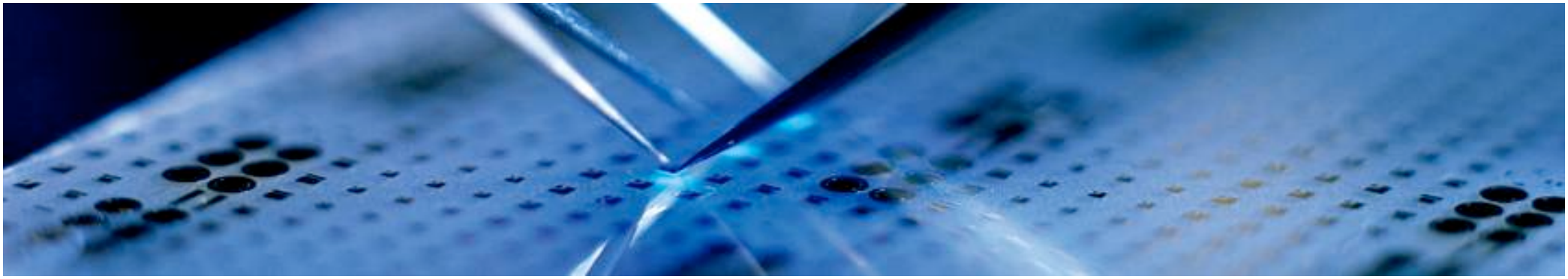


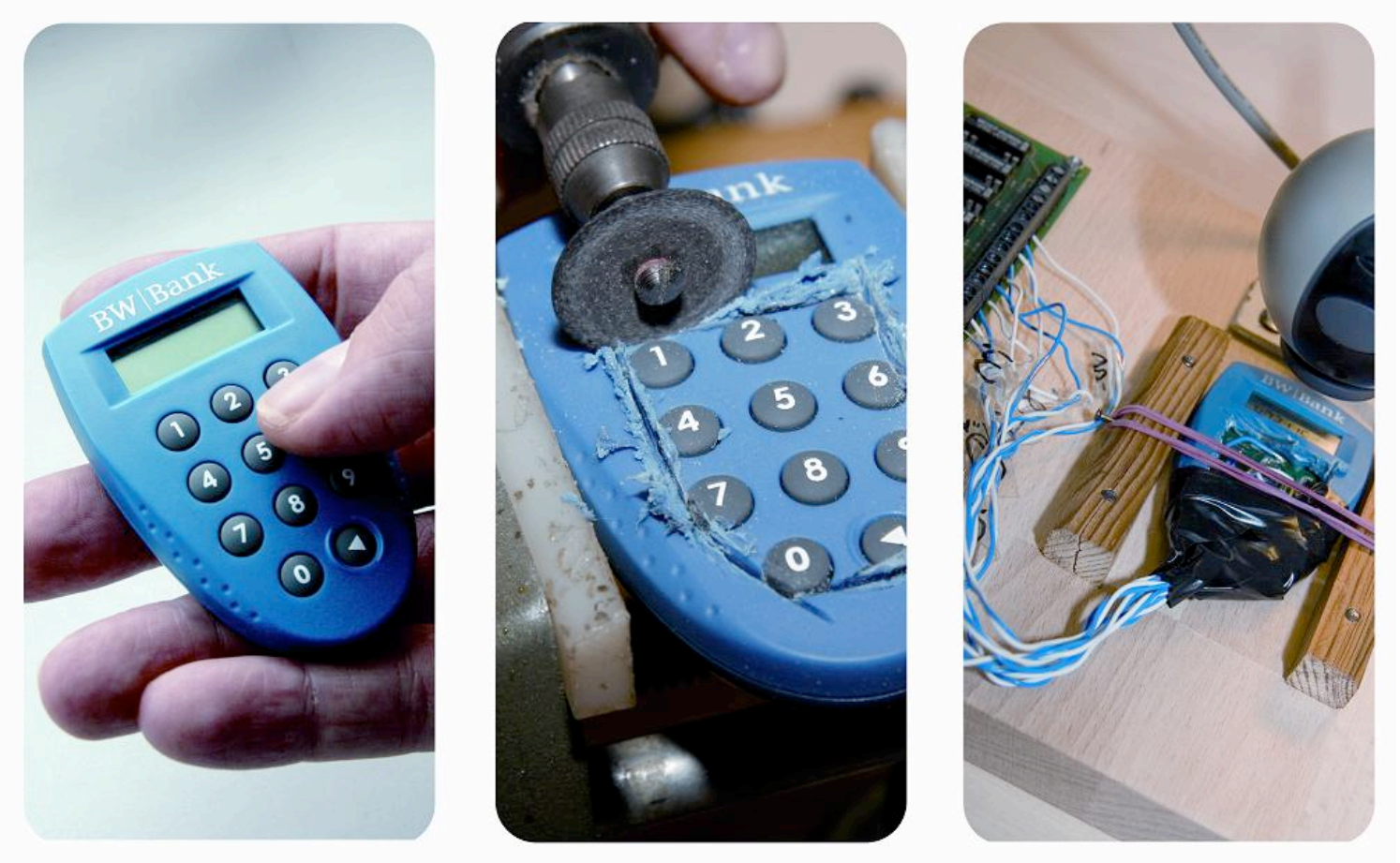
Sven Türpe, Andreas Poller, Jan Steffan,
Jan-Peter Stotz, Jan Trukenmüller

