APPENDIX

Table 1: **Context-free properties extracted from existing CVEs, relevant protocol software RFCs, GitHub issues, and an understanding of program implementations. Note: A *match* indicates that program behavior which satisfies the specified property constitutes a bug, whereas a *fail* denotes that program behavior violating the property is considered a bug.**

Prop	Program	Description of the context-free property
LN1	`luna`(0.1.1)	$S \rightarrow A\ S\ B \mid B\ S\ A \mid S\ S \mid \epsilon$ **(fail)** The number of calls to the **A**(`scan_string()`) function is **not equal to** the number of **B**(`buf_assignment`) operations.
LN2	`luna`(0.1.1)	$S \rightarrow Q\ B \mid S\ B \mid S\ S$ $Q \rightarrow A\ Q\ B \mid B\ Q\ A \mid Q\ Q \mid \epsilon$ **(match)** The number of times **A**(`Selfexpr_notnull`) is **fewer than** the number of calls to the **B**(`visit_unary_op()`) function.
LN3	`luna`(0.1.1)	$S \rightarrow Q\ P \mid S\ P \mid S\ S$ $P \rightarrow B \mid C$ $Q \rightarrow A\ Q\ P \mid P\ Q\ A \mid Q\ Q \mid \epsilon$ **(match)** The number of occurrences of the **A**(`RK_Cnot0`) event is **fewer than** the combined number of occurrences of the **B**(`LUNA_OP_MOD`) and **C**(`LUNA_OP_DIV`) events.
MJ1	`mujs`(1.0.6)	$S \rightarrow Q\ B \mid S\ B \mid S\ S$ $Q \rightarrow A\ Q\ B \mid B\ Q\ A \mid Q\ Q \mid \epsilon$ **(match)** The number of calls to the **A**(`js_error()`) function is **less than** the number of occurrences of the **B**(`js_regexec_less0`) event.
MJ2	`mujs`(1.0.6)	$S \rightarrow Q\ B \mid S\ B \mid S\ S$ $Q \rightarrow A\ Q\ B \mid B\ Q\ A \mid Q\ Q \mid \epsilon$ **(match)** The number of calls to the **A**(`die_overflow()`) function is **less than** the number of occurrences of the **B**(`g_yymin_yymaxREPINF`) event.
MJ3	`mujs`(1.0.8)	$S \rightarrow Q\ B \mid S\ B \mid S\ S$ $Q \rightarrow A\ Q\ B \mid B\ Q\ A \mid Q\ Q \mid \epsilon$ **(match)** The number of calls to the **A**(`die_sequence()`) function is **less than** the number of occurrences of the **B**(`missing_end_of_string`) event.
MJ4	`mujs`(1.0.9)	$S \rightarrow Q\ B \mid S\ B \mid S\ S$ $Q \rightarrow A\ Q\ B \mid B\ Q\ A \mid Q\ Q \mid \epsilon$ **(match)** The number of calls to the **A**(`jsG_markobject()`) function is **less than** the number of occurrences of the **B**(`obj_gcmark_notmark`) event.
MJ5	`mujs`(1.0.9)	$S \rightarrow A\ S\ B \mid B\ S\ A \mid S\ S \mid \epsilon$ **(fail)** The number of calls to the **A**(`jsR_run()`) function is **not equal to** the number of occurrences of the **B**(`OP_RETURN`) event.
LV3	`Live555`(0.92)	$S \rightarrow A\ Q \mid A\ S \mid S\ S$ $Q \rightarrow A\ Q\ B \mid B\ Q\ A \mid Q\ Q \mid \epsilon$ **(match)**

