

# Measuring the Effectiveness of a Security Development Process

Mike Grimm, Microsoft  
Helmut Kurth, atsec

# Agenda

- Assurance in IT and non-IT products
- Development process analysis and deficiencies in the CC
- How to measure process assurance
- Example of security assurance measures in a software development process
- How could those be taken into account in an evaluation
- Proposed enhancements of the CC
- Benefits

# Example: Car industry

- Independent analysis of car design
- Independent analysis of critical components of the car
  - Brakes, engine, tires, ....
- Testing of a prototype
  - Driving under different conditions (street, weather), crash tests, usability test, function test
- Testing of critical components in specific testbeds
  - Simulating extreme conditions, simulating life-cycle, ....
- Analysis of the developer's assurance process
  - Models used and their calculation results, quality assurance measures in manufacturing, ....

# Assurance for Cars and IT World

- **Assurance for cars** comes as a combination of all
  - Analysis of components shows that they are reliable **when integrated correctly**
  - Analysis of car shows that the car has been built using approved practices
  - Testing of components validates properties of components against requirements
  - Testing of prototype validates properties of **that single car**
  - Analysis of manufacturing process validates that the properties of the car hold **for all cars “similar enough” to the prototype tested**

# Assurance for Cars and IT World

## ● Assurance for the IT World

- Analysis of the product design: addressed by the CC
- Analysis of the product components: vaguely addressed by the CC
- Testing of a product prototype: addressed by the CC
- Testing of individual components in special testbeds: vaguely addressed by the CC
- Analysis of the assurance methods applied during the development

**Not addressed by the CC**

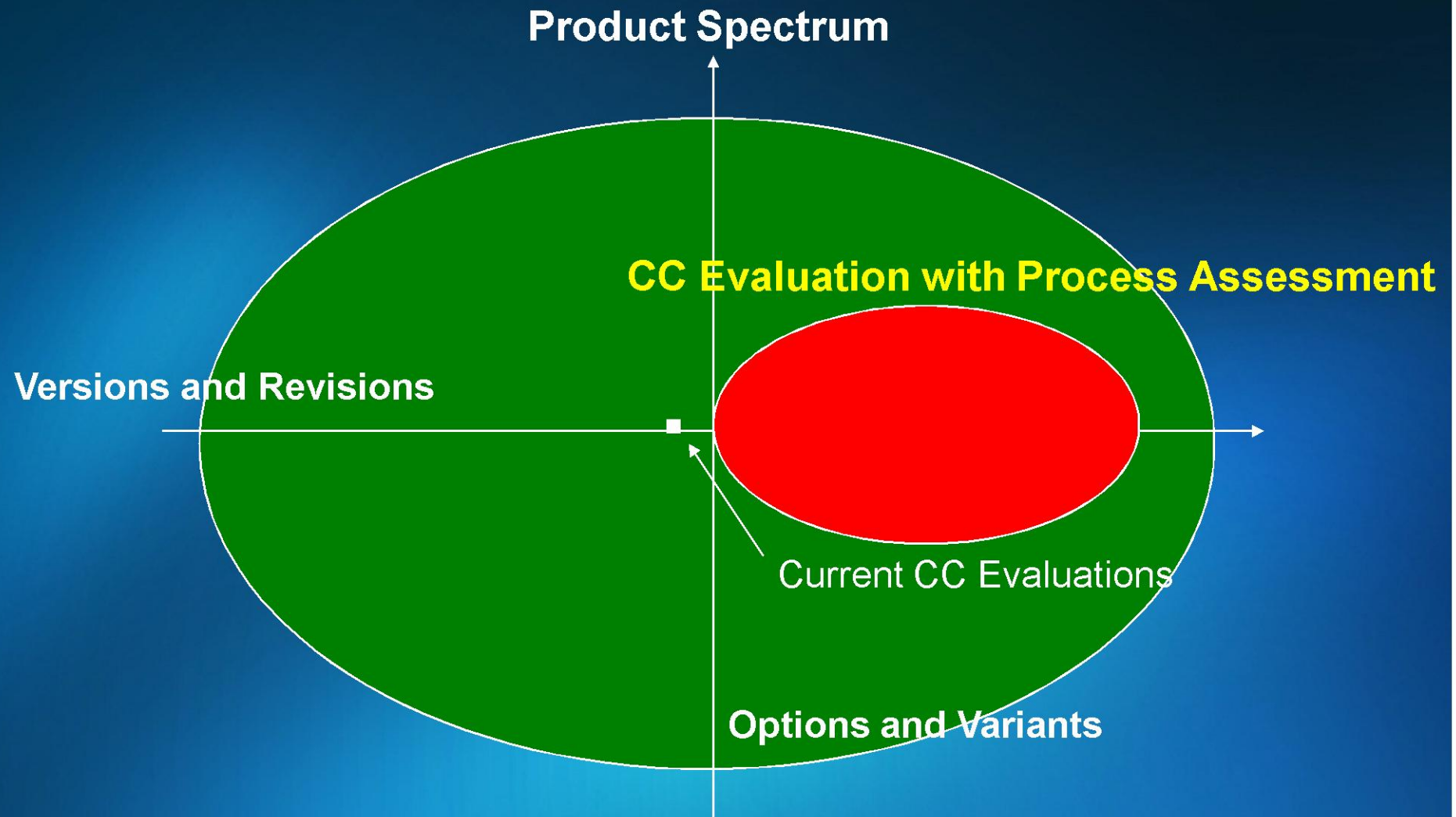
# Development Process Assurance and the CC

