

A Internet Evaluation Statistics

		min	25%	median	75%	max	average
CH_1_HappyFlow	States	2	7	9	9	16	8.36
	Hypotheses	2	5	31	158	3,454	123.87
	Queries Replied by Cache	83,974	423,352	907,320	2,572,937	278,606,819	4,000,033.98
	Queries Replied by SUL	7	541	1,760	3,675	37,434	2,692.9
	Symbols Used	336,545	2,195,518	4,287,020	11,847,074	1,317,893,626	18,649,320.90
	Received with Expectation	36	2,489	7,330	15,432	178,850	12,724.80
	Received Total	40	3,034	9,234	18,995	214,324	15,436.12
CH_1_Extended	Cache Conflicts	0	1	15	60	2,034	51.98
	States	4	14	15	19	30	15.57
	Hypotheses	3	95	264	640	14,045	562.72
	Queries Replied by Cache	167,695	8,658,513	22,006,064	58,568,008	839,996,752	48,756,511.94
	Queries Replied by SUL	939	26,739	48,048	70,691	147,734	51,099.30
	Symbols Used	758,924	44,440,894	108,897,878	281,722,099	4,107,762,442	237,882,777.32
	Received with Expectation	4,371	166,290	278,450	423,128	919,796	311,965.23
CH_1_Vuln	Received Total	5,914	196,480	332,622	503,468	1,089,777	370,128.83
	Cache Conflicts	0	15	50	127	3,081	109.71
	States	4	14	17	20	28	17.8
	Hypotheses	3	10	39	185	4,381	211.81
	Queries Replied by Cache	171,512	2,102,254	5,281,187	14,300,606	548,186,539	16,856,248.51
	Queries Replied by SUL	61	3,269	8,206	42,507	505,581	29,111.35
	Symbols Used	766,926	12,221,617	28,794,488	71,414,736	2,693,118,595	84,930,488.95
CH_1_All	Received with Expectation	161	16,490	46,927	186,681	1,803,995	130,485.5
	Received Total	222	19,957	55,344	231,222	2,338,176	161,056.35
	Cache Conflicts	0	0	4	23	1,149	30.87
	States	4	14	17	19	28	16.95
	Hypotheses	3	12	28	86	6,137	113.67
	Queries Replied by Cache	168,718	2,136,020	4,633,802	12,465,915	387,573,309	13,684,329.77
	Queries Replied by SUL	348	6,095	9,254	19,017	426,588	17,486.11
CH_2_HappyFlow	Symbols Used	759,803	11,702,652	25,815,202	65,358,696	1,892,015,764	70,194,596.5
	Received with Expectation	754	28,712	45,181	93,736	1,898,809	84,601.13
	Received Total	1,114	35,439	54,860	113,814	2,346,059	103,109.66
	Majority Votes	0	0	3	12	2,237	18.25
	States	2	7	9	9	13	8.16
	Hypotheses	2	3	3	6	12,822	33.21
	Queries Replied by Cache	84,004	369,698	377,623	624,743	390,632,827	1,764,639.82
CH_2_Extended	Queries Replied by SUL	16	417	700	1,208	41,176	1,526.46
	Symbols Used	335,561	1,992,386	2,010,499	3,183,494	1,642,501,005	8,458,824.79
	Received with Expectation	15	1,844	2,654	5,090	331,522	8,944.54
	Received Total	31	2,314	3,414	6,494	378,737	10,783.74
	Cache Conflicts	0	0	0	1	2,621	7.97
	States	4	14	15	19	27	15.78
	Hypotheses	3	14	45	171	14,842	282.37
CH_2_Extended	Queries Replied by Cache	168,508	2,165,210	5,975,916	20,595,337	1,708,823,334	34,036,563.29
	Queries Replied by SUL	357	6,306	11,494	24,597	577,743	24,935.60
	Symbols Used	757,388	12,178,816	31,601,852	106,119,486	8,141,049,170	168,274,454.15
	Received with Expectation	1,500	42,909	79,174	167,330	3,379,048	166,078.14
	Received Total	1,856	49,794	92,359	197,309	4,045,490	194,455.40
	Cache Conflicts	0	1	6	27	1,650	38.42