		After establishing the connection, the number of times the first valid **A**(`setup request`) is received is **greater than** the number of times `a` **B**`(valid MediaSource)` is created.
LV4	`Live555`(0.92)	$S \rightarrow Q\ B \mid S\ B \mid S\ S$ $Q \rightarrow A\ Q\ B \mid B\ Q\ A \mid Q\ Q \mid \epsilon$ **(match)** After establishing the connection, the number of **A**(`valid MediaTable entries`) is **fewer than** the number of **B**(`valid setup requests`).
TD4	`TinyDTLS`(0.9-rcl)	$S \rightarrow Q\ P \mid S\ P \mid S\ S$ $P \rightarrow B\ C$ $Q \rightarrow A\ Q\ P \mid P\ Q\ A \mid Q\ Q \mid \epsilon$ **(match)** The number of times the server rejects and **B**(`sends an Alert`) is **fewer than** the number of occurrences of the sequence where the server receives a **B**(`ClientHello`), gives a **B**`(HelloVerifyRequest) response`, and then receives an `over-large packet`.
EV1	`Exiv2`(0.27.6)	$S \rightarrow Q\ B \mid S\ B \mid S\ S$ $Q \rightarrow A\ Q\ B \mid B\ Q\ A \mid Q\ Q \mid \epsilon$ **(match)** The number of occurrences of the **A**(`err_return`) event is **less than** the number of occurrences of the **B**(`total_out_of_bounds`) event.
OS1	`OpenSSL`(1.0.2)	$S \rightarrow Q\ A\ C$ $Q \rightarrow A\ Q\ B \mid B\ Q\ A \mid Q\ Q \mid Q\ A \mid A\ Q \mid \epsilon$ **(match)** The number of occurrences of the **A**(`Sig_A`) event is **greater than** the number of occurrences of the **B**(`Slen_A`) event, and it concludes with the sequence of `Sig_A` followed by **C**(`Slen_U`) events.
OS2	`OpenSSL`(1.1.0)	$S \rightarrow Q\ B \mid S\ B \mid S\ S$ $Q \rightarrow A\ Q\ B \mid B\ Q\ A \mid Q\ Q \mid \epsilon$ **(match)** The number of calls to the **A**(`SSLerr()`) function is **less than** the number of occurrences of the **B**(`ssl_generate_pkey_isnull`) event.
OS3	`OpenSSL`(1.1.1)	$S \rightarrow Q\ A\ C$ $Q \rightarrow A\ Q\ B \mid B\ Q\ A \mid Q\ Q \mid Q\ A \mid A\ Q \mid \epsilon$ **(match)** The number of occurrences of the **A**(`Tmpsig_A`) event is **greater than** the number of occurrences of the **B**(`Tmpslen_A`) event, and it concludes with the sequence of `Tmpsig_A` followed by **C**(`Tmpslen_U`) events.
LA1	`lua`(5.4.3)	$S \rightarrow A\ S\ B \mid B\ S\ A \mid S\ S \mid \epsilon$ **(fail)** The number of occurrences of the event **A** (`status_NotOK`) is **not equal to** the number of occurrences of the event **B**(`L_nCcalls_increment`).
LA2	`lua`(5.4.2)	$S \rightarrow A\ S\ B \mid B\ S\ A \mid S\ S \mid \epsilon$ **(fail)** The number of occurrences of the event **A** (`n_LQ_nextra`) is **not equal to** the number of occurrences of the event **B**(`Notfind`).

Table 2: Grammar Complexity Metrics for Context-Free Properties

Property	`Program`	**# Prod. Rules**	**# Non-ter.**	**# Ter.**
LN1	`luna(0.1.1)`	6	3	3
LN2	`luna(0.1.1)`	9	4	3
LN3	`luna(0.1.1)`	11	5	4
MJ1	`mujs(1.0.6)`	9	4	3
MJ2	`mujs(1.0.6)`	9	4	3
MJ3	`mujs(1.0.8)`	9	4	3
MJ4	`mujs(1.0.9)`	9	4	3
MJ5	`mujs(1.0.9)`	6	3	3
LV3	`Live555(0.92)`	9	4	3
LV4	`Live555(0.92)`	9	4	3
TD4	`TinyDTLS(0.9-rc1)`	10	5	4
EV1	`Exiv2(0.27.6)`	9	4	3
OS1	`OpenSSL(1.0.2)`	10	5	4
OS2	`OpenSSL(1.1.0)`	9	4	3
OS3	`OpenSSL(1.1.1)`	10	5	4
LA1	`lua(5.4.3)`	6	3	3
LA2	`lua(5.4.2)`	6	3	3