

# CodeSonar Analysis Report

generated by Administrator on Wed Aug 23 15:52:20 2017  
for analysis crypto analysis 1

# Summary

Table 1: crypto analysis 1 Summary

Active Warnings	File Count	Project Name	Time Started	Time Finished	Machine
322	420	crypto	Mon Jul 10 15:29:01 2017	Mon Jul 10 15:34:31 2017	eduECFA.kent.ac.uk

# Warnings

Figure 1: crypto analysis 1, Warnings by Class

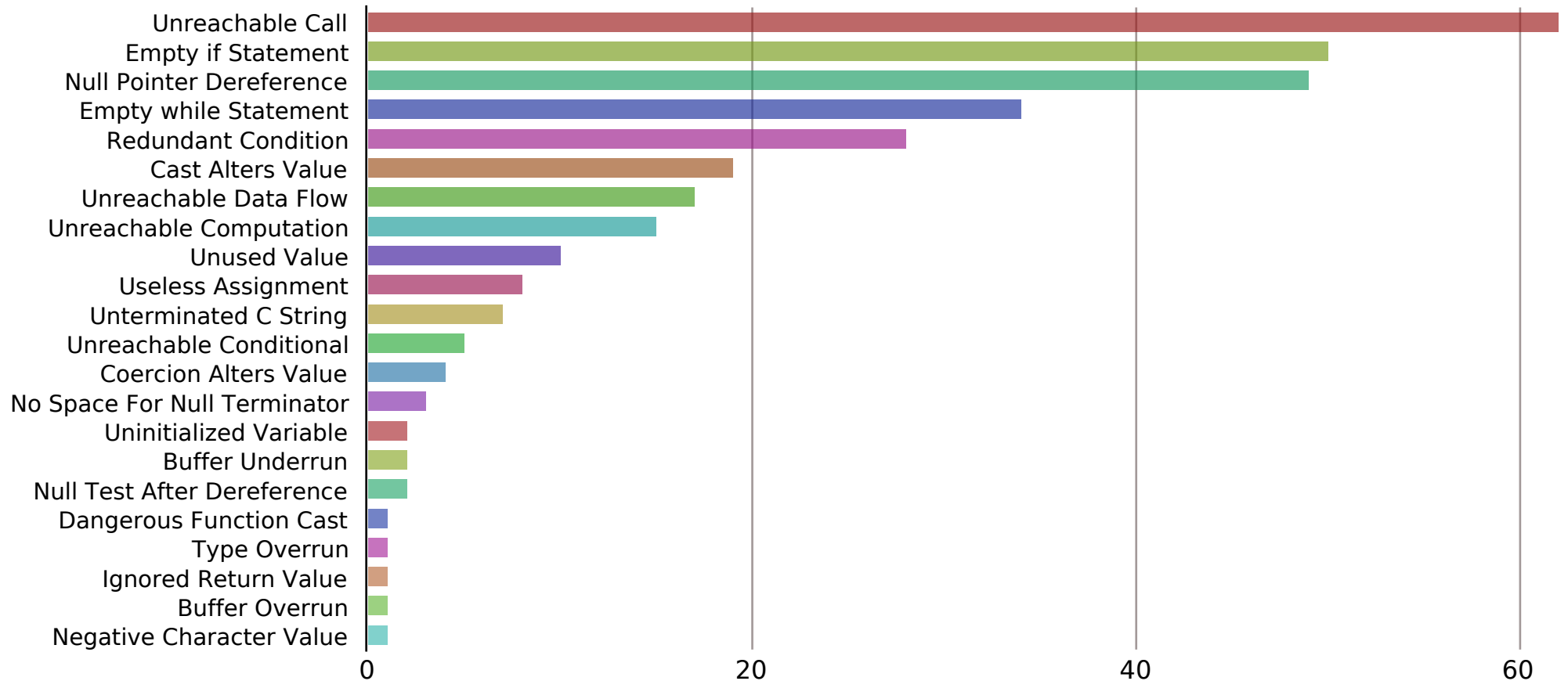


Table 2: crypto analysis 1, Warnings by Class

Table 2: crypto analysis 1, Warnings by Class

Warning Class	Active Warnings
Unreachable Call	62
Empty if Statement	50
Null Pointer Dereference	49
Empty while Statement	34
Redundant Condition	28
Cast Alters Value	19
Unreachable Data Flow	17
Unreachable Computation	15
Unused Value	10
Useless Assignment	8
Unterminated C String	7
Unreachable Conditional	5
Coercion Alters Value	4
No Space For Null Terminator	3
Buffer Underrun	2
Uninitialized Variable	2

