TCPA / TCG:
Trusted Computing und Linux

Wilhelm Dolle
Director Information Technology
interActive Systems GmbH

Chemnitzer Linux-Tag 2004
07. März 2004, Chemnitz

Agenda

- Ziele / Hintergründe / Historie
- Status Quo
- Technik hinter TCPA und dem TPM
- IBM-Linux-Experimentalpaket
- (MS Palladium / NGSCB)
- Wahrheit und Spekulation? Forderungen!

Ziele von Trusted Computing / IT-Sicherheit

- Schutz vor Malware
- Integritätsüberprüfung des Betriebssystems vor dem Booten
- Authentisierung von Hard- und Software gegenüber dem Betriebssystem und externen Kommunikationspartnern
- Verbesserter Datenschutz und verbesserte Sicherheit beim Aufbewahren und Übertragen von Daten
- Vertraulichkeit, Integrität, Verfügbarkeit

Nebenwirkungen von Trusted Computing

- Zensur
- Verletzung der Privatsphäre
- Einschränkung der Nutzung des Computers und von Daten (DRM)

Trusted Computing / Sicherheitsmodelle

- **Bell-LaPadula Modell**
  - Verschiedene Sicherheitsstufen
  - No read-up / no write-down
  - Fokus: Vertraulichkeit (militärische Nutzung)
- **Biba Modell**
  - No read down / no write up
  - Fokus: Integrität von Daten (kommerzielle Nutzung)
- **Clark-Wilson Modell**
  - Zugriff auf Daten nur durch berechtigte Programme
  - Separation of duties
  - Audit wird zwingend vorgeschrieben

Trusted Computing / Sichere Systeme

- **1972: Referenzmonitor - abstrakte Maschine die alle Zugriffe von Subjekten (z. B. Benutzer, Prozesse) auf Objekte (z. B. Dateien, Ressourcen) überwacht und vermittelt**
- **Trusted Computing Base (TCB, Orange Book, 1985-2000): Einheit von integrer Hard- und Software zur Durchsetzung von Sicherheitsrichtlinien**
- **TCB sollte einfach und kompakt sein (Code-Audit)**
- **1997: AEGIS – Trennung des BIOS in zwei Teile**
  - Bisherige BIOS Aufgaben
  - Kryptographische Prüfsummen und digitale Signaturen von Hardware (und Software)

TCPA (Trusted Computing Platform Alliance)

- 1999 von Microsoft, Intel, IBM, Compaq und HP gegründetes Hersteller-Konsortium
- 180 Mitglieder (u.a. Infineon, Siemens, RSA, Nokia)
- Erste Veröffentlichung der Spezifikationen in Version 0.9 im August 2000
- Ziel: Durch den Einsatz von spezieller Krypto-Hardware und darauf aufbauenden Betriebssystemen die Sicherheit verbessern

TCG (Trusted Computing Group)

TCG

- **Anfänglich von AMD, HP, Intel und Microsoft gegründet**
- **Seit April 2003 Rechtsnachfolger der TCPA**
- **Nicht ganz so basisdemokratisch wie TCPA**
  - Kein Veto für Mitglieder mehr (2/3 Mehrheit)
  - Promotor (50.000$/Jahr), Contributor (15.000$/Jahr), Adopter (7.500 $/Jahr, kein Stimmrecht)
  - Ende 2003 etwa 40 Mitglieder
- **Ziel: Entwicklung und Support von offenen Industriestandards für „Trusted Computing“ auf verschiedenen Plattformen (PC‘s, Server, Handys und PDA‘s)**

iAS

TCG Spezifikationen

TCG

- **Hardware: TPM (Trusted Platform Module)**
- **Software: TSS (Trusted Software Stack)**

- **TCG TPM Main Specification (alte Version 1.1b)**
- **TCG Software Stack Specification (Version 1.1, September 2003)**

- **TCG TPM Specification Version 1.2 (November 2003)**
  - Design Principles
  - Structures of the TPM
  - TPM Commands

iAS

Status Quo

- **TPM nach 1.1b Spezifikation erhältlich, z. B.**
  - Atmel, Infineon, National Semiconductor
- **Konforme Systeme werden ausgeliefert, z. B.**
  - IBM (ThinkPad Notebooks, NetVista Desktops) und HP
- **Zunehmender Applikations-Support, z. B.**
  - RSA Secure ID, Checkpoint VPN
- **Software von IBM**
  - Windows: verändertes Login, rudimentäre Verschlüsselungswerkzeuge
  - Linux: Testpaket (samt Quellen) mit Kernel-Modul, Bibliothek, API und Beispielprogrammen

TPM (Trusted Platform Module)

- **Nach US-Senator Fritz Hollings benannter Prozessor „Fritz Chip“**
- **In Zukunft direkt in der CPU eingebaut (LaGrande von IBM, AMD-Prozessoren, als Firmware-Version in Transmetas Crusoe TM5800**

- **Wesentliche Designziele**
  - Sicherer Hardwarespeicher für kryptographische Schlüssel
  - Unterstützung eines sicheren Bootvorgangs
  - Sealing
  - Platform Attestation

TPM – Designziele

- **Sealing (Versiegelung)**
  - Daten werden durch Verschlüsselung an aktuelle Systemkonfiguration gebunden
  - Verschlüsselung mit Authorisierungscode und Berücksichtigung des Inhalts von Registern (PCRs) mit Hash-Werten der Konfiguration von Systemkomponenten
  - Unsealing nur, wenn Register und Code stimmen
  - Anwendung muss Hardwarefehler berücksichtigen

- **Platform Attestation (Beglaubigung der Plattform)**
  - Öffentlicher Teil eines Schlüssels (EK), signiert von einer vertrauenswürdigen Instanz, beweist Kommunikationspartner das Vorhandensein eines „registrierten“ TPMs
  - Gefahr einer „Seriennummer“

