SPARK for Security

Yannick Moy – AdaCore
Journée thématique du GT SSLR
procedure Stabilize (Mode : in Mode_T;
    Success : out Boolean)
with Global => (Input => (Accel, Giro),
    In_Out => Rotors);
procedure Stabilize (Mode : in Mode_T;
    Success : out Boolean)
with Pre => Mode /= Off,
    Post => (if Success then
        Delta_Change (Rotors'Old, Rotors));
SPARK – a Subset of Ada

- unrestricted pointers
- exception handlers
- function with effects
- strong typing
- low level programming
- generics
- object orientation
- concurrency

Ada

Ada features outside the SPARK subset

Core language constructs common to Ada and SPARK

Additional SPARK aspects

Abstract_State
Initializes
Initial_Condition
Contract_Cases
Global
Depends
SPARK Open Source Ecosystem

Ada program
→ SPARK 2014
→ gnatprove
→ Why3 code
→ Why3 VC generator
→ Why3 logic formulas

Alt-Ergo  CVC4  Z3  Coq  Isabelle/HOL
Degree of automation

PROPERTY COMPLEXITY

- modular arith + quantifiers
- higher proof level
- lemma library

USER-PERCEIVED COMPLEXITY

- complex boolean + arith + quantifiers
- intermediate assertions
- ghost code
- yet more complex
- compiler correctness
- manual proof

default settings
Software Assurance Levels

Toward implementation guidance

- **Platinum:** Full functional requirements
- **Gold:** Key integrity properties
  - Only for a subset of the code subject to specific key integrity properties (functional, safety, security)
- **Silver:** Runtime errors & CWE
  - The default target for critical software (subject to costs and limitations)
- **Bronze:** Flow constraints
  - For the largest part of the code as possible
- **Stone:** Safer, analysable language subset
  - An intermediate level during adoption

Effort & Skills
Some SPARK Projects in Security

Rockwell Collins
Turnstile/SecureOne
cross-domain switch
Silver and Gold

Secunet MLW
multilevel workstation
Silver and Gold (for encryption-related properties)

MBDA EISR
secure in-the-field updating with code-signing
Silver

NVIDIA SP/FW
Falcon/RISC-V security processors
Security-critical firmware
Silver and Gold
Program Proof Tools

Academic

<table>
<thead>
<tr>
<th>Dafny</th>
<th>JML</th>
<th>SPARK 2014</th>
</tr>
</thead>
</table>

Industrial
SPARK for Security

SPARK supports 5 levels of increasing software assurance

From strong semantic coding standard to full functional correctness

Bronze level (correct information flow) is key for confidentiality

Silver level (AoRTE) is a must-have for secure software

SPARK can be combined with Ada at fine-grain (subprogram) level

SPARK can be combined with C at coarser-grain (file) level

Common Code Generator (CCG) generates C code from SPARK
SPARK Resources

SPARK toolset

SPARK adoption guidance
www.adacore.com/knowledge/technical-papers/implementation-guidance-spark

AdaCore Technologies for Cyber Security booklet
https://www.adacore.com/books/adacore-tech-for-cyber-security

https://www.adacore.com/documentation/#SPARK

SPARK online training
http://learn.adacore.com