Evaluating Windows: Something Old, Something New, Something Borrowed, Something Blue

September 11, 2013

Mike Grimm, Microsoft Corp.

Agenda

- History of Windows CC evaluations
- Experiences with Windows 7 and Windows 8 OS PP evaluations
- Experiences with Windows 8 and IPsec VPN Client and Software Disk Encryption evaluations

Something Old

Previous Windows CC Evaluations

Product	When	Protection Profile
Microsoft Windows 2000 Professional, Server, and Advanced Server with SP3 and Q326886	2002-10-01	Controlled Access Protection Profile (CAPP), Version 1.d
Microsoft Windows 2003 and Microsoft Windows XP	2005-11-06	Controlled Access Protection Profile (CAPP), Version 1.d
Microsoft Windows Server 2003 and Microsoft Windows XP with x64 Hardware Support	2006-09-18	Controlled Access Protection Profile (CAPP), Version 1.d
Microsoft Windows Server 2003 and Microsoft Windows XP	2007-04-01	Controlled Access Protection Profile (CAPP), Version 1.d
Microsoft Windows Server 2003 SP2 including R2, Standard, Enterprise, Datacenter, x64, and Itanium Editions; Windows XP Professional SP2 and x64 SP2; Windows XP Embedded SP2	2008-02-07	Controlled Access Protection Profile (CAPP), Version 1.d
Microsoft Windows Vista and Windows Server 2008	2008-09-17	Security Target (EAL1)
Microsoft Windows Server 2008 Hyper-V Role with HotFix KB950050	2009-07-24	Security Target
Windows Vista Enterprise; Windows Server 2008 Standard Edition; Windows Server 2008 Enterprise Edition; Windows Server 2008 Datacenter Edition	2009-08-31	Controlled Access Protection Profile (CAPP), Version 1.d
Microsoft Windows 7, Microsoft Windows Server 2008 R2	2011-03-24	US Government Protection Profile for General-Purpose Operating Systems in a Networked Environment (GPOSPP)
Microsoft Windows Server 2008 R2 Hyper-V Release 6.1.7600	2012-02-06	Security Target

Something New

Recent Windows CC Evaluations

Product	Started	Protection Profile
Windows 8, Windows RT, Windows Server 2012	2013-02-05	General-Purpose Operating System Protection Profile (OSPP), Version 3.9 (?!)
Windows 8, Windows RT, Windows Server 2012	2013-02-22	Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.1
Windows 8, Windows RT, Windows Server 2012	2013-06-03	Protection Profile for Software Full Disk Encryption Version 1.0

Something Borrowed

Comparing Protection Profiles

SFR Family	CAPP (Windows 2000 – Vista)	GPSOPP (Windows 7)	OSPP (Windows 8)
Audit	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.2 FAU_SAR.3 FAU_SEL.1 FAU_STG.1 FAU_STG.3 FAU_STG.4	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.2 FAU_SAR.3 FAU_SEL.1 FAU_STG.1 FAU_STG.3	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.2 FAU_SEL.1 FAU_STG.1 FAU_STG.3 FAU_STG.4
Cryptographic Support		FCS_BCM_EXT.1 FCS_CKM.1 (x2) FCS_CKM.4 FCS_COA_EXT.1 FCS_COP.1 (x3) FCS_RBG_EXT.1	
Data Protection	FDP_ACC.1 FDP_ACF.1 FDP_RIP.1	FDP_ACC.1 FDP_ACF.1 FDP_RIP.2	FDP_ACC.1 FDP_ACF.1 FDP_IFC.1 FDP_IFF.1 FDP_RIP.2
Identification & Authentication	FIA_ATD.1 FIA_SOS.1 FIA_UAU.1 FIA_UAU.7 FIA_UID.1 FIA_USB.1	FIA_AFL_EXT.1 FIA_ATD.1 FIA_SOS.1 FIA_UAU.1 FIA_UAU.6 FIA_UAU.7 FIA_UID.1 FIA_USB.1	FIA_AFL.1 FIA_ATD.1 FIA_UAU.1 (x2) FIA_UAU.5 FIA_UAU.7 FIA_UID.1 FIA_USB.1 FIA_PK_EXT.1
Management	FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 (x3) FMT_REV.1 (x2) FMT_SMR.1	FMT_MOF.1 (x2) FMT_MSA.1 (x2) FMT_MSA.2 FMT_MSA.3 FMT_MTD.1 (x7) FMT_REV.1 (x2) FMT_SMF.1 FMT_SMR.1	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 (x2) FMT_MSA.4 FMT_MTD.1 (x9) FMT_REV.1 (x2) FMT_SMR.1
TSF Protection	FPT_AMT.1 FPT_RVM.1 FPT_SEP.1 FPT_STM.1	FPT_ITT.1 FPT_ITT.3 FPT_RCV.1 FPT_STM.1 FPT_TRC_EXT.1 FPT_TST_EXT.1	FPT_STM.1
Resource Utilization		FRU_RSA.1	
TOE Access		FTA_MCS.1 FTA_SSL.1 FTA_SSL.2 FTA_TAB.1 FTA_TAH.1	FTA_SSL.1 FTA_SSL.2
Trusted Path / Channel			FTP_ITC.1
Other	EAL3 CC 2.X, 3.X	EAL2 + ALC_FLR.2 CC3.1 R2	EAL1 ++ CC 3.1 R4