Für fünf Euro Sicherheit

BitLocker, Trusted Computing und gezielte Angriffe

Fraunhofer Institut
Sichere Informations-
Technologie

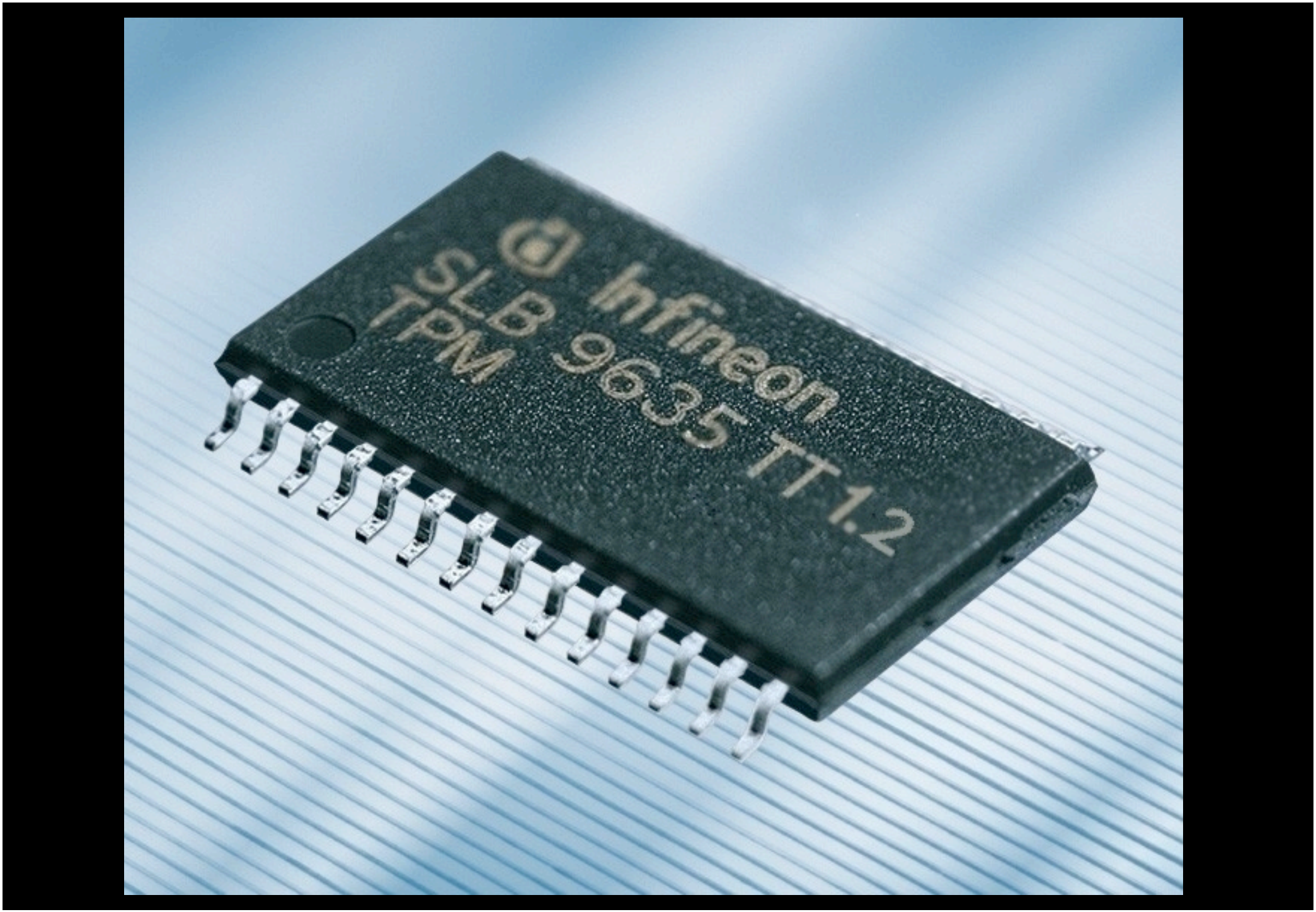
http://testlab.sit.fraunhofer.de



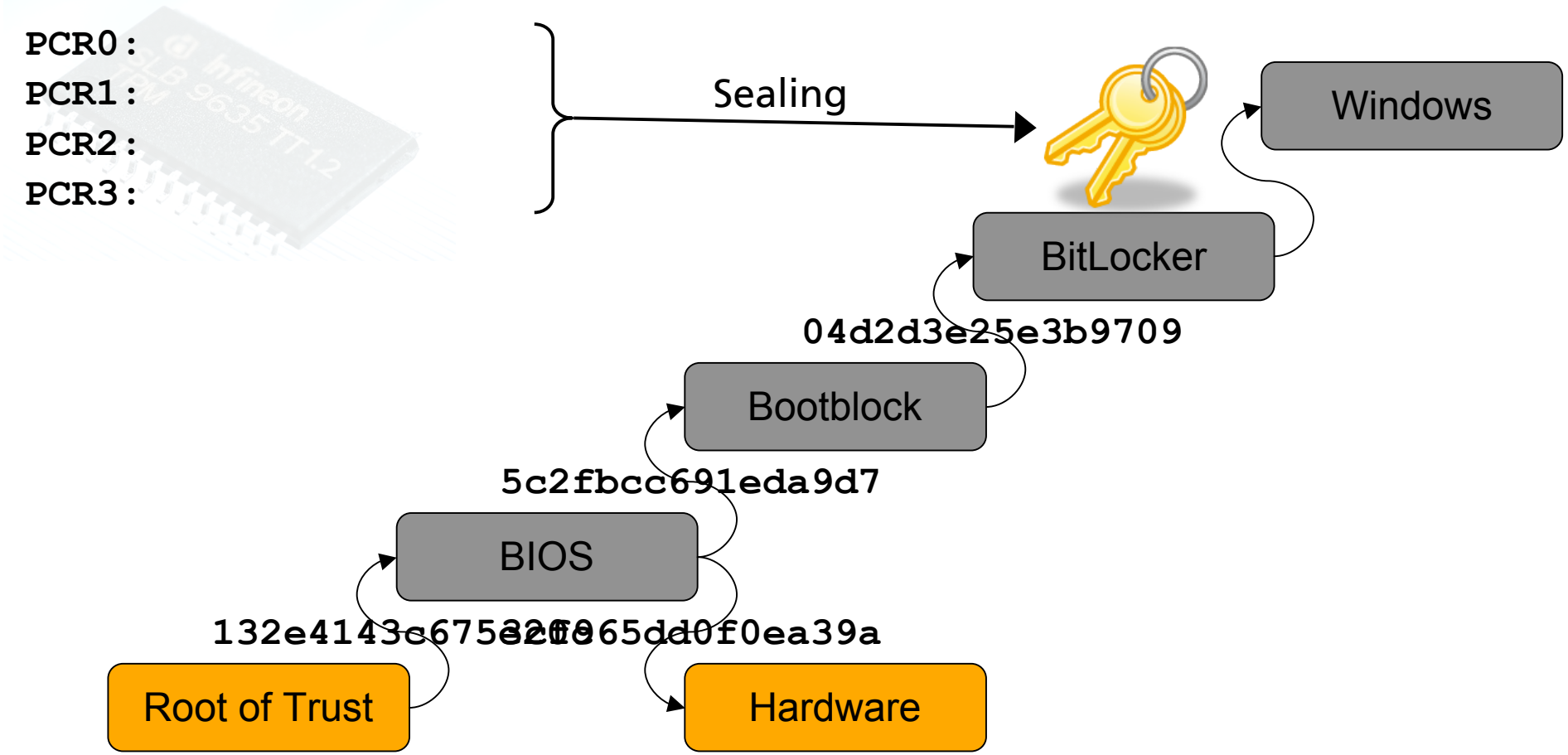
BitLocker ganz kurz

- Partitionsverschlüsselung mit AES
- »Lost Laptop Problem«
  - Opportunistischer Angriff
- Schlüsselverwaltung durch Nutzer und TPM

