TLS-Anvil

Adapting Combinatorial Testing for TLS Libraries

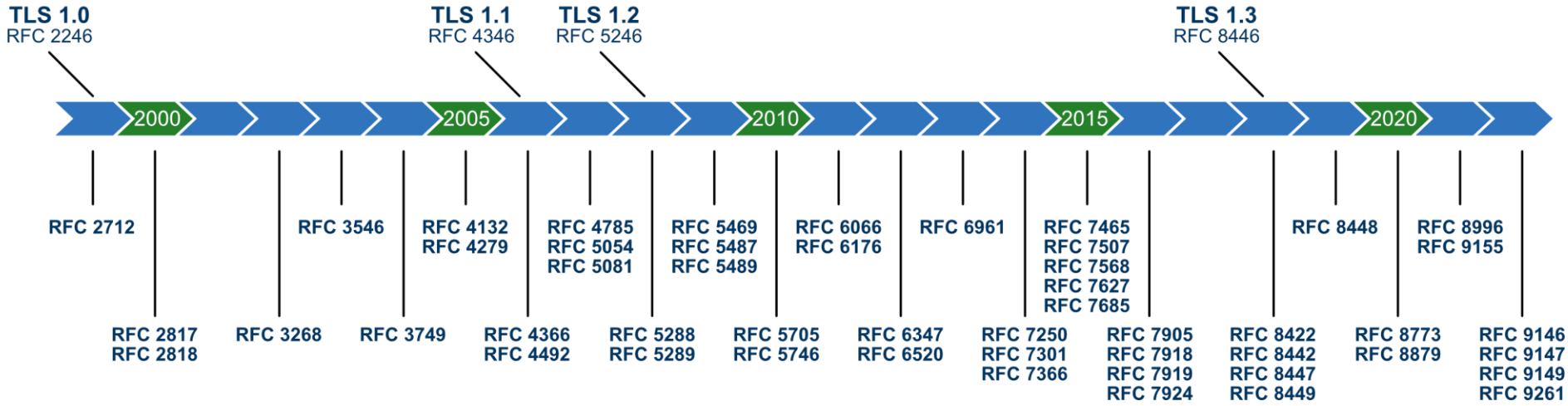
USENIX Security ‘22

Marcel Maehren[1], Philipp Nieting[1], Sven Hebrok[2], Robert Merget[1], Juraj Somorovsky[2], Jörg Schwenk[1]

1 Ruhr University Bochum
2 Paderborn University

TLS Is a Complex Protocol

TLS Is a Complex Protocol



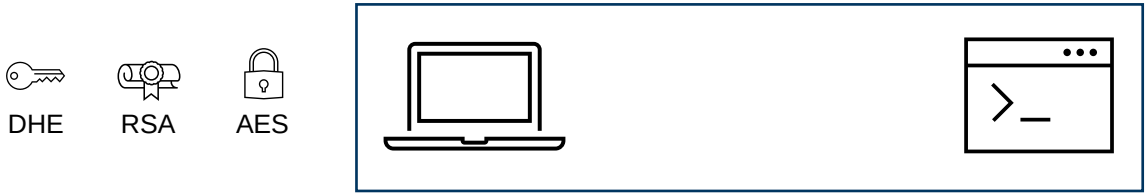
RFC Requirement Example

> The receiver **MUST** check this padding and **MUST** use the **bad_record_mac alert** to indicate padding errors.
>
> - RFC 5246 (CBC Block Cipher)

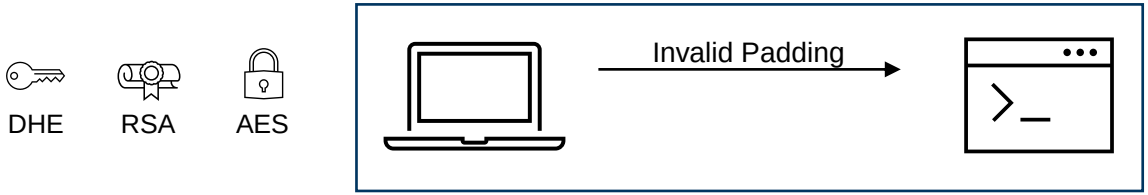
Security measure to avoid **Padding Oracle** attacks