- **CC Weaknesses for development process assurance**
  - Looks only at protection of design and code, configuration management, delivery process, “life-cycle model”, definition of tools
  - Looks at flaw remediation only from a procedural point of view
  - Does not analyze the effectiveness of the development process to identify and eliminate design and coding errors
  - Does not analyze the effectiveness of tools and techniques for assuring that the product meets its security objectives
  - Does not analyze how the developer learns from flaws, tries to identify similar flaws and ensures that similar flaws are avoided already during development
  - Focusing on process parts that have little effect on assurance
  - Neglecting significant assurance analysis work performed by the developer

# Development Process Assurance and the CC

- **Certificate restricted to specific evaluated configurations**
  - Does not fit all usage scenarios
  - No statement what happens when using a different configuration
- **Current CC evaluations address a single point in the product spectrum**
  - Assurance continuity may extend this slightly in the “version and revision” direction

# Scope of an Evaluation





# How to Measure Process Assurance

- **Do it similar to product assurance**
  - Define the process assurance objectives
  - Identify the elements in the process that contribute to meeting the objectives
  - Assess the effectiveness of those elements in contributing to the assurance objectives
  - Assess the application of the elements in the process
    - Are they applied, are they applied correctly, are they applied for all parts of the product
  - Give a rating (like a “process assurance level”)
  - During product assessment, check that process elements “fit” the product’s design and technology

# Some Questions (and Answers)

- **Yet another assessment process!**
  - Must bring significant benefits to get accepted
- **Can this replace product assessment?**
  - **No**, as the car industry example has shown
- **Can this bring additional assurance?**
  - **Yes**, as the car industry example has shown
- **Can this be combined with product evaluation?**
  - **Yes**, as the car industry example has shown
- **Can this extend the product certificate to cover not just a single point in the product spectrum**
  - **Yes**, this is the main advantage

# Assurance Measures in a Development Process

Mike Grimm, Microsoft Corp.