Table 3: crypto analysis 1, Warnings by File

Warning Class	Active Warnings
Null Test After Dereference	2
Type Overrun	1
Dangerous Function Cast	1
Buffer Overrun	1
Ignored Return Value	1
Negative Character Value	1

Table 3: crypto analysis 1, Warnings by File

File	Active Warnings	Total Lines	Language
resolv.c	22	1521	C
rpl-dag.c	15	1631	C
rpl-icmp6.c	14	1367	C
cfs-coffee.c	14	1346	C
ccm-test.c	11	708	C
cc2538-rf.c	10	1126	C
gcm-test.c	10	669	C
contikimac.c	9	1102	C

Table 3: crypto analysis 1, Warnings by File

File	Active Warnings	Total Lines	Language
ccm.c	9	142	C
lpm.c	8	390	C
gcm.c	8	125	C
sha256.c	7	356	C
ctr-test.c	7	352	C
aes.c	7	330	C
cbc-test.c	7	696	C
ecb-test.c	7	662	C
cbc-mac-test.c	7	506	C
framer-802154.c	6	274	C
rpl-ext-header.c	6	665	C
startup-gcc.c	6	330	C
cfs-coffee-arch.c	6	144	C
uip6.c	6	2362	C
cc2538-ccm-star.c	5	130	C
websocket.c	5	724	C
psock.c	5	319	C

Table 3: crypto analysis 1, Warnings by File

File	Active Warnings	Total Lines	Language
usb-arch.c	5	1295	C
sha256-test.c	5	261	C
cbc-mac.c	5	91	C
uip-ds6.c	4	716	C
nbr-table.c	4	483	C
tcpip.c	4	849	C
rpl.c	4	355	C
websocket-http-client.c	4	347	C
ecc-algorithm.c	4	201	C
csma.c	4	507	C
rpl-dag-root.c	3	268	C
phase.c	3	252	C
soc.c	3	108	C
ctr.c	3	77	C
sys-ctrl.c	3	135	C
udp-socket.c	3	199	C
sicslowpan.c	2	1806	C

Table 3: crypto analysis 1, Warnings by File

File	Active Warnings	Total Lines	Language
rpl-of0.c	2	238	C
dhcpc.c	2	431	C
random.c	2	136	C
ip64-addr.c	2	123	C
usb-core.c	2	631	C
rpl-timers.c	2	497	C
frame802154e-ie.c	2	585	C
tcp-socket.c	2	409	C
rpl-nbr-policy.c	2	256	C
sensors.c	1	137	C
simple-udp.c	1	183	C
ifft.c	1	168	C
contiki-main.c	1	252	C
uip-ds6-route.c	1	721	C
serial-line.c	1	137	C
dbg.c	1	117	C
watchdog.c	1	109	C



Table 3: crypto analysis 1, Warnings by File

File	Active Warnings	Total Lines	Language
frame802154.c	1	623	C
slip.c	1	457	C
uip-icmp6.c	1	378	C
cc2538-aes-128.c	1	121	C
uart.c	1	398	C
core_cm3.h	1	1776	C
uip-ds6-nbr.c	1	361	C
ieee-addr.c	1	92	C
adc.c	1	99	C
rtimer-arch.c	1	158	C
clock.c	1	255	C
slip-arch.c	1	86	C
nullrdc.c	1	368	C
usb-serial.c	1	307	C
ctimer.c	1	175	C
etimer.c	1	272	C
stimer.c	0	163	C

Table 3: crypto analysis 1, Warnings by File

File	Active Warnings	Total Lines	Language
ecc-driver.c	0	559	C
websocket.h	0	113	C
bignum-driver.c	0	1064	C
uip-nameserver.c	0	236	C
websocket-http-client.h	0	123	C
compower.c	0	98	C
vdd3-sensor.c	0	78	C
vdd3-sensor.h	0	71	C
cc2538-sensors.h	0	72	C
ifft.h	0	58	C
cc2538-temp-sensor.h	0	71	C
button-sensor.c	0	252	C
uip-split.c	0	158	C
cc2538-temp-sensor.c	0	77	C
als-sensor.c	0	95	C
procinit.c	0	48	C
bignum-driver.h	0	462	C

