TCPA

Markus Gerstel

Hauptseminar: Digital Rights Management
Technische Universität München

November 17, 2005

Vortragsinhalt

Vortragsinhalt

Vortragsinhalt

Vortragsinhalt

Vortragsinhalt

Was ist TCPA ?

TCPA = Trusted Computing Platform Alliance

- gegründet Oktober 1999
- Von u.a. Compaq, Intel, HP, IBM, Microsoft
- mit dem Ziel sichere Geschäftsvorgänge am PC zu ermöglichen, indem bestehende Schwächen in Hard- und Software beseitigt werden

Was ist TCPA ?

TCPA = Trusted Computing Platform Alliance

- gegründet Oktober 1999
- Von u.a. Compaq, Intel, HP, IBM, Microsoft
- mit dem Ziel sichere Geschäftsvorgänge am PC zu ermöglichen, indem bestehende Schwächen in Hard- und Software beseitigt werden

Was ist TCPA ?

TCPA = Trusted Computing Platform Alliance

- gegründet Oktober 1999
- Von u.a. Compaq, Intel, HP, IBM, Microsoft
- mit dem Ziel sichere Geschäftsvorgänge am PC zu ermöglichen, indem bestehende Schwächen in Hard- und Software beseitigt werden

Was ist TCPA ?

TCPA = Trusted Computing Platform Alliance

- gegründet Oktober 1999
- Von u.a. Compaq, Intel, HP, IBM, Microsoft
- mit dem Ziel sichere Geschäftsvorgänge am PC zu ermöglichen, indem bestehende Schwächen in Hard- und Software beseitigt werden

Was ist TCPA ?

TCPA = Trusted Computing Platform Alliance

- gegründet Oktober 1999
- Von u.a. Compaq, Intel, HP, IBM, Microsoft
- mit dem Ziel sichere GeschäftsVorgänge am PC zu ermöglichen, indem bestehende Schwächen in Hard- und Software beseitigt werden

Bestehende Schwächen

Welche Schwachstellen will Trusted Computing schließen ?

- Debugger
- Viren und Trojaner
- Buffer Overflows
- Gerätetreiber
- Hardware über DMA
- PRNGs

Bestehende Schwächen

Welche Schwachstellen will Trusted Computing schließen ?

- Debugger
- Viren und Trojaner
- Buffer Overflows
- Gerätetreiber
- Hardware über DMA
- PRNGs

Bestehende Schwächen

Welche Schwachstellen will Trusted Computing schließen ?

- Debugger
- Viren und Trojaner
- Buffer Overflows
- Gerätetreiber
- Hardware über DMA
- PRNGs

Bestehende Schwächen

Welche Schwachstellen will Trusted Computing schließen ?

- Debugger
- Viren und Trojaner
- Buffer Overflows
- Gerätetreiber
- Hardware über DMA
- PRNGs

Bestehende Schwächen

Welche Schwachstellen will Trusted Computing schließen ?

- Debugger
- Viren und Trojaner
- Buffer Overflows
- Gerätetreiber
- Hardware über DMA
- PRNGs

Bestehende Schwächen

Welche Schwachstellen will Trusted Computing schließen ?

- Debugger
- Viren und Trojaner
- Buffer Overflows
- Gerätetreiber
- Hardware über DMA
- PRNGs

Bestehende Schwächen

Welche Schwachstellen will Trusted Computing schließen ?

- Debugger
- Viren und Trojaner
- Buffer Overflows
- Gerätetreiber
- Hardware über DMA
- PRNGs

Verwendete Technik

Wie funktioniert Trusted Computing ?

- Trusted Platform Module (TPM): Chip auf Mainboard
- Public Key Infrastructure (PKI)
- Chain of Trust

Verwendete Technik

Wie funktioniert Trusted Computing ?

- Trusted Platform Module (TPM): Chip auf Mainboard
- Public Key Infrastructure (PKI)
- Chain of Trust

Verwendete Technik

Wie funktioniert Trusted Computing ?

- Trusted Platform Module (TPM): Chip auf Mainboard
- Public Key Infrastructure (PKI)
- Chain of Trust

Verwendete Technik

Wie funktioniert Trusted Computing ?

- Trusted Platform Module (TPM): Chip auf Mainboard
- Public Key Infrastructure (PKI)
- Chain of Trust

Wer steht hinter TCPA ?

Das Interesse an der Trusted Computing-Technologie ist so groß, dass der TCPA ab 2003 bereits über 200 Mitglieder angehörten.
Jedes Mitglied hatte ein Veto-Recht, und in Folge war die TCPA handlungsunfähig.