Sealing bindet Schlüssel an TPM + Zustand


infineon
SLB 9635 TT1.2
TPM

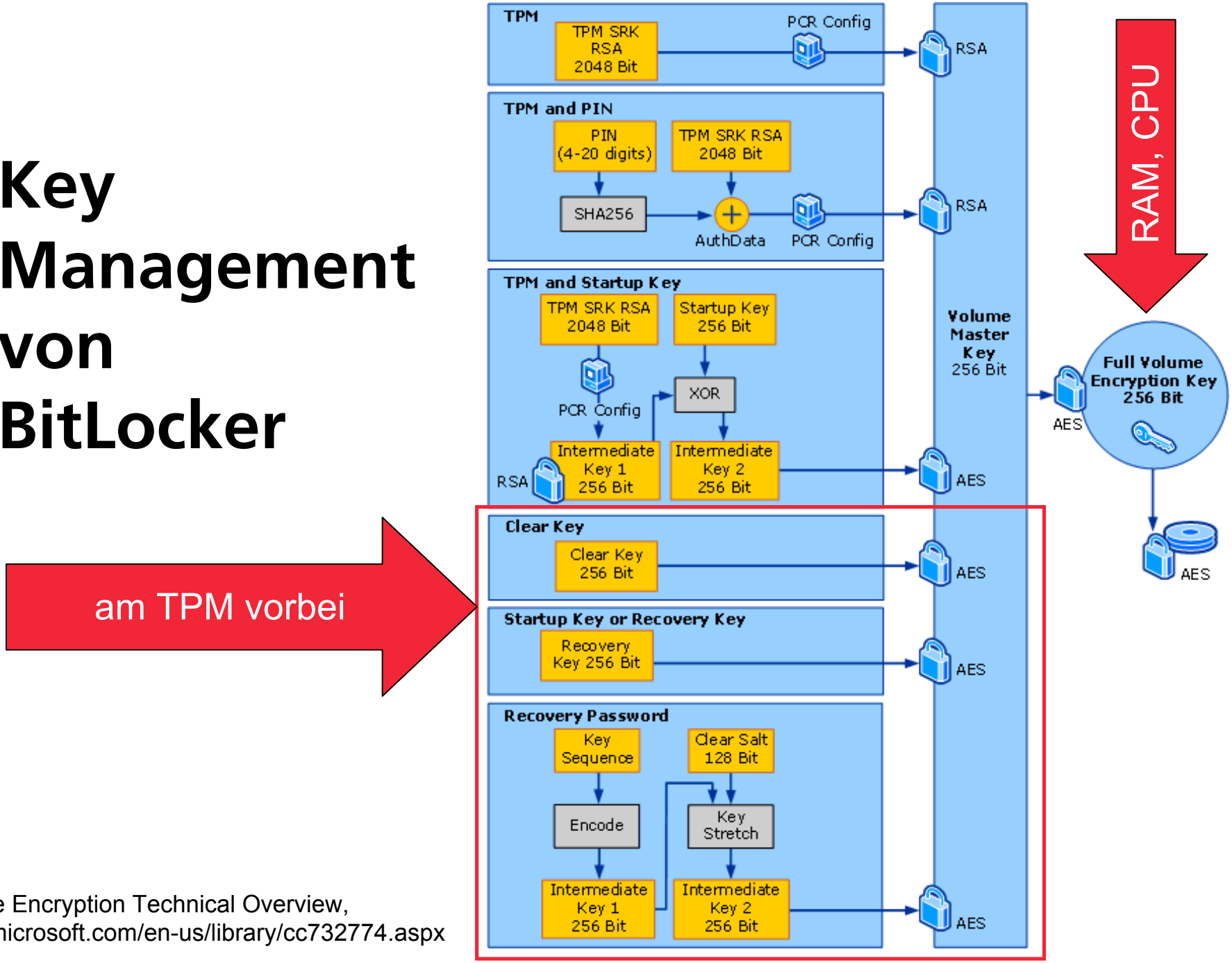
Überwachtes Booten



Optionen zur Schlüsselverwaltung

