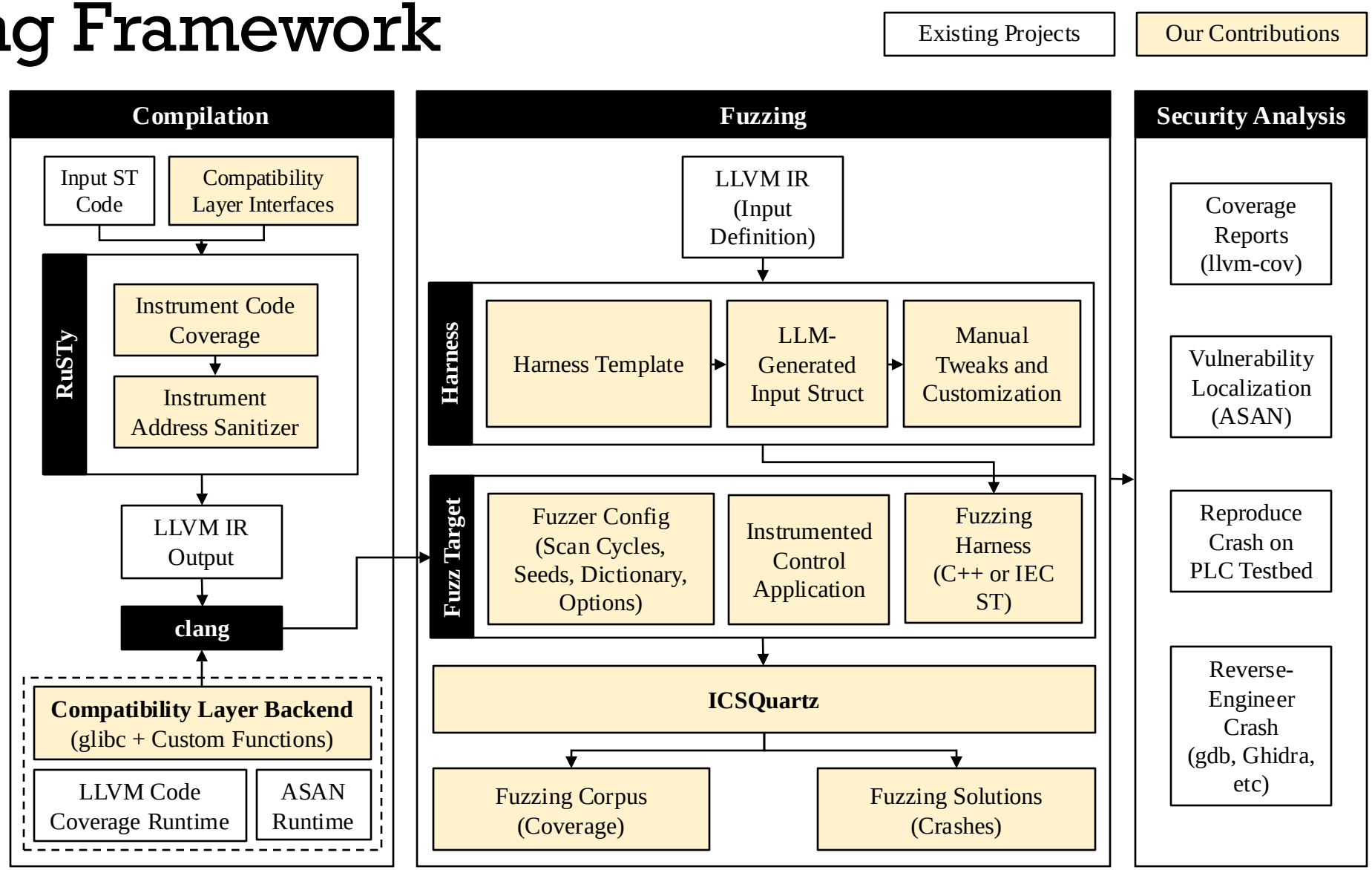


Fuzzing Framework

Existing Projects | Our Contributions



Fuzzing Framework



Results: Performance

Order of Magnitude Improvement in Key Metrics.

Results: Performance

Order of Magnitude Improvement in Key Metrics.