→ Requirement must be met regardless of negotiated parameters

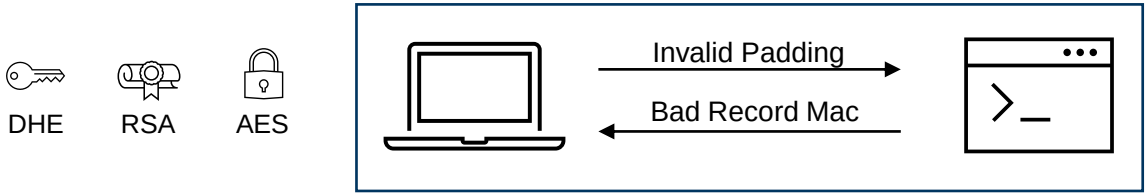
Parameters Example



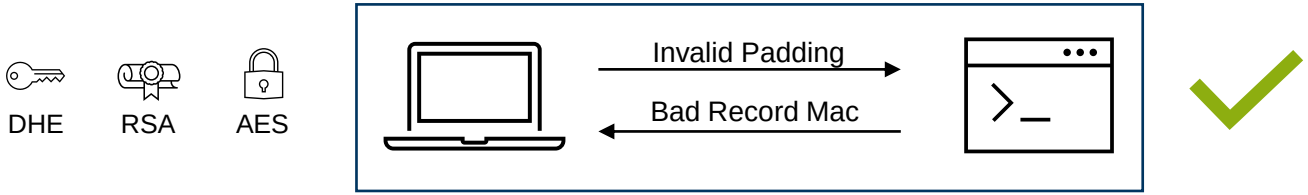
Parameters Example



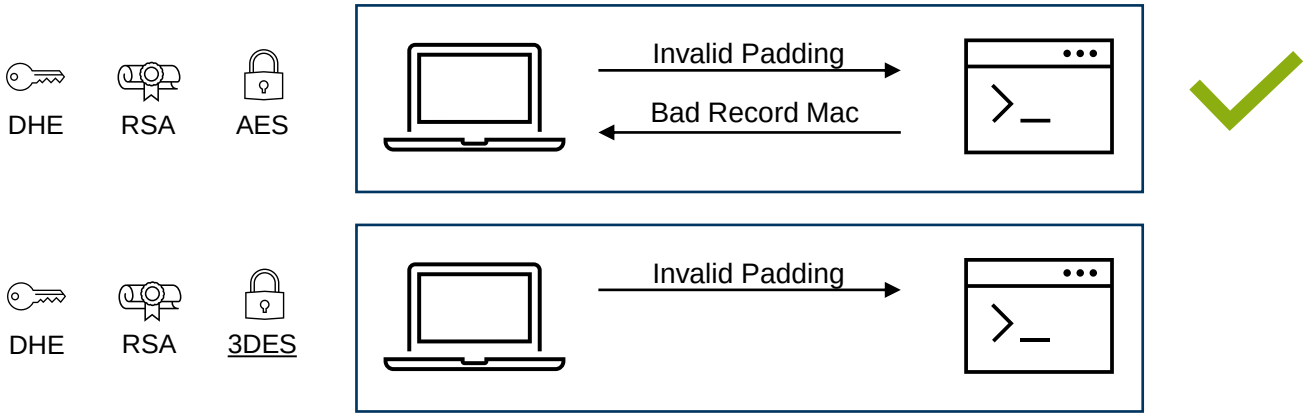
Parameters Example



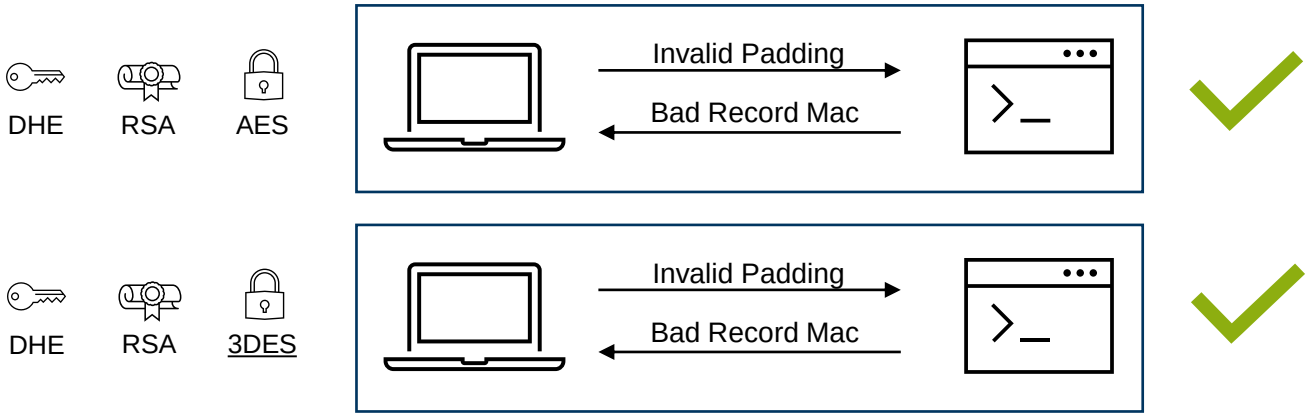
Parameters Example



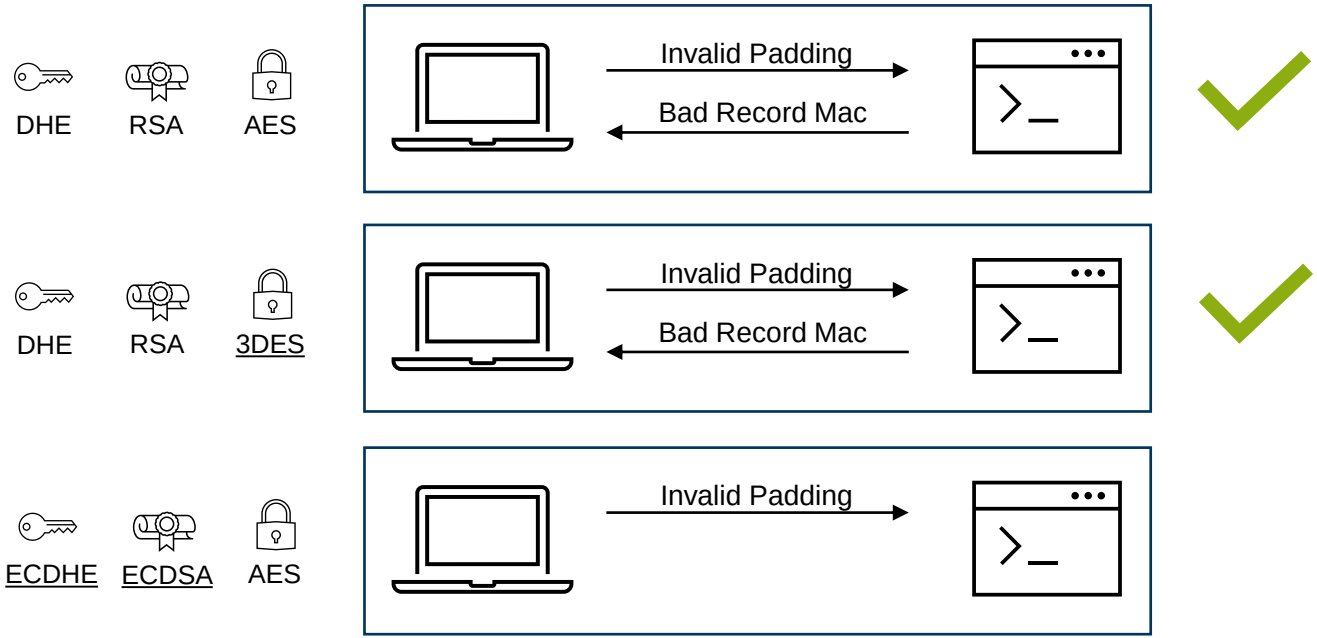
Parameters Example



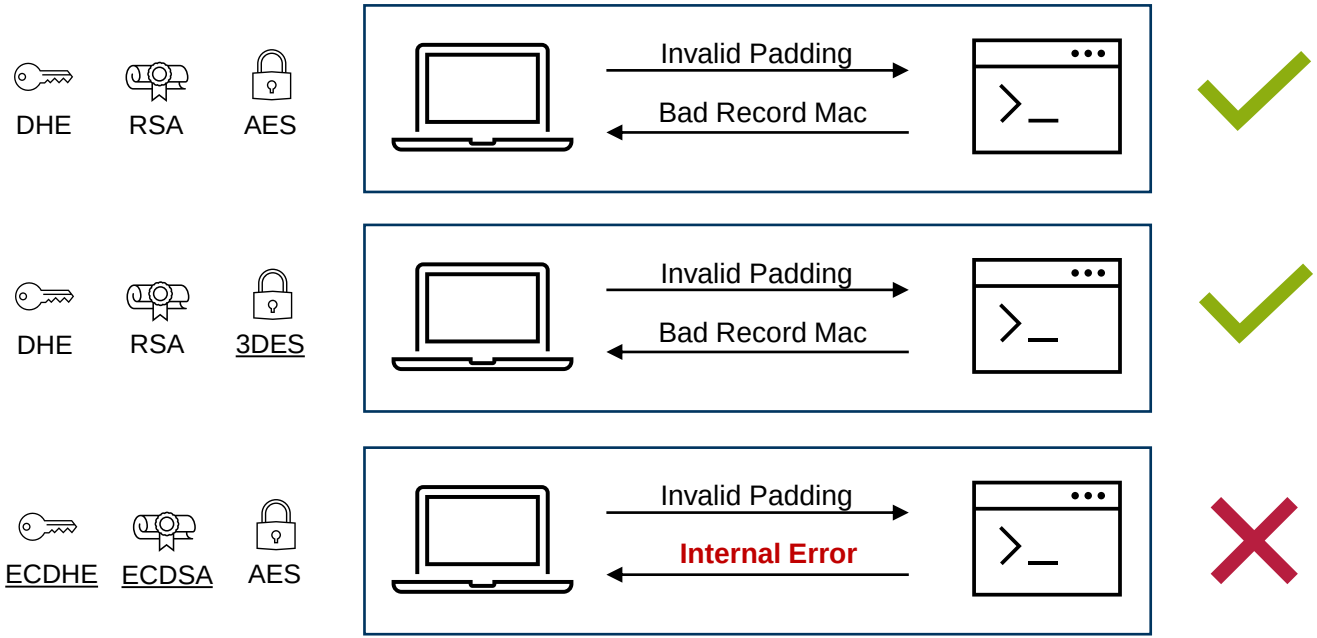
