Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Adaptation of the Common Criteria for Authentication and Certification

JACOB BENZ, MATT MACDOUGALL, KEITH TOLK

Pacific Northwest National Laboratory

Novel Technologies and Approaches Workshop, SNL, August 29-30 2017

Outline

- Introduction to the Common Criteria
- Common Criteria Approach
- Adaptation of Approach to Authentication and Certification
- Conclusions and Future Work

- Takeaways from Presentation:
  - What is the Common Criteria?
  - What are the needs of authentication and certification?
  - What aspects of the Common Criteria could be useful for authentication and certification?

Introduction to the Common Criteria

- Common Criteria for Information Technology Security Evaluation
- Common Methodology for Information Technology Security Evaluation
- Internationally recognized standard: ISO/IEC 15408
- Provides for consistent evaluation approach for Information Technology (IT) products across laboratories, countries

- In the U.S., managed by National Information Assurance Partnership (NIAP)
  - Partnership between NIST and NSA
  - Review and approval of IT equipment for national security applications

Authentication and Certification

- Authentication
  - **Is a process** through which monitoring party gains and maintains confidence that the equipment and resulting data reflect the true state of the monitored, treaty accountable, item(s).
  - Initial authentication: Evaluate equipment to establish a trusted copy
  - On-site authentication: Limited evaluation just prior to use
  - Chain of custody: technologies to maintain integrity of equipment
- Certification
  - **Is a process** by which a monitored party to a treaty or agreement assures itself that an inspection/monitoring system meets required safety and security requirements and will not divulge classified or proliferative information to a monitoring party
  - Safety certification: well defined process that may be facility specific
  - Security certification: Very similar to authentication, but focused on protection of information
  - Managed Access: Approach to maintain certification during inspections

Authentication and Certification Needs

- Evaluate, confirm and maintain authenticity and integrity of equipment
- Safety certification tends to be well established and facility defined

- Current approach to authentication and security certification can be inconsistent and subjective

- **Can the internationally accepted, consistent, and quantifiable CC evaluation approach be leveraged to enhance authentication and security aspects of certification?**

Common Criteria Evaluation Approach

- Define a Protection Profile (PP)
  - Defining a common set of security needs
  - Provides: Narrative, expected functions, security requirements, and operational environment for Target of Evaluation
  - *Call for Proposal*
- Define a Security Target (ST)
  - Identifies security requirements met by TOE and defines scope of evalulation
  - *Response to Call for Proposal*
- Identify a Target of Evaluation (TOE)
  - Specific piece or model of equipment for evaluation
- Define Assurance Requirements and Levels
  - Evaluation Assurance Level (EAL) selection for Target of Evaluation
  - May be defined as part of PP or ST
- Perform Evaluation Activities
  - Actual evaluation of TOE based on security and assurance requirements

Current Status of Approaches for Authentication and Security Certification

- Current processes for authentication are not well defined, and evaluation may be inconsistently applied
  - This may lead to inconsistent confidence applied to equipment
- Ongoing research looking to better define approaches
  - Tiers I – IV which identify steps of varying cost, complexity and intrusiveness to allow for varying levels of confidence
  - Importance of Vulnerability Assessments (VAs) to identify potential weaknesses/vulnerabilities
    - Help to define design changes or on-site authentication measures to mitigate
  - No well-defined methodology to define confidence with respect to evaluated equipment
  - Difficult to identify a single approach which applies to all potential equipment

- **How can the CC process be adapted to address current weaknesses in authentication and security certification approaches and research?**

Well Defined Methodology to Define Assurance: Evaluation Assurance Levels

- EAL1: Functionally Tested
- EAL2: Structurally Tested
- EAL3: Methodically Tested and Checked
- EAL4: Methodically Designed, Tested, and Reviewed
- EAL5: Semi formally Designed and Tested
- EAL6: Semi formally Verified and Tested
- EAL7: Formally Verified and Tested

- Increasing EAL increases the scope, depth, and rigor of evaluations to provide higher confidence
  - EAL is broken down into Assurance Classes which define areas of evaluation
  - Classes broken down into Assurance Components. Components broken down into Assurance Elements
  - Elements are the lowest level security requirements which must be met through evaluation

Assurance Class	Assurance components (EAL4)
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Well Defined Methodology to Quantify Assurance

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- 2001 report authored by PNNL as part of Authentication Task Force (ATF) effort
- Defined a set of AALs
  - Created to address unique assurance requirements for monitoring systems
    - Under former Soviet Union and Russian Federation bilateral treaties/agreements
  - Represented increasing levels of assurance through:
    - Increased rigor, scope, and/or depth of evaluation
- AAL0- Unauthenticated
- AAL1- Minimally Authenticated
- AAL2- Limited Authentication
- AAL3- Critical Authentication
- AAL4- Optimal Authentication

- AAL1: Functionally Authenticated
- AAL2: Structurally Authenticated
- AAL3: Methodically Tested and Authenticated
- AAL4: Methodically Designed, Tested and Authenticated
- AAL5: Critically Tested and Authenticated
- AAL6: Critically Designed, Tested and Authenticated
- AAL7: Formally Designed and Authenticated

- Breakdown each AAL into functional areas and requirements which must be met through evaluation
- End result would be a consistent and quantifiable level of assurance in equipment

Vulnerability Analysis (VA)

- Key activity to gain confidence in equipment
- Conduct of a VA may seem like a black box
  - Quality of VA depends on evaluator

- **How can community ensure consistency and transparency in equipment evaluation?**

- VAN1: Vulnerability Survey
- VAN2: Vulnerability Analysis
- VAN3: Focused Vulnerability Analysis
- VAN4: Methodical Vulnerability Analysis
- VAN5: Advanced Methodical Vulnerability Analysis

VA: Adversary Attack Potential

- Adversary Considerations:
  - Elapsed Time for attack
  - Expertise required
  - Available knowledge of TOE
  - Window of opportunity for attack
  - Equipment required for successful attack
- Evaluation for each VAN level
  - Well defined
  - Provides activities which must be completed based on requirements
    - Includes considerations for completion
  - Rigorously developed to allow different evaluators to walk through process and obtain similar results

Vulnerability Component	TOE resistant to attacker with attack potential of:	Residual vulnerabilities only exploitable by attacker with attack potential of:
VAN.5	High	Beyond High
VAN.4	Moderate	High
VAN.3	Enhanced-Basic	Moderate
VAN.2	Basic	Enhanced-Basic
VAN.1	Basic	Enhanced-Basic

Conclusions and Future Work

- CC provides a rigorous and comprehensive framework
  - Documentation defines expectations and requirements places on equipment
  - Evaluation confirms equipment meets expectations and requirements to given EAL
  - Allows different evaluators to arrive at similar conclusions regarding equipment assurance
- Arms control protection profiles
  - Identify assumptions and constraints on equipment
  - Define expected use cases of equipment
    - How radiation detectors perform warhead confirmation activities
- Arms control security targets
  - Define how equipment conforms to requirements relevant to protection profiles
- Evaluation- Authentication and Certification of equipment
  - Rigorous and comprehensive approach with greatest benefit
  - Attempt to remove qualitative and subjective nature of authentication and certification (SME knowledge)
  - Flexibility in confidence based on how and where equipment may be used
    - How much confidence is required

Acknowledgement: This work is currently sponsored by the Office of Nuclear Verification.

Questions?