Third Party Evaluation

Presented by

Aaron Grothe

Heimdall Linux, Inc.

Overview

¥ Assurance?

¥ TCSEC

¥ Common Criteria

¥ ICSA

¥ Heimdall Linux Case Study

¥ Predictions

¥ Q&A

Assurance?

- Spencer the Katt a few years ago reported a rumor that IBM was considering dropping Underwriter's Laboratory evaluations of their computers
  - This turned out to be a false rumor
  - A company like IBM would never ship a computer without the UL seal
  - The Operating System on that Machine is unlikely to have any warranty

Assurance?

¥ Problems with a simple UL-type Seal

- UL on a hairdryer has to do with lightning strikes, on software you are dealing with potentially malicious users
- A hairdryer is released and not modified. A software user has to patch his/her software regularly (IIS users)
- Composition: You don't install you hair dryer on top of a power drill

Assurance?

- Potential benefits of Assurance:
  - Better documentation
  - Improved security
  - Opens product to new markets

Assurance?

- The U.S. Government intelligence agencies recognized the need for the ability to evaluate systems since the late 1970s.
- The Computer Security Act of 1987 prohibits the NSA from attempting to directly address the needs of commercial systems
  - With the move from GOTS (Government Off The Shelf) software to COTS (Commercial Off the Shelf) Software, there has been an attempt to find common ground

NSTISSP Number 11

- National Security Telecommunications and Information Systems Security Policy No. 11
- Systems used to enter, process, store, display or transmit national security information
  - Effective January 1, 2001 preference will be given to evaluated products
  - July 1, 2002 acquisition shall be limited to evaluated systems
  - Waivers of course are possible

TCSEC

- TCSEC (Trusted Computer System Evaluation Criteria)
- TCSEC has been largely superseded by Common Criteria Program
  - No new evaluations are supposed to be being done under TCSEC
  - Several evaluations are still pending

TCSEC

¥ TCSEC is commonly referred to as one of the following

- Orange book: the cover of the standards book for basic security
- Rainbow Series: there is a whole series of books in the TCSEC system, each with a different colored cover
- C2 or B1 the most common certifications

TCSEC

- TCSEC was published in 1985
- There are seven classifications in the TCSEC hierarchy listed in ascending security level
  - D
  - C1, C2
  - B1, B2, B3
  - A1

Class D: Minimal Protection

¥ Was Available to any product that sought an evaluation

¥ Provided a description of security mechanisms E.g. auditing, user login

¥ Available as a subsystem to add to an existing product E.g. Mac OS 9.x multi-user support

¥ This is where MS-DOS, MS Windows 9x and Mac OS out of the box would be evaluated

Class C1: Discretionary Security Policy

¥ Provides separation of users and data

¥ Achievable by most modern Operating Systems

¥ Limited support for this evaluation by the testing Labs

¥ This is where most stock UNIX systems or Microsoft Windows NT/2000 would be evaluated

Class C2: Controlled Access Protection

- Discretionary Access Control (DAC)
- Auditing
- Obtainable by most Modern Operating Systems with modifications
- Windows NT 3.5/4.0 in special configurations and many UNIX variants

Class B1: Labeled Security Protection

- Mandatory Access Control (MAC)
- Smaller number of Options
- Requires a much higher level of changes to an Operating System
- Sun Trusted Solaris and SGI IRIX are available at this level
- SGI released their B1 code from IRIX under an Open Source License and are porting it to Linux

Class B2 or Higher

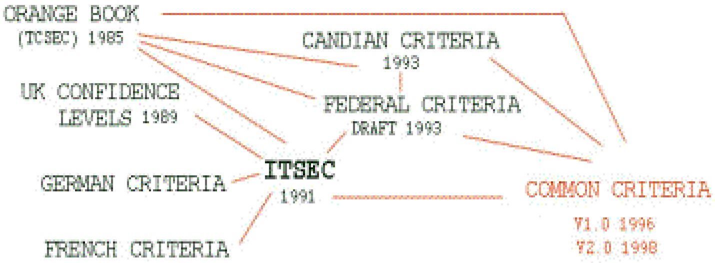
- Increasing emphasis on design
- At A1 level almost requiring mathematical proofs
- Diminished functionality
- Increasing Costs
- Most Common system was dockmaster a B2-evaluated Honeywell Multics System used as an e-mail/news hub for much of the TCSEC project

Summary of TCSEC

- TCSEC while being superseded by the Common Criteria is still an important standard
- Common Criteria evaluated versions of Operating systems such as Microsoft Windows NT/2000 and Sun Solaris currently are not available
- Proven standard

Common Criteria

- History



ORANGE BOOK
(TCSEC) 1985

CANDIAN CRITERIA
1993

UK CONFIDENCE
LEVELS 1989

FEDERAL CRITERIA
DRAFT 1993

ITSEC
1991

GERMAN CRITERIA

FRENCH CRITERIA

COMMON CRITERIA
V1.0 1996
V2.0 1998

Common Criteria

- There are currently seven levels in the CC program
  - EAL1-EAL7
- Common Criteria is an attempt to unify the European/United States and Canadian certifications programs into one standard
- The full name of the Common Criteria is Common Criteria for Information Technology Security Evaluation (CCITSE)

Differences with TCSEC

¥ CC is a multi-national arrangement

– Currently 14 counties are signatories

¥ CC is an evolving standard with a future

¥ A product can be evaluated on a platform that is not evaluated. Under TCSEC to get a certified product you had to certify it on a certified platform, using either the Trusted Database Implementation (TDI) or Trusted Network Implementation (TNI)