TPM – Blick in den TCPA-Chip

Funktionale Einheit	Nicht flüchtiger Speicher	Flüchtiger Speicher
Random Number Generator	Endorsement Key (2048 Bit)	RSA Key Slot-0 … RSA Key Slot-9
Hash (SHA-1)	Storage Root Key (2048 Bit)	PCR-0 … PCR-15
HMAC	Owner Auth Secret (160 Bit)	Key Handle
RSA Key Generation		Auth Session Handle
RSA Encrypt/Decrypt		

TPM – Kryptographische Funktionseinheiten

- Random Number Generator (RNG)
- Hash-Einheit (SHA-1)
- HMAC (Keyed Hashing for Message Authentication)
- Generator für RSA-Schlüssel mit bis zu 2.048 Bit
- RSA Engine zum Erzeugen von Signaturen (nicht prüfen) sowie Ver- und Entschlüsseln

TPM – Blick in den TCPA-Chip

Funktionale Einheit	Nicht flüchtiger Speicher	Flüchtiger Speicher
Random Number Generator	Endorsement Key (2048 Bit)	RSA Key Slot-0 … RSA Key Slot-9
Hash (SHA-1)	Storage Root Key (2048 Bit)	PCR-0 … PCR-15
HMAC	Owner Auth Secret (160 Bit)	Key Handle
RSA Key Generation		Auth Session Handle
RSA Encrypt/Decrypt		

TPM – Nicht flüchtiger Speicher

- **Endorsement Key (EK)**
  - 2.048 Bit RSA Schlüsselpaar
  - Wird beim Herstellungsprozess zufällig generiert und mit einem „Master-Key“ signiert
  - Kann nicht gelöscht oder geändert werden (ab TPM 1.2 ist dies möglich)
  - Privater Schlüssel verlässt den Chip nie
  - Nicht migrierbar
  - Öffentlicher Schlüssel dient zur „attestation“ und zur Verschlüsselung von sensitiven Daten die an den Chip gesendet werden (zum Beispiel beim „Besitz übernehmen“)
  - Da der öffentliche Schlüssel aus Sicht der Privatsphäre kritisch ist, kann er durch den Benutzer „abgeschaltet“ werden

TPM – Nicht flüchtiger Speicher

- **Storage Root Key (SRK)**
  - 2.048 Bit RSA Schlüsselpaar
  - Initial ist dieser Speicherplatz leer
  - Wird beim „Besitz übernehmen“ generiert
  - Privater Schlüssel verlässt den Chip nie – nicht migrierbar
  - Kann vom Systembesitzer gelöscht werden
  - Dient zum Verschlüsseln (wrap) von privaten Schlüsseln die außerhalb des Chips gespeichert werden sollen, sowie beim Entschlüsseln dieser privaten Schlüssel (im TPM)
- **Owner Authorization Secret**
  - 160 Bit Schlüssel den der Besitzer mit dem Chip teilt
  - Wird beim „Besitz übernehmen“ in den Chip geladen
  - Autorisierung von sensitiven Benutzerbefehlen

TPM – Blick in den TCPA-Chip

Funktionale Einheit	Nicht flüchtiger Speicher	Flüchtiger Speicher
Random Number Generator	Endorsement Key (2048 Bit)	RSA Key Slot-0 … RSA Key Slot-9
Hash (SHA-1)	Storage Root Key (2048 Bit)	PCR-0 … PCR-15
HMAC	Owner Auth Secret (160 Bit)	Key Handle
RSA Key Generation		Auth Session Handle
RSA Encrypt/Decrypt		

TPM – Flüchtiger Speicher

- **Zehn Plätze für temporäre RSA Schlüssel**
  - Extern gespeicherte Schlüssel können hier in den Chip geladen und von dort genutzt werden
  - Können hinausgeworfen (evicted) werden um Platz zu schaffen

- **16 Plätze für PCR‘s (Platform Configuration Register)**
  - 160 Bit Hash-Werte der Konfiguration
  - Beim Booten können z.B. Messungen vom BIOS, erweitertem BIOS, MBR, LILO, GRUB bootstrap stages, anderen Dateien wie dem Kernel, aber auch von Hardware die dies unterstützt erzeugt und hier gespeichert werden
  - Nicht zwangsläufig ein Wert pro Objekt