Parameters Example



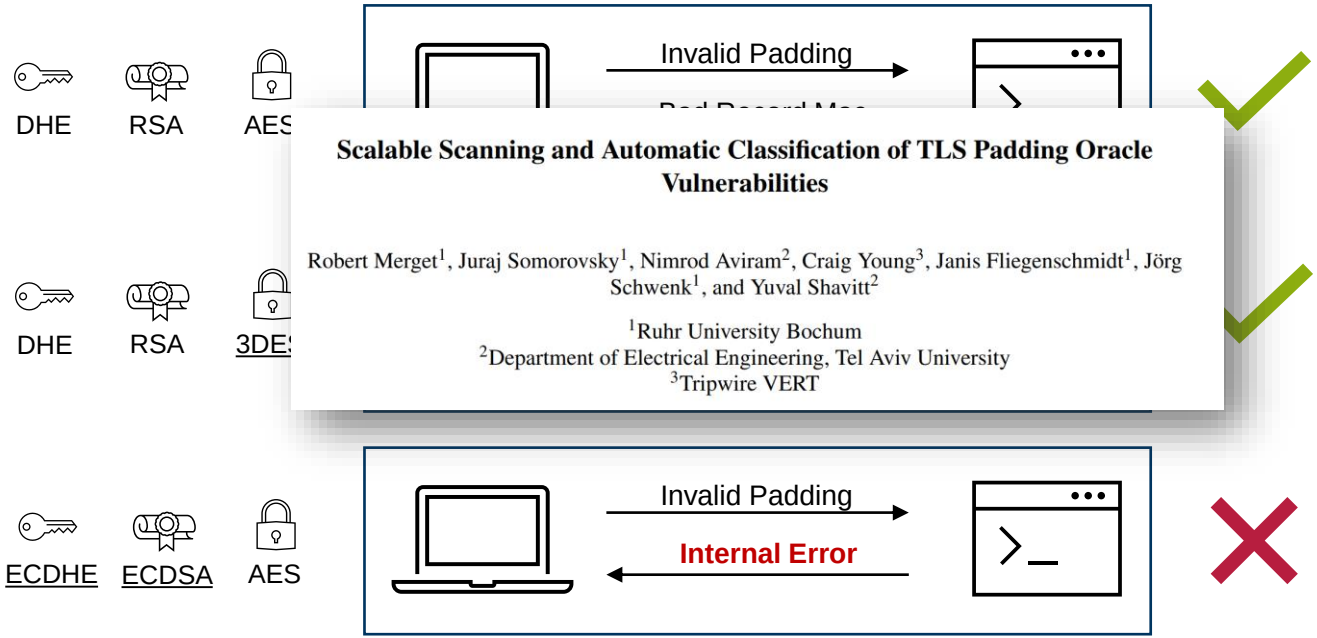
Parameters Example



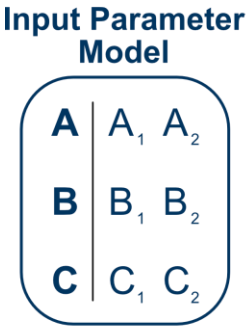
Parameters Example



Parameters Example



t-way Testing



t-way Testing

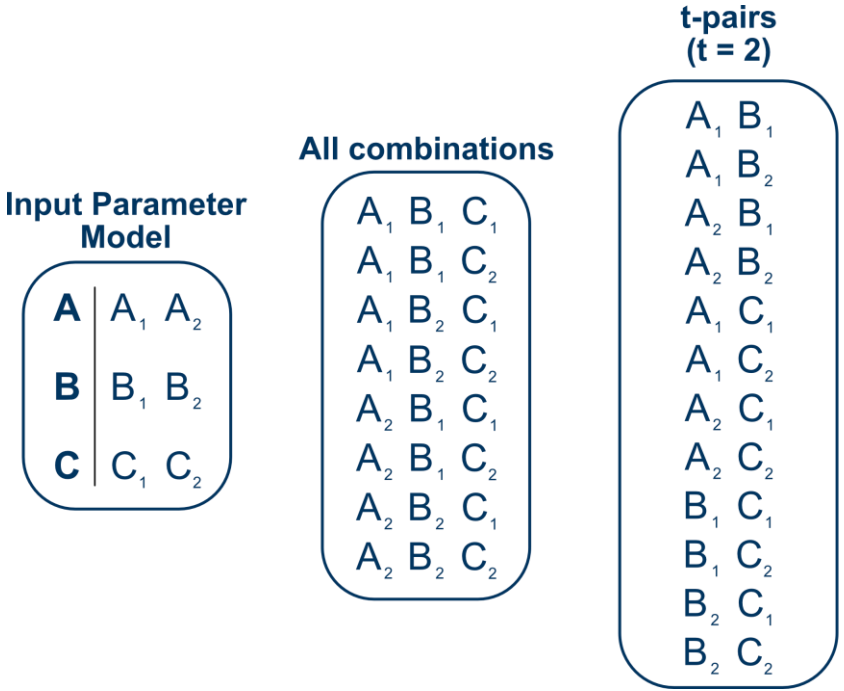
Input Parameter Model

A	A_1 A_2
B	B_1 B_2
C	C_1 C_2

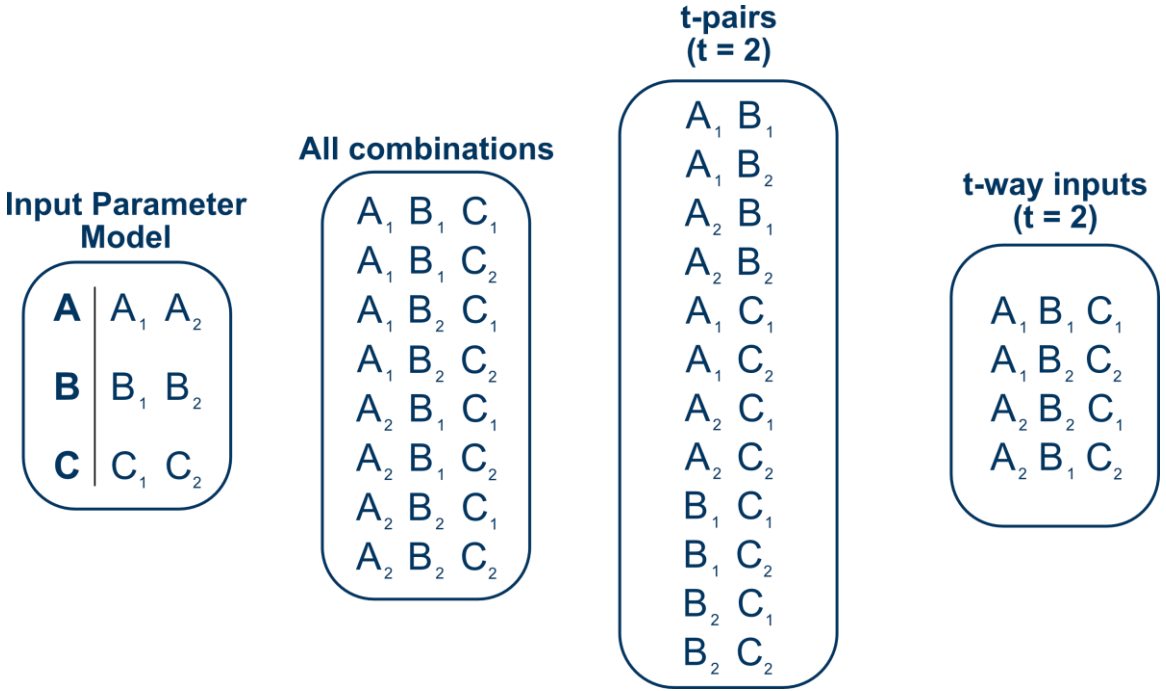
All combinations

A_1	B_1	C_1
A_1	B_1	C_2
A_1	B_2	C_1
A_1	B_2	C_2
A_2	B_1	C_1
A_2	B_1	C_2
A_2	B_2	C_1