Darum wurde 2003 die TCG (Trusted Computing Group) gegründet.

Wer steht hinter TCPA ?

Das Interesse an der Trusted Computing-Technologie ist so groß, dass der TCPA ab 2003 bereits über 200 Mitglieder angehörten. Jedes Mitglied hatte ein Veto-Recht, und in Folge war die TCPA handlungsunfähig.

Darum wurde 2003 die TCG (Trusted Computing Group) gegründet.

Wer steht hinter TCPA ?

Das Interesse an der Trusted Computing-Technologie ist so groß, dass der TCPA ab 2003 bereits über 200 Mitglieder angehörten. Jedes Mitglied hatte ein Veto-Recht, und in Folge war die TCPA handlungsunfähig.

Darum wurde 2003 die TCG (Trusted Computing Group) gegründet.

Wer steht hinter TCPA ?

Das Interesse an der Trusted Computing-Technologie ist so groß, dass der TCPA ab 2003 bereits über 200 Mitglieder angehörten. Jedes Mitglied hatte ein Veto-Recht, und in Folge war die TCPA handlungsunfähig.

Darum wurde 2003 die TCG (Trusted Computing Group) gegründet.

Wer steht hinter TCPA/TCG

AMD - Hewlett-Packard - IBM - Intel Corporation - Microsoft - Sun Microsystems, Inc. - Adaptec, Inc. - Agere Systems - American Megatrends, Inc. - ARM - ATI Technologies Inc. - Atmel - AuthenTec, Inc. - AVAYA - Broadcom Corporation - Certicom Corp. - Check Point Software , Inc. - Citrix Systems, Inc - Comodo - Dell, Inc. - Endforce, Inc. - Ericsson Mobile Platforms AB - France Telecom Group - Freescale Semiconductor - Fujitsu Limited - Fujitsu Siemens Computers - Funk Software, Inc. - General Dynamics C4 Systems - Giesecke & Devrient - Hitachi, Ltd. - Infineon - InfoExpress, Inc. - InterDigital Communications - iPass - Lenovo Holdings Limited - Lexmark International - M-Systems Flash Disk Pioneers - Maxtor Corporation - Meetinghouse Data Communications - Mirage Networks - Motorola Inc. - National Semiconductor - nCipher - NEC - Nevis Networks, USA - Nokia - NTRU Cryptosystems, Inc. - NVIDIA - OSA Technologies, Inc - Philips - Phoenix - Pointsec Mobile Technologies - Renesas Technology Corp. - Ricoh Company LTD - RSA Security, Inc. - Samsung Electronics Co. - SanDisk Corporation - SCM Microsystems, Inc. - Seagate Technology - Siemens AG - SignaCert, Inc. - Silicon Integrated Systems Corp. - Sinosun Technology Co., Ltd. - SMSC - Sony Corporation

Wer steht hinter TCPA/TCG - Teil II

STMicroelectronics - Symantec - Symbian Ltd - Synaptics Inc. - Texas Instruments - Toshiba Corporation - TriCipher, Inc. - Unisys - UPEK, Inc. - Utimaco Safeware AG - VeriSign, Inc. - Vernier Networks - Vodafone Group Services LTD - Wave Systems - Winbond Electronics Corporation - Advanced Network Technology Laboratories - Apani Networks - Apere, Inc - BigFix, Inc. - BlueRISC, Inc. - Bradford Networks - Caymas Systems - Cirond - ConSentry Networks - CPR Tools, Inc. - Credant Technologies - Fiberlink Communications - Foundstone, Inc. - GuardianEdge - ICT Economic Impact, Ltd. - Industrial Technology Research Institute - Infosec Corporation - Integrated Technology Express Inc. - LANDesk Software - Lockdown Networks - Marvell Semiconductor, Inc. - MCI - Meganet Corporation - Roving Planet - SafeBoot - Safend LTD. - Sana Security - Secure Elements - Senforce Technologies, Inc - SII Network Systems Inc. - Silicon Storage Technology, Inc. - Softex, Inc. - StillSecure - Swan Island Networks, Inc. - Telemidic Co. Ltd. - Toppan Printing Co., Ltd. - Trusted Network Technologies - ULi Electronics Inc. - Valicore Technologies, Inc. - Websense, Inc.