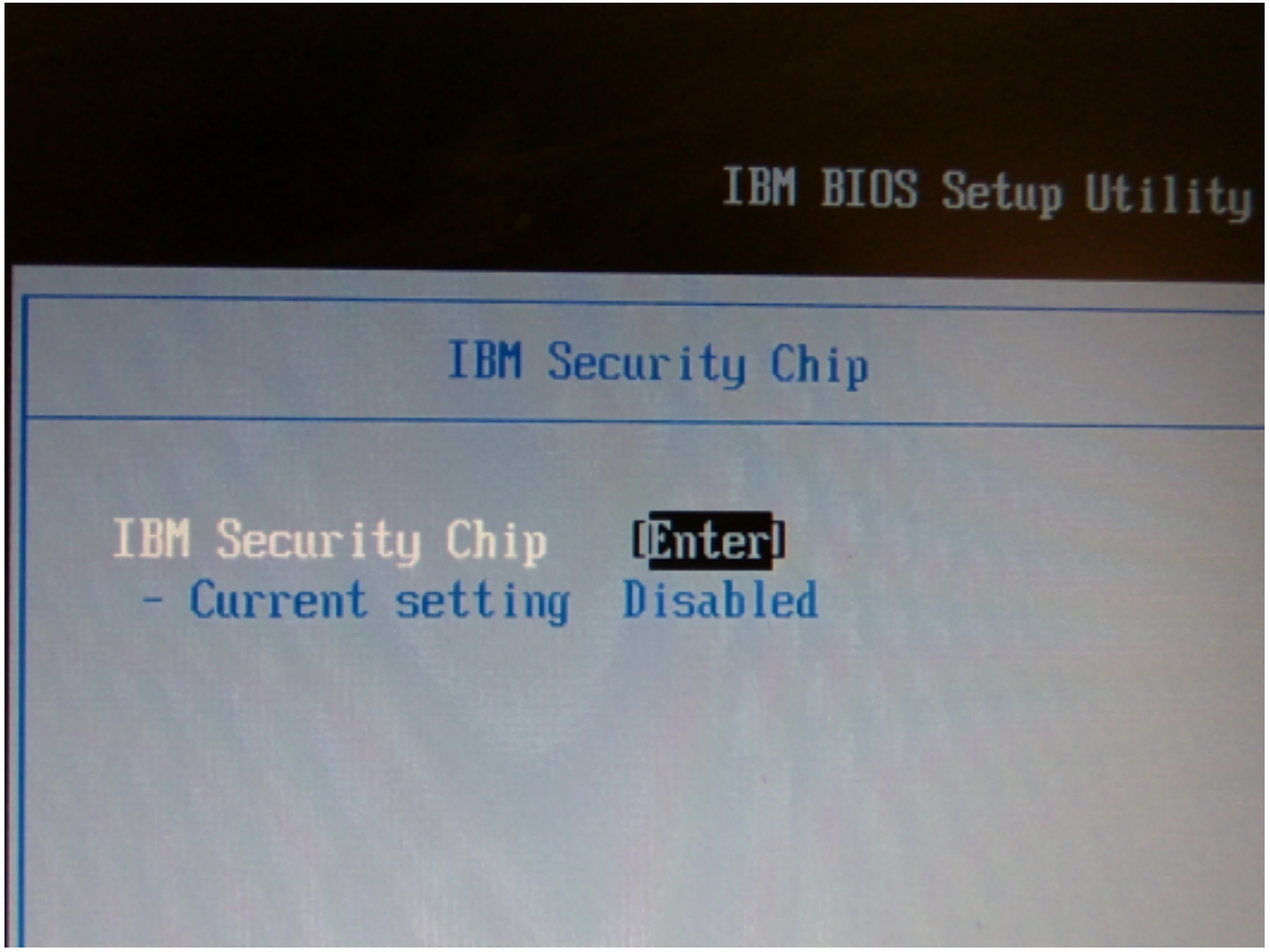
TPM – Flüchtiger Speicher

- **Key Handles**
  - Um temporär geladenen Schlüsseln Namen zur weiteren Bearbeitung zuzuweisen
  - Werden gelöscht wenn der Schlüssel aus dem Chip geworfen wird
- **Authorization Session Handle**
  - Wird genutzt um den Status der Autorisation für mehrere hintereinander abfolgende Befehle beizubehalten
- **Ab TPM 1.2 zusätzlich weitere mindestens 20 Byte große Speicherplätze (Data Integrity Register)**

