INTEGRITY™
GLOBAL SECURITY

MAKING COMPUTING SECURE™

A Green Hills Software company

Lessons Learned from the First High Assurance (EAL 6+) Common Criteria Software Certification

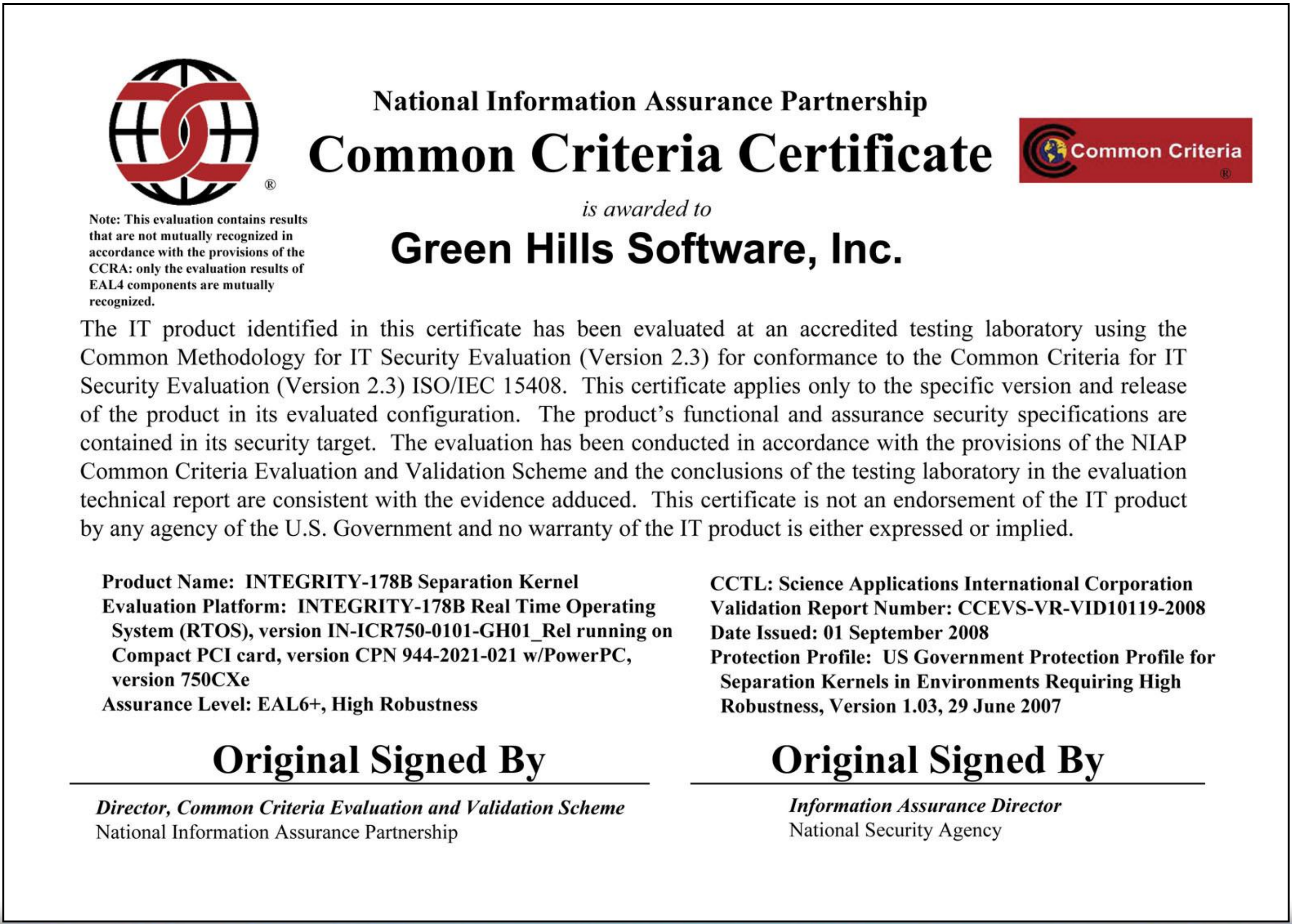
David Kleidermacher, CTO

davek@integrityglobalsecurity.com

Agenda

- Background of EAL 6+ Software and Certification
- Lessons Learned

INTEGRITY: 1st Software Certified to EAL6+ High Robustness



National Information Assurance Partnership

Common Criteria Certificate

Common Criteria

Note: This evaluation contains results that are not mutually recognized in accordance with the provisions of the CCRA: only the evaluation results of EAL4 components are mutually recognized.

is awarded to

Green Hills Software, Inc.