Control Application	Execution Speed (inputs/sec)			First Crash (seconds)			First Crash (inputs)		
	ICSQuartz (x64)	FieldFuzz (x64)	ICSFuzz (A8)	ICSQuartz (x64)	FieldFuzz (x64)	ICSFuzz (A8)	ICSQuartz (x64)	FieldFuzz (x64)	ICSFuzz (A8)
bf_mcpy_1	19649.9	593.0	70.9	0.0008	0.25	234	15.7	148	15270
bf_mcpy_6	1403.4	642.4	64.2	0.0140	1.43	188	19.6	898	12172
bf_mcpy_8	1355.6	645.6	66.1	0.0151	7.08	279	20.5	4566	18216
bf_mcpy_12	328.2	526.2	62.1	0.2630	1.95	426	86.3	999	26645
bf_mset_1	7526.0	560.6	64.6	0.0026	0.04	208	19.6	22	13441
bf_mset_3	9961.5	571.2	62.7	0.0020	0.03	174	19.5	17	10906
bf_mset_5	2227.1	503.2	68.8	0.0088	0.56	254	19.6	281	17554
bf_mmove_1	2626.4	660.2	64.6	0.0078	0.005	176	20.5	2	11245
bf_mmove_4	6674.9	578.2	63.1	0.0046	0.003	159	30.5	1	10070
bf_mmove_7	1924.3	573.0	66.3	0.0158	0.005	229	30.5	3	15317
bf_mmove_12	1932.5	508.2	64.5	0.0158	182.14	783	30.5	92456	50643
oob_1_arr_1	21747.2	598.8	71.9	0.0073	0.14	55	159.4	83	3880
oob_1_arr_6	53965.5	591.0	77.0	0.0068	1.39	103	367.1	821	8085
oob_1_arr_13	24039.7	507.0	75.2	0.0071	97.86	207	171.6	49165	27241
oob_2_arr_1	27174.2	520.8	73.5	0.0093	154.42	117	252.0	80080	8558
oob_2_arr_5	53055.0	520.4	71.1	0.0069	155.62	165	367.1	80662	22759
oob_2_arr_13	24999.5	502.2	71.0	0.0054	97.86	192	134.8	48694	13401
Average	15328.88	564.8	68.1	0.0231	41.22	232.29	103.81	21111.65	16788.41

Results: Performance

Order of Magnitude Improvement in Key Metrics.

Control Application	Execution Speed (inputs/sec)			First Crash (seconds)			First Crash (inputs)		
	ICSQuartz (x64)	FieldFuzz (x64)	ICSFuzz (A8)	ICSQuartz (x64)	FieldFuzz (x64)	ICSFuzz (A8)	ICSQuartz (x64)	FieldFuzz (x64)	ICSFuzz (A8)
bf_mcpy_1	19649.9	593.0	70.9	0.0008	0.25	234	15.7	148	15270
bf_mcpy_6	1403.4	642.4	64.2	0.0140	1.43	188	19.6	898	12172
bf_mcpy_8	1355.6	645.6	66.1	0.0151	7.08	279	20.5	4566	18216
bf_mcpy_12	328.2	526.2	62.1	0.2630	1.95	426	86.3	999	26645
bf_mset_1	7526.0	560.6	64.6	0.0026	0.04	208	19.6	22	13441
bf_mset_3	9961.5	571.2	62.7	0.0020	0.03	174	19.5	17	10906
bf_mset_5	2227.1	503.2	68.8	0.0088	0.56	254	19.6	281	17554
bf_mmove_1	2626.4	660.2	64.6	0.0078	0.005	176	20.5	2	11245
bf_mmove_4	6674.9	578.2	63.1	0.0046	0.003	159	30.5	1	10070
bf_mmove_7	1924.3	573.0	66.3	0.0158	0.005	229	30.5	3	15317
bf_mmove_12	1932.5	508.2	64.5	0.0158	182.14	783	30.5	92456	50643
oob_1_arr_1	21747.2	598.8	71.9	0.0073	0.14	55	159.4	83	3880
oob_1_arr_6	53965.5	591.0	77.0	0.0068	1.39	103	367.1	821	8085
oob_1_arr_13	24039.7	507.0	75.2	0.0071	97.86	207	171.6	49165	27241
oob_2_arr_1	27174.2	520.8	73.5	0.0093	154.42	117	252.0	80080	8558
oob_2_arr_5	53055.0	520.4	71.1	0.0069	155.62	165	367.1	80662	22759
oob_2_arr_13	24999.5	502.2	71.0	0.0054	97.86	192	134.8	48694	13401
Average	15328.88	564.8	68.1	0.0231	41.22	232.29	103.81	21111.65	16788.41

Average	15328.88	564.8	68.1	0.0231	41.22	232.29	103.81	21111.65	16788.41

Results: Scan Cycle Mutations

Evaluation of Proposed Mutation Strategies.