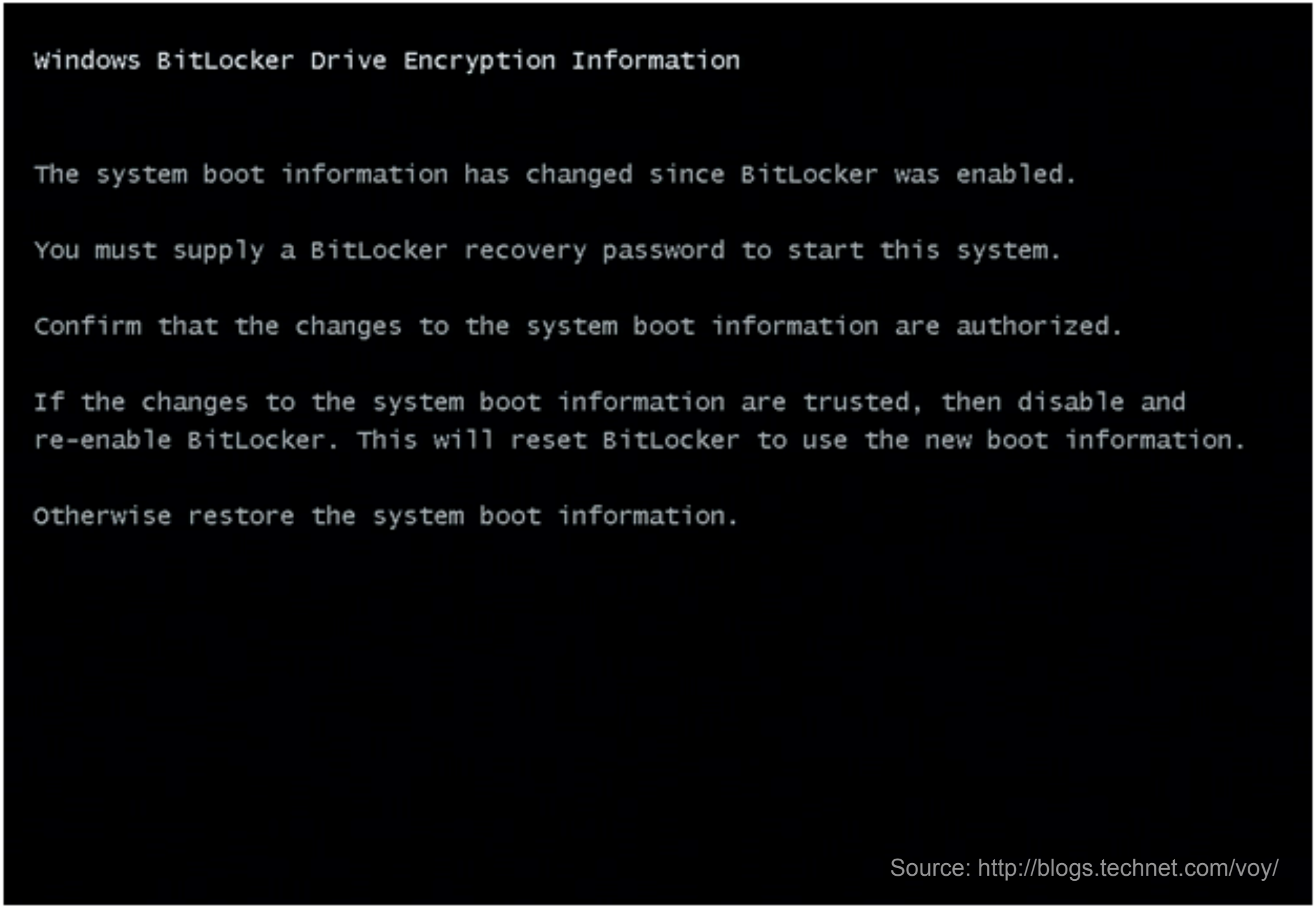
- nur TPM
- TPM + PIN
- TPM + USB-Key
- TPM + PIN + USB-Key (SP1)
- Nur USB-Key (normal/recovery)
- Recovery-Passwort