Grundlegende Bausteine

- RTM: Root of trust for mesuring integrity metrics
- RTS: Speichern von sicherheitskritischen Daten
- RTR: Melden von sicherheitskritischen Daten
- TPM: Trusted Platform Module

Grundlegende Bausteine

- RTM: Root of trust for mesuring integrity metrics
- RTS: Speichern von sicherheitskritischen Daten
- RTR: Melden von sicherheitskritischen Daten
- TPM: Trusted Platform Module

Grundlegende Bausteine

- RTM: Root of trust for mesuring integrity metrics
- RTS: Speichern von sicherheitskritischen Daten
- RTR: Melden von sicherheitskritischen Daten
- TPM: Trusted Platform Module

Grundlegende Bausteine

- RTM: Root of trust for mesuring integrity metrics
- RTS: Speichern von sicherheitskritischen Daten
- RTR: Melden von sicherheitskritischen Daten
- TPM: Trusted Platform Module

Grundlegende Bausteine

- RTM: Root of trust for mesuring integrity metrics
- RTS: Speichern von sicherheitskritischen Daten
- RTR: Melden von sicherheitskritischen Daten
- TPM: Trusted Platform Module

Grundlegende Bausteine

- RTM: Root of trust for mesuring integrity metrics
- RTS: Speichern von sicherheitskritischen Daten
- RTR: Melden von sicherheitskritischen Daten
- TPM: Trusted Platform Module

Grundlegende Bausteine

- RTM: Root of trust for mesuring integrity metrics
- RTS: Speichern von sicherheitskritischen Daten
- RTR: Melden von sicherheitskritischen Daten
- TPM: Trusted Platform Module

Grundlegende Bausteine

- RTM: Root of trust for mesuring integrity metrics
- RTS: Speichern von sicherheitskritischen Daten
- RTR: Melden von sicherheitskritischen Daten
- TPM: Trusted Platform Module

Im TPM aufbewahrte Schlüssel

- Endorsement Keys:
  Einzigartiges Schlüsselpaar, im TPM aufbewahrt - nicht exportierbar
- AIKs:
  Attestation Identity Keys - Benutzergenerierte Schlüsselpaare
- Storage Root Key:
  Zur Verschlüsselung von AIKs und anderen Keys innerhalb des TPM

Im TPM aufbewahrte Schlüssel

- Endorsement Keys:
  Einzigartiges Schlüsselpaar, im TPM aufbewahrt - nicht exportierbar
- AIKs:
  Attestation Identity Keys - Benutzergenerierte Schlüsselpaare
- Storage Root Key:
  Zur Verschlüsselung von AIKs und anderen Keys innerhalb des TPM

Im TPM aufbewahrte Schlüssel

- Endorsement Keys:
  Einzigartiges Schlüsselpaar, im TPM aufbewahrt - nicht exportierbar
- AIKs:
  Attestation Identity Keys - Benutzergenerierte Schlüsselpaare
- Storage Root Key:
  Zur Verschlüsselung von AIKs und anderen Keys innerhalb des TPM

Im TPM aufbewahrte Schlüssel

- Endorsement Keys:
  Einzigartiges Schlüsselpaar, im TPM aufbewahrt - nicht exportierbar
- AIKs:
  Attestation Identity Keys - Benutzergenerierte Schlüsselpaare
- Storage Root Key:
  Zur Verschlüsselung von AIKs und anderen Keys innerhalb des TPM

Im TPM aufbewahrte Schlüssel

- Endorsement Keys:
  Einzigartiges Schlüsselpaar, im TPM aufbewahrt - nicht exportierbar
- AIKs:
  Attestation Identity Keys - Benutzergenerierte Schlüsselpaare
- Storage Root Key:
  Zur Verschlüsselung von AIKs und anderen Keys innerhalb des TPM

Im TPM aufbewahrte Schlüssel

- Endorsement Keys:
  Einzigartiges Schlüsselpaar, im TPM aufbewahrt - nicht exportierbar
- AIKs:
  Attestation Identity Keys - Benutzergenerierte Schlüsselpaare
- Storage Root Key:
  Zur Verschlüsselung von AIKs und anderen Keys innerhalb des TPM

Zertifikate

- Endorsement Zertifikat: Signiert mit Endorsement Key. Dieses Cert soll sicherstellen dass das TPM echt ist und von einem geprüften Hersteller bereitgestellt wurde
- Plattformzertifikat: vom Plattformhersteller ausgestellt, garantiert TCG-Konformität der Komponenten
- Conformance Zertifikat: Garantiert TCG-Konformität des TPM
- Validation Zertifikat: Garantiert Integrität einer oder mehrerer Teilkomponenten