Comparing Security Targets

	Windows Vista (CAPP)		Windows 7 (GPOSPP)		Windows 8 (OSPP)	
Total # PP SFRs	30		57		43	
# PP SFRs by class	FAU	9	FAU	8	FAU	8
	FCS		FCS	9	FCS	
	FDP	3	FDP	3	FDP	5
	FIA	6	FIA	8	FIA	9
	FMT	8	FMT	17	FMT	17
	FPT	4	FPT	6	FPT	1
	FRU		FRU	1	FRU	
	FTA		FTA	5	FTA	2
	FTP		FTP		FTP	1
# ST SFRs	107		110		65	
# ST SFRs by class	FAU	10	FAU	9	FAU	8
	FCS	13	FCS	13	FCS	
	FDP	17	FDP	23	FDP	13
	FIA	8	FIA	8	FIA	9
	FMT	40	FMT	35	FMT	31
	FPT	10	FPT	11	FPT	1
	FRU	1	FRU	1	FRU	
	FTA	7	FTA	7	FTA	2
	FTP	1	FTP	1	FTP	1
			FCO	2		

Comparing Time to Completion

	Windows Vista (CAPP)	Windows 7 (GPOSPP)	Windows 8 (OSPP)
General Availability (GA)	November 6, 2006	July 22, 2009	October 26, 2012
CC Evaluation Completed On	September 17, 2008	March 24, 2011	[work in progress]
Delta between GA and CC certification	1 year, 10 months	1 year, 8 months	10 months and counting

Something New

Changes in Windows Evaluations

- Windows 7 and earlier evaluations primarily reviewed non-public design material
    - Focus was consistency between OS components, tracing from interfaces to functional requirements.
    - Testing was driven by interfaces.
    - Developed a scalable, repeatable process.
    - Included the newest OS features.
        - This is where customers need assurance.
- Windows 8 evaluation based on a hybrid OS PP
    - Focus on auditing, vanilla access control and management not compelling for customers.
        - PP philosophy attempted to include both new and mature operating systems.
    - Evaluation phase for design intends to use only public information.
    - Evaluation phase for testing is a combination of developer testing and evaluator testing.
        - Evaluators test security functions.
        - Developers test interfaces.
    - Unclear if this approach is scalable or repeatable.

Objectivity, Repeatability Isn’t Easy

Assurance activities in the OS PP

- “The evaluator needs to be able to identify that the audit records are actually generated by the TSF and not by a part of the TOE . The developer needs to provide sufficient arguments that the audit record generation can be influenced or even bypassed by a user.”
- “The functional specification (which is publically available) shall identify all the interfaces to the TSF where access control is enforced as well as all the interfaces used to manage the access control policy or the security attributes used in the access control policies. Each interface where access control is enforced needs to describe how the caller is informed in the case access is denied. All the interfaces need to be described such that they can be used in testing the access control policy or the management activity.”
- “After successfully authenticating, the evaluator will attempt X number of failed authentication attempts … Upon satisfying the number of failed attempts, the evaluator shall observe that the TOE electrocutes the user with sufficient amperage to cause much harm.”

Functionally Based Evaluations

- IPsec VPN Client
  - Windows 8, Windows RT, Server 2012 as a IPsec VPN client.
  - Focus on ciphersuites and related protocol parameters.
  - Testing is mostly black-box testing by evaluator.
  - Limited design information but also protocol documentation.
  - Net result was a targeted evaluation of IKEv1 and IKEv2.
- Software Full Disk Encryption
  - BitLocker for Windows 8 and Server 2012; Device Encryption in Windows RT.
  - Focus on use of Suite B crypto; key derivation; authentication factors.
  - Testing is mostly black-box testing by evaluator.
  - Detailed design information (and requirements) for combining authentication factors.
  - Commercial products are more complex than the PP imagined.

Something Blue…

…not my state of mind after these evaluations

What I think we’ve learned

- Comparing old and new
  - Focus on reviewing interfaces was excessive, unclear if emphasis on design documentation will do more than stoke evaluators’ curiosity.
  - Hybrid approach may be problematic
    - OS PP essentially combines EAL1 design with EAL4 testing.
  - Evaluation with only the OS PP does not provide assurance for a mature OS.
- Comparing borrowed and blue
  - Functionally-based evaluations do provide meaningful assurance within narrow boundaries.
  - Evaluation activities are more transparent; what the evaluator needs to include in their report is not defined.
  - May have a halting problem: will the PP development program run forever?
- Will need to save some silver (“and a silver sixpence in her shoe”)
  - Evaluations have fixed overhead costs for the developer and evaluator (preparing and evaluating the security target, writing evaluation reports) and scheme (managing evaluations, reviewing evaluation reports) that will make large number of functional evaluations unreasonably costly.
  - Consider combining multiple functional PPs as optional packages in an updated OS profile.

- Thank you for your time and attention!
- Questions? MGrimm@microsoft.com

Backup

ICCC Abstract

- This presentation will describe Microsoft’s experience evaluating Windows 7 against the Controlled Access Protection Profile (EAL4), and Windows 8 against the BSI/NIAP Operating System Protection Profile. In addition to comparing the functional and assurance approaches for these two OS protection profiles, the presentation will also cover recent evaluations of Windows against the IPsec VPN Client and Software Full Disk Encryption protection profiles.