ORACLE®

The Common Criteria, What's Next?

2017 International Cryptographic Module Conference

Joshua Brickman
Director, Security Evaluations

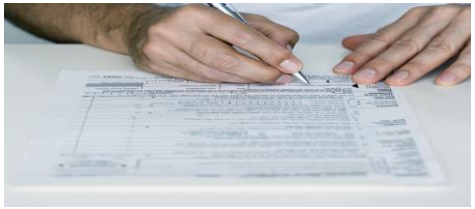
May 2017

Today's Speaker

Joshua Brickman, Director, Security Evaluations

- Leads Product Security Evaluations @ Oracle
- Frequent Speaker at Security Conferences
- Completed Many Cert. Projects since 2006

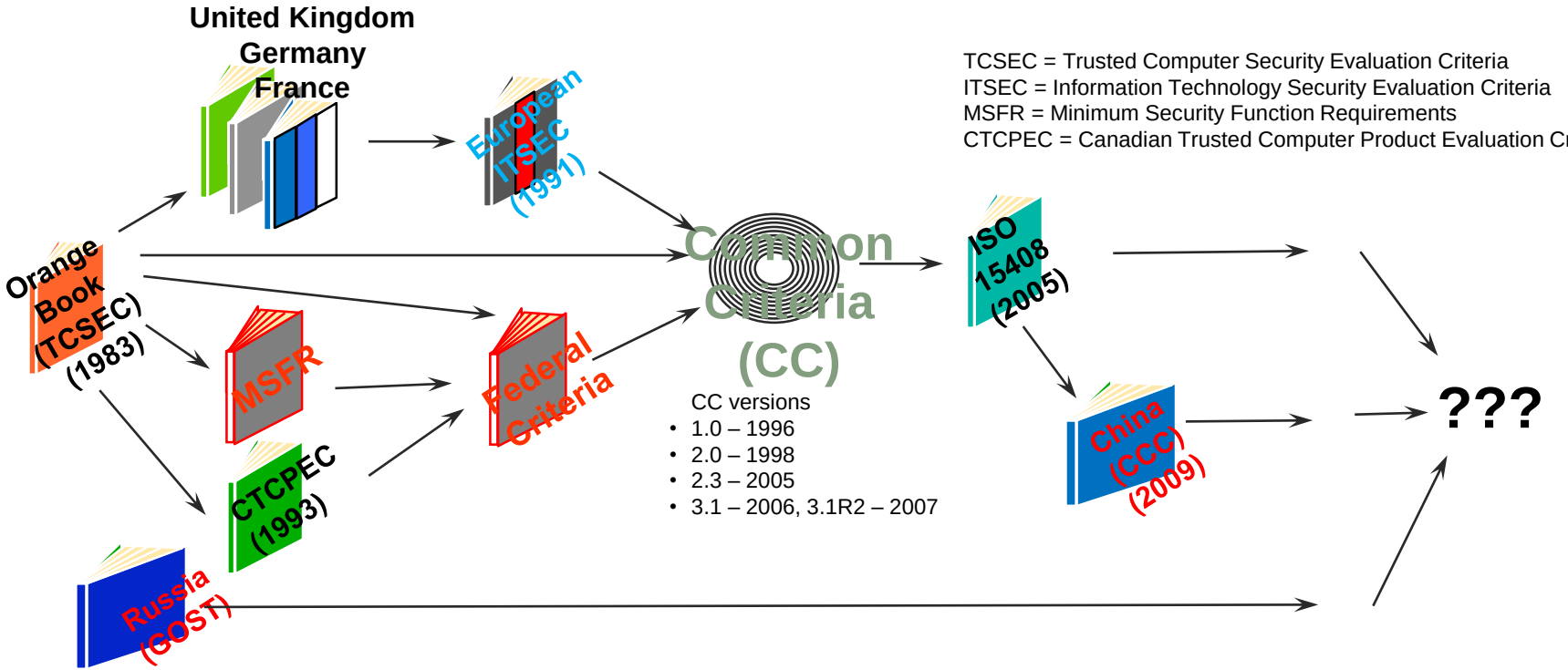
Agenda



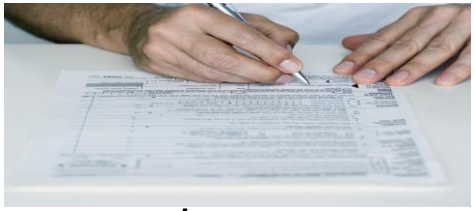
- The Common Criteria a ***brief*** history
  - Recent changes—CCRA
  - Transition to new CCRA
- Balkanization of the CC
- Keeping the “Common” in CC
- Examples
- Conclusions
- Q and A

Product Security Evaluation Criteria

Evolution



Why *Common* Criteria?