CH_2_Vuln	States	4	15	19	23	35	19.15
	Hypotheses	3	8	17	118	4,950	195.4
	Queries Replied by Cache	169,619	1,991,488	3,701,622	15,849,095	845,367,195	21,734,174.70
	Queries Replied by SUL	11	830	2,796	20,320	429,963	17,558.60
	Symbols Used	760,634	11,654,684	21,616,690	84,156,921	4,819,503,470	114,464,729.74
	Received with Expectation	66	5,425	17,069	101,670	1,725,314	87,745.23
	Received Total	78	6,290	20,110	122,569	2,175,399	106,222.68
CH_2_All	Cache Conflicts	0	0	1	10	693	17.82
	States	4	19	21	23	35	21.71
	Hypotheses	3	16	46	203	6,111	209.35
	Queries Replied by Cache	170,324	3,366,250	7,780,684	28,182,164	754,060,646	26,793,968.59
	Queries Replied by SUL	44	6,144	10,606	23,664	216,053	19,453.87
	Symbols Used	763,218	19,490,968	43,431,742	147,600,155	3,715,929,044	138,585,399.0
	Received with Expectation	132	31,711	54,870	126,115	1,064,390	100,894.36
CH_3_HappyFlow	Received Total	177	38,263	66,266	150,439	1,290,892	121,481.64
	Cache Conflicts	0	0	3	18	511	19.46
	States	2	7	9	9	13	8.11
	Hypotheses	2	2	3	5	1,177	10.52
	Queries Replied by Cache	84,020	373,127	377,566	484,845	97,839,766	917,525.71
	Queries Replied by SUL	18	395	701	894	75,109	1,404.60
	Symbols Used	335,545	1,991,861	1,997,115	2,511,536	482,607,601	4,635,837.54
CH_3_Extended	Received with Expectation	17	1,477	2,390	3,367	627,187	8,102.40
	Received Total	35	1,906	3,131	4,306	720,413	9,857.92
	Cache Conflicts	0	0	0	1	340	2.66
	States	4	13	15	19	27	15.65
	Hypotheses	3	11	29	114	4,926	179.28
	Queries Replied by Cache	168,156	1,607,528	4,123,286	14,183,236	559,552,791	21,791,421.22
	Queries Replied by SUL	226	5,208	8,626	20,508	214,062	18,377.42
CH_3_Vuln	Symbols Used	756,350	9,134,717	22,328,831	75,487,835	2,643,104,101	109,062,644.96
	Received with Expectation	1,136	33,313	57,054	134,231	1,317,859	118,717.74
	Received Total	1,372	39,166	66,592	156,836	1,556,874	139,472.22
	Cache Conflicts	0	1	4	16	605	24.0
	States	4	17	25	29	41	23.81
	Hypotheses	3	14	86	746	8,156	589.69
	Queries Replied by Cache	172,414	3,209,807	14,818,153	98,870,635	1,590,930,557	77,829,124.50
CH_3_All	Queries Replied by SUL	10	3,424	33,319	90,013	454,657	56,532.15
	Symbols Used	770,705	18,673,008	83,299,702	513,030,890	8,656,385,112	413,077,046.33
	Received with Expectation	51	18,703	150,290	429,113	2,358,937	271,385.46
	Received Total	62	22,281	187,638	523,089	2,750,672	330,986.58
	Cache Conflicts	0	0	7	57	943	48.53
	States	4	18	25	30	39	23.96
	Hypotheses	3	18	63	260	7,023	309.60
CH_3_HappyFlow	Queries Replied by Cache	169,246	4,244,567	12,356,191	40,860,751	969,321,238	46,066,047.16
	Queries Replied by SUL	37	5,153	18,044	40,610	419,943	31,615.80
	Symbols Used	760,035	23,909,740	70,106,460	220,865,904	4,958,711,590	243,545,457.36
	Received with Expectation	125	29,322	88,914	206,930	2,131,469	161,799.96
	Received Total	167	35,226	105,925	248,668	2,566,313	195,166.3
	Cache Conflicts	0	0	4	24	972	27.26

Table 1: Performance statistics for the state learning of the 1304 results presented in our paper. The final *Heartbeat* alphabet has been excluded as its size varies significantly between hosts depending on their supported cipher suites.