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3) ISO/IEC 15408. This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: INTEGRITY-178B Separation Kernel
Evaluation Platform: INTEGRITY-178B Real Time Operating System (RTOS), version IN-ICR750-0101-GH01_Rel running on Compact PCI card, version CPN 944-2021-021 w/PowerPC, version 750CXe
Assurance Level: EAL6+, High Robustness

CCTL: Science Applications International Corporation
Validation Report Number: CCEVS-VR-VID10119-2008
Date Issued: 01 September 2008
Protection Profile: US Government Protection Profile for Separation Kernels in Environments Requiring High Robustness, Version 1.03, 29 June 2007

Original Signed By

Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By

Information Assurance Director
National Security Agency

Operating System Protection Profiles

NAME	TITLE	SECURITY LEVEL	THREAT ENVIRONMENT
SKPP	**Separation Kernel in High Robustness Environments**	**EAL 6+ / High Robustness**	**"management of classified and other high-valued information, whose confidentiality, integrity or releasability must be protected"** **"presence of both sophisticated threat agents and high value resources"**
CAPP	Controlled Access Protection Profile	EAL 4+	"non-hostile and well-managed user community" "inadvertent or casual attempts to breach the system security" "not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well-funded attackers"
CCOPP-OS	COTS Compartmentalized Operations Protection Profile – Operating Systems	EAL 4	"not expected to adequately protect against sophisticated attacks" "users are highly trusted not to attempt to maliciously subvert the system or to maliciously exploit the information stored thereon"
LSPP	Labeled Security Protection Profile	EAL 4+	"non-hostile and well-managed user community" "inadvertent or casual attempts to breach the system security" "not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well-funded attackers"
SLOS	Single Level Operating Systems in Medium Robustness Environments	EAL 4+	"suitable for use in unclassified environments" Not appropriate for "organization's most sensitive/proprietary information" when exposed to "a publicly accessible network" "likelihood of an attempted compromise is medium" "motivation of the threat agents will be average"
MLOS	Multilevel Operating Systems in Medium Robustness Environments	EAL 4+	"suitable for use in unclassified environments" Not appropriate for "organization's most sensitive/proprietary information" when exposed to "a publicly accessible network" "likelihood of an attempted compromise is medium" "motivation of the threat agents will be average"

Lessons Learned

- Lesson #1: Don’t underestimate pain of validating the PP
  - SKPP first authored in 2002
  - Certified in 2007
  - New NIAP policy: no custom STs
  - Review by committee (Open Group)

INTEGRITY Historical Overview

- 1997 – First INTEGRITY shipment
  - B1-B Bomber
- 2000 – INTEGRITY selected for F-35 Joint Strike Fighter
  - Since: F-16, F-22, S-92, A380, A400, 787, others
- 2002 – First FAA DO-178B level A certification
- 2005 – Entered EAL6+ High Robustness Evaluation
- 2006 – First delivery of INTEGRITY PC
- 2008 – EAL6+ High Robustness certification
- 2008 – INTEGRITY Global Security, LLC launched
- 2009 – #1 High Reliability RTOS by rev. market share

(Image courtesy of U.S. Air Force/Jet Fabara)

(Image courtesy of US Air Force/Tom Reynolds)

Why EAL 6+ / High Robustness?

- EAL 6+ High Robustness evaluation
  - U.S. Government program to protect sensitive national secrets
    - “***high robustness***”: the most valuable information exposed to the most determined and resourceful attackers
    - “management of classified and other high-valued information, whose confidentiality, integrity or releasability must be protected.”
    - “appropriate to support critical security policies for the Department of Defense (DoD), Intelligence Community, the Department of Homeland Security, Federal Aviation Administration, and industrial sectors such as finance and manufacturing.”
  - INTEGRITY compliant to CC v3.1 EAL 7

High Robustness

		Attack Threat		
		Low Threat	***Medium Threat***	***High Threat***
Asset Value	***High Value***	Basic	Medium	**HIGH**
	Medium Value	Basic	Medium	Medium
	Low Value	Basic	Basic	Basic

