HS SEDI
Homeland Security Systems Engineering and Development Institute

Refining the Common Criteria for Objective and Predictable Security Measurement

Sean Barnum

December 14, 2010

Homeland Security

Today's Situation

HS SEDI
Homeland Security Systems Engineering and Development Institute

- **Common Criteria offers significant value**
  - Internationally agreed to process
  - International reciprocity

- **Common Criteria has significant limitations**
  - Focuses almost all measurement on product security functionality & structure
  - Provides almost no objective measurement of actual security (vulnerability) of the product
    - What little objective measurement it does contain is very ambiguous and mostly left up to each lab to define
    - Very difficult to predict or scope effectively
    - Left unsure of what results actually mean

Desired Goals

- **Objectively Measurable Security**
  - Measure actual vulnerability of product

  CWE & CAPEC

- **Consistency of Analysis from lab to lab and evaluation to evaluation**

  Structured assurance cases utilizing CWE & CAPEC

- **Predictable Scope for Evaluations**

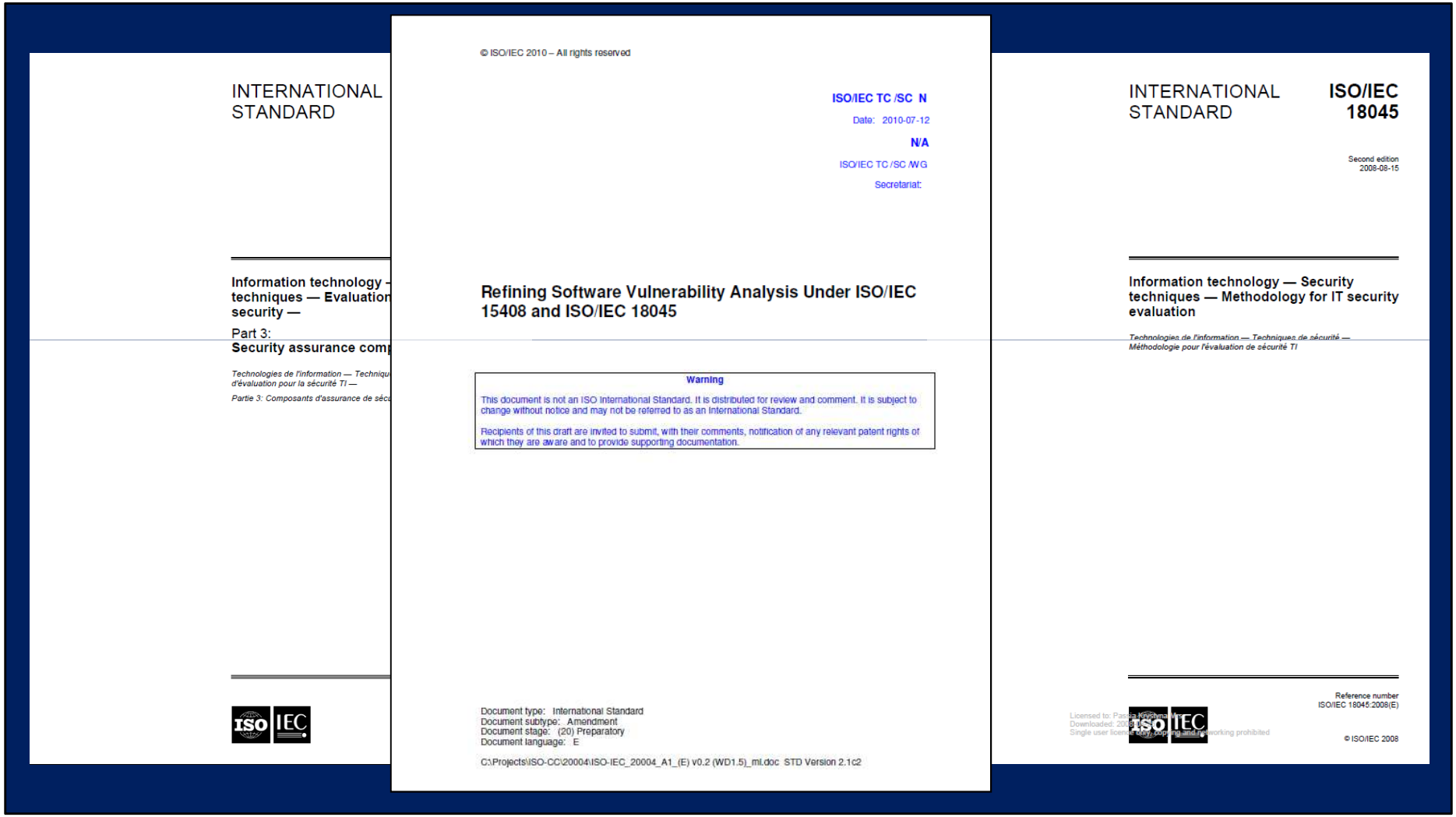
  Structured assurance cases utilizing CWE & CAPEC