Table 4: crypto analysis 1, Warning Instances

File	Active Warnings	Total Lines	Language
als-sensor.h	0	63	C
ctr.h	0	89	C
pwm.c	0	369	C
pwm.h	0	182	C
me_tabs.c	0	121	C
mt.c	0	109	C
ctype.h	0	169	C

(Showing 100 of 420 Files)

Table 4: crypto analysis 1, Warning Instances

Score	Warning Class	File Name	Procedure Name	Line Number	State	Owner
68	Negative Character Value	resolv.c	dns_name_isequal	400	None	None
63	Uninitialized Variable	frame802154.c	frame802154_check_dest_panid	214	None	None
62	Uninitialized Variable	uip-ds6-route.c	uip_ds6_route_lookup	272	None	None
61	No Space For Null Terminator	resolv.c	remove_trailing_dots	1252	None	None
60	Unterminated C String	resolv.c	resolv_set_hostname	1095	None	None
60	Unterminated C String	resolv.c	resolv_set_hostname	1096	None	None

Table 4: crypto analysis 1, Warning Instances

Score	Warning Class	File Name	Procedure Name	Line Number	State	Owner
60	Unterminated C String	resolv.c	resolv_set_hostname	1097	None	None
59	No Space For Null Terminator	websocket.c	parse_url	143	None	None
58	Unterminated C String	resolv.c	resolv_lookup	1380	None	None
58	Unterminated C String	resolv.c	resolv_query	1287	None	None
58	Unterminated C String	resolv.c	resolv_query	1312	None	None
58	Unterminated C String	resolv.c	resolv_query	1319	None	None
57	No Space For Null Terminator	resolv.c	resolv_query	1312	None	None
51	Null Test After Dereference	frame802154e-ie.c	frame80215e_create_ie_tsch_channel_hopping_sequence	303	None	None
51	Null Test After Dereference	rpl-dag.c	rpl_print_neighbor_list	110	None	None
49	Null Pointer Dereference	cbc-mac.c	cbc_mac_auth_start	59	None	None
49	Null Pointer Dereference	cfs-coffee-arch.c	cfs_coffee_arch_erase	81	None	None
49	Null Pointer Dereference	startup-gcc.c	reset_handler	317	None	None
49	Null Pointer Dereference	gcm.c	gcm_auth_crypt_start	63	None	None
49	Null Pointer Dereference	aes.c	aes_load_keys	69	None	None
49	Null Pointer Dereference	aes.c	aes_load_keys	81	None	None
49	Null Pointer Dereference	ctr.c	ctr_crypt_start	62	None	None
49	Null Pointer Dereference	ccm.c	ccm_auth_crypt_start	74	None	None

Table 4: crypto analysis 1, Warning Instances

Score	Warning Class	File Name	Procedure Name	Line Number	State	Owner
49	Null Pointer Dereference	sha256.c	sha256_process	262	None	None
49	Null Pointer Dereference	cbc-mac-test.c	process_thread_cbc_mac_test_process	484	None	None
49	Null Pointer Dereference	cbc-test.c	process_thread_cbc_test_process	674	None	None
49	Null Pointer Dereference	ccm-test.c	process_thread_ccm_test_process	637	None	None
49	Null Pointer Dereference	ccm-test.c	process_thread_ccm_test_process	685	None	None
49	Null Pointer Dereference	ctr-test.c	process_thread_ctr_test_process	330	None	None
49	Null Pointer Dereference	ecb-test.c	process_thread_ecb_test_process	640	None	None
49	Null Pointer Dereference	gcm-test.c	process_thread_gcm_test_process	646	None	None
49	Null Pointer Dereference	sha256-test.c	process_thread_sha256_test_process	240	None	None
49	Null Pointer Dereference	cfs-coffee-arch.c	cfs_coffee_arch_write	125	None	None
49	Null Pointer Dereference	cfs-coffee-arch.c	cfs_coffee_arch_write	101	None	None
49	Null Pointer Dereference	sha256.c	sha256_process	273	None	None
49	Null Pointer Dereference	cbc-mac-test.c	process_thread_cbc_mac_test_process	451	None	None
49	Null Pointer Dereference	cbc-test.c	process_thread_cbc_test_process	646	None	None
49	Null Pointer Dereference	ecb-test.c	process_thread_ecb_test_process	613	None	None
49	Null Pointer Dereference	cfs-coffee-arch.c	cfs_coffee_arch_write	115	None	None
49	Null Pointer Dereference	ctr-test.c	process_thread_ctr_test_process	301	None	None