Results: Scan Cycle Mutations

Evaluation of Proposed Mutation Strategies.

ICSQuartz vs. SOTA

	Fuzzer	Aircraft Oobr	Aircraft Oobw 4	Aircraft Oobw 5	Anaerobic Oobr 1	Anaerobic Oobr 2	Anaerobic Oobw 1	Anaerobic Oobw 2	Anaerobic Oobw 3	Chemical Oobr 1	Chemical Oobw 1	Smart Grid Oobr 1	Smart Grid Oobw 1
Crashes	ICSQuartz	10	8	10	10	10	5	10	10	10	10	10	10
	AFL++	1	0	0	0	1	0	0	0	0	0	3	1
	FieldFuzz	0	0	9	0	0	0	0	0	0	0	0	0
	ICSFuzz	0	0	0	0	0	0	0	0	0	0	0	0
Time (s)	ICSQuartz	12.4	56.9	0.8	1.5	0.1	30.7	3.1	0.1	0.2	0.2	0.1	0.5
	AFL++	78.8	-	-	-	0.8	-	-	-	-	-	2.4	0.9
	FieldFuzz	-	-	42.5	-	-	-	-	-	-	-	-	-
	ICSFuzz	-	-	-	-	-	-	-	-	-	-	-	-
Execs.	ICSQuartz	5.6M	14M	95k	560k	1.0k	14M	480k	240	1.6k	6.1k	2.4k	100k
	AFL++	32k	-	-	-	1.3k	-	-	-	-	-	1.6k	2.1k
	FieldFuzz	-	-	2.7k	-	-	-	-	-	-	-	-	-
	ICSFuzz	-	-	-	-	-	-	-	-	-	-	-	-

TABLE V: **Scan Cycle Benchmark Evaluation (10 Trials).**

Results: Scan Cycle Mutations

Evaluation of Proposed Mutation Strategies.

ICSQuartz vs. SOTA

	Fuzzer	Aircraft Oobr	Aircraft Oobw 4	Aircraft Oobw 5	Anaerobic Oobr 1	Anaerobic Oobr 2	Anaerobic Oobw 1	Anaerobic Oobw 2	Anaerobic Oobw 3	Chemical Oobr 1	Chemical Oobw 1	Smart Grid Oobr 1	Smart Grid Oobw 1
Crashes	ICSQuartz	10	8	10	10	10	5	10	10	10	10	10	10
	AFL++	1	0	0	0	1	0	0	0	0	0	3	1
	FieldFuzz	0	0	9	0	0	0	0	0	0	0	0	0
	ICSFuzz	0	0	0	0	0	0	0	0	0	0	0	0
Time (s)	ICSQuartz	12.4	56.9	0.8	1.5	0.1	30.7	3.1	0.1	0.2	0.2	0.1	0.5
	AFL++	78.8	-	-	-	0.8	-	-	-	-	-	2.4	0.9
	FieldFuzz	-	-	42.5	-	-	-	-	-	-	-	-	-
	ICSFuzz	-	-	-	-	-	-	-	-	-	-	-	-
Execs.	ICSQuartz	5.6M	14M	95k	560k	1.0k	14M	480k	240	1.6k	6.1k	2.4k	100k
	AFL++	32k	-	-	-	1.3k	-	-	-	-	-	1.6k	2.1k
	FieldFuzz	-	-	2.7k	-	-	-	-	-	-	-	-	-
	ICSFuzz	-	-	-	-	-	-	-	-	-	-	-	-

TABLE V: **Scan Cycle Benchmark Evaluation (10 Trials).**

Results: Scan Cycle Mutations

Evaluation of Proposed Mutation Strategies.