B Symbol Chains

Previous Input	Next Input	Condition
<start>	TLS12_CLIENT_HELLO	-
TLS12_CLIENT_HELLO	CLIENT_KEY_EXCHANGE	NOT_CLIENT_AUTH_REQUESTED
TLS12_CLIENT_HELLO	BLEICHENBACHER	NOT_CLIENT_AUTH_REQUESTED
TLS12_CLIENT_HELLO	CERTIFICATE	CLIENT_AUTH_REQUESTED
CERTIFICATE	CLIENT_KEY_EXCHANGE	CLIENT_AUTH_REQUESTED
CERTIFICATE	BLEICHENBACHER	CLIENT_AUTH_REQUESTED
CLIENT_KEY_EXCHANGE	CERTIFICATE_VERIFY	CLIENT_AUTH_REQUESTED
BLEICHENBACHER	CERTIFICATE_VERIFY	CLIENT_AUTH_REQUESTED
CERTIFICATE_VERIFY	ANY_CCS	CLIENT_AUTH_REQUESTED
CLIENT_KEY_EXCHANGE	ANY_CCS	NOT_CLIENT_AUTH_REQUESTED
BLEICHENBACHER	ANY_CCS	NOT_CLIENT_AUTH_REQUESTED
RESUMING_HELLO	ANY_CCS	IN_RESUMPTION_FLOW
CCS	FINISHED	NOT_BLEICHENBACHER_PATH
FINISHED	ANY_APP_DATA	HANDSHAKE_FINISHED_CORRECTLY
ANY_APP_DATA	ANY_APP_DATA	HANDSHAKE_FINISHED_CORRECTLY
RESET_CONNECTION	TLS12_CLIENT_HELLO	-
RESET_CONNECTION	RESUMING_HELLO	CAN_RESUME_CORRECTLY_TLS12
ANY_APP_DATA	RESUMING_HELLO	CAN_RESUME_CORRECTLY_TLS12
FINISHED	RESUMING_HELLO	CAN_RESUME_CORRECTLY_TLS12
FINISHED	TLS12_CLIENT_HELLO	-
FINISHED	TLS13_CLIENT_HELLO	REJECTS_RENEGOTIATION
FINISHED	HRR_ENFORCING_CLIENT_HELLO	REJECTS_RENEGOTIATION
ANY_CLIENT_HELLO	RESUMING_HELLO	REJECTS_RENEGOTIATION
ANY_CLIENT_HELLO	ANY_APP_DATA	REJECTS_RENEGOTIATION
<any>	RESET_CONNECTION	-
<any>	HEARTBEAT	-
<start>	TLS13_CLIENT_HELLO	-
<start>	HRR_ENFORCING_HELLO	-
HRR_ENFORCING_HELLO	TLS13_CLIENT_HELLO	-
TLS13_CLIENT_HELLO	FINISHED	NOT_CLIENT_AUTH_REQUESTED
TLS13_CLIENT_HELLO	CERTIFICATE	CLIENT_AUTH_REQUESTED
CERTIFICATE	CERTIFICATE_VERIFY	CLIENT_AUTH_REQUESTED
FINISHED	KEY_UPDATE	-
KEY_UPDATE	ANY_APP_DATA	-
ANY_APP_DATA	ANY_APP_DATA	-
ANY_APP_DATA	KEY_UPDATE	-
RESET_CONNECTION	RESUMING_HELLO	CAN_RESUME_CORRECTLY_TLS13
RESUMING_HELLO	FINISHED	-
RESET_CONNECTION	TLS13_CLIENT_HELLO	-
RESET_CONNECTION	HRR_ENFORCING_HELLO	-
<any>	RESET_CONNECTION	-
<any>	ANY_CCS	HANDSHAKE_UNFINISHED

Table 2: The *symbol chains* used to trace the HSG of TLS protocol flows. Note that not all chains are mandatory as some protocol features are optional.

C State Machine Illustrations

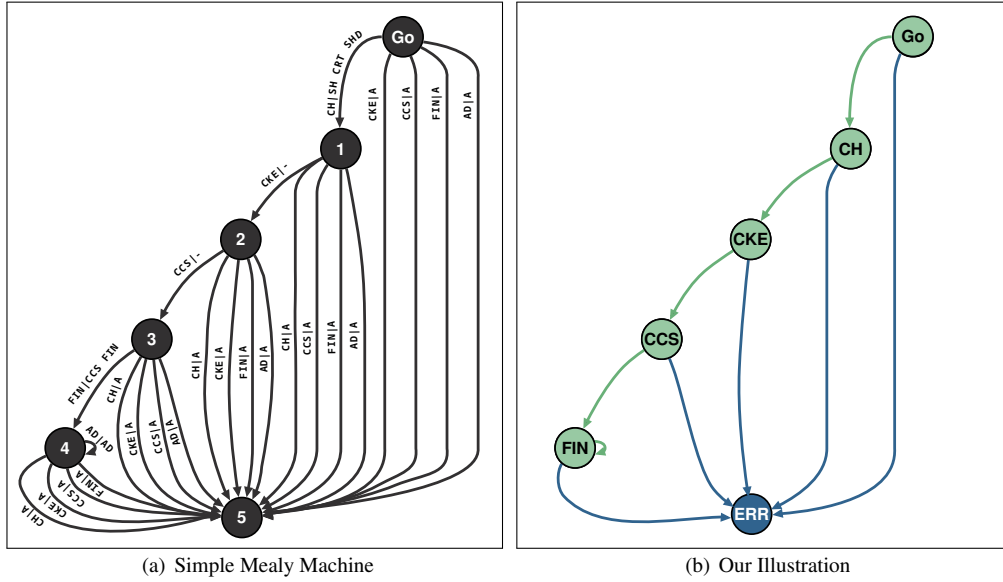


Figure 1: Depiction of a simple mealy machine showing all $\langle \text{input} \rangle \mid \langle \text{output} \rangle$ pairs compared to the illustration we use in our paper. As shown, we merge edges of invalid inputs transitioning into the error state (ERR). We further omit any inputs and outputs. Instead, we apply names to states based on the messages the server received when we entered the state. For example, after the server receives the *ClientHello* and sent its reply, we reached the 'CH' state. Note that in some illustrations, we also omit the error state for better readability.

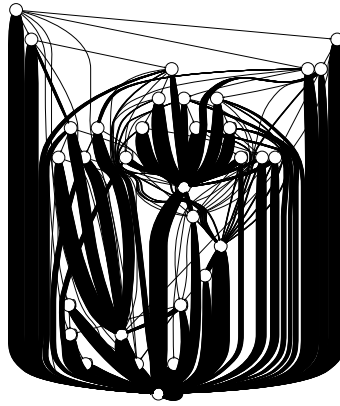


Figure 2: An extracted state machine with all 32 states and 1856 edges showcasing the complexity of real state machines implemented in real-world servers. Labels indicating the input and output symbols have been omitted.