Inside AdaCore

How would you like your newsletter?

PRINTED or DIGITAL?

VOTE at adacore.com/paperless

July–December 2018

- *AdaCore Technologies for Cyber Security* Available
- CodePeer Support for the Common Weakness Enumeration
- Smaller and More Secure with SPARK
- AdaCore Training Services
- Workshop on Sound Static Analysis for Security
- New Platform Support
- AdaCore Blogs
- Interview with Emma Adby
- Tech Days 2018
- Put Some SPARK in Your Ada

AdaCore Technologies for Cyber Security Available

Why is it so difficult to make a cyber system secure, and how can programming languages and tools contribute to a solution? The latest book in AdaCore's series of publications on high-assurance software, authored by Rod Chapman and Yannick Moy, answers these questions.

The chapter "The Challenge of Secure Software" identifies the various factors that make security so hard to achieve, ranging from the interconnected nature of modern systems to the limits of testing as a verification mechanism. The chapter concludes with "A Manifesto for Secure Software" that outlines the basic principles for high-integrity software engineering, which lay the foundations for secure software.

The chapter "Languages, Tools and Technologies Overview" summarizes the Ada and SPARK languages, as well as AdaCore's tools and technologies, and highlights their contributions to system security.

The chapter "Security Vulnerabilities and Their Mitigation" considers a number of specific high-profile software vulnerabilities, inspired by the CWE/SANS "Top 25 Most Dangerous Software Errors", and discusses how each can be prevented or mitigated using Ada, SPARK, and AdaCore's tools.

The chapter "Industrial Scenario Examples" presents a number of security-related scenarios that may arise in real-world projects. Each opens with a description of the context and the security issue, and then shows how either Ada or SPARK, in conjunction with the relevant AdaCore tools, can contribute. Each scenario is illustrated with one or more examples drawn from experience with customers and industrial projects.

Complementing the discussion in these chapters, additional details and examples are provided in two appendices. One appendix focuses on the MITRE Corporation's Common Weakness Enumeration (CWE) and shows how the use of Ada and/or SPARK, as well as AdaCore's tools, can address specific CWEs. The second appendix shows how contract-based programming in SPARK or Ada, verified by the corresponding static or dynamic analysis, can help avoid the "SQL Injection" vulnerability.

AdaCore Technologies for Cyber Security is available on-line at **adacore.com/cyber-security-book/**. To request a printed copy, please contact **info@adacore.com**.

CodePeer Support for the Common Weakness Enumeration

The MITRE Corporation's Common Weakness Enumeration has become a *de facto* benchmark for categorizing security-related software vulnerabilities, and AdaCore's CWE-Compatible CodePeer tool—an advanced static analysis tool for Ada—can serve an essential role during software verification by identifying and helping to eliminate instances of more than twenty CWEs. Among those detected are the only ones from the CWE/SANS "Top 25 Most Dangerous Software Errors" that could potentially arise in Ada:

- CWE 120 (Classic Buffer Overflow),
- CWE 131 (Incorrect Calculation of Buffer Size), and
- CWE 190 (Integer Overflow or Wraparound).

CodePeer detects a broad range of other weaknesses; these include:

- CWE 369 (Division by Zero),
- CWE 457 (Use of Uninitialized Variable),
- CWE 476 (Null Pointer Dereference),
- CWE 682 (Range Constraint Violation), and
- CWEs 362, 366 and 820 (Race Condition / Unprotected Shared Access).

CodePeer also flags constructs that may reflect latent bugs, for example:

- CWE 561 (Dead/Unreachable Code),
- CWE 563 (Unused or Redundant Assignment), and
- CWE 835 (Infinite Loop).

A complete list of CWEs detected by CodePeer appears in the CodePeer User's Guide, which has been updated for V18 with improved descriptions: **adaco.re/codepeercwe**.

CodePeer can be used retrospectively on existing code bases to find vulnerabilities in legacy systems or in software that is being upgraded. It can also be used as part of the development workflow in new projects, to prevent vulnerabilities from being introduced. CodePeer has been qualified as a verification tool under DO-178B and EN 50128.

For more information about CodePeer please visit **www.adacore.com/codepeer/**.