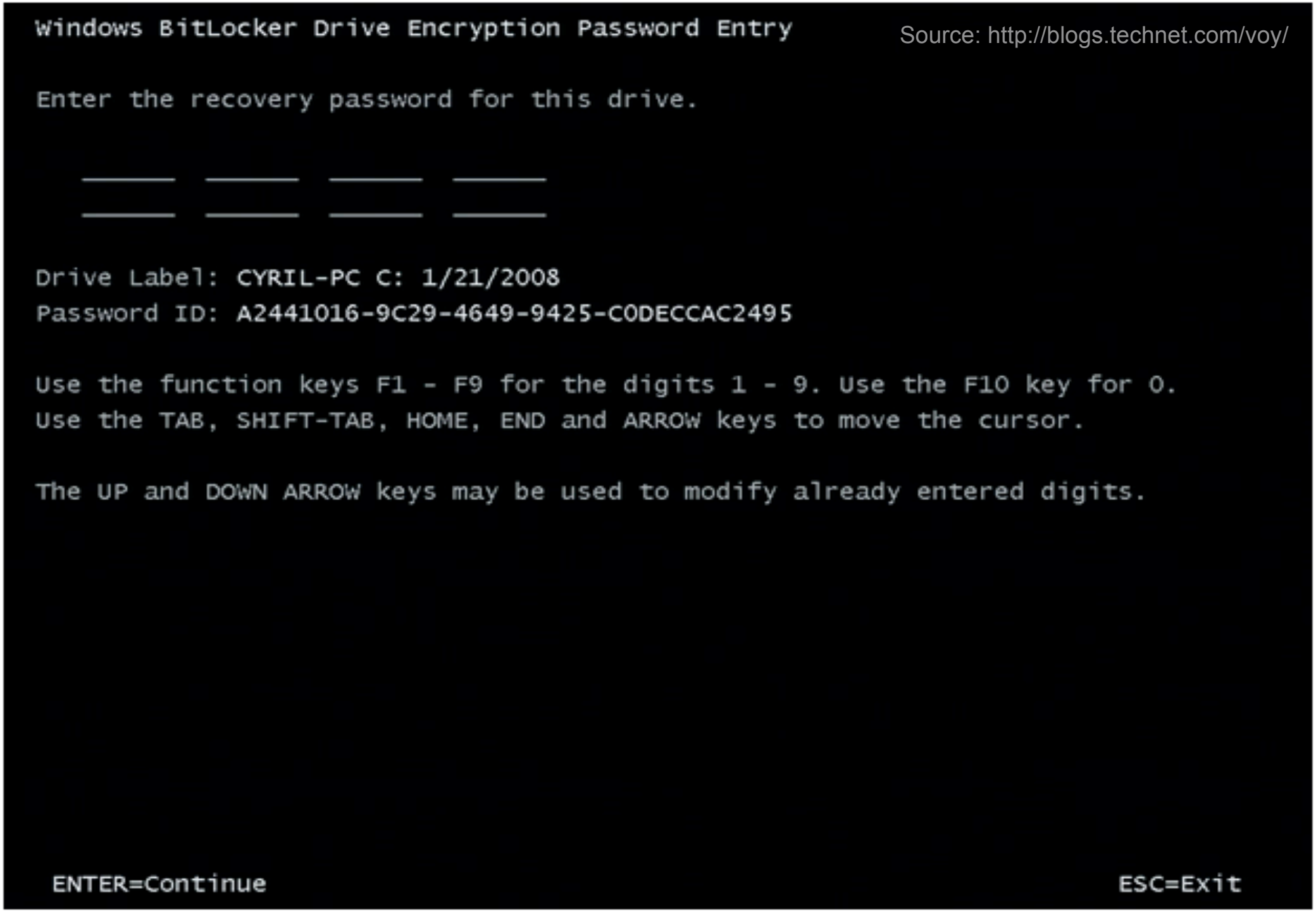
Key Management von BitLocker



Quelle:
BitLocker Drive Encryption Technical Overview,
http://technet.microsoft.com/en-us/library/cc732774.aspx


Source: http://blogs.technet.com/voy/
Windows BitLocker Drive Encryption key needed.
Insert key storage media.
Press ESC to reboot after the media is in place.
Drive Label: CYRIL-PC C: 1/21/2008
Key Filename: D978F0A8-16F9-4AEB-8381-147B330E2117.BEK
ENTER=Recovery
ESC=Reboot


Windows BitLocker Drive Encryption Information
The system boot information has changed since BitLocker was enabled.
You must supply a BitLocker recovery password to start this system.
Confirm that the changes to the system boot information are authorized.
If the changes to the system boot information are trusted, then disable and re-enable BitLocker. This will reset BitLocker to use the new boot information.
Otherwise restore the system boot information.
Source: http://blogs.technet.com/voy/


Windows BitLocker Drive Encryption Password Entry
Source: http://blogs.technet.com/voy/
Enter the recovery password for this drive.
Drive Label: CYRIL-PC C: 1/21/2008
Password ID: A2441016-9C29-4649-9425-C0DECCAC2495
Use the function keys F1 - F9 for the digits 1 - 9. Use the F10 key for 0.
Use the TAB, SHIFT-TAB, HOME, END and ARROW keys to move the cursor.
The UP and DOWN ARROW keys may be used to modify already entered digits.
ENTER=Continue
ESC=Exit

Angreifermodell

- Gezielter Angriff
  - Mehrmalige Interaktion mit dem Ziel möglich
  - Spätere Entdeckung akzeptabel
  - Physischer Zugriff
- Gesucht:
  Lesezugriff auf Klartext

Zum Beispiel:

Erfolgsfälle

1) PIN / USB-Key + TPM-versiegelter Teil + Geheimtext

2) Wiederherstellungsgeheimnis + Geheimtext

3) Bootfähiges System + Schlüssel aus dem RAM lesen

4) Kompromittierte Software + Kommunikation

Reset- und Runtime-Angriffe

- Erfordern Zugriff auf Hardware
- Reset
  - TPM zurücksetzen
  - Replay der Messungen
- Runtime
  - Zugriff auf RAM-Inhalt (FVEK)
  - z.B. DMA (Firewire)
  - z.B. Cold Boot