A_2	B_2	C_2

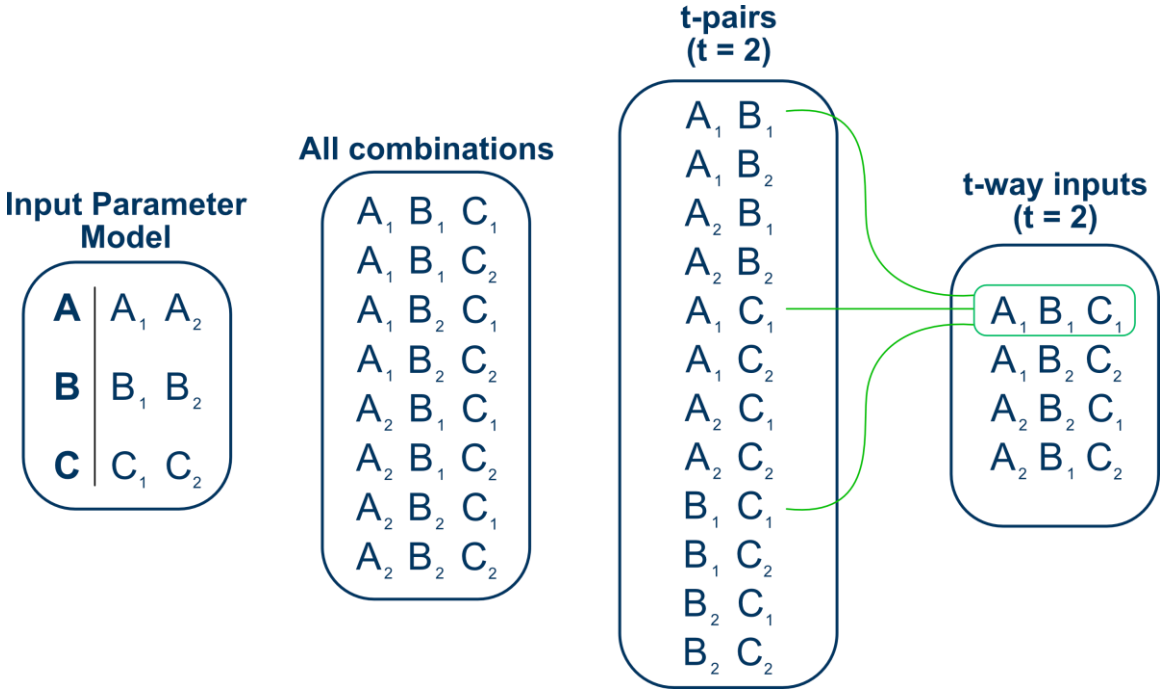
t-way Testing



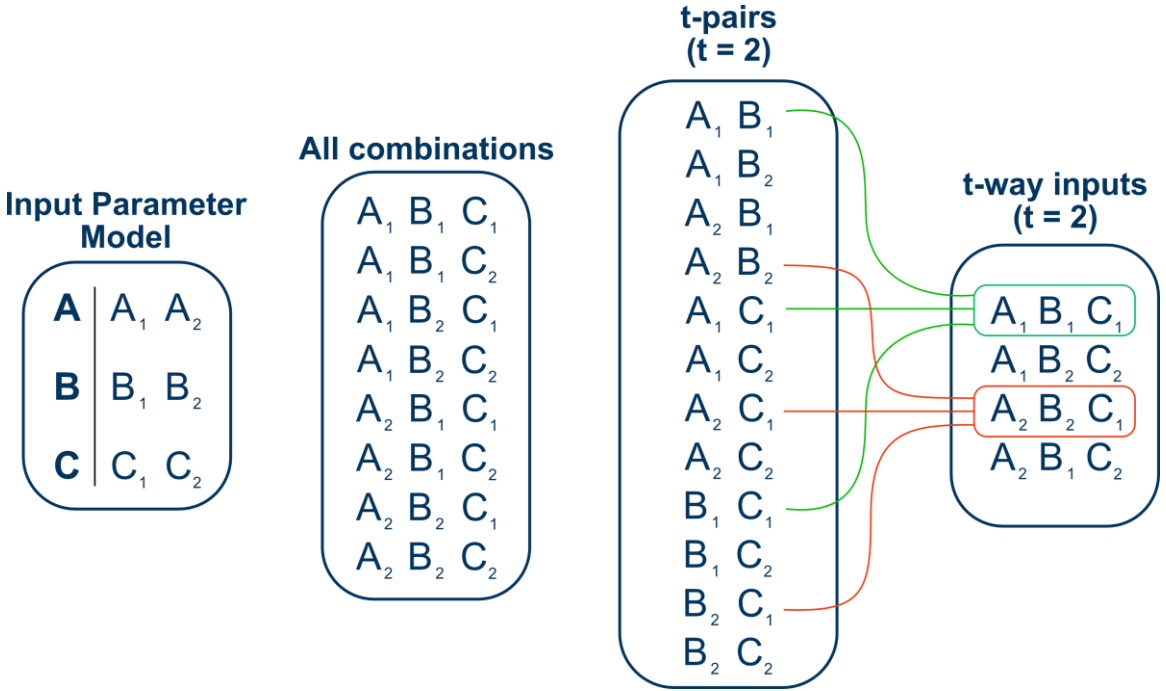
t-way Testing



t-way Testing



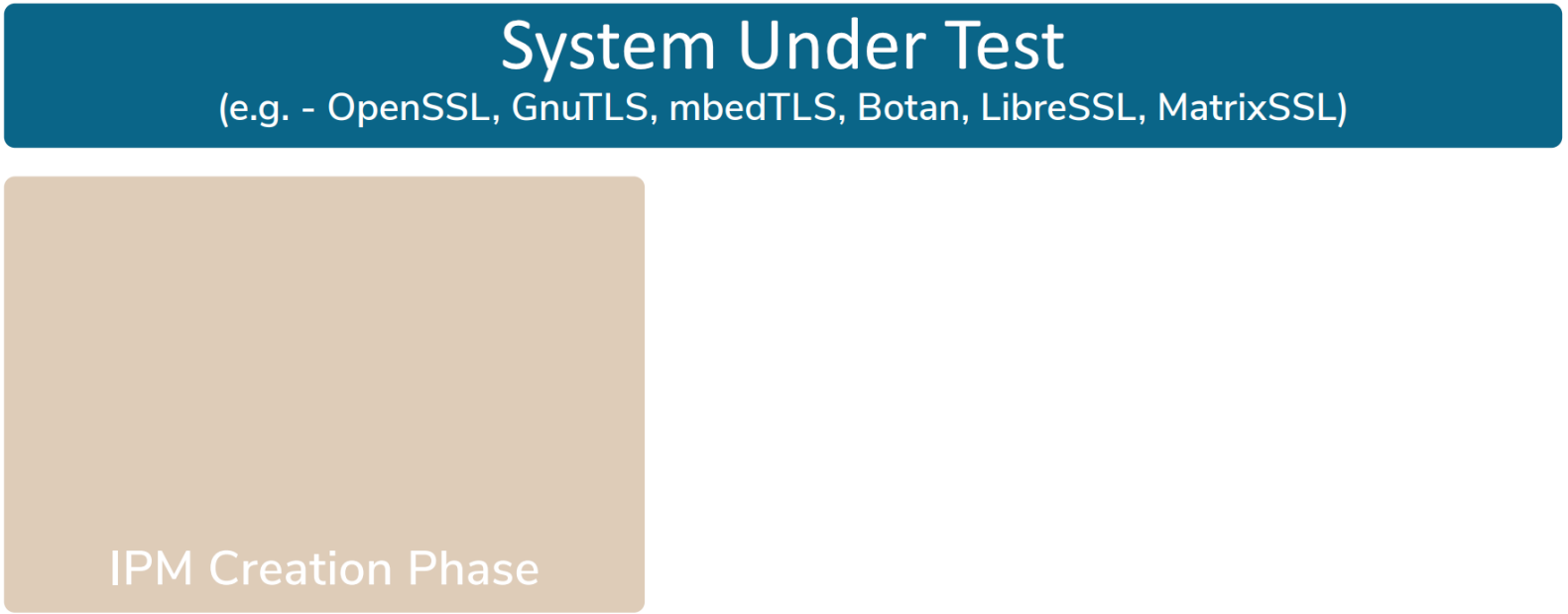
t-way Testing



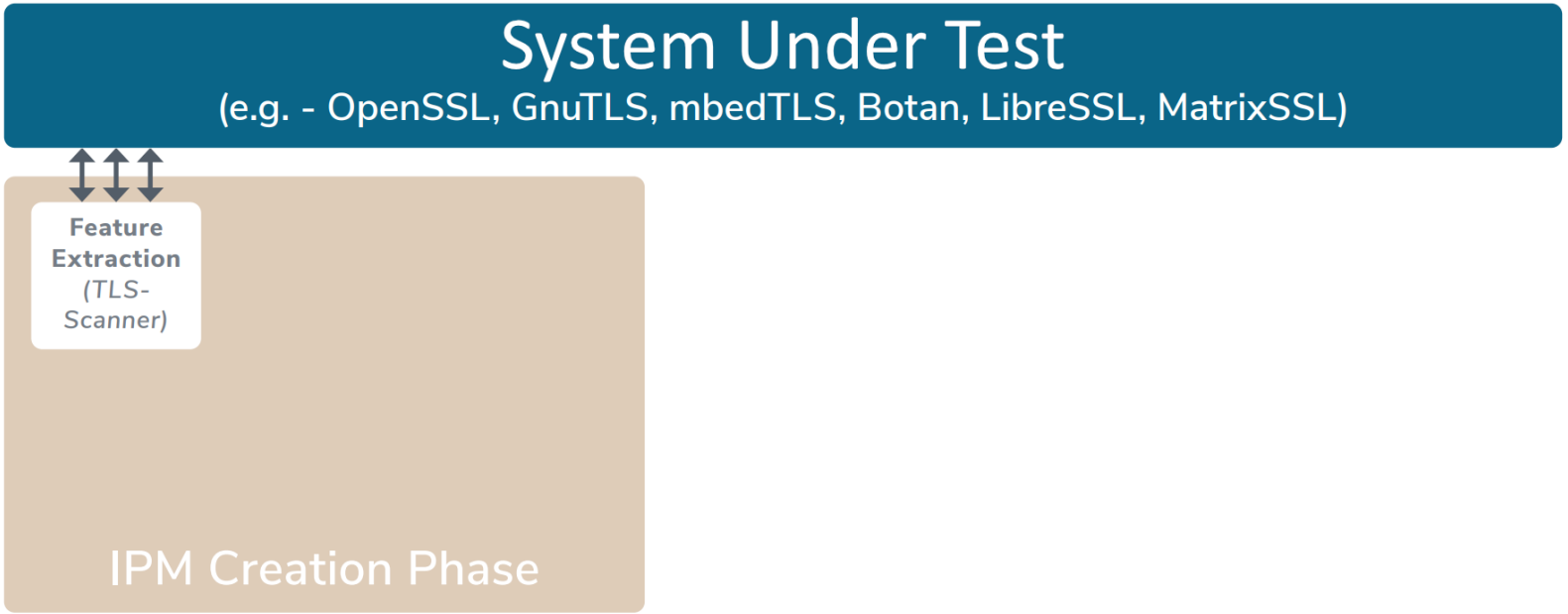
TLS-Anvil

- TLS test suite for **black box** evaluation of clients and servers
- **t-way coverage** of parameters with carefully constrained inputs
- Based on **mandatory** RFC statements
