Security by Construction—Engineering Software to Exceed EAL5

David Cooper

Praxis Critical Systems Limited

James Widmaier, R2 *NSA*

Randy Johnson, R2 *NSA*

Bill Everett, *SPRE Inc*

Industry does not produce low-defect software

- Many can't, and don't
- Many can't, but would like to
- Some can, but argue that it is un-economic

- There are sectors where low-defect, high security systems are essential

We don’t have to live with this

- It is possible to produce low-defect software
  - cost-effectively
  - using proven approaches
  - conforming to current security certification processes (e.g. the Common Criteria)

Top level principles

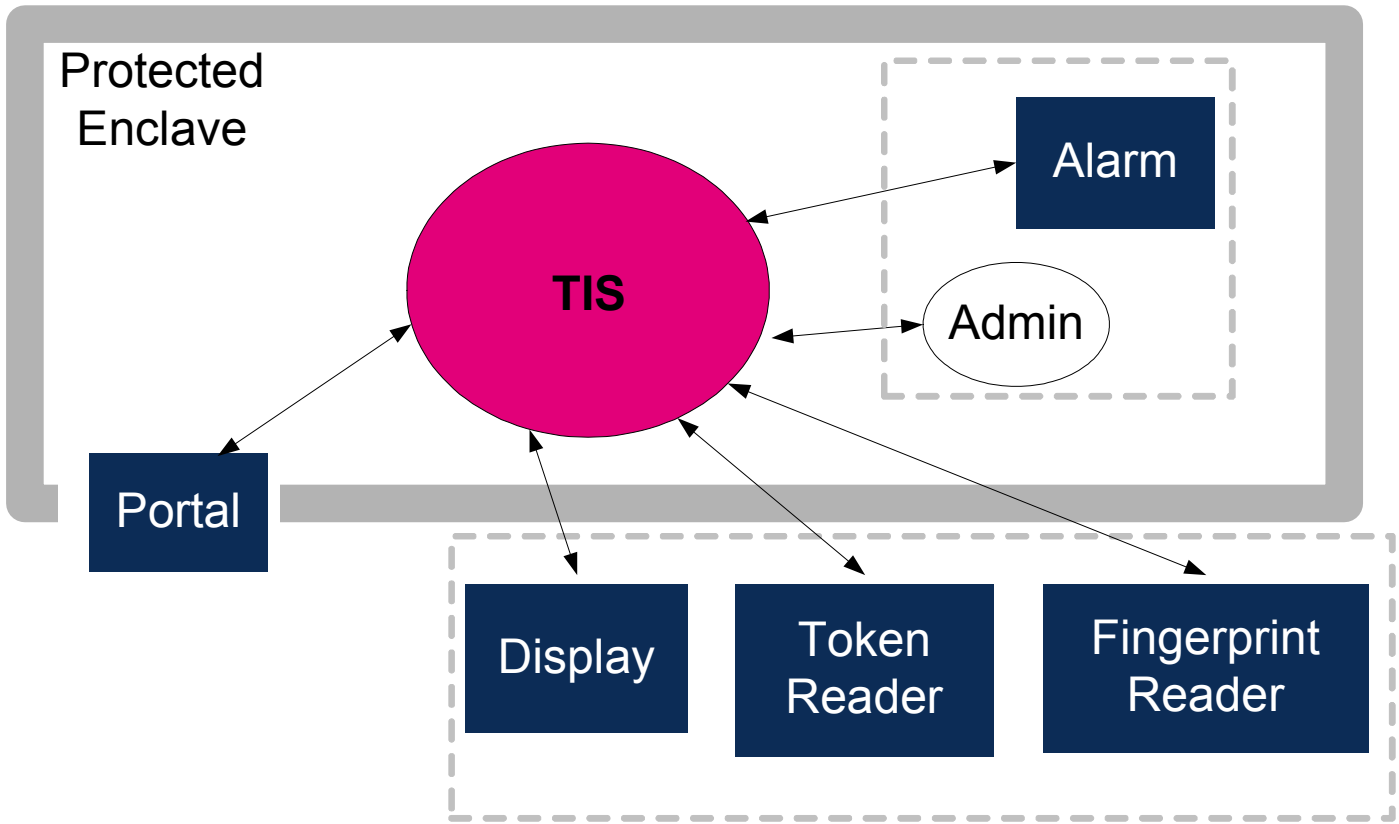
- Don’t introduce defects
- Remove defects ASAP after introduction