Smaller and More Secure with SPARK

Two recent open-source projects demonstrated how the SPARK programming language and formal verification technology can produce smaller and more secure software.

Componolit, a German startup developing secure mobile software, has designed a system architecture that meets a seemingly self-contradictory goal: ensuring that the system as a whole is trustworthy even though it contains untrustworthy building blocks such as a Web browser or a network stack. The key was to force untrusted components to communicate through trusted ones. Componolit used the Genode component-based operating system to ensure that that no other communications occurred, and relied on SPARK to prove the program properties guaranteeing that trusted components can really be trusted. For more information please visit **componolit.com/**.

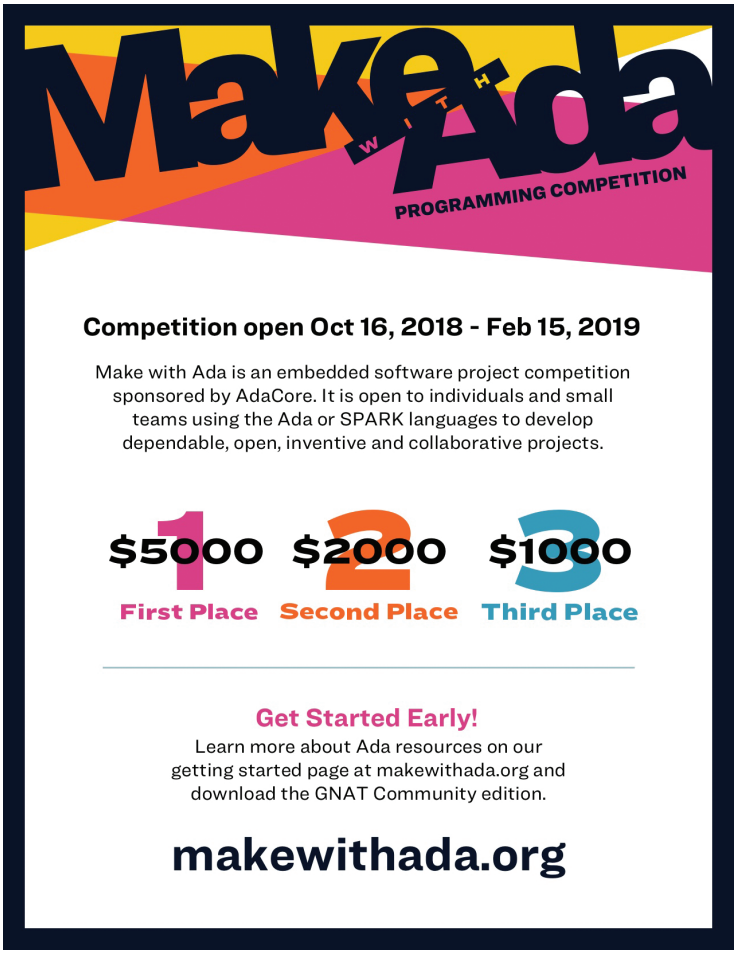
ANSSI, the French government security agency, has developed a custom STM32-based USB thumb drive with mass storage capabilities. Known as WooKey, this open-source hardware / software platform was designed in response to the BadUSB exploit from several years ago that transforms USB-connected devices into attack vectors. WooKey provides user data encryption and protection along with a full-fledged set of in-depth security defenses, and uses SPARK as the preferred programming language for the largest part of the software in the USB key's microkernel. For more information please visit **tinyurl.com/sstic-2018-wookey/**.

These projects achieved higher security by using better software engineering and by reducing the size of the trusted codebase, but this is not a new concept. A 2006 article chronicling the successful security history of the qmail Mail Transfer Agent for Unix—see **cr.yp.to/qmail/qmailsec-20071101.pdf**—cited three factors in achieving security: eliminating bugs, eliminating code, and minimizing the code that must be trusted. The new news is the additional guarantees that SPARK can bring with formal verification, ranging from absence of run-time errors to full functional correctness.

Helping new users get up to speed with the Ada language is a major objective for AdaCore, and several company initiatives are contributing towards this goal.