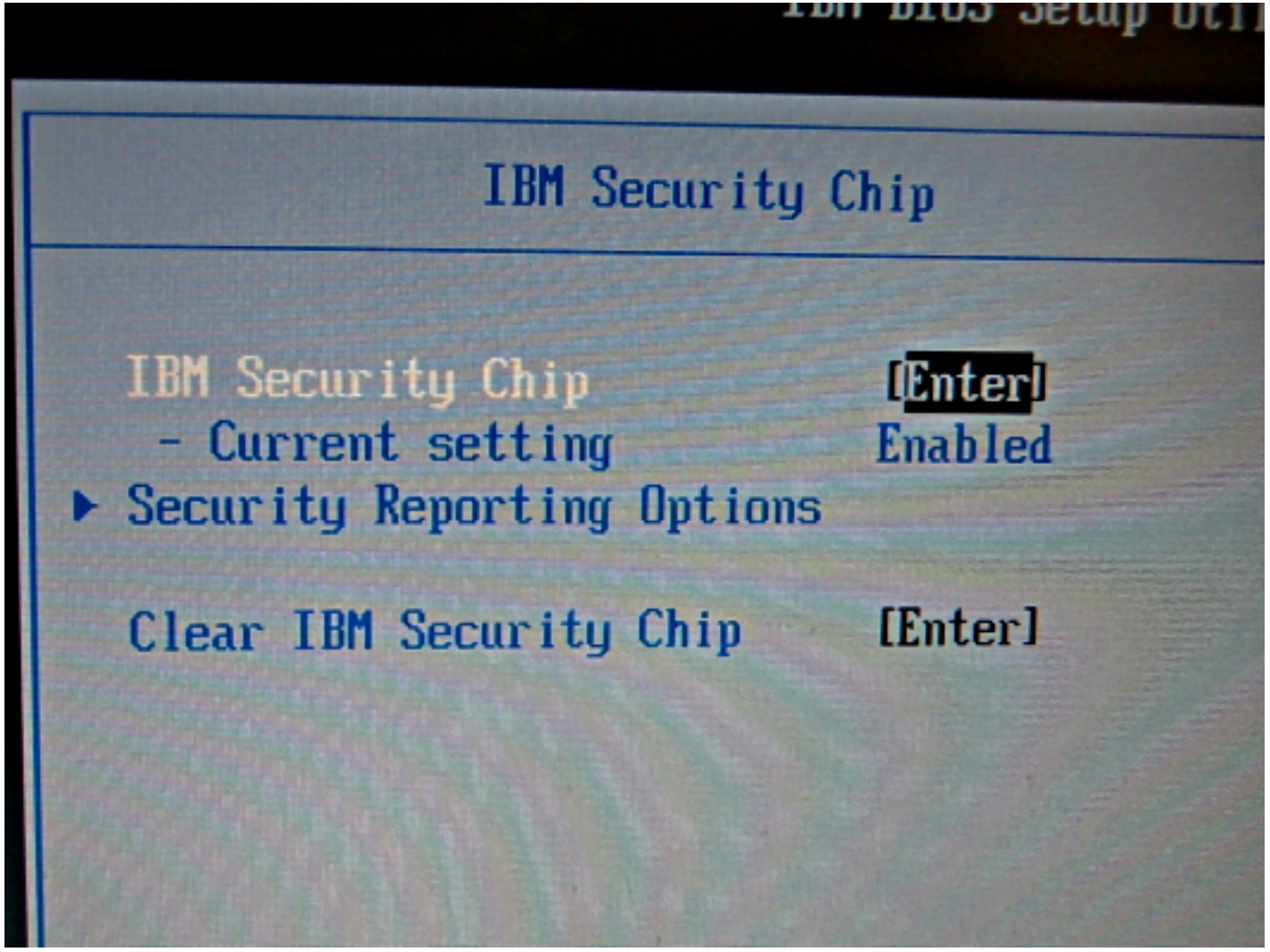
BIOS: Aktivieren und Löschen des TPM

- **BIOS gibt TPM beim Einschalten des Rechners ein Startkommando (drei Möglichkeiten)**
  - TPM deaktivieren (kann bis zum Einschalten nicht mehr aktiviert werden)
  - TPM starten und Reset der PCR-Register, Inhalte der PCR werden neu berechnet beim Booten
  - TPM starten und PCR-Register wieder herstellen (falls vorher gespeichert – resume-Modus)
- **BIOS kann TPM „komplett“ resetten (ForceClear)**
  - Benötigt Beweis der physikalischen Präsenz (z. B. beim IBM R32/T30: Fn beim Systemstart gedrückt halten und mit F1 ins BIOS wechseln)
  - Wirft alle geladenen Schlüssel und Handles raus und löscht SRK sowie das Owner Authorization Secret

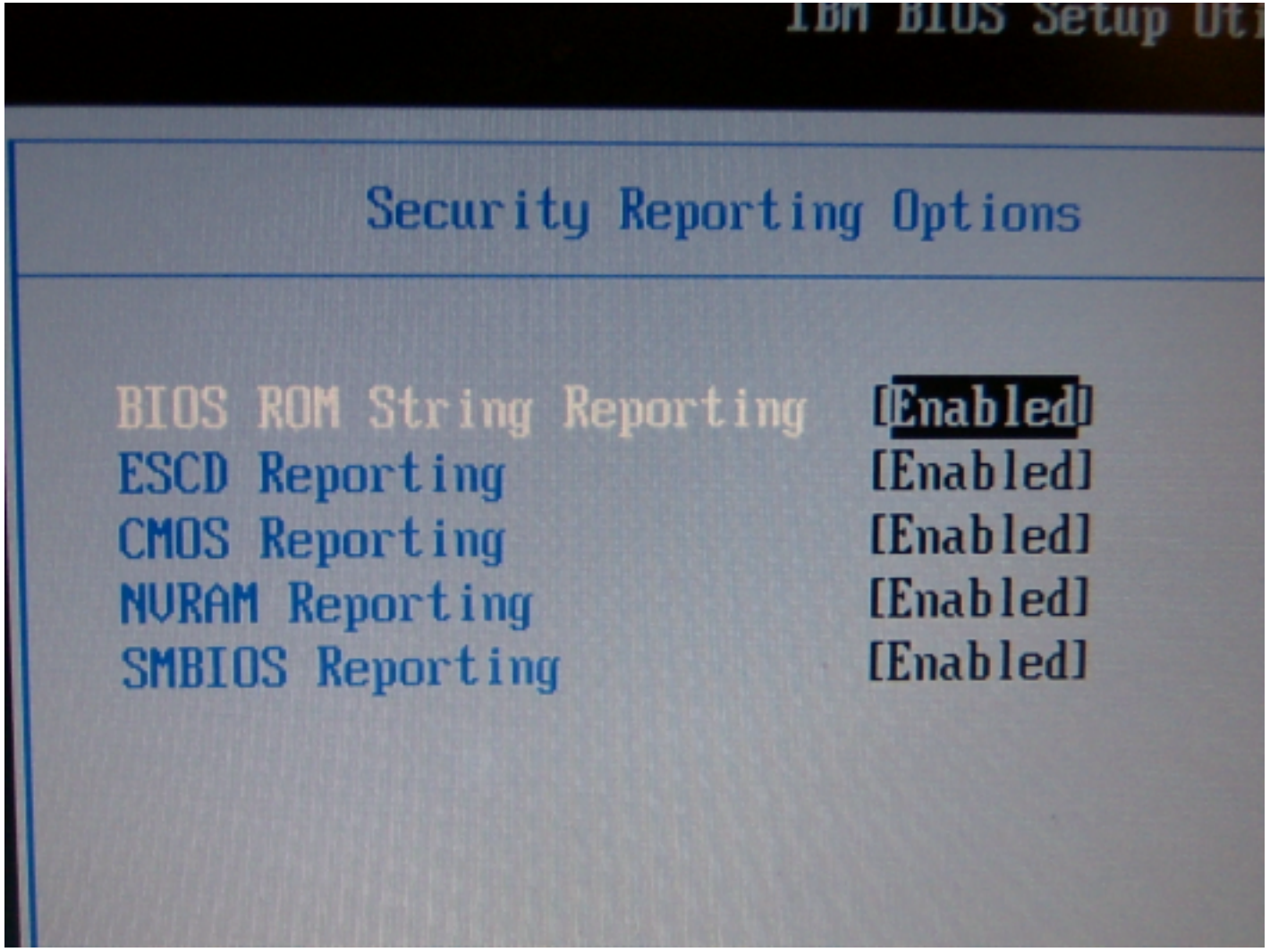
IBM R32 ThinkPad (BIOS)



IBM R32 ThinkPad (BIOS)



IBM R32 ThinkPad (BIOS)