- Seven guiding principles to achieve this cost-effectively

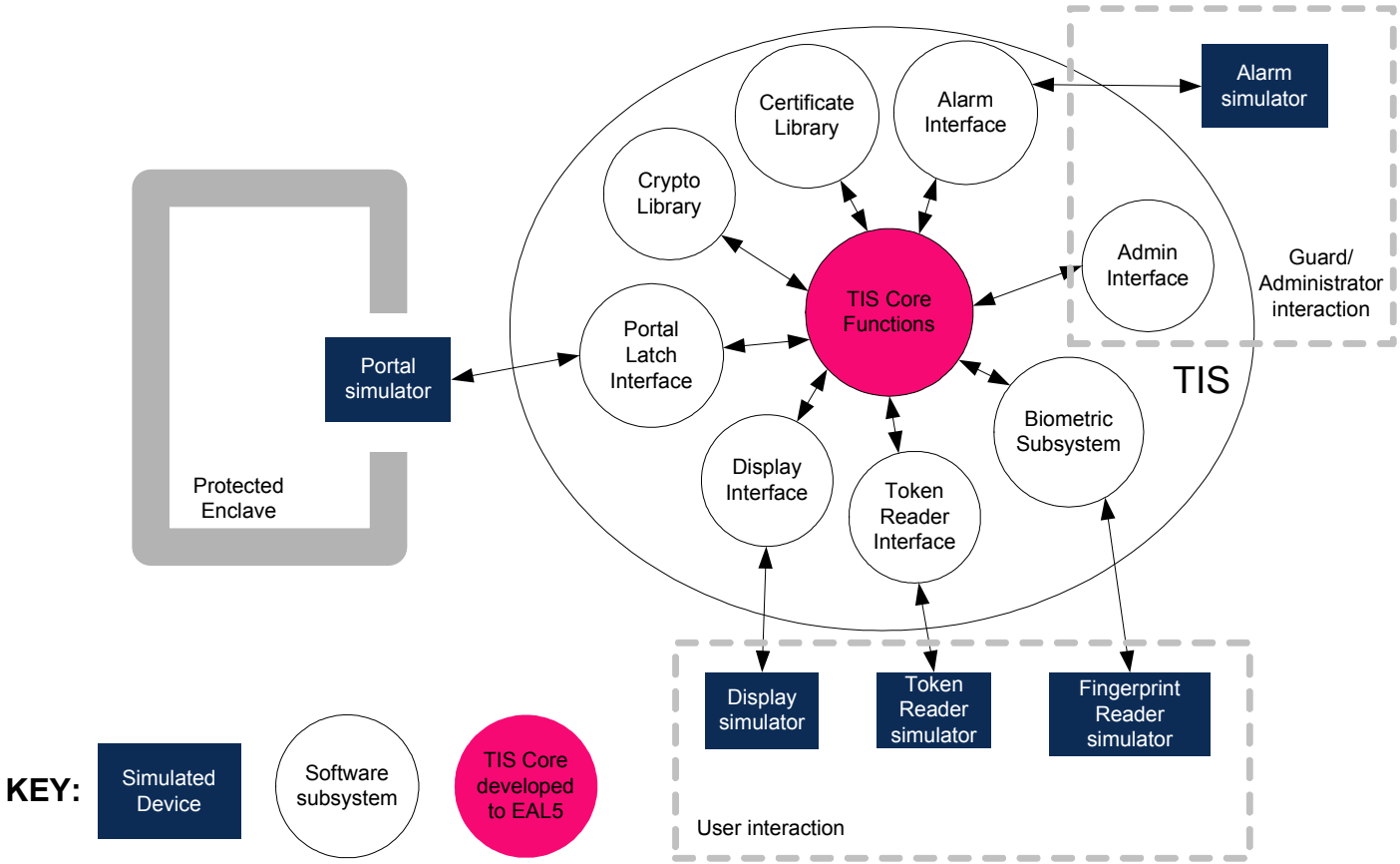
Background

- Sponsored by the NSA
  - Customer = NSA
  - Developer = Praxis Critical Systems
  - Tester/Environment = SPRE Inc.
- To demonstrate cost-effective EAL5
- Subset of existing Tokeneer