Table 4: crypto analysis 1, Warning Instances

Score	Warning Class	File Name	Procedure Name	Line Number	State	Owner
49	Null Pointer Dereference	gcm-test.c	process_thread_gcm_test_process	565	None	None
49	Null Pointer Dereference	ccm-test.c	process_thread_ccm_test_process	599	None	None
49	Null Pointer Dereference	soc.c	soc_print_info	99	None	None
49	Null Pointer Dereference	cbc-mac.c	cbc_mac_auth_get_result	78	None	None
49	Null Pointer Dereference	ccm.c	ccm_auth_crypt_get_result	104	None	None
49	Null Pointer Dereference	gcm.c	gcm_auth_crypt_get_result	84	None	None
49	Null Pointer Dereference	cbc-mac.c	cbc_mac_auth_get_result	85	None	None
49	Null Pointer Dereference	ccm.c	ccm_auth_crypt_get_result	98	None	None
49	Null Pointer Dereference	gcm.c	gcm_auth_crypt_get_result	91	None	None
49	Null Pointer Dereference	tcpip.c	tcpip_uipcall	792	None	None
48	Null Pointer Dereference	rpl-icmp6.c	dao_input_storing	667	None	None
48	Null Pointer Dereference	resolv.c	process_thread_resolv_process	1174	None	None
48	Null Pointer Dereference	rpl-dag-root.c	rpl_dag_root_init_dag_immediately	215	None	None
48	Null Pointer Dereference	rpl-dag.c	rpl_add_dag	1220	None	None
48	Null Pointer Dereference	rpl-dag.c	rpl_print_neighbor_list	106	None	None
48	Null Pointer Dereference	nbr-table.c	nbr_table_add_lladdr	368	None	None
47	Null Pointer Dereference	rpl.c	rpl_remove_routes_by_nexthop	218	None	None

Table 4: crypto analysis 1, Warning Instances

Score	Warning Class	File Name	Procedure Name	Line Number	State	Owner
47	Coercion Alters Value	websocket.c	websocket_open	591	None	None
47	Null Pointer Dereference	rpl-dag.c	rpl_print_neighbor_list	113	None	None
47	Null Pointer Dereference	rpl-icmp6.c	dao_input_storing	770	None	None
47	Null Pointer Dereference	rpl-dag.c	rpl_get_any_dag	1041	None	None
46	Coercion Alters Value	usb-arch.c	ep0_get_data_pkt	943	None	None
46	Coercion Alters Value	uip6.c	uip_process	1546	None	None
45	Coercion Alters Value	ifft.c	ifft	123	None	None
44	Null Pointer Dereference	uip-icmp6.c	uip_icmp6_send	281	None	None
42	Type Overrun	usb-arch.c	fill_buffers	885	None	None
42	Cast Alters Value	rpl-dag-root.c	set_global_address	153	None	None
42	Cast Alters Value	rpl.c	rpl_link_neighbor_callback	260	None	None
42	Cast Alters Value	tcpip.c	udp_broadcast_new	328	None	None
42	Cast Alters Value	rpl-icmp6.c	dis_output	268	None	None
42	Cast Alters Value	rpl.c	rpl_init	342	None	None
42	Cast Alters Value	dhcpc.c	create_msg	149	None	None
42	Cast Alters Value	resolv.c	process_thread_resolv_process	1174	None	None
42	Cast Alters Value	uip-ds6.c	uip_ds6_init	118	None	None