Zertifikate

- Endorsement Zertifikat: Signiert mit Endorsement Key. Dieses Cert soll sicherstellen dass das TPM echt ist und von einem geprüften Hersteller bereitgestellt wurde
- Plattformzertifikat: vom Plattformhersteller ausgestellt, garantiert TCG-Konformität der Komponenten
- Conformance Zertifikat: Garantiert TCG-Konformität des TPM
- Validation Zertifikat: Garantiert Integrität einer oder mehrerer Teilkomponenten

Zertifikate

- Endorsement Zertifikat: Signiert mit Endorsement Key. Dieses Cert soll sicherstellen dass das TPM echt ist und von einem geprüften Hersteller bereitgestellt wurde
- Plattformzertifikat: vom Plattformhersteller ausgestellt, garantiert TCG-Konformität der Komponenten
- Conformance Zertifikat: Garantiert TCG-Konformität des TPM
- Validation Zertifikat: Garantiert Integrität einer oder mehrerer Teilkomponenten

Zertifikate

- Endorsement Zertifikat: Signiert mit Endorsement Key. Dieses Cert soll sicherstellen dass das TPM echt ist und von einem geprüften Hersteller bereitgestellt wurde
- Plattformzertifikat: vom Plattformhersteller ausgestellt, garantiert TCG-Konformität der Komponenten
- Conformance Zertifikat: Garantiert TCG-Konformität des TPM
- Validation Zertifikat: Garantiert Integrität einer oder mehrerer Teilkomponenten

Zertifikate

- Endorsement Zertifikat: Signiert mit Endorsement Key. Dieses Cert soll sicherstellen dass das TPM echt ist und von einem geprüften Hersteller bereitgestellt wurde
- Plattformzertifikat: vom Plattformhersteller ausgestellt, garantiert TCG-Konformität der Komponenten
- Conformance Zertifikat: Garantiert TCG-Konformität des TPM
- Validation Zertifikat: Garantiert Integrität einer oder mehrerer Teilkomponenten

Zertifikate

- Endorsement Zertifikat: Signiert mit Endorsement Key. Dieses Cert soll sicherstellen dass das TPM echt ist und von einem geprüften Hersteller bereitgestellt wurde
- Plattformzertifikat: vom Plattformhersteller ausgestellt, garantiert TCG-Konformität der Komponenten
- Conformance Zertifikat: Garantiert TCG-Konformität des TPM
- Validation Zertifikat: Garantiert Integrität einer oder mehrerer Teilkomponenten

Zertifikate

- Endorsement Zertifikat: Signiert mit Endorsement Key. Dieses Cert soll sicherstellen dass das TPM echt ist und von einem geprüften Hersteller bereitgestellt wurde
- Plattformzertifikat: vom Plattformhersteller ausgestellt, garantiert TCG-Konformität der Komponenten
- Conformance Zertifikat: Garantiert TCG-Konformität des TPM
- Validation Zertifikat: Garantiert Integrität einer oder mehrerer Teilkomponenten

Zertifikate

- Endorsement Zertifikat: Signiert mit Endorsement Key. Dieses Cert soll sicherstellen dass das TPM echt ist und von einem geprüften Hersteller bereitgestellt wurde
- Plattformzertifikat: vom Plattformhersteller ausgestellt, garantiert TCG-Konformität der Komponenten
- Conformance Zertifikat: Garantiert TCG-Konformität des TPM
- Validation Zertifikat: Garantiert Integrität einer oder mehrerer Teilkomponenten

Funktionen des TPM

- Erstellung von 2048 Bit RSA-Schlüsselpaaren
- Speicherung der einmaligen Endorsement Keys
- Authentifizierung gegenüber anderen Plattformen
- Zufallsgenerator
- Platform Configuration Register:
  Speichert Ergebnisse von Integritätstests, Hashwert (SHA-1) der Hardwareausstattung
- Sicheres Logging

Funktionen des TPM

- Erstellung von 2048 Bit RSA-Schlüsselpaaren
- Speicherung der einmaligen Endorsement Keys
- Authentifizierung gegenüber anderen Plattformen
- Zufallsgenerator
- Platform Configuration Register:
  Speichert Ergebnisse von Integritätstests, Hashwert (SHA-1) der Hardwareausstattung
- Sicheres Logging

Funktionen des TPM

- Erstellung von 2048 Bit RSA-Schlüsselpaaren
- Speicherung der einmaligen Endorsement Keys
- Authentifizierung gegenüber anderen Plattformen
- Zufallsgenerator
- Platform Configuration Register:
  Speichert Ergebnisse von Integritätstests, Hashwert (SHA-1) der Hardwareausstattung
- Sicheres Logging