One such effort is the launch of **learn.adacore.com**, a new Ada training website geared to programmers familiar with a language such as C or C++. Starting from the standard "Hello, World" example and leading up to advanced topics such as Object-Oriented Programming, this online introductory course covers Ada's statements, type structure, encapsulation support, generic templates, exception handling, and tasking. It also explains interfacing with C and summarizes the packages in the predefined environment. The website will evolve with additional training material as well as other courses, and will serve as a successor to the AdaCore U (**u.adacore.com**) e-learning center.

AdaCore encourages the use of Ada and SPARK for teaching purposes at colleges and universities, and the GNAT Academic Program (GAP) makes it easier for instructors to make these languages part of their curricula. Numbering more than 200 member institutions, GAP augments the GNAT Community technology—a complete Ada and SPARK toolset—with front-line support to answer any questions that the instructor may have concerning the Ada or SPARK languages or the tools. AdaCore can also make available an extensive set of Ada and SPARK course material—lectures, quizzes, workshops—to GAP members. Over the years GAP participants have used the Ada and SPARK technologies to teach courses ranging from formal methods to hard real-time programming, and to implement systems such as CubeSat control and information security enforcement. For more information about GAP and member projects, please visit **www.adacore.com/academia/**.



AdaCore Training Services

AdaCore offers professional training both at customer sites and at public venues. The 5-day courses include Ada Fundamentals, Ada Advanced Topics, and SPARK, as well as specialized shorter courses on AdaCore's tools such as CodePeer and GPS. For information on these offerings please visit **www.adacore.com/training/** or contact **info@adacore.com**.

Workshop on Sound Static Analysis for Security

A two-day workshop on Sound Static Analysis for Security was held at the National Institute for Standards and Technology (NIST) headquarters in Gaithersburg, Maryland, on June 27 and 28. Organized by AdaCore and CEA Tech, the workshop showed how sound static analysis provides the guarantees that can reduce software security vulnerabilities by orders of magnitude. The sessions were built around three thematic topics—analysis of legacy code, use of sound static analysis in new developments, and accountable software quality—and featured keynote talks from Paul Black (NIST), David Wheeler (Institute for Defense Analyses), K. Rustan M. Leino (Amazon) and David Cok (CEA Tech / Independent Consultant). Tutorials on the SPARK and Frama-C formal methods technologies rounded out the program, and vendor exhibits included displays from AdaCore, CEA Tech, Kestrel Technology and TrustInSoft.

New Platform Support

In 2018 the GNAT Pro target platform coverage is being extended in several areas:

ARM: With a special focus on the 64-bit versions of the Cortex A series, GNAT Pro is targeting several RTOSes on this processor family—Embedded Linux, VxWorks 7, and QNX—and is also supplying a Bare Metal option.

FACE: Continuing the company's ongoing support for the Future Airborne Capability Environment initiative, which includes implementations of GNAT Pro on the Wind River VxWorks 653 2.5 and VxWorks 653 3.x platforms on PowerPC, AdaCore is extending its support with GNAT Pro targeted to Lynx Software Technologies LynxOS-178 2.2.4 on Intel x86.

RISC-V: AdaCore is introducing support for the RISC-V open-source Instruction Set Architecture, with a GNAT Pro implementation targeted to a 32-bit Bare Metal configuration. The RISC-V ISA is being adopted by a growing number of hardware vendors, and GNAT Pro will make Ada one of the first in a small number of languages supported on this target.

AdaCore Blogs

For an informal look at some of the ongoing activities at AdaCore, across a wide range of topics, visit the company's blog site **blog.adacore.com**. Among the articles posted earlier this year was "Bitcoin blockchain in Ada: Lady Ada meets Satoshi Nakamoto" by AdaCore senior software engineer Johannes Kanig. In this blog Johannes explained the basics of blockchain technology—in effect a secure distributed database—and then showed how to implement some of the underlying data structures and security-related functionality in Ada. For details see **blog.adacore.com/bitcoin-in-ada/**.

interview

Emma Adby

Marketing Operations Manager

Emma, tell us about your background and how you came to be involved with Ada and AdaCore. What is your current role?