Table 4: crypto analysis 1, Warning Instances

Score	Warning Class	File Name	Procedure Name	Line Number	State	Owner
42	Cast Alters Value	resolv.c	mdns_write_announce_records	522	None	None
42	Cast Alters Value	resolv.c	process_thread_resolv_process	1208	None	None
42	Cast Alters Value	resolv.c	newdata	907	None	None
42	Cast Alters Value	uip-ds6.c	uip_ds6_init	127	None	None
42	Cast Alters Value	resolv.c	check_entries	756	None	None
42	Cast Alters Value	uip-ds6.c	uip_ds6_init	130	None	None
42	Cast Alters Value	rpl-icmp6.c	dio_output	613	None	None
42	Cast Alters Value	rpl-dag-root.c	rpl_dag_root_init_dag_immediately	224	None	None
42	Cast Alters Value	resolv.c	newdata	1070	None	None
41	Cast Alters Value	uip6.c	uip_udp_new	593	None	None
41	Cast Alters Value	core_cm3.h	NVIC_SetPriority	1541	None	None
41	Null Pointer Dereference	rpl-dag.c	rpl_select_dag	806	None	None
41	Null Pointer Dereference	rpl-dag.c	rpl_select_dag	773	None	None
39	Null Pointer Dereference	rpl-dag.c	rpl_select_dag	764	None	None
39	Buffer Underrun	nbr-table.c	remove_key	195	None	None
38	Dangerous Function Cast	uip-ds6-nbr.c	uip_ds6_neighbors_init	79	None	None
34	Buffer Overrun	sicslowpan.c	uncompress_addr	611	None	None



Table 4: crypto analysis 1, Warning Instances

Score	Warning Class	File Name	Procedure Name	Line Number	State	Owner
33	Buffer Underrun	resolv.c	remove_trailing_dots	1251	None	None
27	Ignored Return Value	contikimac.c	send_packet	708	None	None
23	Unused Value	cc2538-ccm-star.c	aead	88	None	None
23	Unused Value	ccm.c	ccm_auth_crypt_start	67	None	None
23	Unused Value	ctr.c	ctr_crypt_start	57	None	None
23	Unused Value	gcm.c	gcm_auth_crypt_start	59	None	None
23	Unused Value	rpl-ext-header.c	rpl_remove_header	627	None	None
23	Unused Value	rpl-icmp6.c	dio_output	539	None	None
23	Unused Value	rpl-icmp6.c	set16	184	None	None

(Showing 100 of 322 Warnings)

# Analysis Metrics

Table 5: crypto analysis 1 Metrics

Metric Name	Value
Blank Lines	9565
Code Lines	44698
Comment Lines	36937
Include file instances	157
Lines with Code	50392
Lines with Comments	42631
Mixed Lines	5694
Top-level file instances	157
Total Lines	96894
User-defined functions	1223

Table 6: crypto analysis 1 File Metrics Summary

# File Metrics

Table 6: crypto analysis 1 File Metrics Summary

Metric Name	Max	Min	Avg
Blank Lines	388	0	22.77
Code Lines	1403	0	106.42
Comment Lines	1302	0	87.95
Cyclomatic Complexity	330	0	13.28
Lines with Code	1476	0	119.98
Lines with Comments	1422	0	101.50
Mixed Lines	649	0	13.56
Modified Cyclomatic Complexity	330	0	12.69
Taint Propagator Total	0	0	0
Taint Sink Total	11	0	0.34
Taint Source Total	0	0	0
Total Lines	2362	2	230.70

Table 7: crypto analysis 1 File Metrics Details

Table 7: crypto analysis 1 File Metrics Details

File	Total Lines	Lines with Code	Lines with Comments	Code Lines	Comment Lines	Blank Lines
uip6.c	2362	1476	723	1403	650	236
uip.h	2219	698	1422	578	1302	219
sicslowpan.c	1806	1060	604	1012	556	190
core_cm3.h	1776	952	1085	303	436	388
rpl-dag.c	1631	1273	215	1256	198	160
resolv.c	1521	1039	313	986	260	222
cmsis_gcc.h	1373	734	382	713	361	278
rpl-icmp6.c	1367	1018	225	983	190	159
cfs-coffee.c	1346	962	239	946	223	161
usb-arch.c	1295	962	163	959	160	173
uip-nd6.c	1147	825	280	779	234	88
cc2538-rf.c	1126	742	255	734	247	137
contikimac.c	1102	776	219	752	195	131
bignum-driver.c	1064	577	273	577	273	214
pka.h	871	191	723	112	644	36
tcpip.c	849	629	184	582	137	83

Table 7: crypto analysis 1 File Metrics Details

File	Total Lines	Lines with Code	Lines with Comments	Code Lines	Comment Lines	Blank Lines
reent.h	794	558	220	462	124	112
stdio.h	769	622	126	577	81	66
websocket.c	724	489	173	488	172	63
uip-ds6-route.c	721	526	157	493	124	71
uip-ds6.c	716	528	158	495	125	63
ccm-test.c	708	632	302	390	60	16
cdefs.h	707	446	211	415	180	81
udma.h	704	294	462	184	352	58
cbc-test.c	696	629	167	517	55	12
uipopt.h	684	159	487	122	450	75
rfcore-xreg.h	673	284	668	4	388	1
gcm-test.c	669	598	215	438	55	16
rpl-ext-header.c	665	440	154	431	145	80
ecb-test.c	662	595	151	499	55	12
gpio.h	635	240	536	66	362	33
usb-core.c	631	553	25	543	15	63
frame802154.c	623	401	194	380	173	49