System



System



Process

- Requirements analysis (REVEAL®)
- Security analysis from PP (CC)
- Functional specification (Z)
- Design (Z and INFORMED)
- Code (SPARK)
- System test (against functional/design)
- Independent demonstration testing

Statistics

	Ada source lines	SPARK annotations	LOC/day
Core	**9,939**	**16,564**	**38**
Support	**3,697**	**2,240**	**88**

- One year (9 months development)
- 3xNSA, 3xPraxis, 2xSPRE (all part-time)
- Zero code defects found
- (Two user-manual defects found)

Orthogonal considerations

Process

Guiding principles

- ?? Capturing information
- ?? Making the transitions
- ?? Where you write what
- ?? Verification
- ?? Getting more out of your checks
- ?? Same tools or different?
- ?? How hard is it?

Capturing information

- Writing multiple descriptions of the system
- Do it without error!
  - Code: unambiguous
  - Design: what, when
  - Spec: black box, complete
  - Req: clarity, user-centred

- Write right

Guiding principles

- Write right
- ?? Making the transitions
- ?? Where you write what
- ?? Verification
- ?? Getting more out of your checks
- ?? Same tools or different?
- ?? How hard is it?

Making the transitions

- Big steps are hard
- Take small steps
- Know what each step does

- Step, don’t leap

Guiding principles

- Write right
- Step, don't leap
- ?? Where you write what
- ?? Verification
- ?? Getting more out of your checks
- ?? Same tools or different?
- ?? How hard is it?

Where you write what

- Lots of work, lots of documents
- Do what is useful
- Know what each document does

- Say something once, why say it again?
  (Talking Heads)

Guiding principles

- Write right
- Step, don't leap
- Say something once, why say it again?
- ?? Verification
- ?? Getting more out of your checks
- ?? Same tools or different?
- ?? How hard is it?

Verification

- Any work can introduce defects
- Check ASAP
  - (and remove the defects)

- Check here before going there

Guiding principles

- Write right
- Step, don't leap
- Say something once, why say it again?
- Check here before going there
- ?? Getting more out of your checks
- ?? Same tools or different?
- ?? How hard is it?

Getting more out of your checks

- Design decisions are made
- Argue for them
- Documented arguments ⇒
  - assure correctness
  - ensure correctness

- Argue your corner

Guiding principles

- Write right
- Step, don’t leap
- Say something once, why say it again?
- Check here before going there
- Argue your corner
- ?? Same tools or different?
- ?? How hard is it?

Same tools or different?

- Tools can help
- Focus on tools that deliver
- Use them wisely

- Screws: use a screwdriver, not a hammer

Guiding principles

- Write right
- Step, don’t leap
- Say something once, why say it again?
- Check here before going there
- Argue your corner
- Screws: use a screwdriver, not a hammer
- ?? How hard is it?

How hard is it?