As part of my undergraduate studies in International Business with French from Sheffield Hallam University in the U.K., I spent a year in France to study at the ESSEC Business School and completed an internship with the marketing group at AdaCore's Paris office. This proved to be a good match—I very much enjoyed the experience of working with a dynamic high-tech company—and on completing my undergraduate degree I joined AdaCore on a permanent basis. My current position is Marketing Operations Manager, or "MOM", which involves coordinating all global marketing activities including events organization, Public Relations, web design and branding.

More recently, I have been jointly leading a team dedicated to strengthening the Ada and SPARK programmer communities, promoting the benefits of these languages in new spaces.

One of the goals of marketing is to promote "brand awareness" for an organization. What do you see as AdaCore's "brand" and how does the company get that message across to existing and prospective customers?

Even with AdaCore's multiple facelifts, our "brand" has largely stayed the same over the years: expertise and support for software technologies that provide the highest levels of reliability, safety and security. Customers put trust in our talented engineers to provide this, and we are respected for it. So part of my job is to help "spread the word" to existing or prospective users.

AdaCore's customer list is a pretty impressive one, including major players in domains such as aerospace, rail, automotive, and other high-tech industries. That being said, it's harder to reach these audiences than you would imagine. With the increasing amount of content marketing following us around the internet, flooding us with email and filling our voicemail box, we have found that providing pure technical content and resources is the most effective way of communicating the AdaCore brand.

Our books, documentation, blogs, articles and webinars provide potential or existing customers, as well as the wider community, the resources to build software that really matters. As a marketer, I'm always interested in extending the reach of this content, and with the rise in digital media platforms, people are looking to engage in conversation and contribute, so its important for us to be at the forefront. It's both an opportunity and a challenge to find the relevant communication channels for our corporate messaging, and we've been reaching out in recent years with "Make with Ada" contests, participation in social platforms (reddit, Facebook, etc.) and other initiatives. And of course an essential piece of our marketing presence is our website, which serves as a corporate "shop window" for the company's products and services.

Any hobbies or outside interests that you'd like to share?

When I'm not working or travelling the world in search of the best gin and tonic—yes I'm a self-proclaimed gin snob—you can usually find me watching films. My all time favorite has to be *The Last of the Mohicans*, but any Tarantino masterpiece will follow close behind.

I have a very keen interest in environmental sustainability and farming practices, and am always looking to engage in friendly debate on the topic! When I'm not worrying about the state of the climate, I'm a keen reader and have set myself a challenge of reading at least 24 books this year.

Tech Days 2018

AdaCore's annual Tech Days user conferences are slated for October 4 (Paris) and November 14–15 (Boston).

This year's events feature the latest news about AdaCore's technologies, product roadmaps, presentations on topics ranging from GPU support to cyber security, and an unmatched opportunity to meet with AdaCore's experts in person. The Paris conference includes customer presentations from David Sibai (BNP Paribas) and Nils Brynedal Ignell (Scandinavian Real Heart), and the Boston event features a keynote talk from CWE expert Bob Martin (MITRE Corporation) on "Assured Software: a Journey and Discussion" as well as product demonstrations.

To register, or to see a detailed agenda, please visit **www.adacore.com/tech-days-eu** (Paris Tech Day) or **www.adacore.com/tech-days-us** (Boston Tech Days).

A Green Alternative

We are considering switching from print to electronic for our semi-annual *Inside AdaCore* newsletter, but first we want to hear from you! Please register your preference at **www.adacore.com/paperless/**.

Emma Adby photograph by Gary Matoso

Put Some SPARK in Your Ada

The latest version of the SPARK language, SPARK 2014, includes a sizable Ada subset and presents an opportunity for existing Ada codebases to integrate SPARK features. By adapting critical code to SPARK Pro and the GNATprove technology, an Ada project can gain the increased assurance that comes from proving security properties such as correct data flows and absence of run-time errors. The initial part of the migration, known as the Stone level of assurance, consists of three steps:

- Convert as much of the existing Ada into SPARK as is practical.
- Run the SPARK analyzer (GNATprove) on the codebase and look at the violations.
- For each violation, decide whether to convert the code to valid SPARK or to exclude the code from analysis.