- Up to 14 parameters considered
- 408 test templates based on 13 TLS RFCs

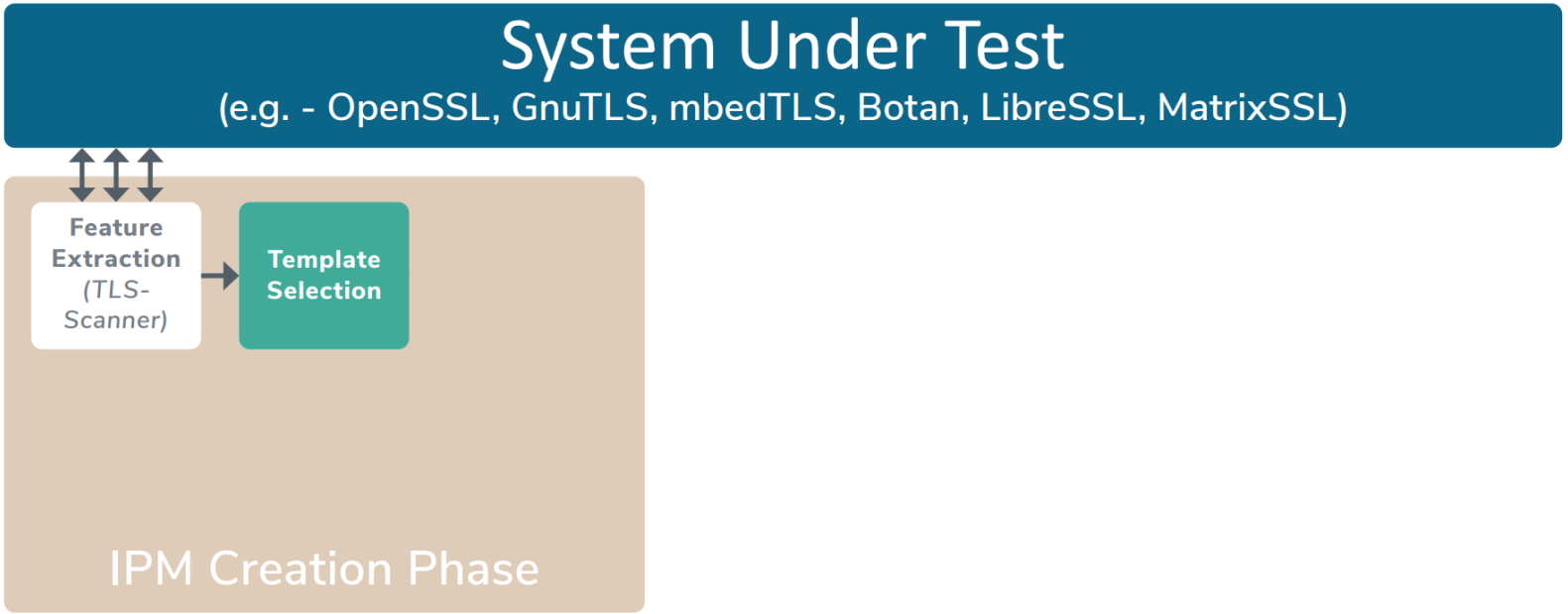
Execution


System Under Test
(e.g. - OpenSSL, GnuTLS, mbedTLS, Botan, LibreSSL, MatrixSSL)
IPM Creation Phase

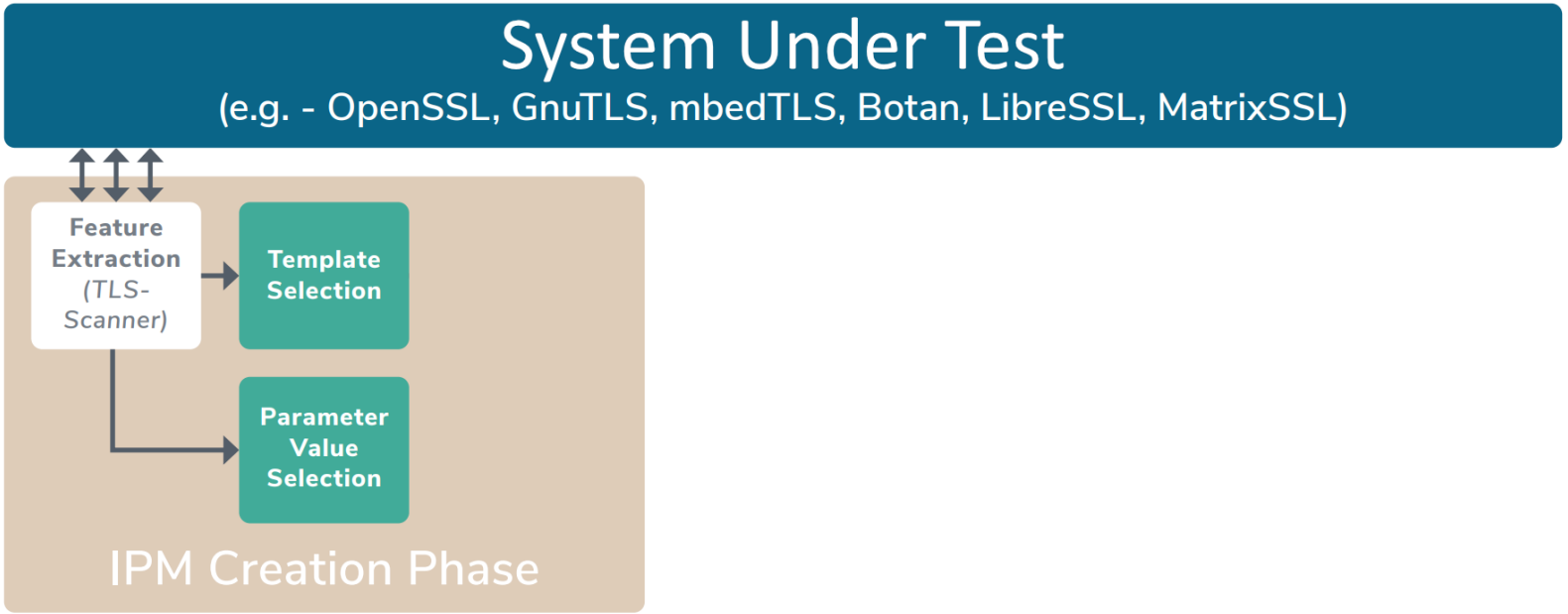
Execution


System Under Test
(e.g. - OpenSSL, GnuTLS, mbedTLS, Botan, LibreSSL, MatrixSSL)
Feature Extraction (TLS-Scanner)
IPM Creation Phase

