

Uso degli strumenti SPARK

Corso di Laurea Magistrale in
Sicurezza Informatica: Infrastrutture e Applicazioni
Università di Pisa – Polo di La Spezia
C. Montangero
Anno accademico 2009/10

Package Standard

```
package Standard is
  type Boolean is (False, True);
  type Integer is range -(2 ** 31) .. +(2 ** 31 - 1);
  subtype Natural is Integer range 0 .. +(2 ** 31 - 1);
  subtype Positive is Integer range 1 .. +(2 ** 31 - 1);
  type Short_Integer is range -(2 ** 15) .. +(2 ** 15 - 1);
  ...
```

- Examiner non vede i valori degli attributi
- Serve il file di configurazione del target
 - switch /config

File di configurazione (.cfg)

package Standard is

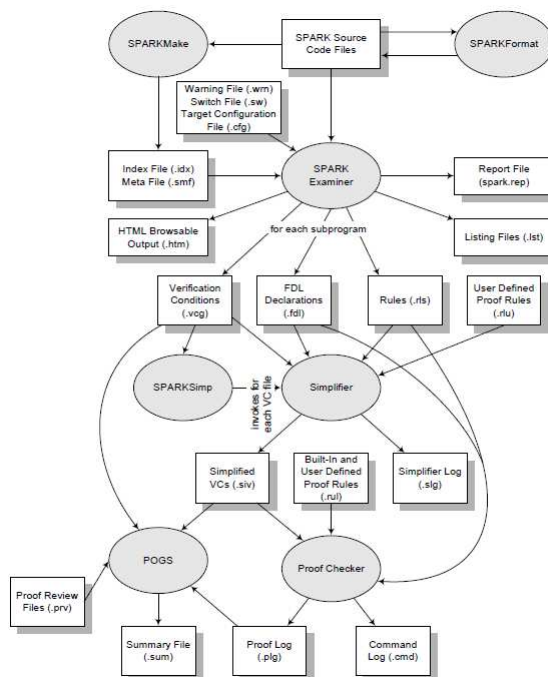
 type Integer is range -2147483648 .. 2147483647;

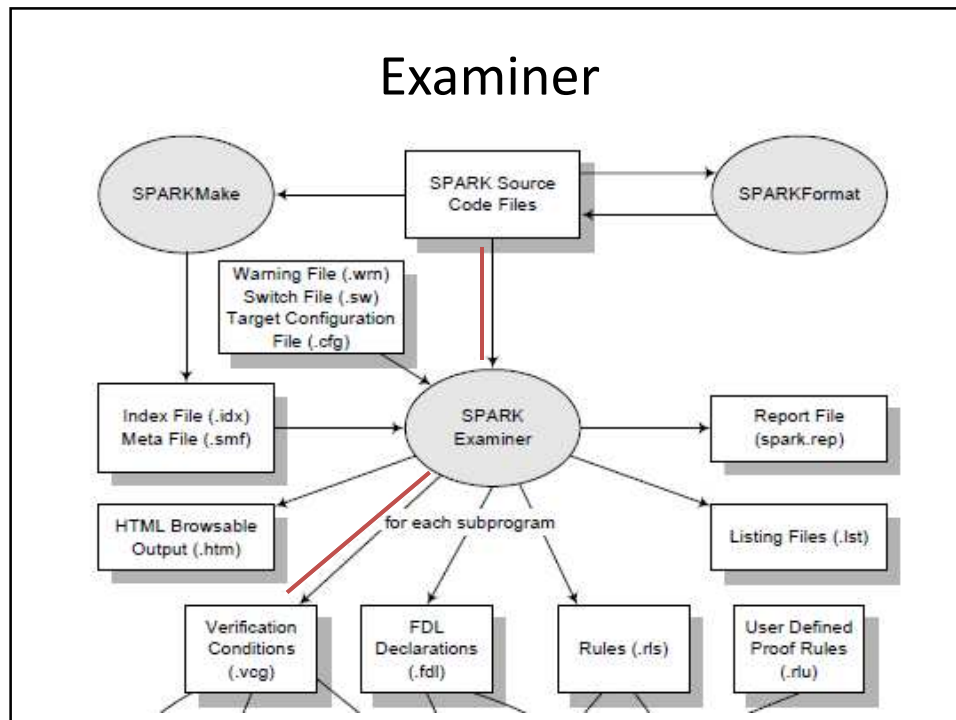
 type Float is digits 6 range -3.40282E+38 .. 3.40282E+38;
end Standard;

package System is ...

- Vengono di conseguenza
 - le definizioni per Natural e Positive
- Se non lo si usa compaiono __base__ ...

