Microsoft SQL Server 2005

Certification Against a Moving Protection Profile

Wolfgang Peter
TUViT (Germany)
Director Evaluation Body for IT Security

Roger French
Microsoft Corporation (USA)
Security and Privacy Program Manager for SQL Server

Agenda

- Introduction
- The Approach
- Motion Dynamics
- Lessons Learned

Introduction

What makes the certification process of SQL Server 2005 “special“?

Concurrent

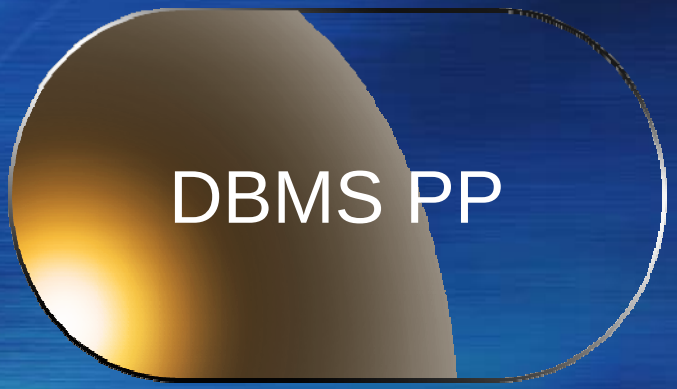
Huge

Moving PP

Introduction

The moving PP

U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments (DBMS PP)



- Validated version V1.0, Sep. 30, 2004
- Several / significant revisions, since
- Validated version V1.1, June 7, 2006

Introduction

Questions to be answered

Why certifying SQL, and why not against DBMS PP V1.0?

Why the moving product/target solution?

What dynamics (so far)?

The Approach

Why certifying SQL Server 2005?

SQL Server 2005 SP2

- Assurance of it's security
- Customer need / Vendor claim
- Governments' Requirement
- Market Preference

Why *not* DBMS PP V1.0?

DBMS PP V1.0

- Fits no COTS product
- Lacking: Groups, ...
- Restrictive: DAC, RIP.2, ...

The Approach

Vendor Initiative

- DBMS Vendors critical after PP V1.0 published
- NSA offers to work w/vendors to create PP V1.1
- Vendors form an informal group to provide a single set of vendor comments
- Vendors also ‘negotiate’ one-on-one
- The Result: a practical PP

“If neither party is totally happy, it is probably a good compromise.”

The Approach

Potential options

Proprietary ST	Stand-alone ST “complying as much as possible”
Static ST	ST development *not* before final release of the DBMS PP
Moving ST	ST development according and concurrently to the development of the DBMS PP

The Approach

Pros and Cons

Proprietary ST

- “Standard”
- Easy
- Fast
- Fits product “up-front”

- No PP claim
- Customer’s demand
  - Governments’ requirement
  - Market preference
- PP wording

The Approach

Pros and Cons

DBMS PP → ST

- Easy
- Know before start whether product will comply

- Slow!
- Risk
  - Time-to-Market
  - Competition

The Approach

Pros and Cons

Moving ST / Moving PP

- PP claim
- Head start on evaluation (not just ST)
- Still fast

- Not easy
- Risk to miss the PP
  - Potential to not get speculated changes
  - Possibly not willing to change product
  - Back to ‘proprietary ST’

The Approach

Summary and decision

“Normal” Evaluation

- Develop the Protection Profile (18 months)
- Develop the product version (24 months)
- Evaluate against stable PP (18 months)

PP ---------

DP ----------

EP ----------

Elapsed time: 48 months

“Moving” Evaluation

- Develop the Protection Profile (18 months)
- Develop the product version (24 months)
- Evaluate against stable PP (18 months)