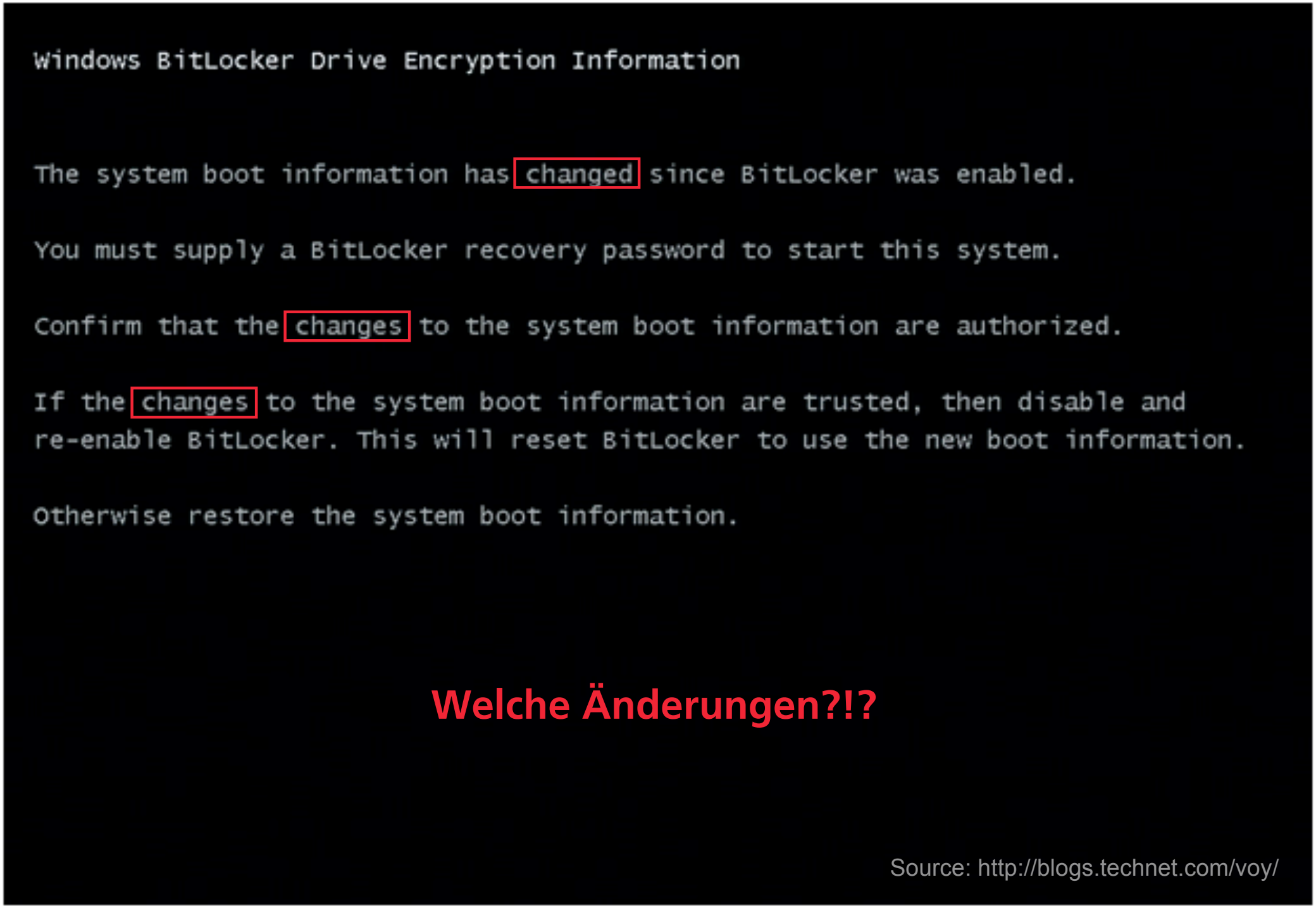
#1: Preemptive Modification

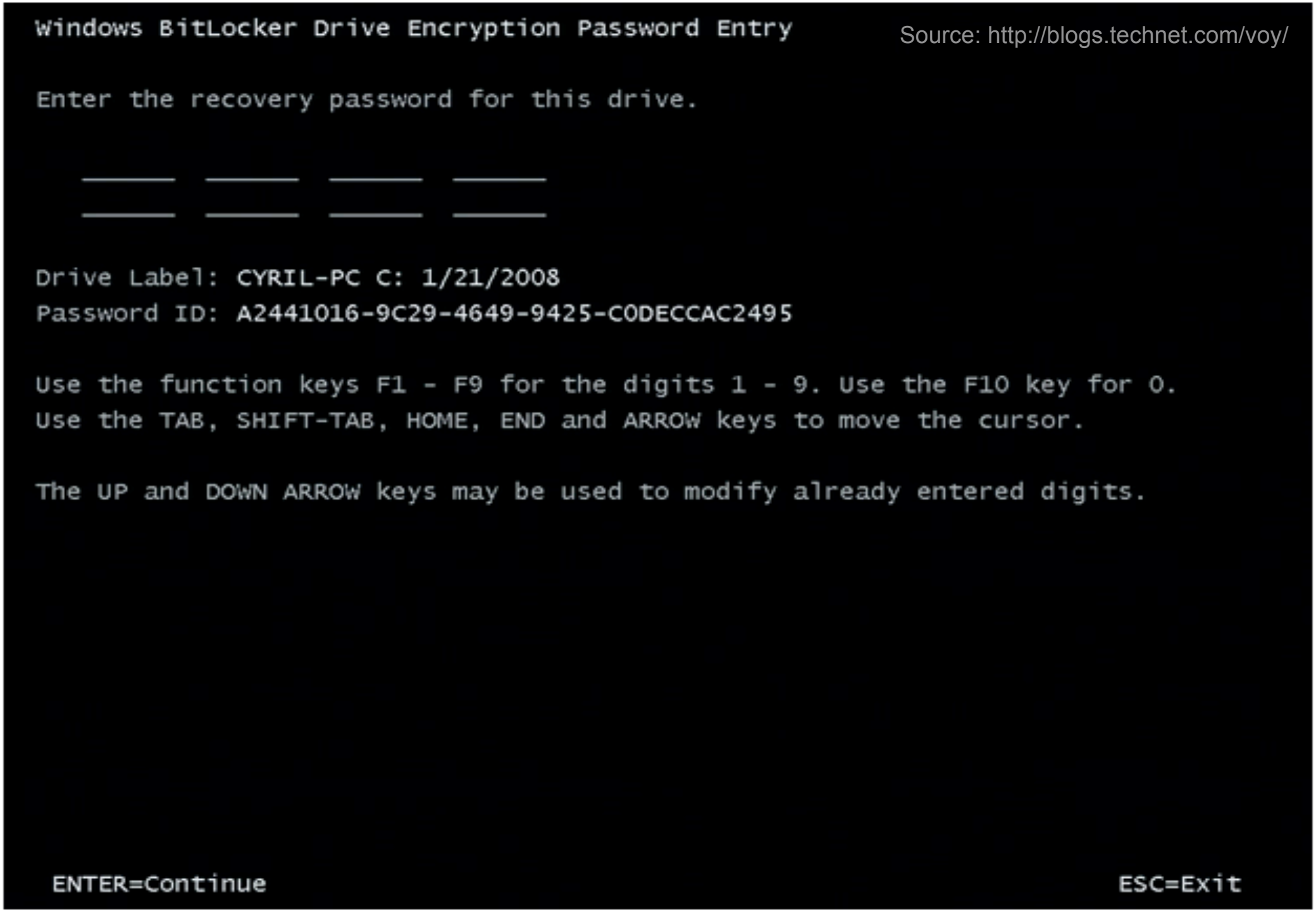
- Manipulation *vor* Aktivierung von BitLocker
  - z.B. durch Lieferanten
- Ergebnis:
  BitLocker nutzt kompromittierten Referenzzustand