The following skeletal package illustrates this approach.

```
package String_Utilities is
   function Pad (Item : String;
                 Char : Character;
                 N    : Natural)
      return String;
   -- Returns Item & (1..N => Char)

   ... -- other subprograms
end String_Utilities;
```

```
package body String_Utilities is
   Count : Natural := 0;

   function Pad (Item : String;
                 Char : Character;
                 N    : Natural)
       return String is
   begin
      Count := Count+1;
      return Item & (1..N => Char);
   end Pad;

   ... -- other subprograms
end String_Utilities;
```

Pad is a classic "memo function": it computes a result but also assigns to a non-local variable that keeps track of how many times the function is invoked. (We are assuming a sequential program; if Pad is to be safe for invocation from concurrent tasks, Count should be encapsulated in a protected object.)

Although perfectly reasonable Ada, this code would be rejected by GNATprove since functions in SPARK are not allowed to assign to non-local variables. One solution is to rewrite the function as a procedure, returning the result through an **out** parameter. However, in a legacy system with many invocations of the function such a strategy would entail a large number of source text changes. Further, in cases such as this one where the function returns a result from an unconstrained array type, the **out** parameter style may be clumsy or problematic.

An alternative and more practical approach is to keep Pad as a function and to add the relevant contracts based on the properties to be proved, but to disable the analysis of the function body:

```
package String_Utilities is
   function Pad (Item : String;
                 Char : Character;
                 N    : Natural)
      return String
   with
     Post => Pad'Result'Length =
             Item'Length+N,
     SPARK_Mode => On,
     Global     => null;

   ... -- other subprograms
end String_Utilities;
```

```
package body String_Utilities is
   Count : Natural := 0;
   function Pad (Item : String;
                 Char : Character;
                 N    : Natural)
      return String
   with SPARK_Mode => Off is
   begin
      Count := Count+1;
      return Item & (1..N => Char);
   end Pad;

   ... -- other subprograms
end String_Utilities;
```

The Post aspect reflects a program property that can be assumed on return from Pad, and the SPARK_Mode=>On aspect makes the function invocations eligible for analysis by GNATprove. The assignment to Count in the body of Pad is not relevant to the analysis; thus Global=>**null**, which indicates that Pad neither reads nor writes non-local variables, is included with Pad's specification.

Since the body of Pad is not to be analyzed by GNATprove, it is declared with SPARK_Mode=>Off. Traditional verification techniques—code review/analysis and testing—rather than formal proof would be needed to establish confidence that the specified postcondition is met. Although the body of Pad cannot be proven, the function can be invoked in code that will be proven. This combination of testing and proof—hybrid verification—is a practical way to realize the best of both technologies.

Further information on adapting existing Ada code to the Stone and higher assurance levels may be found in the SPARK implementation guidance booklet authored by AdaCore and Thales, available on line at **www.adacore.com/spark-guidance** or in hard copy on request from **info@adacore.com**.

Real Heart Selects AdaCore

Scandinavian Real Heart AB in Sweden has selected AdaCore's GNAT Pro and SPARK Pro toolsuites to develop the heart pump controller software for its Total Artificial Heart product. Real Heart's innovative solution can adjust the power of the pumping depending on the patient's blood pressure, enabling optimal energy consumption and increased patient comfort. The need to meet the highest levels of reliability and safety led Real Heart to choose AdaCore's SPARK and Ada technologies, which are being used to develop and verify all but the lowest levels of the code.

AdaCore at TU-Automotive

AdaCore exhibited at the TU-Automotive conference in Detroit, June 6–7, and featured its technologies for reliable, safe and secure software. Highlights included demonstrations of the QGen debugger with its unique interactive model-level cross-debugging functionality (including support for multicore targets) and the SPARK Pro toolsuite for proving critical program properties.

AdaCore Extends Wind River Platform Coverage

GNAT Pro Ada is now available for the VxWorks 7 RTOS on the ARM (64-bit), PowerPC (64-bit) and Intel (32-bit) multi-core architectures, under both Linux and Windows development environments. These releases add to the existing GNAT Pro support for VxWorks 7 targets (ARM 32-bit, PowerPC 32-bit and Intel 64-bit), VxWorks 6 and VxWorks 653, reinforcing the longstanding strategic alliance between AdaCore and Wind River.