SPARK: Il processo di verifica



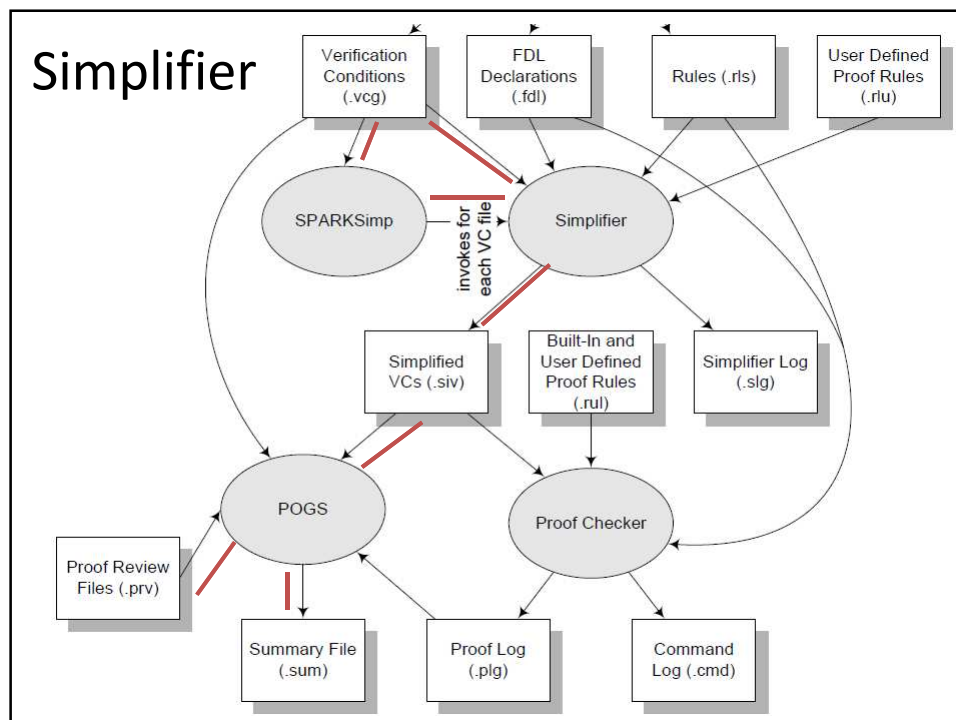


File Ausiliari: .fdl

- Dichiarazioni FDL
 - Functional Description Language [HIS, sez. 11.8]
 - legato al Pascal, target degli originali strumenti SPADE
- contiene la trascrizione delle dichiarazioni SPARK
 - variabili
 - attributi dei tipi (dal Target Configuration File)
- generato da Examiner
- usato da Simplifier e Checker

File Ausiliari: .rls

- Regole (di semplificazione/trasformazione)
 - relative agli attributi
 - es: `integer__first <= integer__last`
 - generato da Examiner
 - usato da Simplifier e Checker
-
- Generati dall'utente:.rlu
 - usati da Simplifier (posposto)



Risultati

- Simplifier: .siv
 - vc eliminate o ridotte
- POGS
 - Proof ObliGation Summariser tool
 - usa .siv e .prv
- .prv : file di prova umana:
 - .prv for procedure Dolt.
 - The following VCs were proved by review:
 - 1 -- Proved by method x (e.g ispezione diretta di CM)
 - 3 -- Proved by method x
 - 4 -- Proved by method y
 - 7 -- Proved by method y

Verifica Call

- Dopo Examiner

```

37 VCs generated 24-APR-2010 15:33:16
38
39 VCs not simplified
40
41 VCs for procedure_call :
42 -----
43 | | | | | -----Proved In----- | | | | |
44 # | From | To | | vcg | siv | plg | prv | False | TO DO |
45 -----
46 1 | start | rtc check @ 27 | | | | | | | YES |
47 2 | start | rtc check @ 28 | | | | | | | YES |
48 3 | start | pre check @ 30 | | | | | | | YES |
49 4 | start | rtc check @ 30 | | | | | | | YES |
50 5 | start | assert @ finish | YES | | | | | |
51 6 | start | assert @ finish | YES | | | | | |
52 -----

```

Verifica Call (2)

- Dopo Simplifier

```

37 VCs generated 24-APR-2010 15:33:16
38
39 VCs simplified 24-APR-2010 16:32:37
40
41 VCs for procedure_call :
42 -----
43 |      |      |      |      | -----Proved In----- |      |      |
44 # | From | To |      | vcg | siv | plg | prv | False | TO DO |
45 -----
46 1 | start | rtc check @ 27 |      | YES |      |      |      |      |
47 2 | start | rtc check @ 28 |      | YES |      |      |      |      |
48 3 | start | pre check @ 30 |      |      |      |      |      | YES |
49 4 | start | rtc check @ 30 |      | YES |      |      |      |      |
50 5 | start | assert @ finish | YES |      |      |      |      |      |
51 6 | start | assert @ finish | YES |      |      |      |      |      |
52 -----

```

Verifica Call (3)

- Review della condizione sospesa

```

procedure_call_3.
H1: f1 >= 0 .
H2: f1 <= 2147483647 .
H3: f2 >= 0 .
H4: f2 <= 2147483647 .
H5: not f2 = 0 -> 2147483647 div f2 >= - 2147483648 and
    2147483647 div f2 <= 2147483647 .
H6: f2 = 0 or f1 <= 2147483647 div f2 .
H7: integer__size >= 0 .
H8: natural__size >= 0 .
->
C1: f1 * f2 <= 2147483647 .

```

Verifica Call (4)

- File di assunzione di responsabilità
 - call.prv
- .prv for procedure Call.
 -- The following VCs were proved by review:
 3 -- Proved by ispezione diretta di CM

Verifica Call (5)

- Dopo Review

```

34 File j:\sparkworkspace\prodotto2\prodmain\call.vcg
35 procedure ProdMain.Call
36
37 VCs generated 24-APR-2010 15:33:16
38
39 VCs simplified 24-APR-2010 16:32:37
40
41 VCs for procedure_call :
42 -----
43 # | From | To | -----Proved In----- | False | TO DO |
44 | | | | vcg | siv | plg | prv | | |
45 -----
46 1 | start | rtc check @ 27 | | YES | | | | |
47 2 | start | rtc check @ 28 | | YES | | | | |
48 3 | start | pre check @ 30 | | | | YES | | |
49 4 | start | rtc check @ 30 | | YES | | | | |
50 5 | start | assert @ finish | YES | | | | | |
51 6 | start | assert @ finish | YES | | | | | |
52 -----

```