Funktionen des TPM

- Erstellung von 2048 Bit RSA-Schlüsselpaaren
- Speicherung der einmaligen Endorsement Keys
- Authentifizierung gegenüber anderen Plattformen
- Zufallsgenerator
- Platform Configuration Register:
  Speichert Ergebnisse von Integritätstests, Hashwert (SHA-1) der Hardwareausstattung
- Sicheres Logging

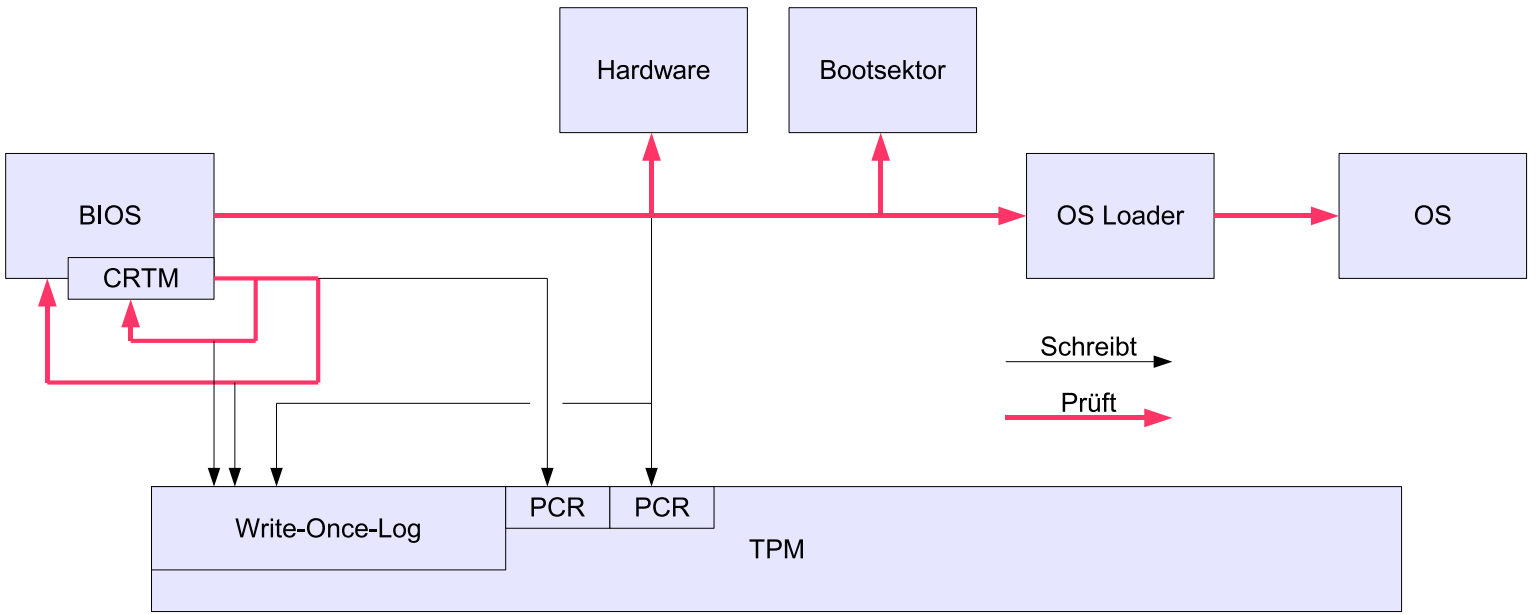
Funktionen des TPM

- Erstellung von 2048 Bit RSA-Schlüsselpaaren
- Speicherung der einmaligen Endorsement Keys
- Authentifizierung gegenüber anderen Plattformen
- Zufallsgenerator
- Platform Configuration Register:
  Speichert Ergebnisse von Integritätstests, Hashwert (SHA-1) der Hardwareausstattung
- Sicheres Logging

Funktionen des TPM

- Erstellung von 2048 Bit RSA-Schlüsselpaaren
- Speicherung der einmaligen Endorsement Keys
- Authentifizierung gegenüber anderen Plattformen
- Zufallsgenerator
- Platform Configuration Register:
  Speichert Ergebnisse von Integritätstests, Hashwert (SHA-1) der Hardwareausstattung
- Sicheres Logging

Secure Bootstrap



Next Generation Secure Computing Base a.k.a. Palladium

Anforderungen an einen Windows-Nachfolger:

- Trusted Computing
- Abwärtskompatibilität auf Treiber und Applikationsebene

Microsofts Lösung:

Zwei voneinander unabhängige Teilsysteme: Windows und Nexus

Next Generation Secure Computing Base a.k.a. Palladium

Anforderungen an einen Windows-Nachfolger:

- Trusted Computing
- Abwärtskompatibilität auf Treiber und Applikationsebene

Microsofts Lösung:

Zwei voneinander unabhängige Teilsysteme: Windows und Nexus

Next Generation Secure Computing Base a.k.a. Palladium

Anforderungen an einen Windows-Nachfolger:

- Trusted Computing
- Abwärtskompatibilität auf Treiber und Applikationsebene

Microsofts Lösung:

Zwei voneinander unabhängige Teilsysteme: Windows und Nexus

Next Generation Secure Computing Base a.k.a. Palladium

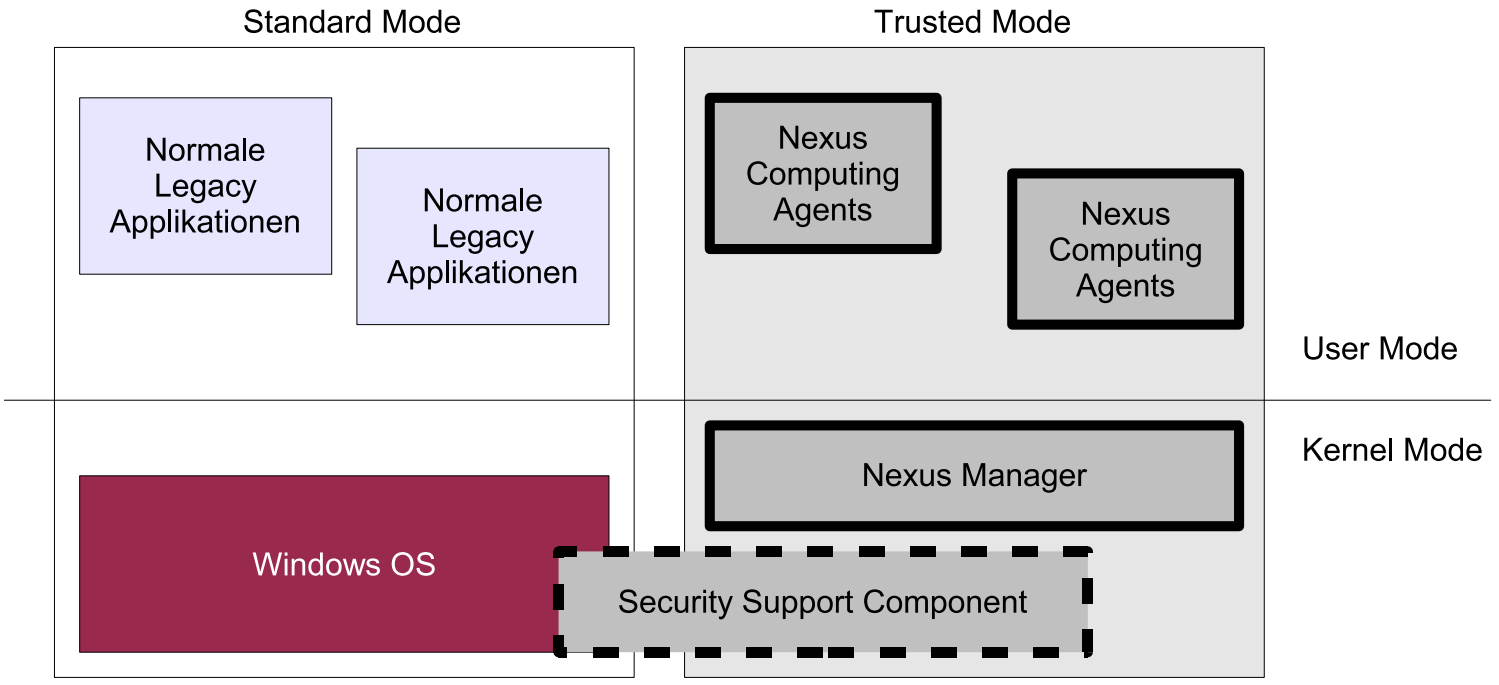
Anforderungen an einen Windows-Nachfolger:

- Trusted Computing
- Abwärtskompatibilität auf Treiber und Applikationsebene

Microsofts Lösung:

Zwei voneinander unabhängige Teilsysteme: Windows und Nexus

NGSCB Architektur



NGSCB Schutzfunktionen

Schutz mit

- Strong Process Isolation: Seitenschutz im Hauptspeicher gegen Beobachtung und Modifikation
- Sealed Storage: Datenschutz auf Festplatte
- Secure Path To/From User: Sichere Ein-/Ausgabekanäle

Demonstration von NGSCB auf WinHEC (Windows Hardware Engineering Conference) 2003.