ICSQuartz vs. SOTA

	Fuzzer	Aircraft Oobr	Aircraft Oobw 4	Aircraft Oobw 5	Anaerobic Oobr 1	Anaerobic Oobr 2	Anaerobic Oobw 1	Anaerobic Oobw 2	Anaerobic Oobw 3	Chemical Oobr 1	Chemical Oobw 1	Smart Grid Oobr 1	Smart Grid Oobw 1
Crashes	ICSQuartz	10	8	10	10	10	5	10	10	10	10	10	10
	AFL++	1	0	0	0	1	0	0	0	0	0	3	1
	FieldFuzz	0	0	9	0	0	0	0	0	0	0	0	0
	ICSFuzz	0	0	0	0	0	0	0	0	0	0	0	0
Time (s)	ICSQuartz	12.4	56.9	0.8	1.5	0.1	30.7	3.1	0.1	0.2	0.2	0.1	0.5
	AFL++	78.8	-	-	-	0.8	-	-	-	-	-	2.4	0.9
	FieldFuzz	-	-	42.5	-	-	-	-	-	-	-	-	-
	ICSFuzz	-	-	-	-	-	-	-	-	-	-	-	-
Execs.	ICSQuartz	5.6M	14M	95k	560k	1.0k	14M	480k	240	1.6k	6.1k	2.4k	100k
	AFL++	32k	-	-	-	1.3k	-	-	-	-	-	1.6k	2.1k
	FieldFuzz	-	-	2.7k	-	-	-	-	-	-	-	-	-
	ICSFuzz	-	-	-	-	-	-	-	-	-	-	-	-

TABLE V: **Scan Cycle Benchmark Evaluation (10 Trials).**

Toggled Mutation Strategies

	ICSQuartz Scan Cycle Mutations	Aircraft Oobr	Aircraft Oobw 4	Aircraft Oobw 5	Anaerobic Oobr 1	Anaerobic Oobr 2	Anaerobic Oobw 1	Anaerobic Oobw 2	Anaerobic Oobw 3	Chemical Oobr 1	Chemical Oobw 1	Smart Grid Oobr 1	Smart Grid Oobw 1
Total Crashes	●	10	8	10	10	10	5	10	10	10	10	10	10
	○	0	0	0	0	1	0	0	0	0	0	0	0
Stale Cycles	●	1.9	20.9	31.3	1.0	1.5	1.3	40.5	30.2	3.1	3.1	6.6	1.9
	○	99.9	99.9	44.0	99.9	99.9	99.9	99.9	99.9	5.4	99.9	99.9	99.9

TABLE VI: **Evaluation of ICSQuartz Mutations (10 Trials).**

Results: Scan Cycle Mutations

Evaluation of Proposed Mutation Strategies.

ICSQuartz vs. SOTA

	Fuzzer	Aircraft Oobr	Aircraft Oobw 4	Aircraft Oobw 5	Anaerobic Oobr 1	Anaerobic Oobr 2	Anaerobic Oobw 1	Anaerobic Oobw 2	Anaerobic Oobw 3	Chemical Oobr 1	Chemical Oobw 1	Smart Grid Oobr 1	Smart Grid Oobw 1
Crashes	ICSQuartz	10	8	10	10	10	5	10	10	10	10	10	10
	AFL++	1	0	0	0	1	0	0	0	0	0	3	1
	FieldFuzz	0	0	9	0	0	0	0	0	0	0	0	0
	ICSFuzz	0	0	0	0	0	0	0	0	0	0	0	0
Time (s)	ICSQuartz	12.4	56.9	0.8	1.5	0.1	30.7	3.1	0.1	0.2	0.2	0.1	0.5
	AFL++	78.8	-	-	-	0.8	-	-	-	-	-	2.4	0.9
	FieldFuzz	-	-	42.5	-	-	-	-	-	-	-	-	-
	ICSFuzz	-	-	-	-	-	-	-	-	-	-	-	-
Execs.	ICSQuartz	5.6M	14M	95k	560k	1.0k	14M	480k	240	1.6k	6.1k	2.4k	100k
	AFL++	32k	-	-	-	1.3k	-	-	-	-	-	1.6k	2.1k
	FieldFuzz	-	-	2.7k	-	-	-	-	-	-	-	-	-
	ICSFuzz	-	-	-	-	-	-	-	-	-	-	-	-

TABLE V: **Scan Cycle Benchmark Evaluation (10 Trials).**

Toggled Mutation Strategies

	ICSQuartz Scan Cycle Mutations	Aircraft Oobr	Aircraft Oobw 4	Aircraft Oobw 5	Anaerobic Oobr 1	Anaerobic Oobr 2	Anaerobic Oobw 1	Anaerobic Oobw 2	Anaerobic Oobw 3	Chemical Oobr 1	Chemical Oobw 1	Smart Grid Oobr 1	Smart Grid Oobw 1
Total Crashes	●	10	8	10	10	10	5	10	10	10	10	10	10
	○	0	0	0	0	1	0	0	0	0	0	0	0
Stale Cycles	●	1.9	20.9	31.3	1.0	1.5	1.3	40.5	30.2	3.1	3.1	6.6	1.9
	○	99.9	99.9	44.0	99.9	99.9	99.9	99.9	99.9	5.4	99.9	99.9	99.9