Mapping TCSEC to CC

This is a rough mapping

EAL 1	D1
EAL 2	C1
EAL 3	C2
EAL 4	B1
EAL 5	B2
EAL 6	B3
EAL 7	A1

EAL1: Functionally Tested

- Can be done without developer interaction
- Examination of documentation as provided to consumers
- No process inspection of developers

EAL2: Structurally Tested

- Requires developer involvement
- Does not require complete development record
- Requires compliance with "good" commercial practices, source code control, documentation, testing and so on

EAL3: Methodically Tested and Checked

- Requires "grey box" testing
- Selective confirmation of test results
- Evidence of developer's search for obvious vulnerabilities

EAL4: Methodically Designed, Tested and Reviewed

- Requires independent search for vulnerabilities
- Highest level at which it is economically feasible to be retrofit to an existing product line
- Highest level for which most testing labs are able to provide certifications

EAL5 through EAL7

- EAL5 and higher are not currently accepted by other countries. E.g. a product evaluated at EAL5 in the United States will only be recognized at EAL4 by other countries
- Requires testing lab involvement throughout the lifecycle

CC Terminology

¥ PP : Protection Profile is a template that addresses a specific set of functions and assurance requirements. E.g. Firewalls

¥ TOE: Target of Evaluation is the part of the system or product that is submitted for evaluation. This allows the evaluation of components such as a web server or database

CC Terminology

- ST: Security Target is a set of functional requirements that will be the standard used to evaluate the product
- FER: Final Evaluation Report is the result of the ST being tested against the product

CC Summary

- Common Criteria is the next generation of certifications
- Still an evolving standard more protection profiles are being created
- Protection profiles will hopefully be mutually accepted

ICSA

¥ ICSA labs is a private company that performs testing and offer certification in several areas

- Anti-Virus Software
- Firewalls
- IPSEC Products
- Cryptography Products

ICSA

- ICSA is a for-profit company
- ICSA performs basic black box testing
- ICSA has a pass-fail system there are no increasing levels

ICSA

- ICSA has performed certifications on over 40 firewalls
  - this outnumbers the number of firewalls evaluated under the CC and TCSEC programs combined

ICSA Summary

¥ ICSA has been beneficial for some companies

¥ ICSA is limited as it only addresses specific areas

¥ Microsoft received ICSA certification for their ISA firewall

  – this being their first firewall a functional evaluation was very beneficial

  – lower curve as opposed to TCSEC and CC made it easier to quickly receive certification

Heimdall Linux Case Study

- HLI was formed in 2000 for the purpose of creating Linux based products that would be certified under the DoD approved certification
- HLI's initial plan was to develop a certified firewall under the TCSEC process

Heimdall Linux Case Study

- There were two potential avenues we considered under the TCSEC program
  - Get the firewall certified as a subsystem in the D range
  - Certify the base Linux Operating System at the C-2 level and then use the Trusted Network Interoperation (TNI) to get the firewall certified

Heimdall Linux Case Study

¥ Problems with D-range certification

- Not considered a valid certification by many
- Limited experience at the testing labs. Only a few products have been evaluated as a subsystem

Heimdall Linux Case Study

- Problem with C2 certification
  - Having to certify the base Operating System and then the firewall subsystem would take a long time

Heimdall Linux Case Study

- Decision
  - While the team's experience was predominately in the TCSEC arena the retirement in favor of Common Criteria program forced us to reconsider our options

Heimdall Linux Case Study

- We decided to do an EAL2 version of the firewall
  - EAL1 was regarded as insufficient to meet our market's security needs
- The availability of a Protection Profile (PP) for a firewall is a major benefit

Heimdall Linux Case Study

- EAL2
  - At the EAL2 we have been able to keep kernel changes to a minimum
    - We have had to change approximately 100 lines in the Linux 2.4 kernel to achieve compliance
  - The practices we have to follow Source Code Control and so on are typical for our company

Heimdall Linux Case Study

- Status
  - HLI has currently finished the Security Target (ST)
  - HLI will be undergoing its evaluation shortly after closing our second round of funding

Heimdall Linux Case Study

- Lessons Learned
  - Evaluate several testing labs
  - Flexibility is key
  - Establishing good relationships are key

Predictions

- Common Criteria will continue to gain ground
- The search for the "Good Housekeeping" or "UL-type seal" will continue
  - Programs like Visa Global Data Security and TruSecure will attempt to address the web side of this component
- As more and more software is written in .NET and Java, security will improve (in the long term)
- "The Journey is the Reward" – Old Zen Buddhist Saying

Presentation (HTTP)

- The Presentation will be available in its entirety on the Heimdall Linux Web Site http://www.heimdall-linux.com in our papers & presentations section

Resources

- Radium Homepage (home of TCSEC and Common Criteria) http://www.radium.ncsc.mil
- Common Criteria Home Page http://www.commoncriteria.org
- ICSA Homepage http://www.icsa.net

Footnotes

1 – "A UL-type Seal For Security? Don't Bet on It."
Scott Berinado, eWeek October 15, 2000
http://www.zdnet.com/eweek/stories/general/0,11011,2640597,00.html

2 – "National Security Telecommunications and Information Systems Security Policy" NSTISSP No. 11 National Information Assurance Acquistion Policy
http://www.nstissc.gov/Assets/pdf/nstissp11.pdf

Contact Us

- E-mail: grothe@heimdall-linux.com
- Website: www.heimdall-linux.com

Q & A

- Questions