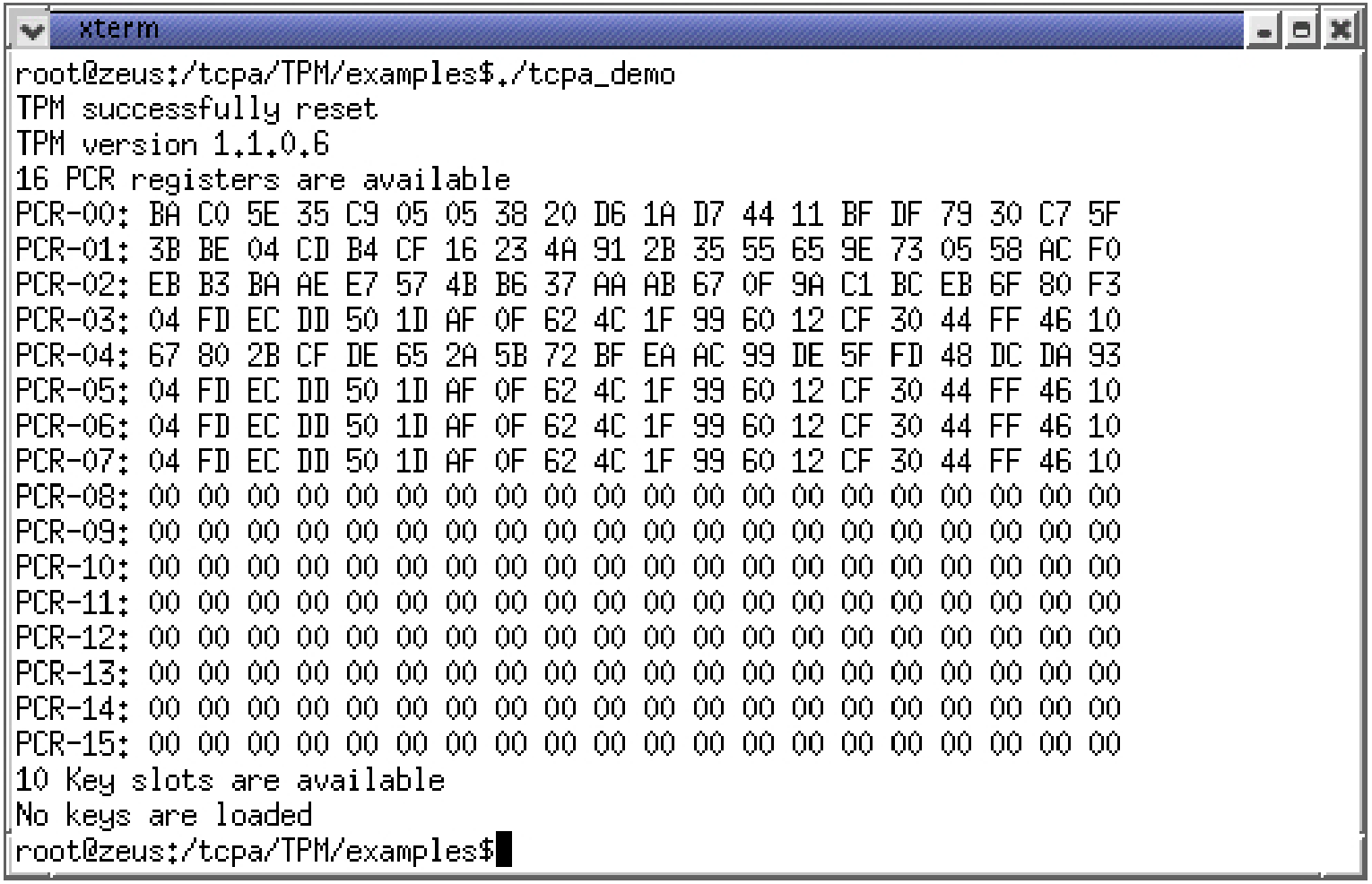
IBM Linux-Experimentalpaket (Installation)

- **TPM im BIOS aktivieren**
- **tpm-1.1b.tar.gz entpacken**
- **Mit make in *TPM/tpm* Kernelmodul tpm.o erzeugen**
- **Mit insmod tpm.o laden, alternativ:**
  - # cp tpm.o /lib/modules/*/unsupported/tpm.o
  - # depmod –a
- **Character Device anlegen**
  - # mknod /dev/tpm c 10 224
- **Mit make in *TPM/libtcpa* zunächst Bibliotheken, dann in *TPM/examples* Demowerkzeuge übersetzen**

IBM Linux-Experimentalpaket (Werkeuge)

- tcpa_demo (zeigt den Inhalt des TPM an)
- takeown (Besitz über das TPM übernehmen)
- sealfile und unsealfile (Dateien versiegeln)
- createkey (Erzeugung eines Schlüssels)
- loadkey (lädt einen Schlüssel in das TPM)
- signfile und verifyfile (Signieren und Signatur prüfen)
- evictkey (Slots im TPM leeren)

IBM Linux-Experimentalpaket (Chipinhalt)