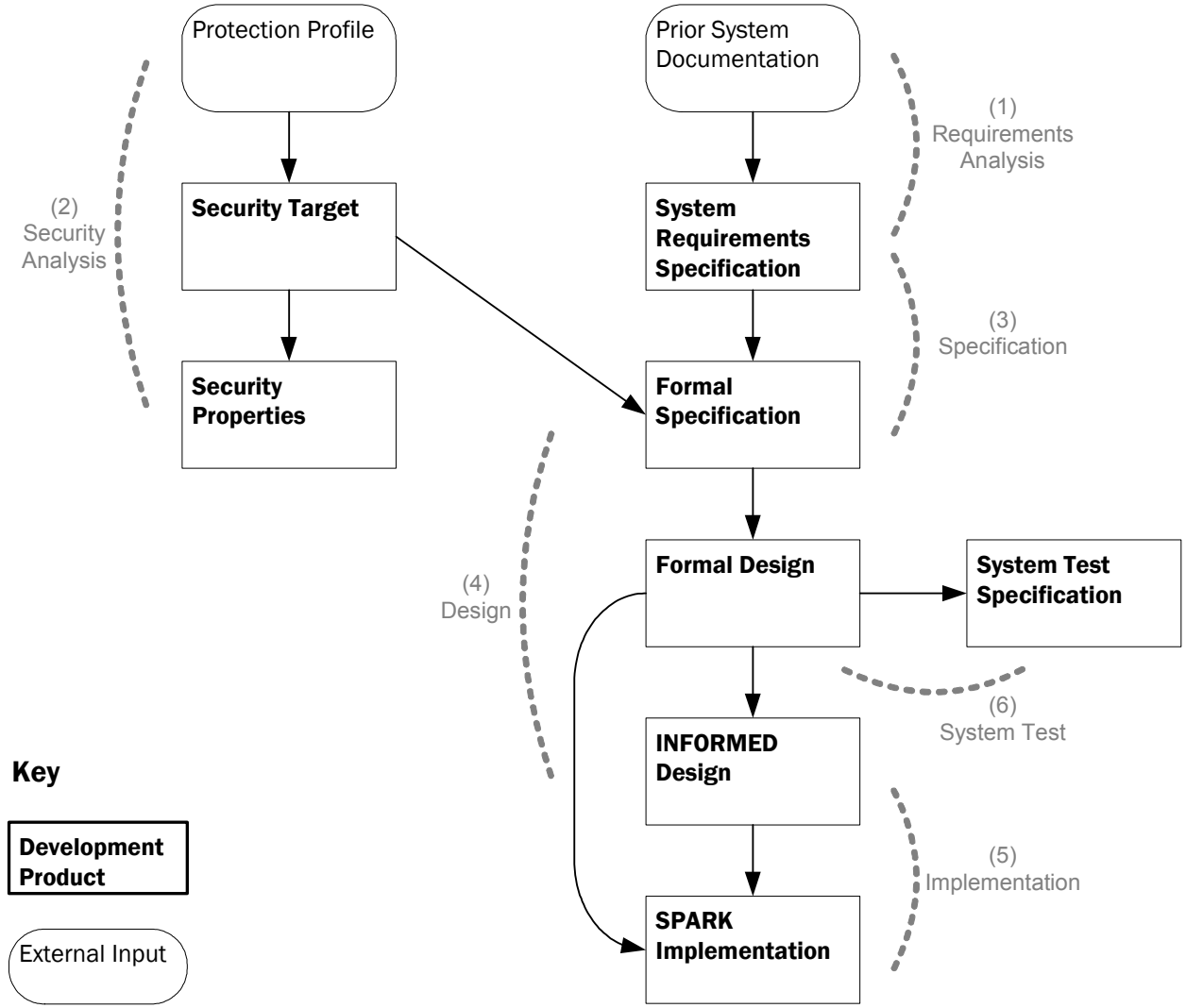
- Development is not handle-turning
- All processes will collapse if not applied intelligently
- Recruit, train and develop --- brains!

- Brains 'R' Us

Guiding principles

- Write right
- Step, don’t leap
- Say something once, why say it again?
- Check here before going there
- Argue your corner
- Screws: use a screwdriver, not a hammer
- Brains ’R’ Us

The development process



Summary

- We can develop low-defect systems cost-effectively
- No magic bullet, but well-understood principles
- Principles have been realised in practical process
  - paper gives process used, tied to the principles

- **Go do it!**

Praxis Critical Systems Limited

20 Manvers Street
Bath BA1 1PX
United Kingdom
Telephone: +44 (0) 1225 466991
Facsimile: +44 (0) 1225 469006
Website: www.praxis-cs.co.uk

Email: David.Cooper@praxis-cs.co.uk

Email: jcwidma@orion.ncsc.mil
Email: drjohns@orion.ncsc.mil
Email: wwe@SPRE-inc.com