Fighting the Bean Counters

Gerald Krummeck, atsec information security

12th ICCC, Kuala Lumpur, Sept. 2011

Issues With CC Evaluations

Last year's ICCC discussions

- Evaluations are too expensive and time-consuming
- Evaluations are not objective and not comparable enough
- Evaluations don't credit developers for their efforts to produce secure code

Proposed solutions

- Honor tools used in development process
- Speed up evaluations by providing **checklists**, avoiding clumsy analysis
  - More focused approach to some vague assurance aspects
  - Better metrics, provide guidance for evaluators

Fighting the Bean Counters

Agenda

- Introduction
- Main Part
- Conclusion

Checklist
for Presentations:
- Introduction
- Main Part
- Conclusion

Verdict: PASS

My Recent Checklist Experiences

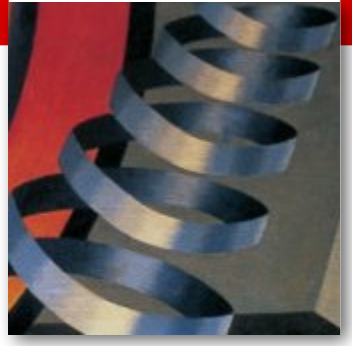
Common sense is irrelevant

Buying a beer in a US supermarket

- Checklist:
  - Request ID document, look up date of birth, calculate age
  - If ID holder is over legal drinking age (21 years), sell item
- ID document: German ID card with German date notation
- Both cashier and her manager could not identify date and calculate my age

- Objective: Don't sell alcoholic beverages to underage kids
- Checklist works most of the time, but does not cover all scenarios
- Checklist algorithm is o.k. for persons close to age of 21

My Recent Checklist Experiences



Common sense must not be applied

Fluids in carry-on baggage

- Checklist:
  - Fluids must be in re-sealable one liter plastic bag
  - Each fluid container must be 3 fl oz or less
- My bag: 1.5 gal freezer bag with 1 toothpaste, 1 shaving cream
- Security guard refused bag (although it got accepted on previous flight), tried to force me to buy a standard-conformant bag

- Objective: plastic bag shall be small enough so guard does not need to count number of containers
- Checklist provided to minimum-wage security guards without any idea why these requirements exist

My Recent Checklist Experiences

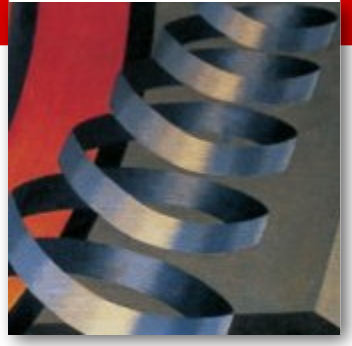
Did I already mention that common sense thing?

Tagging visitors

- Checklist:
  - Every visitor in the lab must wear a visitor's badge
- A common measure in larger companies
- In a small lab, visitor badges serve no purpose at all

- Objective: No access to evaluation information for unauthorized individuals
- Auditor's arguments
  - Fair treatment of all labs
  - “We did not make the checklist, we only must follow it”

My Recent Checklist Experiences

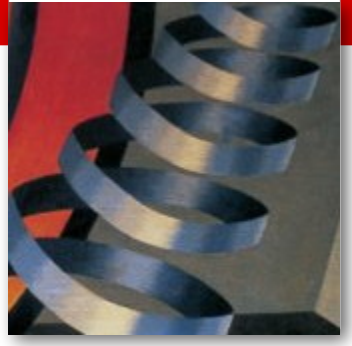


From CCDB's department of redundancy department

CEM requirements

- ASE_REQ.2.2:
  - The evaluator determines that all SARs are identified by one of the following means:
  - a) by reference to an individual component in CC Part 3;
  - b) by reference to an extended component in the extended components definition of the ST;
  - c) by reference to an individual component in a PP that the ST claims to be conformant with;
  - d) by reference to an individual component in a security requirements package that the ST claims to be conformant with;
  - e) by reproduction in the ST.
- Why not just state “EAL4”?
  - Exact identification of the SARs, no selections in SARs below EAL6
- Nobody needs that in the ST, additional work for ST author, evaluator, certifier
- CB's argument: Sorry, not in the CEM's checklist

What Went Wrong



Checklists start to live a life of their own!

- Checklists seem to work for those who wrote them
  - Because authors implicitly know about their constraints
- Training vs. education
  - Learn to execute a sequence of steps without understanding why
- Checklist authors pretend to know better than checklist users
  - We already twisted our brain so you don't have to
  - We removed the overhead: no objectives, no rationale, just do it
- Alternate ways to achieve objectives usually not considered
  - Covering all possible scenarios requires extensive expertise!
  - You still might miss some!
- Ever noticed the difference between ***check*** and ***examine*** ?

Conclusions for Cheklists

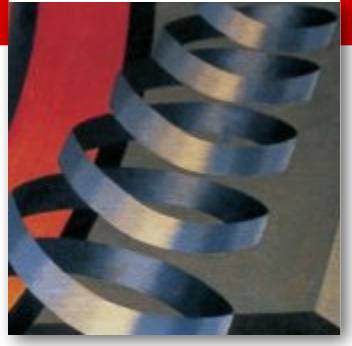
Matt Bishop on the SANS/CWE Top 25

- Just because your meet all elements of a checklist, that does not mean you are secure
- Forget a perfect checklist. It is as elusive as perfect security. A key skill is …

knowing when to ignore it

- Never confuse satisfying a checklist with security
- Satisfying a checklist is not a goal. It is a means to a goal
- **Security is the goal**
  - If the checklist helps, use it. If not, discard it

How to Use Checklists



A fool with a tool is still a fool...

- Checklists are tools ...
  - If they fit your scenario, they may save time and effort
  - They may help you to cover all aspects of your analysis
  - I use checklists all the time...
  - but I use mine, adapted for the current project
- ... to achieve **objectives**
  - Rather than tick boxes
  - Use checklist only as guidance
  - Allow other means as long as objectives are met
  - Don't require rationale for every point – bloated reports hide the important stuff!
  - Require rationale how objective was met – even when using checklists

Where to go from here

All rules have exceptions (even this one :-)

We need to focus on the objectives!

- Unfortunately, they seem to have been lost over time
- Objectivity is useless unless you meet your objectives
- CC and CEM updates should have this as a primary goal
- For every CEM work unit, evaluators must know why it is important to perform it
  - Not performing the work unit should bear the risk of undetected vulnerabilities
  - If that's not the case, get rid of it
- If you want to compensate for the additional effort, reduce ACM_CMC and ACM_CMS, for starters
- If I gave you all of our points, somebody might use it as a checklist...

Thank you!

Questions?
Comments?