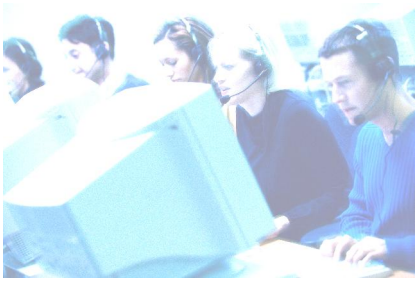
The 7th International Common Criteria Conference, 19-21 September, Lanzarote, Spain
20 September, Track 3, 11:00-11:30 am

Software Security Reviews

- Summarized experiences that led to a new methodology.



COMBITECH

About the Speakers.

Peter Bayer
M.Sc. Software Engineering

Project leading
Tech. Software Security Reviews

peter.bayer@combitech.se

Magnus Ahlbin
B.Sc. Computer Science

Head of ITSEF at Combitech AB
Senior Expert of Security Reviews

magnus.ahlbin@combitech.se

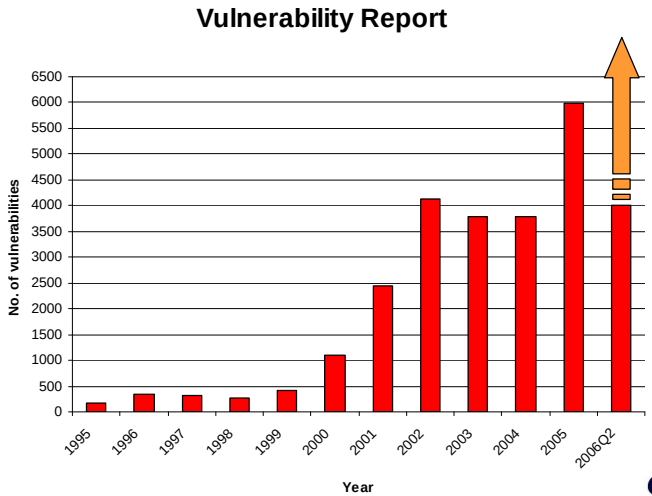
COMBITECH

Agenda.

- Background
- Motivation, Aim and Goal
- Work Process
- Outcome
- Connections to Common Criteria
- Summary

COMBITECH

Background.



In total: ***26,713 pcs.***

Source: CERT/CC (Aug-2006)

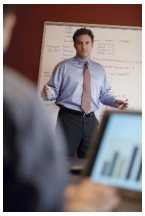
COMBITECH

Motivation, Aim and Goal.

- Motivation
  - Deeper review for the money, penetration vs. correctness, funnier to perform, etc.
- Aim
  - Less vulnerabilities in software, faster security review
- Goal
  - Short guidelines, cheap to use, effective (90%), easy to introduce, use and repeat, easy to map to well-known software development processes, etc.

COMBITECH

Work Process.



- Interviews, experiences from security reviews, literature studies, remittance, feedback, lecturing (course)

COMBITECH

Outcome – A Methodology Handbook.

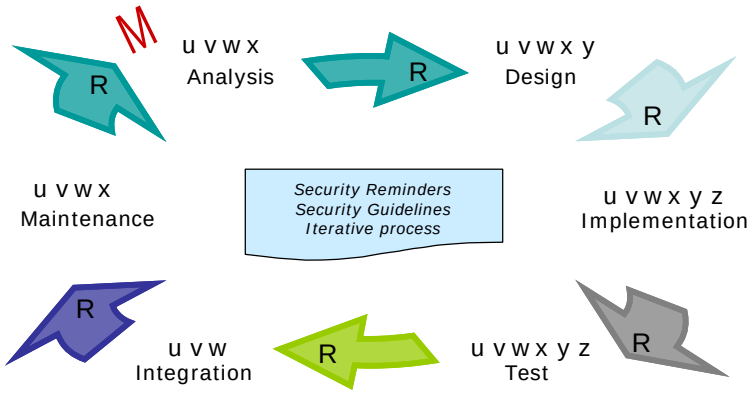
~50 pages

- Target group
  - Software Engineers and Technical Project Leaders
- Contents
  - Security vocabulary explained, brief intro to security standards, guidance, requirements, static/dynamic analysis, security patterns, examples of vulnerabilities and how to avoid them, etc.
- Checklists
  - Questions to be answered Yes or No for all development phases
- A one-day intensive course

COMBITECH

ITSI
Software Security Principals

ITSI – A consciously way of working.

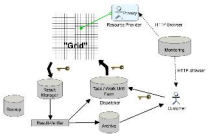


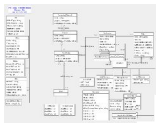
COMBITECH

ITSI
Software Security Principals

Important Concepts.

- Security awareness:
  ”There are potential threats against what YOU do”
- A security role in the project group





COMBITECH

ITSI
Software Security Principals

Security Issues.

- Security marks in design documents
- Buffer overflows, Race conditions, Declarations, Synchronization, Temporary buffers, Error handling, Random numbers, Parameter control, etc.
- Static/Dynamic analysis
- Examples of free and commercial tools for security tests, etc.

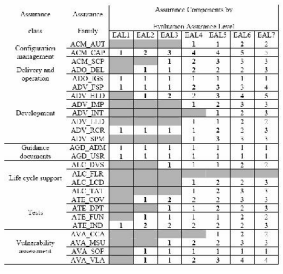
COMBITECH

References.

- Academy
  - Blekinge Institute of Technology, Sweden
- Authority
  - Swedish Coast Guard

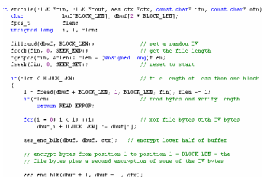
Connections to Common Criteria.

- The most primary connection between ITSI and Common Criteria (CC) is the assurance class ADV
- ITSI has also connections to the assurance classes ATE and AVA
- ITSI has some relatives to the assurance classes ALC and AGD



Connections to Common Criteria.

- Assurance class ADV
  - Generally
    - ITSI gives guidelines for the specification and description of security functions
  - Assurance family ADV_IMP
    - ITSI requires that security functions are labeled in the source code
    - ITSI includes guidelines and check lists for the implementation
  - Assurance family ADV_INT
    - ITSI recommends design in security relevant and non-security relevant modules



COMBITECH

Connections to Common Criteria.

- Assurance class ATE
  - The test required by ATE.DPT on basic design, modules and implementation levels are easier to realize and review/confirm if the ITSI guidelines are followed
- Assurance class AVA (family AVA_VAN)
  - Our experience is that software bugs are the must common cause to exploitable vulnerabilities
  - The risks are minimized if the source code is well designed/ structured and if the developers understands secure coding
  - It is very helpful for the vulnerability analysis if the developer can give evidence that the source code is reviewed for well-known weaknesses as buffer overflows

COMBITECH

Connections to Common Criteria.

- Assurance class ALC and AGD
  - ITSI includes some recommendations for secure development and flaw remediation
  - ITSI gives advices for secure installation (Installation manual)

COMBITECH

Effects on Reviews.

- Less vulnerabilities
- Faster evaluations
- Easier reevaluations
- More efficient dialogs between developers and evaluators

COMBITECH

ITSI
Software Security Principals

Summary.

- The creation of a new methodology
  - ITSI
  - Target group: Software Engineers, Programmers and Technical Project leaders
- Advantages
  - Increased understanding and knowledge of information security among developers
  - Fewer software vulnerabilities
  - Faster CC evaluations, a greater chance of approval

COMBITECH