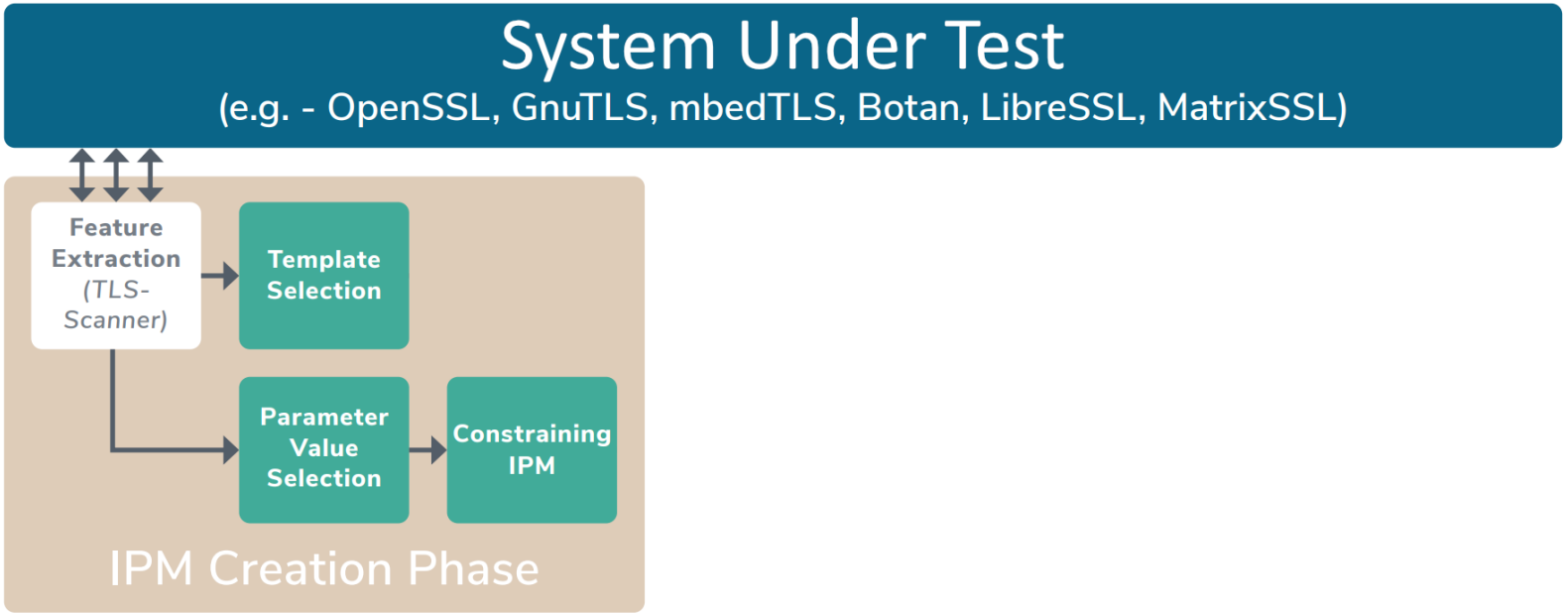
Execution


System Under Test
(e.g. - OpenSSL, GnuTLS, mbedTLS, Botan, LibreSSL, MatrixSSL)
Feature Extraction (TLS-Scanner)
Template Selection
IPM Creation Phase

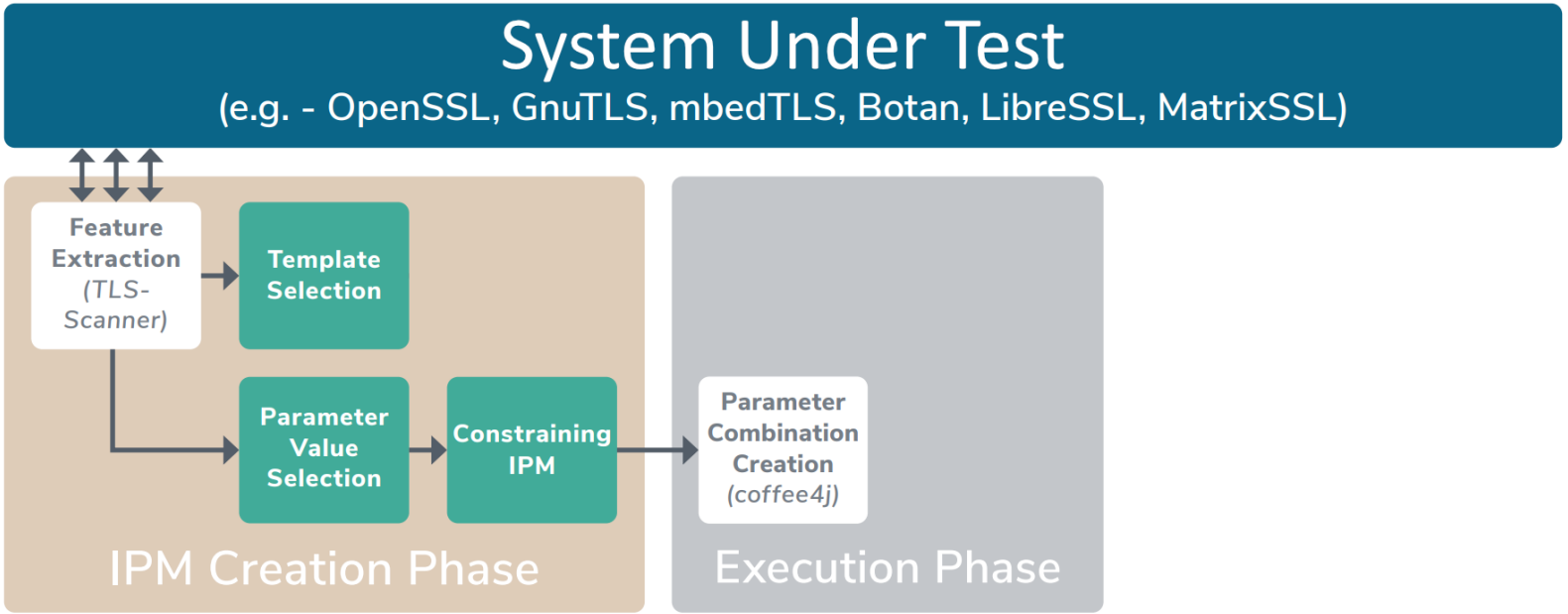
Execution


System Under Test
(e.g. - OpenSSL, GnuTLS, mbedTLS, Botan, LibreSSL, MatrixSSL)
Feature Extraction (TLS-Scanner)
Template Selection
Parameter Value Selection
IPM Creation Phase