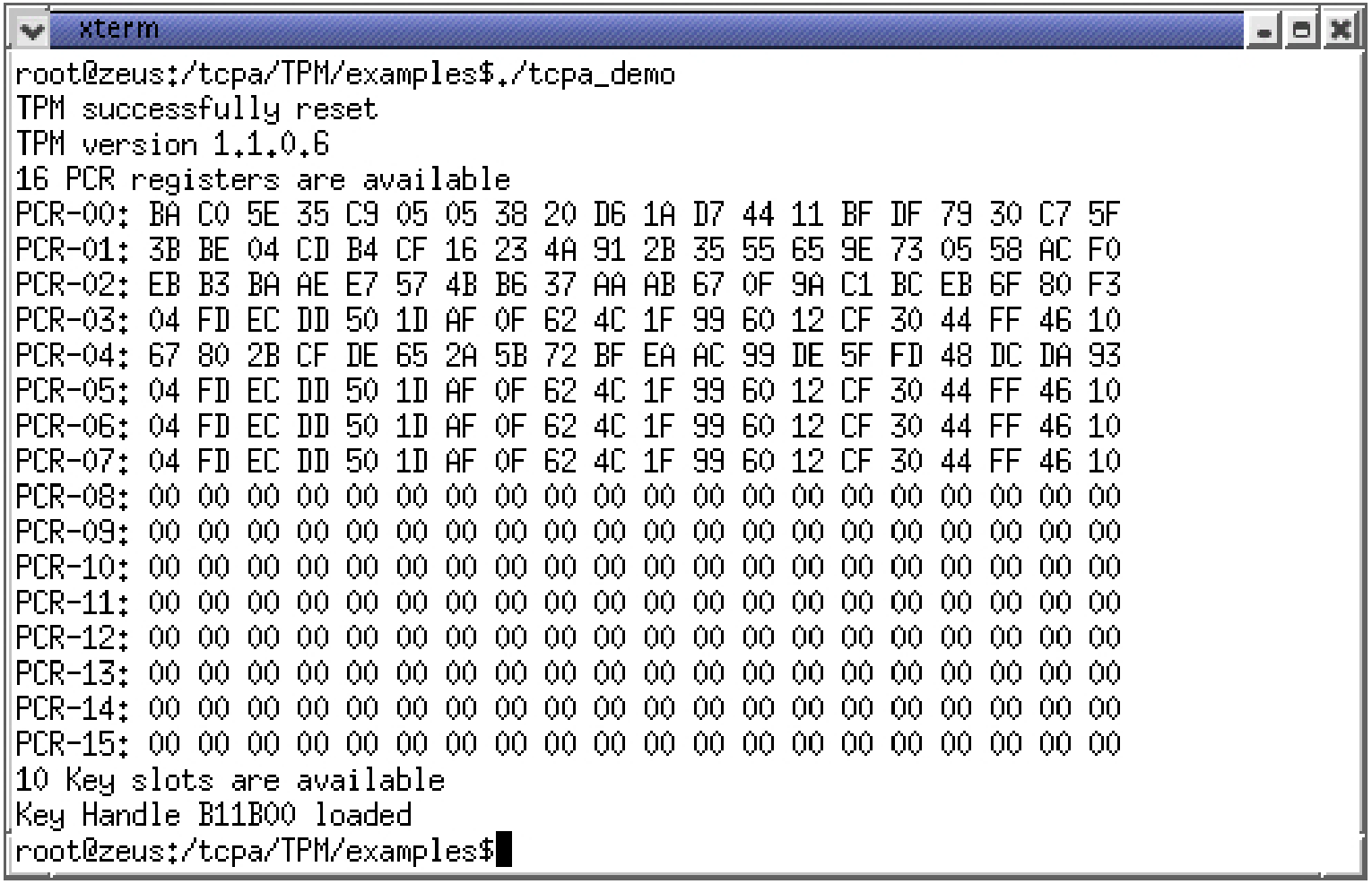
Übernehmen des Besitzes

- **Vier kritische Funktionen**
  - Owner Authorization Secret wird im TPM installiert.
  - Storage Root Key Schlüsselpaar wird im TPM erzeugt
  - SRK Authorization Secret wird auf den Schlüssel angewandt
  - Öffentlicher Teil des SKR kann ausgegeben werden
- **Befehl um den Besitz zu übernehmen benötigt Benutzerpasswort (Owner Authorization Secret) und das Passwort, dass den Storage Root Key schützen soll**
  - # ./takeown owner_password srk_password
- **TPM ist nun voll funktionsfähig**

Erzeugen von Schlüsseln

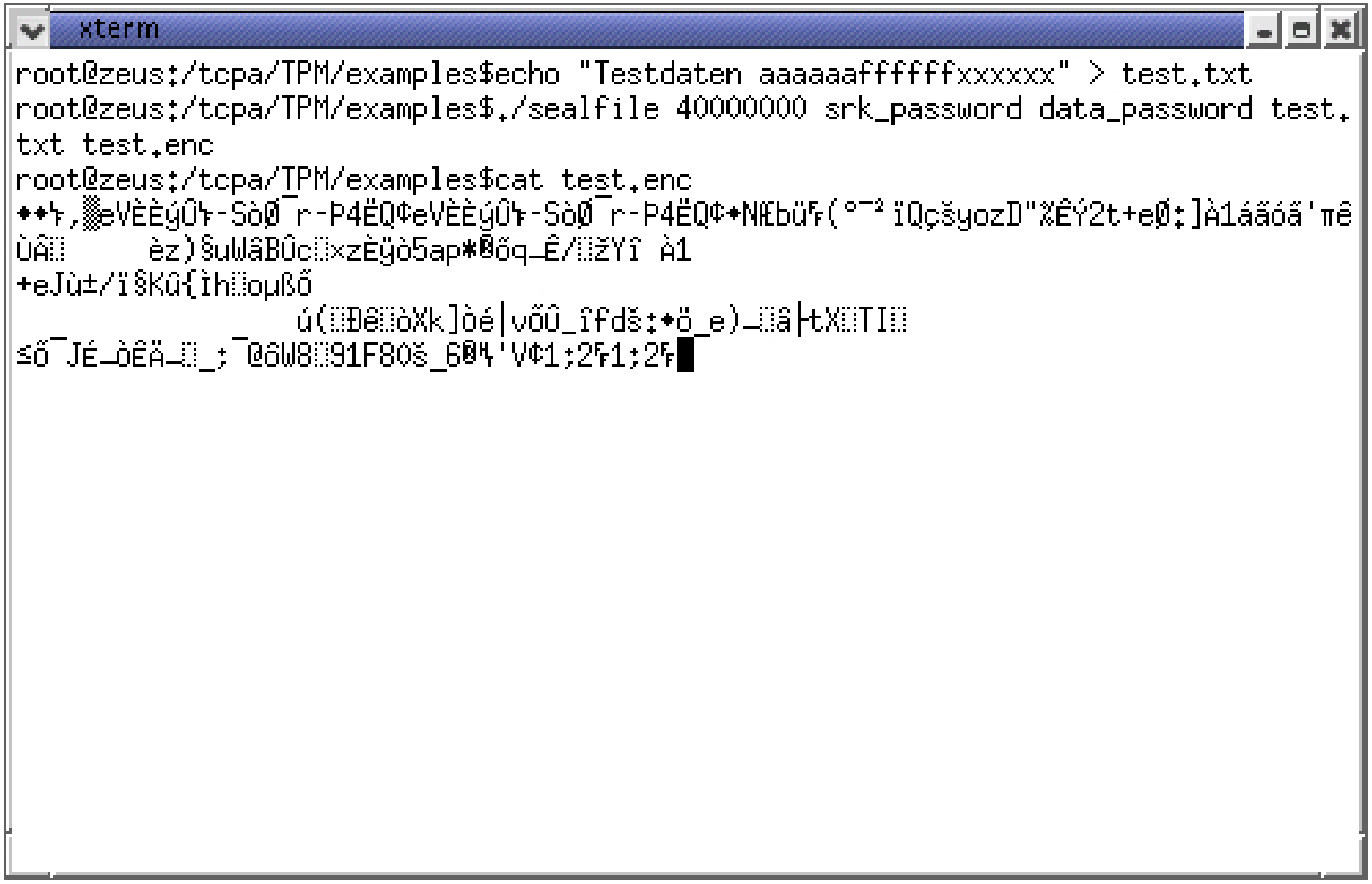
- Zufallszahlengenerator im TPM wird benutzt
- Schlüssel muss entweder zur Ver- und Entschlüsselung oder zum Signieren deklariert werden
- Ein Schlüssel für beide Aufgaben ist nicht erlaubt
- Optionale Angabe eines Passworts für den Schlüssel
- Schlüssel kann zusätzlich an PCRs gebunden werden
- Schlüssel benötigt Vater-Schlüssel, um privaten Teil zu verschlüsseln bevor er an den Benutzer übergeben wird
- Vater kann, muss aber nicht, der Storage Root Key sein