DELL
DELL

#2: Plausible Recovery

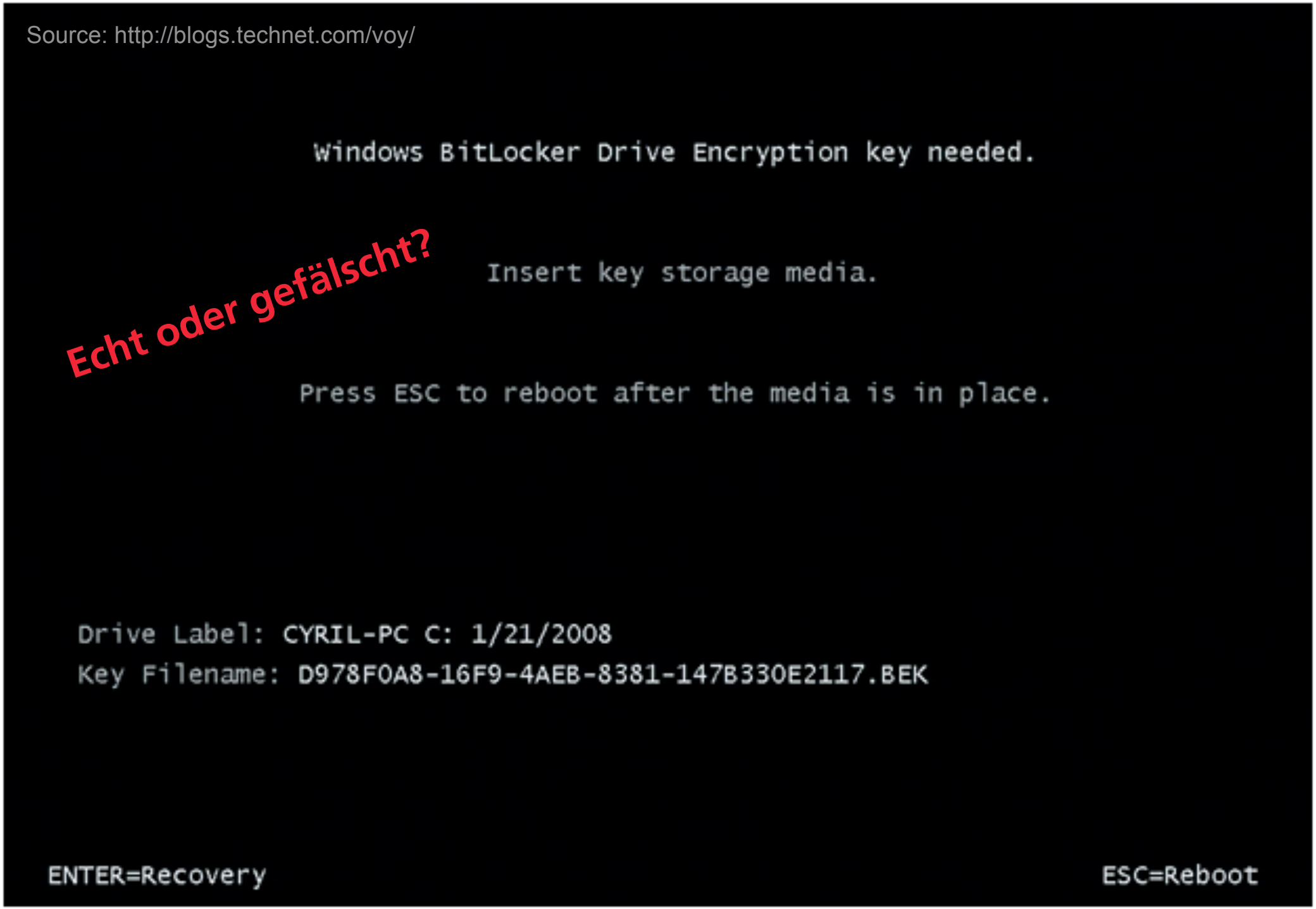
- Trojanisches Pferd installieren
- Nutzer verwendet Recovery-Mechanismen und akzeptiert neuen Zustand
- Kann plausibel sein, z.B. Reparatur
- Ergebnis:
  Software kompromittiert