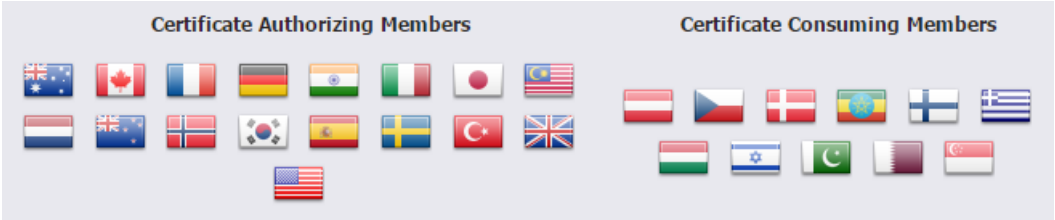


- Why governments moved from their single country IT product security evaluation criteria
- Why product vendors encouraged move to single international criteria
- Governments understood that
  - Vendor repetition in each country/scheme ⇨
  - Reduced choice of evaluated products ⇨
  - Reduced national security

CC Recognition Arrangement

Initial arrangement until 2014 update

- 27 countries of CCRA



- ***CCRA is essential for product vendors***
- SOGIS

- Austria, Bundeskanzleramt
- Finland, FICORA - Finnish Communications Regulatory Authority
- France, ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information
- Germany, BSI - Bundesamt für Sicherheit in der Informationstechnik
- Italy, OCSI - Organismo di Certificazione della Sicurezza Informatica
- The Netherlands , NLNCSA - Netherlands National Communications Security Agency, Ministry of the Interior and Kingdom Relations
- Norway, SERTIT - Norwegian National Security Authority operates the Norwegian Certification Authority for IT Security
- Poland, NASK - Naukowa i Akademicka Siec Komputerowa
- Spain, CCN - Centro Criptológico Nacional, Organismo de Certificación de la Seguridad de las Tecnologías de la Información
- Sweden, FMV - Försvarets Materielverk
- United Kingdom, NCSC - National Cyber Security Centre

U.S. Led Change of Strategy

CC was never perfect

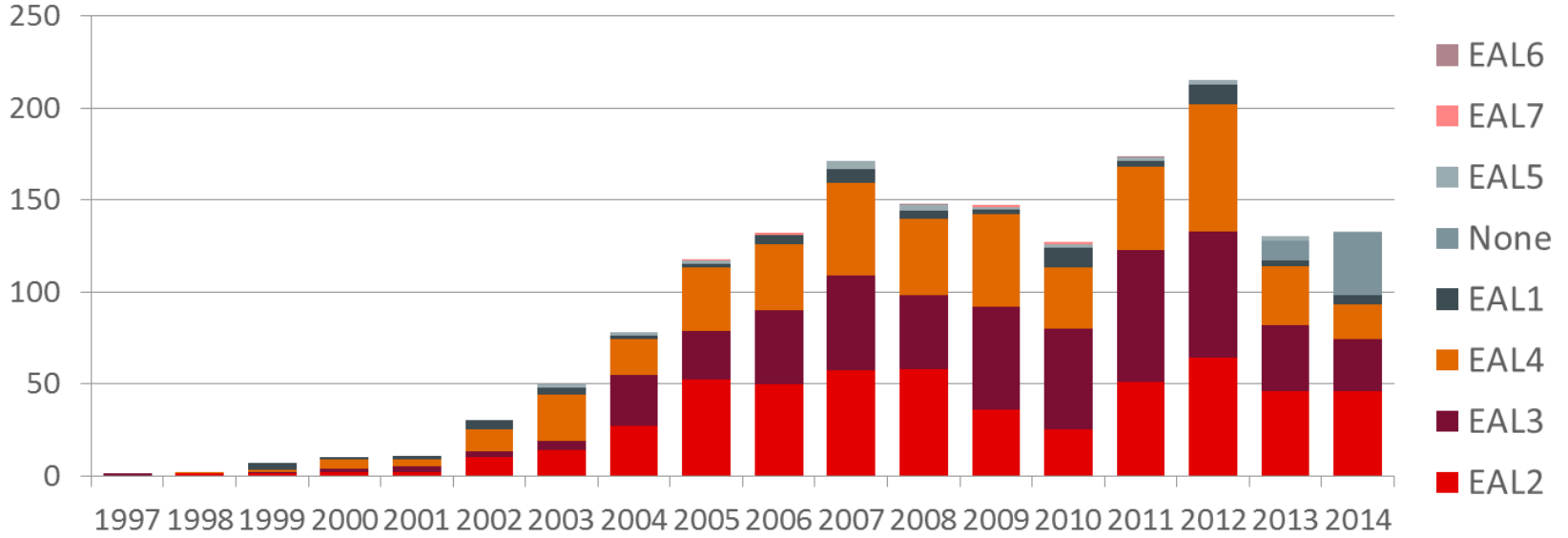
- NIAP - US Common Criteria scheme owners, part of NSA
  - CC evaluations not “meaningful”, “unrealistic” configurations
  - Hacker attack methods untested
  - Too slow, too expensive, not repeatable (by different labs)
  - Too much IP delivered to labs
- 2011 International CC Conference, Kuala Lumpur, Malaysia
  - Elimination of EALs (Evaluation Assurance Levels)
  - Requiring PP’s (Protection Profiles)for all evaluations
  - Assurance requirements detailed in the PP’s vs. in the Common Criteria