Table 7: crypto analysis 1 File Metrics Details

File	Total Lines	Lines with Code	Lines with Comments	Code Lines	Comment Lines	Blank Lines
strformat.c	617	550	13	545	8	59
frame802154e-ie.c	585	458	119	434	95	32
uip-nd6.h	575	203	346	183	326	46
ecc-driver.c	559	290	156	290	156	113
aes.h	544	303	432	103	232	9
process.h	531	90	386	88	384	57
features.h	515	276	205	270	199	40
trickle-timer.h	514	76	418	65	407	31
contiki-conf.h	510	265	222	224	181	64
csma.c	507	369	99	364	94	44
cbc-mac-test.c	506	438	135	358	55	13
rpl-timers.c	497	345	112	336	103	49
nbr-table.c	483	331	132	328	129	23
settings.c	475	284	104	281	101	90
queuebuf.c	473	365	103	345	83	25
stdint.h	466	388	34	387	33	45
bignum-driver.h	462	76	366	75	365	21

Table 7: crypto analysis 1 File Metrics Details

File	Total Lines	Lines with Code	Lines with Comments	Code Lines	Comment Lines	Blank Lines
slip.c	457	343	90	327	74	40
stddef.h	443	313	166	246	99	31
ieeefp.h	434	303	68	293	58	73
dhcpc.c	431	337	55	336	54	40
trickle-timer.c	410	243	128	238	123	44
tcp-socket.c	409	307	66	307	66	36
rpl-private.h	408	258	127	224	93	57
psock.h	404	59	321	49	311	34
uart.c	398	255	95	255	95	48
lpm.c	390	184	163	183	162	44
process.c	388	233	113	229	109	46
uip-ds6.h	385	208	152	179	123	54
uip-icmp6.c	378	247	89	245	87	44
tcpip.h	378	55	283	53	281	42
packetbuf.h	371	153	185	141	173	45
pwm.c	369	241	84	241	84	44
nullrdc.c	368	271	87	247	63	34

Table 7: crypto analysis 1 File Metrics Details

File	Total Lines	Lines with Code	Lines with Comments	Code Lines	Comment Lines	Blank Lines
spi.c	362	241	91	240	90	31
uip-ds6-nbr.c	361	261	93	251	83	17
uart.h	360	149	338	14	203	8
sha256.c	356	211	108	211	108	37
usb-regs.h	355	127	316	27	216	12
rpl.c	355	243	77	240	74	38
settings.h	352	173	134	156	117	62
ctr-test.c	352	285	109	231	55	12
websocket-http-client.c	347	247	73	246	72	28
sys-ctrl.h	342	150	249	81	180	12
rpl-conf.h	341	146	183	127	164	31
rpl.h	340	182	155	164	137	21
gptimer.h	335	137	325	8	196	2
stdlib.h	335	291	28	277	14	30
aes.c	330	179	103	179	103	48
startup-gcc.c	330	254	234	83	63	13
list.c	330	123	182	123	182	25



Table 7: crypto analysis 1 File Metrics Details

File	Total Lines	Lines with Code	Lines with Comments	Code Lines	Comment Lines	Blank Lines
sicslowpan.h	327	111	188	97	174	42
pt.h	322	57	231	56	230	35
psock.c	319	200	87	200	87	32
rpl-mrhof.c	316	204	105	186	87	25
usb-serial.c	307	217	66	217	66	24
tcp-socket.h	299	63	212	62	211	25
radio.h	294	62	186	61	185	47
config.h	286	218	35	210	27	41
contiki-default-conf.h	285	95	185	63	153	37
mtarch.c	285	145	129	145	129	11
cfs.h	285	61	200	60	199	25
ioc.h	278	154	147	124	117	7
noncoresec.c	275	181	76	170	65	29
framer-802154.c	274	172	80	165	73	29
announcement.h	274	35	213	34	212	27
etimer.c	272	171	74	171	74	27

(Showing 100 of 420 Files)