NGSCB Schutzfunktionen

Schutz mit

- Strong Process Isolation: Seitenschutz im Hauptspeicher gegen Beobachtung und Modifikation
- Sealed Storage: Datenschutz auf Festplatte
- Secure Path To/From User: Sichere Ein-/Ausgabekanäle

Demonstration von NGSCB auf WinHEC (Windows Hardware Engineering Conference) 2003.

NGSCB Schutzfunktionen

Schutz mit

- Strong Process Isolation: Seitenschutz im Hauptspeicher gegen Beobachtung und Modifikation
- Sealed Storage: Datenschutz auf Festplatte
- Secure Path To/From User: Sichere Ein-/Ausgabekanäle

Demonstration von NGSCB auf WinHEC (Windows Hardware Engineering Conference) 2003.

NGSCB Schutzfunktionen

Schutz mit

- Strong Process Isolation: Seitenschutz im Hauptspeicher gegen Beobachtung und Modifikation
- Sealed Storage: Datenschutz auf Festplatte
- Secure Path To/From User: Sichere Ein-/Ausgabekanäle

Demonstration von NGSCB auf WinHEC (Windows Hardware Engineering Conference) 2003.

NGSCB Schutzfunktionen

Schutz mit

- Strong Process Isolation: Seitenschutz im Hauptspeicher gegen Beobachtung und Modifikation
- Sealed Storage: Datenschutz auf Festplatte
- Secure Path To/From User: Sichere Ein-/Ausgabekanäle

Demonstration von NGSCB auf WinHEC (Windows Hardware Engineering Conference) 2003.

Diskussion um TCPA I

TCPA selbst ist nur die Technik - Policies werden von Dritten vorgegeben

TCPA ist Opt-In - Muss explizit aktiviert werden

„Ein Auto mit Benzin zu betanken ist ebenfalls Opt-In.“

Diskussion um TCPA I

TCPA selbst ist nur die Technik - Policies werden von Dritten vorgegeben

TCPA ist Opt-In - Muss explizit aktiviert werden

„Ein Auto mit Benzin zu betanken ist ebenfalls Opt-In.“

Diskussion um TCPA I

TCPA selbst ist nur die Technik - Policies werden von Dritten vorgegeben

TCPA ist Opt-In - Muss explizit aktiviert werden

„Ein Auto mit Benzin zu betanken ist ebenfalls Opt-In.“

Diskussion um TCPA II

Allerdings wurde von Content-Anbietern in den USA (RIAA/MPAA) versucht durch Gesetze den Verkauf von nicht-TCPA-kompatiblen Systemen unter Strafe zu verbieten:

„The penalties proposed for breaking this law would have ranged from 5 to 20 years in prison and fines between $\$50,000$ to $\$1$ million.“ (SSSCA/CBDTPA)

Diskussion um TCPA II

Allerdings wurde von Content-Anbietern in den USA (RIAA/MPAA) versucht durch Gesetze den Verkauf von nicht-TCPA-kompatiblen Systemen unter Strafe zu verbieten:

„The penalties proposed for breaking this law would have ranged from 5 to 20 years in prison and fines between $\$50,000$ to $\$1$ million.“ (SSSCA/CBDTPA)

Diskussion um TCPA III

Einsatz von PKI begünstigt Monopolbildung

KMU und OSS könnten vom Markt ausgeschlossen werden

Juristen sehen TCPA nicht unbedingt als im Einklang mit geltendem EU-Wettbewerbsrecht

Diskussion um TCPA III

Einsatz von PKI begünstigt Monopolbildung

KMU und OSS könnten vom Markt ausgeschlossen werden

Juristen sehen TCPA nicht unbedingt als im Einklang mit geltendem EU-Wettbewerbsrecht

Diskussion um TCPA III

Einsatz von PKI begünstigt Monopolbildung

KMU und OSS könnten vom Markt ausgeschlossen werden

Juristen sehen TCPA nicht unbedingt als im Einklang mit geltendem EU-Wettbewerbsrecht

Diskussion um TCPA IV

Die vieldiskutierte Idee einer globalen Sperrliste erlaubt auch nachträgliche Zensur

Aktuell: Fall „Rafik al Hariri“

Früher: z.B. DeCSS

Im Zweifelsfall werden gewisse Staaten technische Möglichkeiten auch zur Kriegsführung verwenden (z.n. TUD)