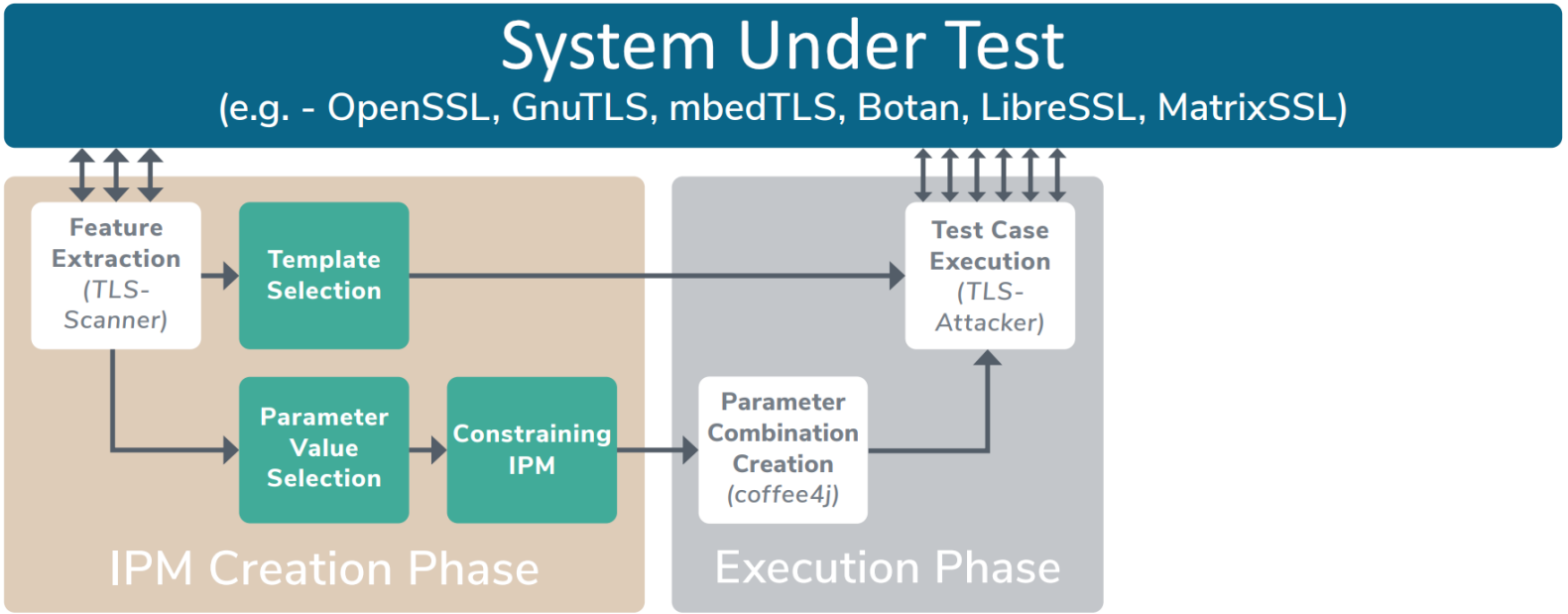
Execution


System Under Test
(e.g. - OpenSSL, GnuTLS, mbedTLS, Botan, LibreSSL, MatrixSSL)
Feature Extraction (TLS-Scanner)
Template Selection
Parameter Value Selection
Constraining IPM
IPM Creation Phase

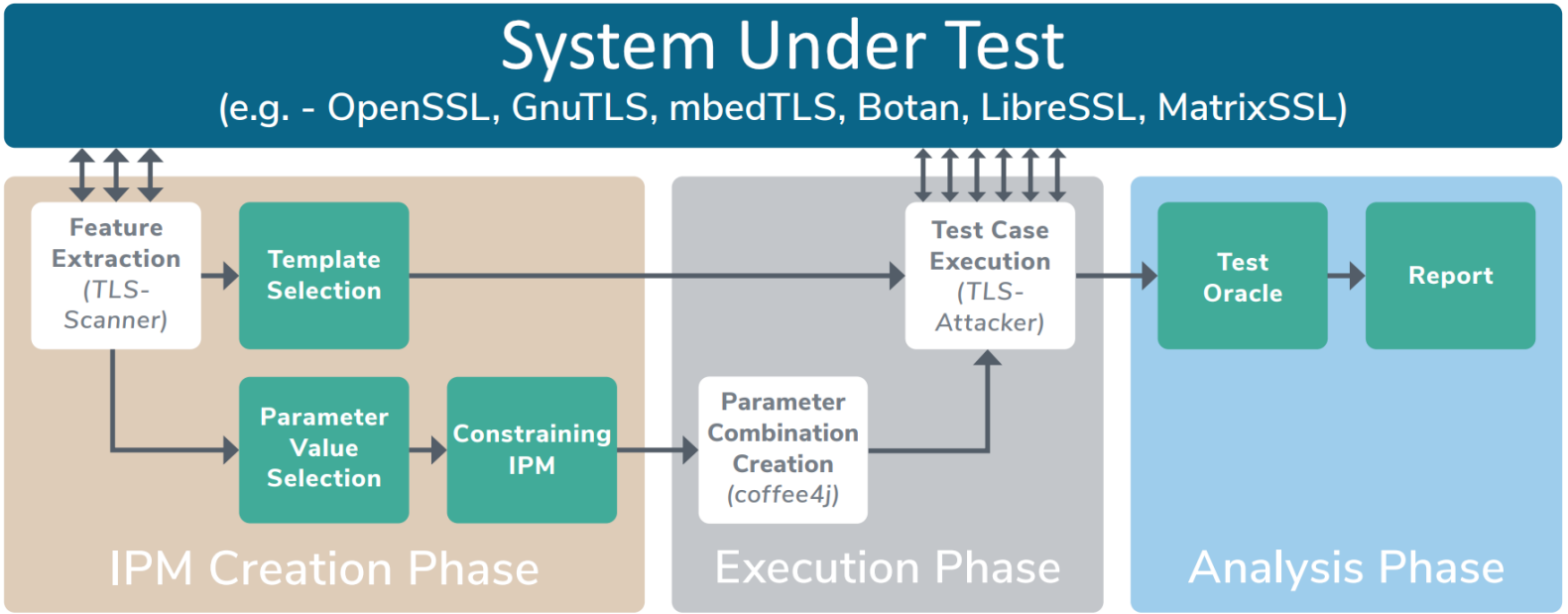
Execution


System Under Test
(e.g. - OpenSSL, GnuTLS, mbedTLS, Botan, LibreSSL, MatrixSSL)
Feature Extraction (TLS-Scanner)
Template Selection
Parameter Value Selection
Constraining IPM
Parameter Combination Creation (coffee4j)
IPM Creation Phase
Execution Phase

Execution


System Under Test
(e.g. - OpenSSL, GnuTLS, mbedTLS, Botan, LibreSSL, MatrixSSL)
Feature Extraction (TLS-Scanner)
Template Selection
Parameter Value Selection
Constraining IPM
IPM Creation Phase
Test Case Execution (TLS-Attacker)
Parameter Combination Creation (coffee4j)
Execution Phase

Execution



Performance Evaluation

	Strength $t = 3$		Strength $t = 2$		Strength $t = 1$	
Library	**Execution Time**	**Connections**	**Execution Time**	**Connections**	**Execution Time**	**Connections**
BearSSL	19.1h	61253	3.7h	12088	0.5h	1825
BoringSSL	14.8h	48929	3.4h	10587	0.6h	1844
Botan	6.1h	26394	1.3h	5485	0.3h	965
GnuTLS	31.2h	88730	6.1h	17328	0.9h	2726
LibreSSL	38.4h	121650	7.7h	25600	1h	3869
MatrixSSL	20.8h	57598	5.1h	12777	1.1h	2541
mbed TLS	67.2h	181265	9.6h	35087	0.9h	4041
NSS	33.6h	91521	7h	18774	1h	2922
OpenSSL	31.2h	95379	5.7h	18522	0.8h	2861
Rustls	13.6h	30761	3.4h	7517	0.1h	568
s2n	5.9h	26669	1.4h	5640	0.3h	1023
tlslite-ng	55.2h	118167	8.7h	22784	1.2h	3389
wolfSSL	50.4h	64079	11.5h	14618	2.6h	2986

Performance Evaluation

	Strength $t = 3$		Strength $t = 2$		Strength $t = 1$	
Library	**Execution Time**	**Connections**	**Execution Time**	**Connections**	**Execution Time**	**Connections**
BearSSL	19.1h	61253	3.7h	12088	0.5h	1825
BoringSSL	14.8h	48929	3.4h	10587	0.6h	1844
Botan	6.1h	26394	1.3h	5485	0.3h	965
GnuTLS	31.2h	88730	6.1h	17328	0.9h	2726
LibreSSL	38.4h	121650	7.7h	25600	1h	3869
MatrixSSL	20.8h	57598	5.1h	12777	1.1h	2541
mbed TLS	67.2h	181265	9.6h	35087	0.9h	4041
NSS	33.6h	91521	7h	18774	1h	2922
OpenSSL	31.2h	95379	5.7h	18522	0.8h	2861
Rustls	13.6h	30761	3.4h	7517	0.1h	568
s2n	5.9h	26669	1.4h	5640	0.3h	1023
tlslite-ng	55.2h	118167	8.7h	22784	1.2h	3389
wolfSSL	50.4h	64079	11.5h	14618	2.6h	2986