TABLE VI: **Evaluation of ICSQuartz Mutations (10 Trials).**

Results: Impact

Results: Impact

Real-World Fuzz Campaign

OSCAT Program	Total Executions		
	ICSQuartz	FieldFuzz	ICSFuzz
CHARNAME	123M	239k	102k
CLEAN	3.73M	239k	99.2k
DEL_CHARS	3.73M	239k	99.6k
DT_TO_STRF	129k	239k	102k
FIND_CHAR	*386k*	239k	102k
FIND_CTRL	*386k*	239k	99.1k
FINDB_NONUM	*436k*	239k	99.1k
FINDB_NUM	*436k*	239k	99.5k
FSTRING_TO_BYTE	817k	239k	99.3k
FSTRING_TO_DWORD	333k	239k	99.0k
IS_CC	3.73M	239k	99.2k
IS_NCC	3.73M	239k	99.3k
MIRROR	*436k*	239k	99.7k
MONTH_TO_STRING	**1.07B**	239k	102k
REAL_TO_STRF	399M	239k	102k
REPLACE_ALL	23.7M	239k	100k
REPLACE_CHARS	23.7M	239k	99.2k
TRIM	436k	240k	100k
TRIM1	436k	239k	99.3k
TRIME	436k	239k	100k
UPPER_CASE	436k	239k	99.7k
WEEKDAY_TO_STRING	966M	240k	102k
BASE64_ENCODE_STR	17.9k	N/A	N/A
XML_READER	*644k*	N/A	N/A

TABLE IV: **OSCAT Fuzzing Campaign. Bold** indicates a vendor-agnostic CVE issued (discovered only by ICSQuartz). *Italics* indicate a RuSTy-specific compiler vulnerability.

Results: Impact

Real-World Fuzz Campaign

OSCAT Program	Total Executions		
	ICSQuartz	FieldFuzz	ICSFuzz
CHARNAME	123M	239k	102k
CLEAN	3.73M	239k	99.2k
DEL_CHARS	3.73M	239k	99.6k
DT_TO_STRF	129k	239k	102k
FIND_CHAR	*386k*	239k	102k
FIND_CTRL	*386k*	239k	99.1k
FINDB_NONUM	*436k*	239k	99.1k
FINDB_NUM	*436k*	239k	99.5k
FSTRING_TO_BYTE	817k	239k	99.3k
FSTRING_TO_DWORD	333k	239k	99.0k
IS_CC	3.73M	239k	99.2k
IS_NCC	3.73M	239k	99.3k
MIRROR	*436k*	239k	99.7k
MONTH_TO_STRING	**1.07B**	239k	102k
REAL_TO_STRF	399M	239k	102k
REPLACE_ALL	23.7M	239k	100k
REPLACE_CHARS	23.7M	239k	99.2k
TRIM	436k	240k	100k
TRIM1	436k	239k	99.3k
TRIME	436k	239k	100k
UPPER_CASE	436k	239k	99.7k
WEEKDAY_TO_STRING	966M	240k	102k
BASE64_ENCODE_STR	17.9k	N/A	N/A
XML_READER	*644k*	N/A	N/A

TABLE IV: **OSCAT Fuzzing Campaign. Bold** indicates a vendor-agnostic CVE issued (discovered only by ICSQuartz). *Italics* indicate a RuSTy-specific compiler vulnerability.