GNAT Pro Chosen for NASA Mission

The University of Colorado's Laboratory for Atmospheric and Space Physics (LASP) has selected the Ada language and the GNAT Pro for ARM Cortex Bare Metal product for NASA's Climate Absolute Radiance and Refractivity Observatory (CLARREO) Pathfinder mission. CLARREO Pathfinder will deploy a Reflected Solar spectrometer on the International Space Station starting in 2021 that will detect the complete spectrum of radiation from the Sun reflected by Earth. LASP selected Ada and the Ravenscar runtime based on efficiency, support for object orientation, increased reliability, and simple tasking support.

GNAT Pro Supports LynxSecure Separation Kernel on Intel

Customers using the Lynx Software Technologies LynxSecure Separation Kernel Hypervisor can take advantage of GNAT Pro in a variety of scenarios to maximize their productivity with Ada. Potential use cases include migrating code from PowerPC LynxOS-178 to Intel LynxOS-178 under LynxSecure, writing safe and secure lightweight Bare-Metal LynxSecure Applications in Ada, and running Ada code under Guest OSes such as Windows and Linux.

AdaCore Partners with BlackBerry for QNX

Partnering with BlackBerry, AdaCore has broadened its embedded platform coverage with an implementation of GNAT Pro Ada for the QNX real-time operating system. GNAT Pro for QNX is initially targeted to the ARM Cortex A family, with plans to cover all architectures in the future. Ada users now have an expanded range of embedded platforms to choose from, and C developers on QNX have an easy migration path to the Ada or SPARK languages.

calendar highlights / July–December 2018

For up-to-date information on conferences where AdaCore is participating, please visit **www.adacore.com/events/**.

22nd International Symposium on Formal Methods
July 14–19, 2018 / Oxford, UK

Yannick Moy is presenting a paper at the the Workshop on Automated Verification of Critical Systems (July 18-19).
www.fm2018.org/workshops/

GNU Tools Cauldron
September 7–9, 2018 / Manchester, UK

AdaCore is exhibiting and is a major sponsor.
gcc.gnu.org/wiki/cauldron2018

Army Aviation FACE Technical Interchange Meeting
September 18, 2018 / Huntsville AL, US

AdaCore is exhibiting at this event.
www.opengroup.org/face/events/

AdaCore Tech Days
October 4, 2018 / Paris, France
November 14–15, 2018 / Boston (Burlington) MA, US

For information about these annual customer-focused events please see the companion article in this newsletter.
www.adacore.com/tech-days-eu/
www.adacore.com/tech-days-us/

Arm TechCon
October 16–18, 2018 / San Jose CA, US

AdaCore is exhibiting at this event.
www.armtechcon.com/

ACM SIGAda HILT 2018
(High Integrity Language Technology)
November 5–6, 2018 / Boston MA, US

AdaCore is exhibiting at this event.
www.sigada.org/conf/hilt2018/

HIS 2018 (High Integrity Software Conference)
November 6, 2018 / Bristol, UK

AdaCore is a co-organizer/sponsor and is exhibiting at this event.
www.his-2018.co.uk/
www.adacore.com/tech-days-us/

FSW 2018
11th Annual Workshop on Spacecraft Flight Software
December 3–6, 2018 / San Antonio TX, US

AdaCore is a sponsor of this workshop.
flightsoftware.jhuapl.edu/

ESE Kongress 2018
(Embedded Software Engineering Kongress)
December 3–7, 2018 / Sindelfingen, Germany

AdaCore is exhibiting at this event.
www.ese-kongress.de/english/

Inside AdaCore is published twice a year simultaneously in New York and Paris by AdaCore.

150 W. 30th Street, 16th floor
New York, NY 10001, USA
tel +1 212 620 7300
fax +1 212 807 0162

46 rue d'Amsterdam
75009 Paris, France
tel +33 1 49 70 67 16
fax +33 1 49 70 05 52

info@adacore.com
www.adacore.com

AdaCore