Commercial OS/VMM Certs

Product/ Technology	Type	Protection Profile	Security Level
INTEGRITY	**Operating System**	**SKPP**	**EAL 6+/ High Robustness**
Windows XP	Operating System	CAPP	EAL 4+
Windows Vista	Operating System	CAPP,SLOS (in eval)	EAL 4+
Linux	Operating System	CAPP, LSPP	EAL 4+
SELinux	Operating System	CAPP, LSPP	EAL 4+
Solaris (and Trusted Solaris)	Operating System	CAPP, LSPP	EAL 4+
HP/UX	Operating System	CCOPP-OS (in eval)	EAL 4+
VMware	Virtualization	Custom	EAL 4+
STOP OS	Operating System	CAPP, LSPP	EAL 5
PR/SM LPAR Hypervisor	Virtualization	Custom	EAL 5

Requirements: CM and Testing

REQUIREMENT	DESCRIPTION	SKPP	CAPP	NOTES
ACM_AUT	Configuration management automation	2	0	SKPP requires complete automation
ATE_COV	Analysis of test coverage	3	2	Complete coverage of functional requirements
ACM_SCP	Configuration management scope	3	1	SKPP CM requires coverage of development tools

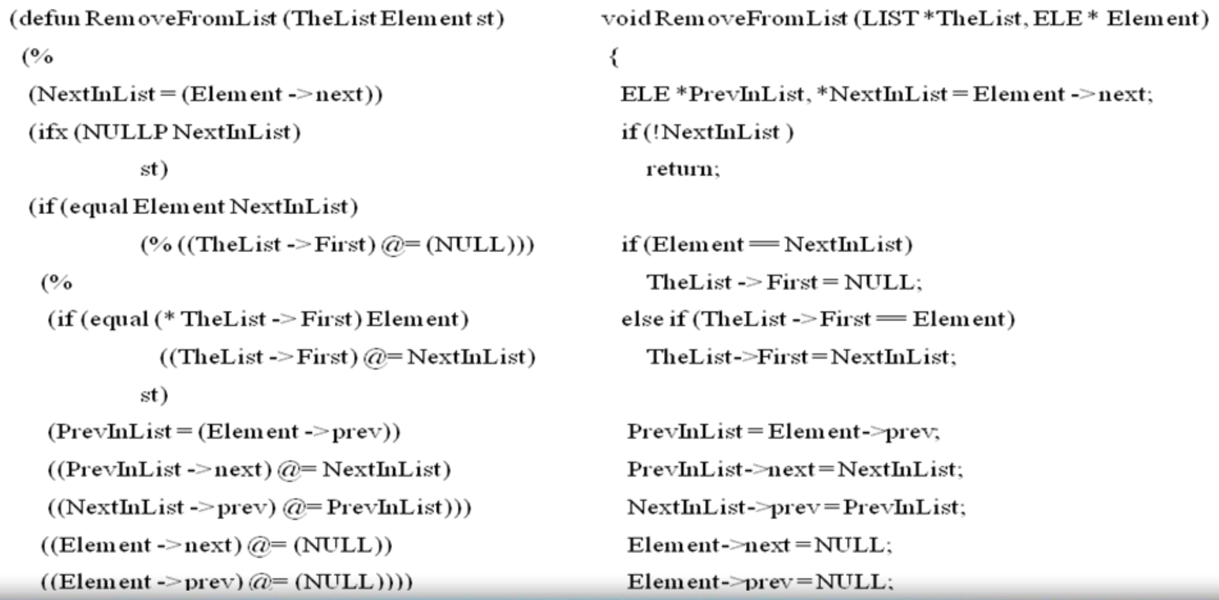
- “Bit provenance”
- 100% FFFI
- Green Hills compiler and tool chain

Lessons Learned

- Lesson #2: Reuse other cert results / artifacts
  - DO-178B Level A shaved years off of evaluation time and cost
  - Many common assurance artifacts – design, testing, CM, etc.