# Security Development Lifecycle



Product Inception

Design

- Threat Modeling

Standards, best practices, and tools

Security Push

Final Security Review  
RTM and Deployment

- Signoff

Security Response



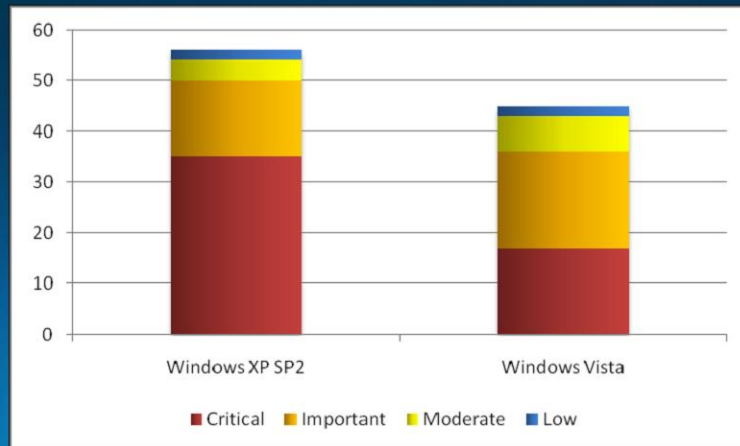
## Internal Microsoft Evaluations

- Microsoft releases 100s of products annually
  - Large variance in risk profile
  - Large variance in hardware profile
  - Attackers have wide range of incentives to exploit
- How to determine if each product is ready?

# SDL Compliance

- New products, new versions undergo standardized risk assessment
- Higher risk products receive additional consulting / monitoring
- Central security team to analyze effectiveness of teams'
  - Development process to identify and eliminate design and coding errors
  - Use of tools and techniques to meet security objectives
  - “security culture”: knowledge depth, exceed compliance requirements

# Case study: SDL & Windows



2007 vulnerability comparison  
(MSRC data)

Since Vista Release:	
Vista vulns	43
XP SP2 vulns	56
Vista-only vulns	8
# Important vulns	6
# Moderate vulns	2
XP SP2-only vulns	21
# Critical vulns	13
# Important vulns	8

# Suggestions for CC Improvements

Helmut Kurth, atsec information systems



# Suggestions for CC Improvement

- **Expansion of the process assessment**
  - Definition of the process objectives
  - Identification of the process assurance measure
  - Assessment of the effectiveness of the process and its measures
- **Matching process assessment with the product's objectives**
  - Do the process assurance measures fit the product security objectives and product technology
- **Identify the gaps**
  - Focus evaluation activities on those gaps
- **Define the scope of the certificate**
  - Covering more than just a single point in the product spectrum

# Benefits

- **Combined process and product assessment is what industry usually does**
  - See the car example
- **Processes are usually more stable than products**
  - Assessment is valid for a longer time
- **Processes are often used for a range of products**
  - Re-use of process assessment contributes to cost-effectiveness
  - Existing CC Site Certification could be extended
- **No useless repetition of developer activities**
  - If the developer has done it right, there is no reason to repeat what he has done

# Benefits for the CC

- Certificates can cover a wider spectrum of a product's versions and configurations
- Ability to focus evaluations on critical aspects
- Reduced evaluation effort
- More aligned with real world requirements

# Contact Information

- Mike Grimm

[MGrimm@microsoft.com](mailto:MGrimm@microsoft.com)

- Helmut Kurth

[helmut@atsec.com](mailto:helmut@atsec.com)

# Additional Material

# Motivation

- The CC bases its assurance mainly on
  - The design and implementation
  - Testing and vulnerability analysis
  - The protection measures in the development process against unauthorized modifications
- A developer usually incorporates his own security assurance measures. Examples are:
  - Design methods designated for the product type
  - Coding standards to avoid known problems
  - Analysis for common problems, design reviews

**Development process assurance measures should be honored in an evaluation**

# Product Assurance in the non-IT World

- Analysis of the product design
  - Addressed by the CC
- Analysis of the components that make up the product
  - Only vaguely addressed by the CC
- Testing of a prototype
  - Addressed by the CC
- Testing of individual components in special testbeds
  - Only vaguely addressed by the CC
- Analysis of the assurance methods applied during the development
  - Not addressed by the CC

# Problems to be Solved

- Current CC evaluations address a single point in the product spectrum
  - Assurance continuity may extend this slightly in the “version and revision” direction
- Certificate restricted to specific evaluated configurations
  - Does not fit all usage scenarios
  - No statement what happens when using a different configuration
- Current CC evaluations don't honor the developer's assurance measures
  - Focusing on process parts that have little effect on assurance
  - Neglecting significant assurance analysis work performed by the developer