Diskussion um TCPA IV

Die vieldiskutierte Idee einer globalen Sperrliste erlaubt auch nachträgliche Zensur

Aktuell: Fall „Rafik al Hariri“

Früher: z.B. DeCSS

Im Zweifelsfall werden gewisse Staaten technische Möglichkeiten auch zur Kriegsführung verwenden (.iq-TLD)

Diskussion um TCPA IV

Die vieldiskutierte Idee einer globalen Sperrliste erlaubt auch nachträgliche Zensur

Aktuell: Fall „Rafik al Hariri“
Früher: z.B. DeCSS

Im Zweifelsfall werden gewisse Staaten technische Möglichkeiten auch zur Kriegsführung verwenden (.iq-TLD)

Diskussion um TCPA IV

Die vieldiskutierte Idee einer globalen Sperrliste erlaubt auch nachträgliche Zensur

Aktuell: Fall „Rafik al Hariri“
Früher: z.B. DeCSS

Im Zweifelsfall werden gewisse Staaten technische Möglichkeiten auch zur Kriegsführung verwenden (.iq-TLD)

Realität von Trusted Computing

Windows Longhorn mit Palladium erscheint voraussichtlich 2004.

Windows Longhorn mit NGSCB erscheint voraussichtlich 2005.

Realität von Trusted Computing

~~Windows Longhorn mit Palladium erscheint voraussichtlich 2004.~~
Windows Longhorn mit NGSCB erscheint voraussichtlich 2005.

Realität von Trusted Computing

~~Windows Longhorn mit Palladium erscheint voraussichtlich 2004.~~
~~Windows Longhorn mit NGSCB erscheint voraussichtlich 2005.~~

Realität von Trusted Computing

Microsoft sah strenge Regeln für die Entwicklung von Programmen für den Nexus vor.

Entwickler sagten aber:

Sicherheit ist Sache des Betriebssystems, wir wollen nur Anwendungen schreiben.

WinHEC 2004: NGSCB $\longrightarrow$ Virtualisierungslösung.

WinHEC 2005: Virtualisierung $\longrightarrow$ „Secure Startup“ mit Verschlüsselung der Systempartitionen

Realität von Trusted Computing

Microsoft sah strenge Regeln für die Entwicklung von Programmen für den Nexus vor.

Entwickler sagten aber:
Sicherheit ist Sache des Betriebssystems, wir wollen nur Anwendungen schreiben.

WinHEC 2004: NGSCB $\longrightarrow$ Virtualisierungslösung.
WinHEC 2005: Virtualisierung $\longrightarrow$ „Secure Startup“ mit Verschlüsselung der Systempartition.

Realität von Trusted Computing

Microsoft sah strenge Regeln für die Entwicklung von Programmen für den Nexus vor.

Entwickler sagten aber:
Sicherheit ist Sache des Betriebssystems, wir wollen nur Anwendungen schreiben.

WinHEC 2004: NGSCB $\longrightarrow$ Virtualisierungslösung.
WinHEC 2005: Virtualisierung $\longrightarrow$ „Secure Startup“ mit Verschlüsselung der Systempartition.

Realität von Trusted Computing

Microsoft sah strenge Regeln für die Entwicklung von Programmen für den Nexus vor.

Entwickler sagten aber:
Sicherheit ist Sache des Betriebssystems, wir wollen nur Anwendungen schreiben.

WinHEC 2004: NGSCB $\longrightarrow$ Virtualisierungslösung.
WinHEC 2005: Virtualisierung $\longrightarrow$ „Secure Startup“ mit Verschlüsselung der Systempartition.

Realität von Trusted Computing

~~Windows Longhorn mit Palladium erscheint voraussichtlich 2004.~~
~~Windows Longhorn mit NGSCB erscheint voraussichtlich 2005.~~
Windows Longhorn mit Secure Startup 2006 ?

Realität von Trusted Computing

~~Windows Longhorn mit Palladium erscheint voraussichtlich 2004.~~
~~Windows Longhorn mit NGSCB erscheint voraussichtlich 2005.~~
Windows Longhorn mit Secure Startup ~~2006~~ 2007 ?

Zurück zum Anfang: Trusted Computing

Wer vertraut hier nun wem ?

US Dept. of Defense: A „trusted system or component“ is defined as „one which can break the security policy“.

Zurück zum Anfang: Trusted Computing

Wer vertraut hier nun wem ?

US Dept. of Defense: A „trusted system or component“ is defined as „one which can break the security policy“.

Fragen ?

Vielen Dank für die Aufmerksamkeit

Fragen ?

Vielen Dank für die Aufmerksamkeit