Requirements: Design and Specification

REQUIREMENT	DESCRIPTION	SKPP	CAPP	NOTES
ADV_FSP	Functional Specification	4	1	SKPP requires formal specification
ADV_IMP	Implementation representation	3	0	SKPP requires rigorously defined transformation from representation to implementation



```
(defun RemoveFromList (TheList Element st)
 (%
  (NextInList = (Element -> next))
  (ifx (NULLP NextInList)
                st)
  (if (equal Element NextInList)
                (% ((TheList -> First) @= (NULL)))
   (%
    (if (equal (* TheList -> First) Element)
                  ((TheList -> First) @= NextInList)
                st)
    (PrevInList = (Element -> prev))
    ((PrevInList -> next) @= NextInList)
    ((NextInList -> prev) @= PrevInList)))
   ((Element -> next) @= (NULL))
   ((Element -> prev) @= (NULL))))
```

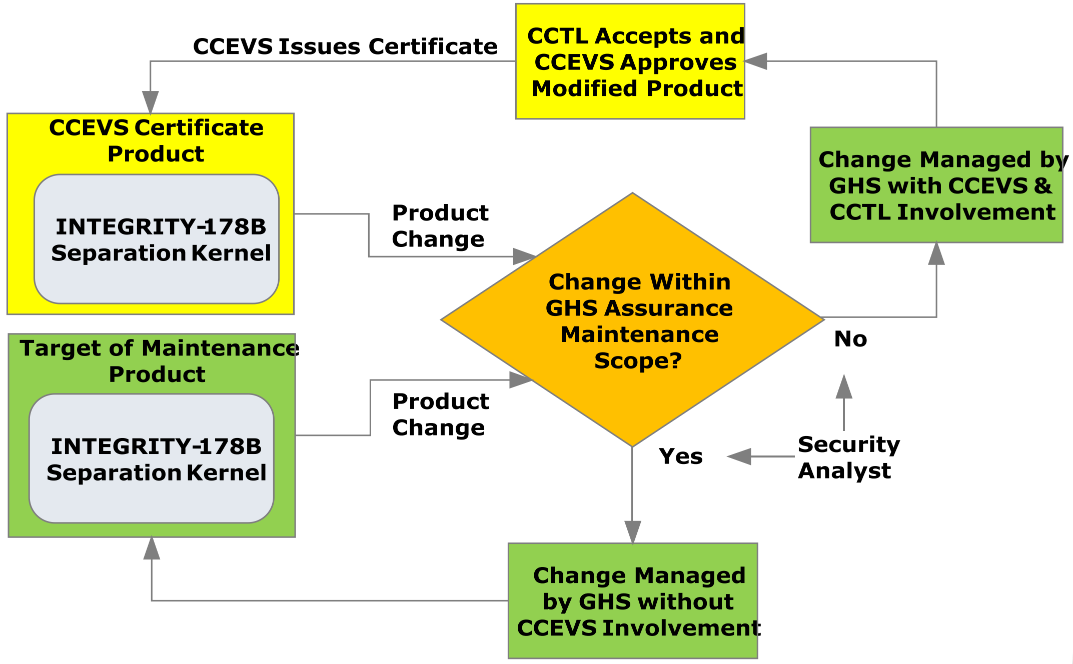
```
void RemoveFromList (LIST *TheList, ELE * Element)
 {
  ELE *PrevInList, *NextInList = Element -> next;
  if (!NextInList )
     return;

  if (Element == NextInList)
     TheList -> First = NULL;
  else if (TheList -> First == Element)
     TheList->First=NextInList;

   PrevInList = Element->prev;
   PrevInList->next=NextInList;
   NextInList->prev=PrevInList;
   Element->next=NULL;
   Element->prev=NULL;
```

Lessons Learned

- Lesson #3: Formal methods are expensive
  - Limited worldwide expertise
  - Must be designed in from the beginning
  - Proof system/approach must be acceptable to evaluators
  - Prove correspondence of formal model to implementation
  - Working on ways to make this more efficient

Requirements: Flaw remediation and Assured maintenance process

REQUIREMENT	DESCRIPTION	SKPP	CAPP	NOTES
ALC_FLR	Flaw remediation	3	0	Systematic remediation
AMA_AMP	Assured maintenance	2+	0	12 explicit requirements


CCEVS Issues Certificate
CCTL Accepts and CCEVS Approves Modified Product
CCEVS Certificate Product
INTEGRITY-178B Separation Kernel
Change Managed by GHS with CCEVS & CCTL Involvement
Product Change
Change Within GHS Assurance Maintenance Scope?
No
Target of Maintenance Product
INTEGRITY-178B Separation Kernel
Product Change
Yes
Security Analyst
Change Managed by GHS without CCEVS Involvement