Impact of U.S. Led Strategy Change

2009-2012 Confusion and Uncertainty

- NIAP started working on persuading other CCRA countries of new direction
- But the change was not rolled out to procurement officers
  - Unclear whether products need a CC certificate
  - Unclear whether products with non-US CC certificate will be accepted
  - U.S. customers still demanding products with CC certificates
- CCRA renegotiation
  - EAL4 down to EAL2
  - PP (technology specific) driven assurance
- Practical impact
  - Oracle broadly advocated strategy, educated customers
  - Significant reduction in non-smartcard evaluations

Certificates by EAL each year non-Smart Card.



EAL2 the biggest overall, but EAL4 dropped since 2012 and 'None' increasing. Number of non-smartcard evaluations dropped from a peak of 213 in 2012 to around 130 a year in 2013/2014 **(~50% drop).**

Impact of U.S. Led Strategy Change

2012-2014 Clarity Emerges

- US scheme (NIAP) strategy more widely accepted (2012)
  - CC roles out their “Vision Statement”
- Technical Communities
  - Writing technology specific PPs
  - Product vendors, lab consultants, national schemes
  - Oracle asked to lead creation of DBMS PP (2012)

Impact of U.S. Led Strategy Change

2014 - Present

- NIAP (2014) Announces initial priorities
  - Issues negative statements on O/S, DBMS and ESM
- Updated CCRA (2014) arrangement signed
- India Telecoms Regulations
- Other countries with “add on”, “top up” requirements
- US and other countries conducting NIAP evaluations
- But all is not well….

Factions

SOG-IS vs CCRA

CC Utilizations	SOG-IS	CCRA
Approach	High Assurance	Fast, Repeatable, Objective
Primary End-Users	Banks, Finance, Government	Defense, Government
Assurance Approach	EAL 5 and 6, strong vulnerability testing requirements	Black box testing
Protection Profile Strategy	Strict conformance (can add on)	Exact Conformance (all or nothing, no add-ons)
View of EAL /ST evaluations?	No problem	EAL2 or less, FiveEyes won't allow if a PP exists (either NIAP or cPP)

Exact Conformance?

- Why do the FiveEyes countries demand exact compliance to National PP's?
  - To ensure all evaluations are done the same way
  - To speed up evaluations
  - To stop vendors using evals as a competitive advantage
- But this approach does not allow for:
  - Innovation
  - Addresses only national concerns
  - Often forces vendors to top-up or do multiple evals of same product
  - Open, international collaboration

Market Demand and Scheme responses

- Customers demand CC whether a PP exists or not
- Hard enough to “educate” customers on reduced EAL requirements
- ST evaluations will continue to be necessary
  - cPP’s take a long time
  - NIAP PP’s (other primary PP authors in CCRA) are NIAP priorities but not necessarily customers/vendors

Balkanization!