IBM Linux-Experimentalpaket (geladener Schlüssel)

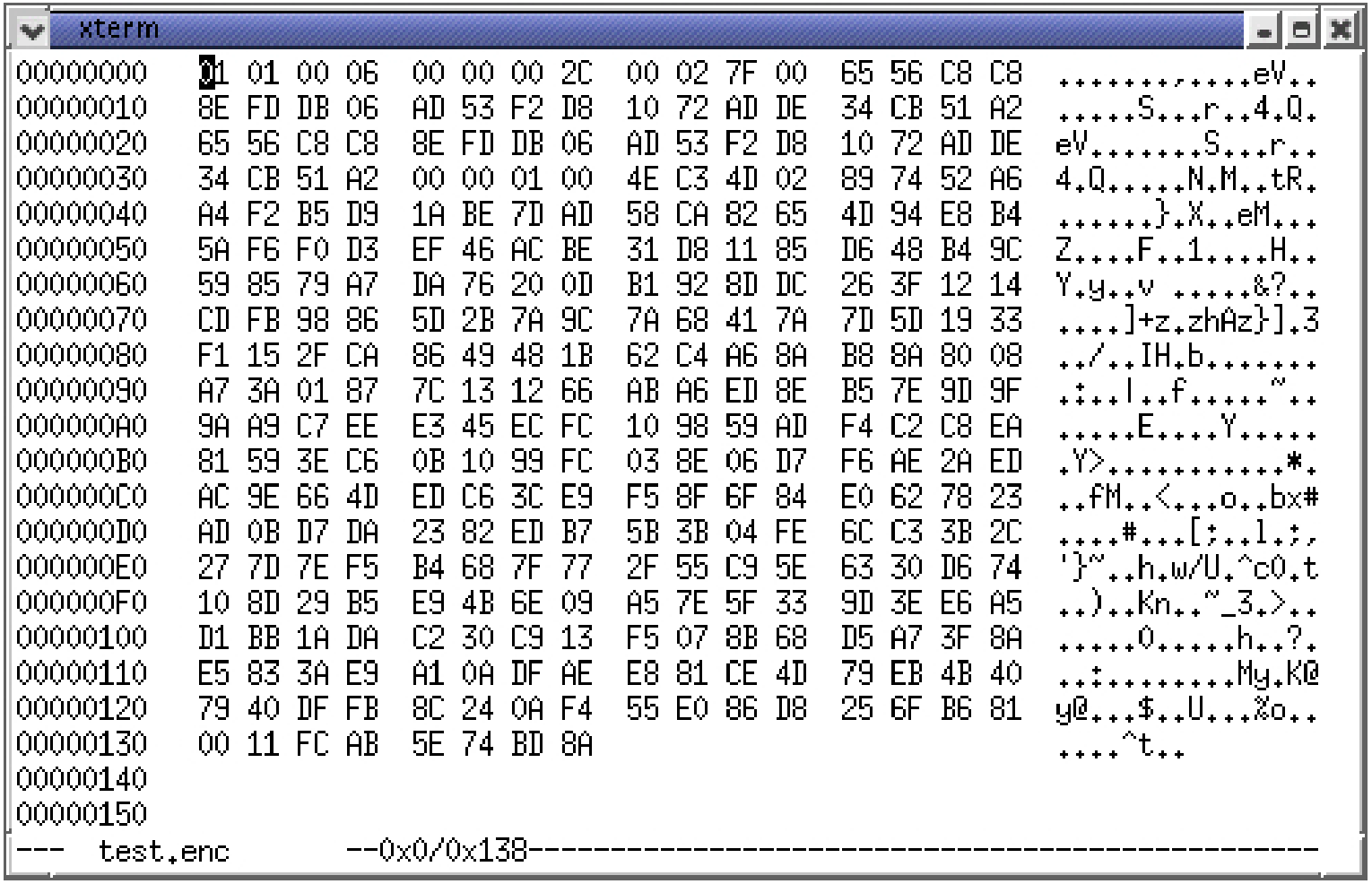


IBM Linux-Experimentalpaket (Sealfile)