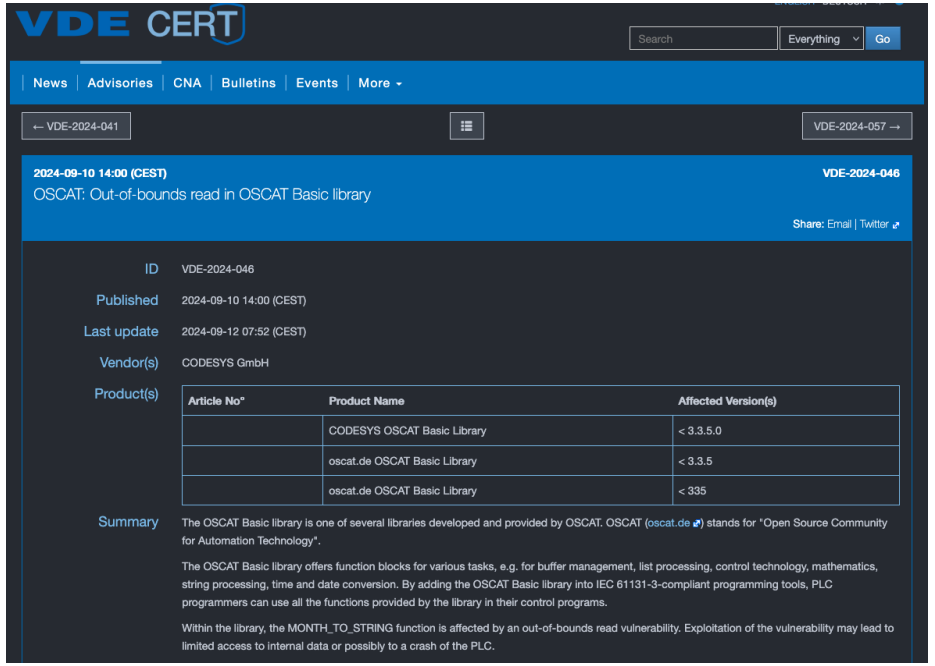
Results: Impact

Real-World Fuzz Campaign

OSCAT Program	Total Executions		
	ICSQuartz	FieldFuzz	ICSFuzz
CHARNAME	123M	239k	102k
CLEAN	3.73M	239k	99.2k
DEL_CHARS	3.73M	239k	99.6k
DT_TO_STRF	129k	239k	102k
FIND_CHAR	*386k*	239k	102k
FIND_CTRL	*386k*	239k	99.1k
FINDB_NONUM	*436k*	239k	99.1k
FINDB_NUM	*436k*	239k	99.5k
FSTRING_TO_BYTE	817k	239k	99.3k
FSTRING_TO_DWORD	333k	239k	99.0k
IS_CC	3.73M	239k	99.2k
IS_NCC	3.73M	239k	99.3k
MIRROR	*436k*	239k	99.7k
MONTH_TO_STRING	**1.07B**	239k	102k
REAL_TO_STRF	399M	239k	102k
REPLACE_ALL	23.7M	239k	100k
REPLACE_CHARS	23.7M	239k	99.2k
TRIM	436k	240k	100k
TRIM1	436k	239k	99.3k
TRIME	436k	239k	100k
UPPER_CASE	436k	239k	99.7k
WEEKDAY_TO_STRING	966M	240k	102k
BASE64_ENCODE_STR	17.9k	N/A	N/A
XML_READER	*644k*	N/A	N/A

TABLE IV: **OSCAT Fuzzing Campaign. Bold** indicates a vendor-agnostic CVE issued (discovered only by ICSQuartz). *Italics* indicate a RuSTy-specific compiler vulnerability.

Disclosed CVE-2024-6876



Key Takeaways:

Key Takeaways:

- First native fuzzer for ICS programs (IEC-61131-3 Structured Text):
  - Surpasses black-box state-of-the-art solutions by an order of magnitude in performance.
  - Provides increased precision for code coverage and vulnerability detection.

Key Takeaways:

- First native fuzzer for ICS programs (IEC-61131-3 Structured Text):
  - Surpasses black-box state-of-the-art solutions by an order of magnitude in performance.
  - Provides increased precision for code coverage and vulnerability detection.
- Introduces novel ICS-specific scan cycle mutation strategies:
  - Detect vulnerabilities not discovered by prior work.
  - Release new scan cycle benchmarks.

Key Takeaways:

- First native fuzzer for ICS programs (IEC-61131-3 Structured Text):
  - Surpasses black-box state-of-the-art solutions by an order of magnitude in performance.
  - Provides increased precision for code coverage and vulnerability detection.
- Introduces novel ICS-specific scan cycle mutation strategies:
  - Detect vulnerabilities not discovered by prior work.
  - Release new scan cycle benchmarks.
- Discover and disclose:
  - The first (to our knowledge) Structured Text CVE.
  - Compiler bug in RuSTy ICS compiler.

MoMA LAB | wp.nyu.edu/momalab

Thank you

Corban Villa
corban.villa@nyu.edu

Lab Website

GitHub

جامعة نيويورك أبوظبي
NYU ABU DHABI