Here is what the CC world looks like after the transition

- CCRA
  - Technically all 27 countries
  - A sub-set not really following it
- SOG-IS
  - 11 countries continuing to mutually recognize high assurance evaluations
- National PP's
  - Dominating author is US Scheme
  - Too hard to get PP's written in cPP approach
- Resulting in…
  - Duplicate and delta evaluations
  - Rising costs of COTS and lowering quality

It’s Already happening…

This appears to be the same product evaluated twice…

Cisco Catalyst 6500-E Series Switches Cisco IOS Software, Version 15.1(1)SY1, RELEASE SOFTWARE (fc5) Cisco Systems, Inc. Certification Report Security Target Protection Profile Maintenance Report(s) 1. 2014-04-14 – Cisco Catalyst 6500-E Series Switches, Hardware models - WS-C6503-E, WS-C6504-E, WS-C6506-E, WS-C6509-E, and WS-C6513-E with Supervisor 2T (Sup2T) Cards (VS-S2T-10G or VS-S2T-10G-XL) Software version - IOS15.1(1)SY1 Maintenance Report Maintenance ST	PP Compliant ND-PP	2014-02-20	DE
Cisco Catalyst 6500-E Series Switches Cisco IOS Software, Version 15.1(1)SY1, RELEASE SOFTWARE (fc5) Cisco Systems, Inc. Certification Report Security Target	EAL2+ ALC_FLR.2	2014-02-20	DE

A possible fix

A proposal

- Let's change what "recognition" means
  - Instead of vendors feeling that they must conduct multiple certs of the same product, allow higher level certs to be conducted, with countries that prefer lower assurance **discounting the superset**
- Allow add-on's or top-ups
  - to National PP's or cPP's to support market demand
- Look to SOG-IS for a template
  - Create a "recommended for use" list
  - Acknowledge all CC evals are valid

How this might work…an example

General Purpose Operating Systems—today*

- NIAP US OSPP (EAL1) v4.1
  - FiveEyes will recognize
  - Some countries will feel not high assurance enough for their use
- BSI German (EAL4+ PP)
  - 22 countries will accept such a product (different than “recognition”)
  - FiveEyes will not recognize
- Conduct an ST evaluation
  - 21 countries will recognize (Germany would expect their PP to be used)
  - FiveEyes will not recognize

*all three have been attempted or are being done at this writing

How this might work…an example continued

General Purpose Operating Systems—a better approach?

- NIAP OSPP v4.1 with top up
  - NIAP should recognize, but leave out/ignore the top up
  - Meets other countries requirements as well
- BSI (German EAL4+ PP) with NIAP specific SFR's
  - NIAP should recognize only the bit that is their PP
  - Meets other countries requirements as well
- Conduct an ST evaluation
  - Not necessary

(note NIAP should remove GPOS position statement)

How this might work…Example 2

DBMS—today

- NIAP
  - No PP not recommended
  - Officially recognized due to CCRA
- BSI (German EAL2+ PP)
  - 22 countries will accept such a product (different than "*recognition*")
  - FiveEyes does not recognize
- Top Up?
  - Go above EAL2 and only recognized in country evaluated
  - FiveEyes will not recognize

How this might work…Example 2 continued

DBMS—a better approach?

- BSI (German EAL2+ PP)
  - An option for now
  - Meets other countries requirements as well
- cPP for DBMS
  - Initially a reduced scope
  - Feedback provided by multiple countries
  - Some FiveEyes willing to evaluate against

(note NIAP should remove DBMS position statement)

Conclusions

- CC is becoming less and less “Common”
  - Too much desire to boost national self-interest than have broad range of CCRA recognized products to choose from.
- Need to re-think what will be best for the community and shelve country specific interests
- CC is the only product security evaluation arrangement that has had such worldwide recognition.
  - Selfish decisions by schemes will leave it very weak
  - Other approaches will step in and try to take evaluation mantle

Common

- of or relating to a community at large **:** PUBLIC work for the *common* good

  ***2a*: belonging to or shared by two or more individuals or things or by all members of a group** a *common* friend buried in a *common* grave ***common* interests**

Questions? Thoughts?

Thank you!

Josh Brickman

joshua.brickman@oracle.com

+1-781-442-0451

Hardware and Software

ORACLE

Engineered to Work Together


ORACLE®