Performance Evaluation

	Strength $t = 3$		Strength $t = 2$		Strength $t = 1$	
Library	**Execution Time**	**Connections**	**Execution Time**	**Connections**	**Execution Time**	**Connections**
BearSSL	19.1h	61253	3.7h	12088	0.5h	1825
BoringSSL	14.8h	48929	3.4h	10587	0.6h	1844
Botan	6.1h	26394	1.3h	5485	0.3h	965
GnuTLS	31.2h	88730	6.1h	17328	0.9h	2726
LibreSSL	38.4h	121650	7.7h	25600	1h	3869
MatrixSSL	20.8h	57598	5.1h	12777	1.1h	2541
mbed TLS	67.2h	181265	9.6h	35087	0.9h	4041
NSS	33.6h	91521	7h	18774	1h	2922
OpenSSL	31.2h	95379	5.7h	18522	0.8h	2861
Rustls	13.6h	30761	3.4h	7517	0.1h	568
s2n	5.9h	26669	1.4h	5640	0.3h	1023
tlslite-ng	55.2h	118167	8.7h	22784	1.2h	3389
wolfSSL	50.4h	64079	11.5h	14618	2.6h	2986

Performance Evaluation

	Strength $t = 3$		Strength $t = 2$		Strength $t = 1$	
Library	**Execution Time**	**Connections**	**Execution Time**	**Connections**	**Execution Time**	**Connections**
BearSSL	19.1h	61253	3.7h	12088	0.5h	1825
BoringSSL	14.8h	48929	3.4h	10587	0.6h	1844
Botan	6.1h	26394	1.3h	5485	0.3h	965
GnuTLS	31.2h	88730	6.1h	17328	0.9h	2726
LibreSSL	38.4h	121650	7.7h	25600	1h	3869
MatrixSSL	20.8h	57598	5.1h	12777	1.1h	2541
mbed TLS	67.2h	181265	9.6h	35087	0.9h	4041
NSS	33.6h	91521	7h	18774	1h	2922
OpenSSL	31.2h	95379	5.7h	18522	0.8h	2861
Rustls	13.6h	30761	3.4h	7517	0.1h	568
s2n	5.9h	26669	1.4h	5640	0.3h	1023
tlslite-ng	55.2h	118167	8.7h	22784	1.2h	3389
wolfSSL	50.4h	64079	11.5h	14618	2.6h	2986

Performance Evaluation

	Strength $t = 3$		Strength $t = 2$		Strength $t = 1$	
Library	**Execution Time**	**Connections**	**Execution Time**	**Connections**	**Execution Time**	**Connections**
BearSSL	19.1h	61253	3.7h	12088	0.5h	1825
BoringSSL	14.8h	48929	3.4h	10587	0.6h	1844
Botan	6.1h	26394	1.3h	5485	0.3h	965
GnuTLS	31.2h	88730	6.1h	17328	0.9h	2726
LibreSSL	38.4h	121650	7.7h	25600	1h	3869
MatrixSSL	20.8h	57598	5.1h	12777	1.1h	2541
mbed TLS	67.2h	181265	9.6h	35087	0.9h	4041
NSS	33.6h	91521	7h	18774	1h	2922
OpenSSL	31.2h	95379	5.7h	18522	0.8h	2861
Rustls	13.6h	30761	3.4h	7517	0.1h	568
s2n	5.9h	26669	1.4h	5640	0.3h	1023
tlslite-ng	55.2h	118167	8.7h	22784	1.2h	3389
wolfSSL	50.4h	64079	11.5h	14618	2.6h	2986

239 RFC violations

Library
BearSSL
BoringSSL
Botan
GnuTLS
LibreSSL
MatrixSSL
mbed TLS
NSS
OpenSSL
Rustls
s2n
tlslite-ng
wolfSSL

239 RFC violations

Library	Exploitable Vulnerabilities
BearSSL	0
BoringSSL	0
Botan	0
GnuTLS	0
LibreSSL	0
MatrixSSL	2
mbed TLS	0
NSS	0
OpenSSL	0
Rustls	0
s2n	0
tlslite-ng	0
wolfSSL	1
	3

239 RFC violations

Library	Exploitable Vulnerabilities	Improper Cryptographic Operations
BearSSL	0	0
BoringSSL	0	0
Botan	0	0
GnuTLS	0	0
LibreSSL	0	1
MatrixSSL	2	2
mbed TLS	0	0
NSS	0	0
OpenSSL	0	0
Rustls	0	0
s2n	0	1
tlslite-ng	0	0
wolfSSL	1	1
	3	5

239 RFC violations

Library	Exploitable Vulnerabilities	Improper Cryptographic Operations	Interoperability Issues
BearSSL	0	0	1
BoringSSL	0	0	0
Botan	0	0	0
GnuTLS	0	0	1
LibreSSL	0	1	1
MatrixSSL	2	2	7
mbed TLS	0	0	1
NSS	0	0	0
OpenSSL	0	0	0
Rustls	0	0	1
s2n	0	1	0
tlslite-ng	0	0	0
wolfSSL	1	1	3
	3	5	15

239 RFC violations

Library	Exploitable Vulnerabilities	Improper Cryptographic Operations	Interoperability Issues	Wrong Alert Codes
BearSSL	0	0	1	15
BoringSSL	0	0	0	6
Botan	0	0	0	3
GnuTLS	0	0	1	9
LibreSSL	0	1	1	7
MatrixSSL	2	2	7	6
mbed TLS	0	0	1	14
NSS	0	0	0	7
OpenSSL	0	0	0	6
Rustls	0	0	1	15
s2n	0	1	0	13
tlslite-ng	0	0	0	2
wolfSSL	1	1	3	13
	3	5	15	116

239 RFC violations

Library	Exploitable Vulnerabilities	Improper Cryptographic Operations	Interoperability Issues	Wrong Alert Codes	Other
BearSSL	0	0	1	15	4
BoringSSL	0	0	0	6	3
Botan	0	0	0	3	3
GnuTLS	0	0	1	9	10
LibreSSL	0	1	1	7	6
MatrixSSL	2	2	7	6	16
mbed TLS	0	0	1	14	5
NSS	0	0	0	7	6
OpenSSL	0	0	0	6	7
Rustls	0	0	1	15	7
s2n	0	1	0	13	12
tlslite-ng	0	0	0	2	10
wolfSSL	1	1	3	13	11
	3	5	15	116	100

239 RFC violations

Library	Exploitable Vulnerabilities	Improper Cryptographic Operations	Interoperability Issues	Wrong Alert Codes	Other
BearSSL	0	0	1	15	4
BoringSSL	0	0	0	6	3
Botan	0	0	0	3	3
GnuTLS	0	0	1	9	10
LibreSSL	0	1	1	7	6
MatrixSSL	2	2	7	6	16
mbed TLS	0	0	1	14	5
NSS	0	0	0	7	6
OpenSSL	0	0	0	6	7
Rustls	0	0	1	15	7
s2n	0	1	0	13	12
tlslite-ng	0	0	0	2	10
wolfSSL	1	1	3	13	11
	3	5	15	116	100

Overall, most libraries still passed a high percentage of tests

Exploitable Vulnerabilities Found

- Padding Oracle in MatrixSSL through crash only for SHA-256 HMAC
- Denial-of-Service bug in MatrixSSL through malformed lengthfields
- Server Authentication bypass for wolfSSL using empty certificate message

Conclusion

- TLS-Anvil, a test suite based on t-way testing
- 239 RFC violations found including 3 exploitable vulnerabilities
- Worth exploring for more RFCs and other protcols e.g QUIC

https://tls-anvil.com https://github.com/tls-attacker/TLS-Anvil @marcelmaehren