Varying Efforts

HS SEDI
Homeland Security Systems Engineering and Development Institute

- **NIAP**
  - Currently investigating how best to integrate use of CWE, CAPEC & structured assurance cases
  - Focusing more on the upfront elements of CC (PPs & STs)
  - First steps currently underway in the form of a new, more structured protection profile for firewalls
- **ISO/IEC**
  - TR 20004 utilizing CWE, CAPEC & structured assurance cases to refine ISO/IEC 15408 & ISO/IEC 18045
- **Common Criteria Development Board (CCDB)**
  - Evaluating and planning how best to integrate CWE, CAPEC & structured assurance cases
  - Collaborating in ISO efforts with a plan to incorporate the results into CCDB policy & guidance

ISO/IEC 20004: Refining Software Vulnerability Analysis Under ISO/IEC 15408 and ISO/IEC 18045



INTERNATIONAL STANDARD

Information technology –
techniques — Evaluation
security —

Part 3:
Security assurance comp

Technologies de l'information — Techniqu
d'évaluation pour la sécurité TI —

Partie 3: Composants d'assurance de séc

ISO IEC

ISO/IEC TC /SC N

Date: 2010-07-12

N/A

ISO/IEC TC /SC /WG

Secretariat:

Refining Software Vulnerability Analysis Under ISO/IEC 15408 and ISO/IEC 18045

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype: Amendment
Document stage: (20) Preparatory
Document language: E

C:\Projects\ISO-CC\20004\ISO-IEC_20004_A1_(E) v0.2 (WD1.5)_ml.doc STD Version 2.1c2

INTERNATIONAL STANDARD

ISO/IEC 18045

Second edition
2008-08-15

Information technology — Security techniques — Methodology for IT security evaluation

Technologies de l'information — Techniques de sécurité — Méthodologie pour l'évaluation de sécurité TI

ISO IEC

Reference number
ISO/IEC 18045:2008(E)

ISO/IEC 20004 Approach

- **Avoid politics as much as possible**
  - Author an ISO/IEC Technical Report (TR) rather than attempt to revise the actual standards
  - Work incrementally to minimize resistance to change
- **Collaborate and coordinate among the authoritative players (ISO, CCDB & NIAP)**

A Brief History of ISO/IEC 20004

HS SEDI
Homeland Security Systems Engineering and Development Institute

- **A New Work Item Proposal (NWIP) was prepared by the US Delegation in preparation for the April 2010 SC27 meetings in Melaka Malaysia**
  - Atypically, this NWIP was an actual full draft of a document
- **NWIP was presented and discussed in Melaka with very positive review and input from several other national bodies**
- **Working Draft 1 (WD1) was prepared based on the comments from Melaka and submitted for review at the Oct 2010 SC27 meetings in Berlin, Germany**
- **WD1 was discussed in Berlin with support and input from several national bodies (US, UK, Sweden, France, Germany, Japan, Korea)**
- **Working Draft 2 (WD2) will be finished this week and submitted for discussion at the April 2011 SC27 meetings in Singapore**
- **Goal is to have first iteration finalized and published by late 2011 or early 2012**

In a nutshell, what does this version contain?

HS SEDI
Homeland Security Systems Engineering and Development Institute

- **Introduces CWE as one of the standard resources for identifying and specifying relevant vulnerabilities (weaknesses)**
  - Filters relevancy based on technical context and maturity of CWEs as well as effectively implemented mitigations
- **Introduces CAPEC attack patterns as a mechanism to objectively characterize attack potential in relation to relevant vulnerabilities and to support the specification of relevant security/penetration tests**
  - Filters relevancy based on technical context and maturity of CAPECs as well as effectively implemented mitigations
- **Introduces concept that in the future evaluations may be specified utilizing PPs or STs based on structured assurance cases**
- **Specifies that penetration tests carried out as part of the evaluation should identify the CWE being tested for, the CAPEC being instantiated and the detailed attack execution flow being carried out**

What is planned for the next revision after publication?

- Introduce weakness identification and analysis activities (e.g. secure code review, architectural risk analysis) in addition to penetration testing

- More comprehensively and formally integrate in the concept and use of structured assurance cases