Lessons Learned

- Lesson #4: EAL 6+ certifications can be reused
  - Assured Maintenance (AMA)
  - From SKPP 6.6.1.1: Explicit: Assurance Maintenance Plan (AMA_AMP_EXP.1)
  - http://www.niap-ccevs.org/st/st_vid10119-add1.pdf

Requirements: Vulnerability Assessment

Requirement	Description	SKPP	CAPP	Notes
AVA_CCA	Covert channel analysis	2+	0	Inter-partition analysis
AVA_MSU	Analysis and testing of insecure states	3	1	All potential insecure states
AVA_VLA	Vulnerability assessment	4	1	NSA pen testing

- Emulate sophisticated attack threat

Lessons Learned

- Lesson #5: high assurance pen testing is a black box
  - Don’t expect to meet a schedule

Lessons Learned

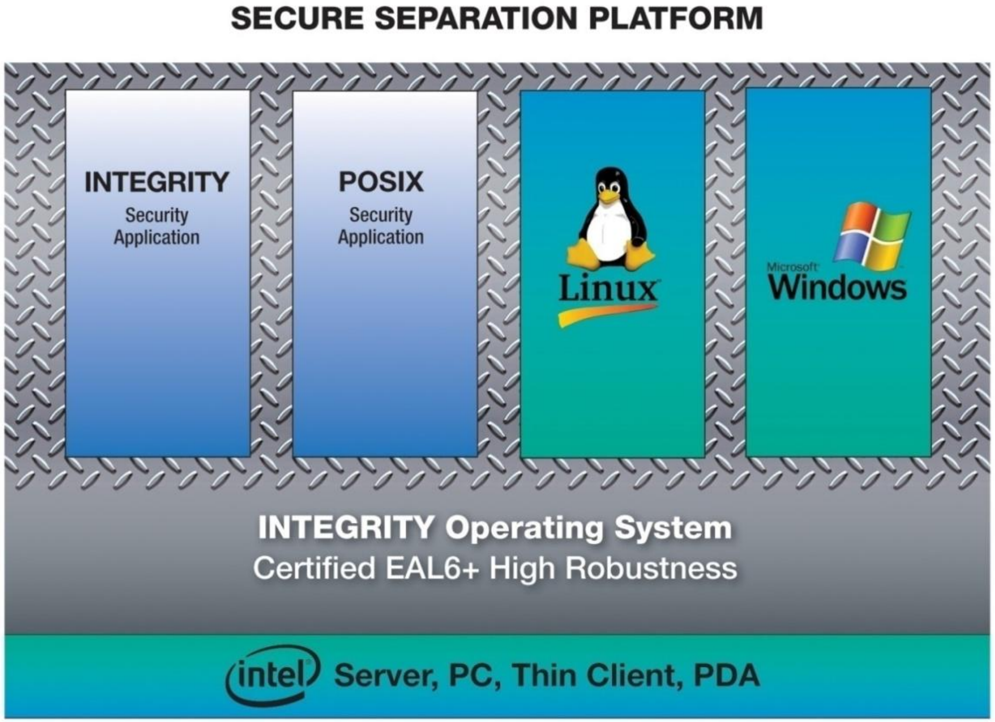
- Lesson #6: Common Criteria has an unfair bad rap
  - 99% of evaluations performed at EAL 4+ or below
  - Huge negative ROI
  - EAL 5 is the start of meaningful
  - EAL 6+ is high assurance
  - Need more high assurance products
  - Common Criteria is a generally sound approach

INTEGRITY PC - High Assurance Platform

- Thin clients, laptops, desktops, servers

<u>Benefits</u>

- Highest security where you need it
- Maintain current investment in Guest OS
- Open migration path—make system increasingly secure and reliable


SECURE SEPARATION PLATFORM
INTEGRITY Security Application
POSIX Security Application
Linux
Microsoft Windows
INTEGRITY Operating System
Certified EAL6+ High Robustness
intel Server, PC, Thin Client, PDA

Summary

- EAL 6+ High Robustness – the Gold Standard
  - Enormous ramifications and applications for application software security
- Lessons Learned
  - Lesson #7: It is possible (and practical) to achieve high assurance for important software projects