PP ---------

DP ----------

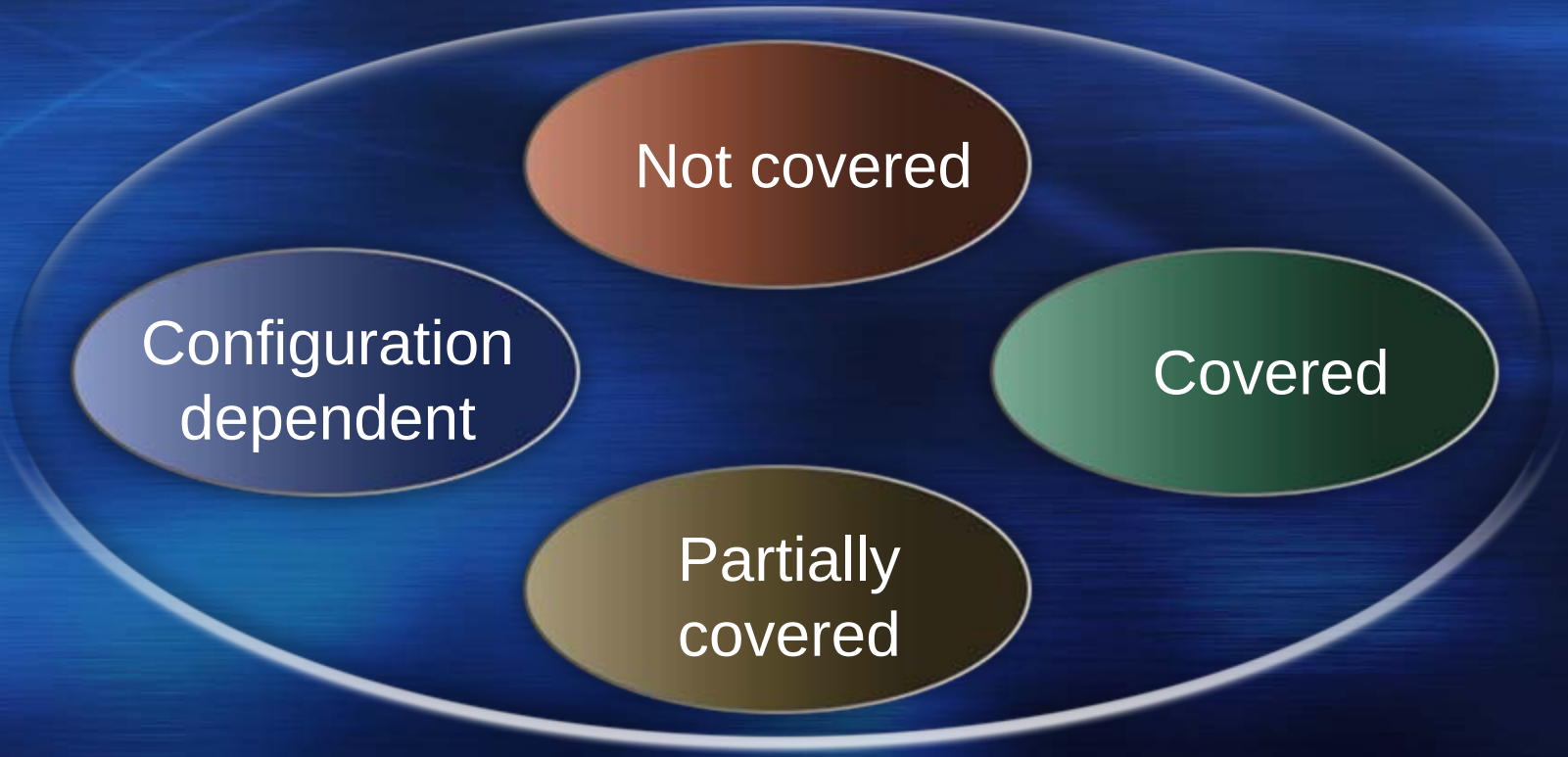
EP ----------

Elapsed time: 30 months

Motion Dynamics

Background

After each revision of the DBMS PP, the “Requirements” (SFRs, Objectives, Threats, etc.) were checked whether ...



Motion Dynamics

Background

... and we worked out, what ...

... features are missing?

... are the time and cost to develop?

... is the impact on customer needs?

Motion Dynamics

Lab's perspective

- Hard to predict ***what*** will change, and ***when***
- Need to plan rework and buffer (ASE and ADV)
- Need to define 'point of no return' and 'deadline'
- Evaluate as according to PP, except PPC.1
- Wording in SER difficult

Motion Dynamics

Vendor's perspective

- Every mismatch between product & PP had to be resolved.
  - The Product changed (by DEV)
  - The PP changed (by NSA)
  - Both changed
  - Then TEST, CC docs, the evaluation changed
- Schedules did not align
  - DEV/TEST building to a market schedule
  - PP building to a different schedule
- ...

Motion Dynamics

Vendor's perspective

- ...
- DEV/TEST had to build on speculation
  - Not every 'enhancement' survived
  - Some Tests were never used
  - Some staffing had to change
  - Redefined the word 'flexibility'
- Document plans, update later
- Risks to schedules/enhancements/evaluation

Lessons Learned

- Hitting a Moving Target is difficult, but not impossible (so far).
- The Evaluated Product's Time-to-Market is still the major goal and the major evaluation problem.
- Vendors need to help PP authors move the target.
- An ST (usually not a PP) moves toward the product.
- Everyone (PP authors, Evaluators, Certifiers, DEV, Test, Support, Release Services, PM's, Senior Management) has to buy into working with *a moving target*.


Gracias
谢谢您
Thank you!
Grazie
Danke
Merci
謝謝您
Takk
Obrigado
Bedankt