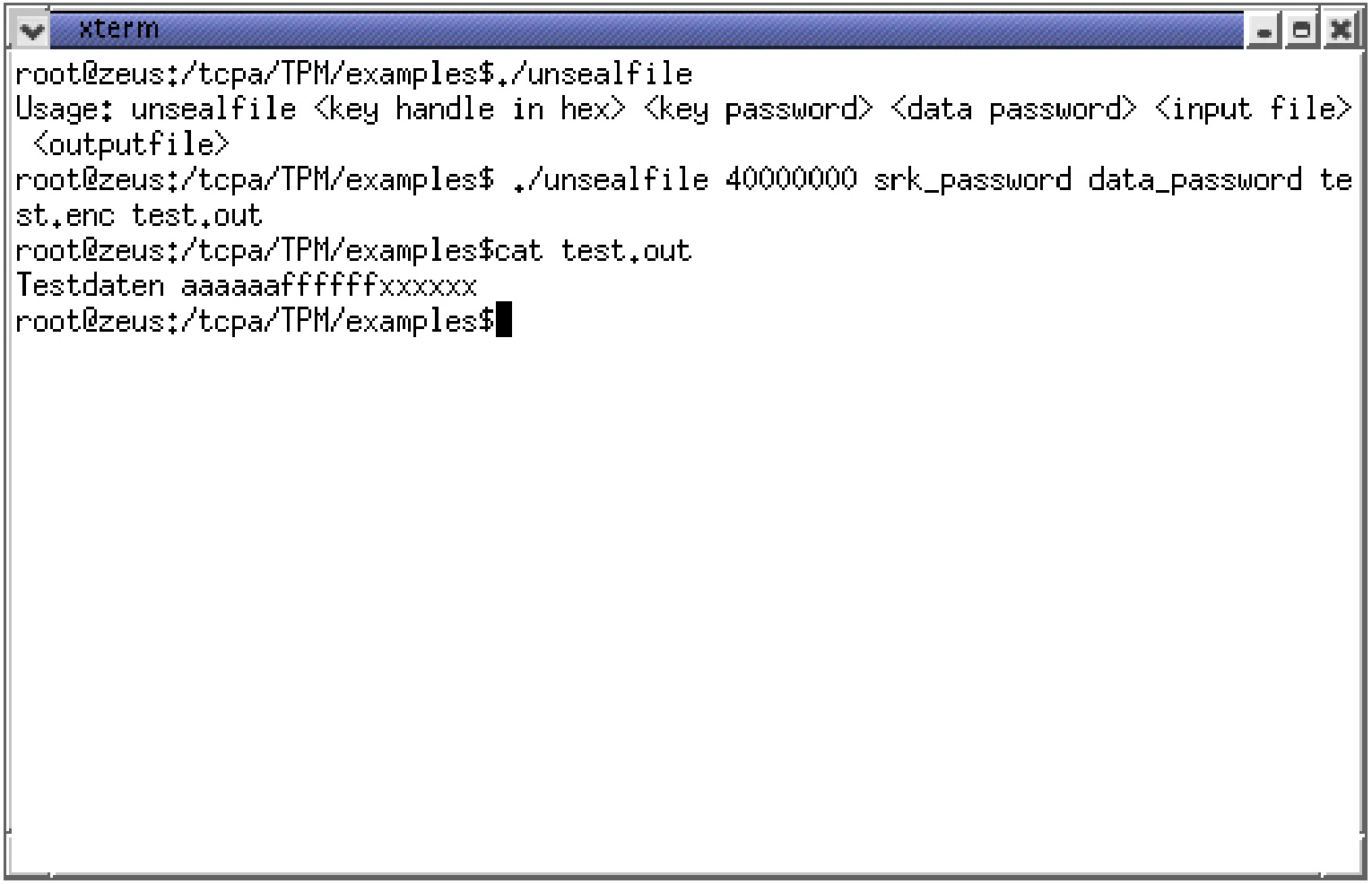
IBM Linux-Experimentalpaket (Sealfile)

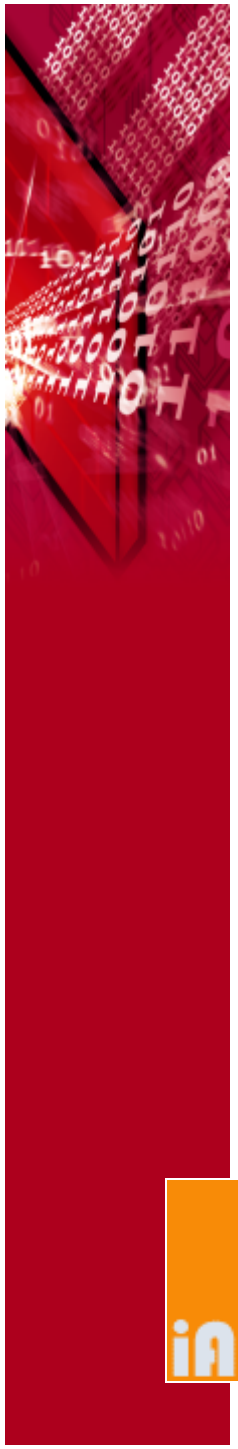


IBM Linux-Experimentalpaket (Sealfile)



IBM Linux-Experimentalpaket (Unsealfile)





Palladium / NGSCB (Next Generation Secure Computing Base)

- Geschützter Speicherbereich (Curtained Memory) um NGSCB-Applikationen vor potentiellen Schadprogrammen abzuschirmen
- Sicherer Speicherbereich (Sealed Storage) zur sicheren Ablage von sensiblen Daten
- Abgesicherte Ein- und Ausgaben (Trusted I/O)
- Software Authentifizierung (Attestation)

- Soll auf TCG-Spezifikationen Version 1.2 aufbauen

- Sicherheitskritische (und DRM) Komponenten werden in einen Nexus zusammengefasst und in eine sichere Hardwareumgebung ausgelagert

- Microsoft definiert den Nexus als sicher und packt hier eine Menge Funktionalität rein

Palladium / NGSCB Versprechungen

- Benutzer bekommen volle Kontrolle darüber ob sie NGSCB nutzen wollen
- Sämtliche heutige Software ist weiter nutzbar
- Programmierschnittstellen für NGSCB werden veröffentlicht und dokumentiert
- Microsoft-Nexus wird zur Evaluierung zur Verfügung stehen
- Keine Zertifizierung von NGSCB-Software nötig
- Besserer Schutz der Privatsphäre der Benutzer als bei heutigen PCs

Wahrheit und Spekulation? Forderungen?

- TCPA = Palladium = DRM?
- GPL und TCPA vereinbar?
- Marktschranken?
- Datenschutz / Privatsphäre?
- Vollständige Kontrolle über alle Schlüssel im TPM (CCC)
- Owner Override (EFF)

Fragen?

Vielen Dank für das Interesse!

Wilhelm Dolle
Director Information Technology

iAS interActive Systems
Dieffenbachstrasse 33c
D-10967 Berlin

phone +49-(0)30-69004-100
fax +49-(0)30-69004-101
mail wilhelm.dolle@interActive-Systems.de
web http://www.interActive-Systems.de