Windows BitLocker Drive Encryption Information
The system boot information has changed since BitLocker was enabled.
You must supply a BitLocker recovery password to start this system.
Confirm that the changes to the system boot information are authorized.
If the changes to the system boot information are trusted, then disable and re-enable BitLocker. This will reset BitLocker to use the new boot information.
Otherwise restore the system boot information.
Welche Änderungen?!?
Source: http://blogs.technet.com/voy/


Windows BitLocker Drive Encryption Password Entry
Source: http://blogs.technet.com/voy/
Enter the recovery password for this drive.
Drive Label: CYRIL-PC C: 1/21/2008
Password ID: A2441016-9C29-4649-9425-C0DECCAC2495
Use the function keys F1 - F9 for the digits 1 - 9. Use the F10 key for 0.
Use the TAB, SHIFT-TAB, HOME, END and ARROW keys to move the cursor.
The UP and DOWN ARROW keys may be used to modify already entered digits.
ENTER=Continue
ESC=Exit

#3: Spoofed Prompt

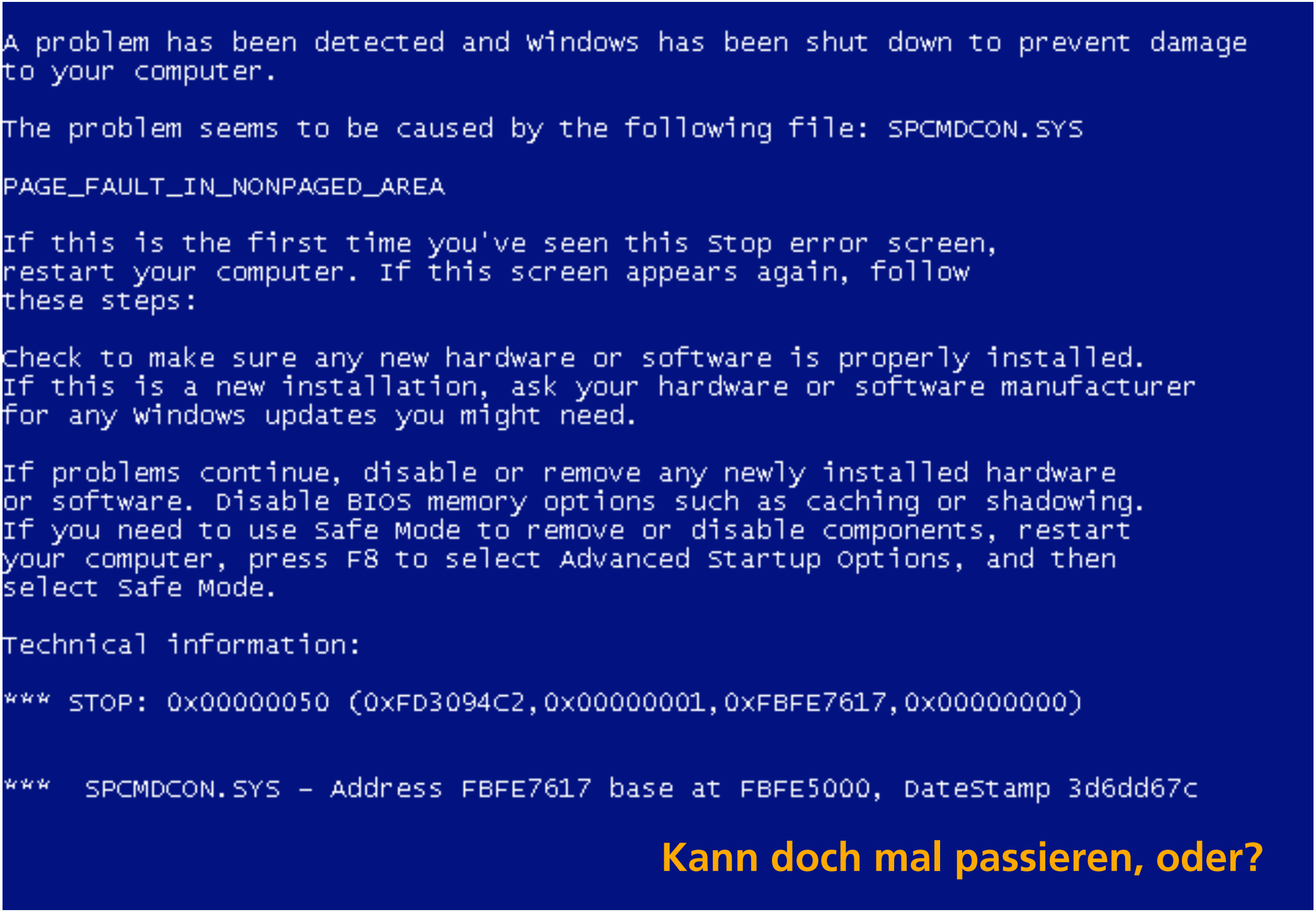
- Trojanisches Pferd installieren
- BitLocker-Prompt nachmachen
  - TPM greift nicht ein
- Ergebnis:
  - PIN, USB-Schlüssel oder Recovery-Key
  - Wird schnell entdeckt, aber ...



Echt oder gefälscht?

#4: Tamper and Revert

- Verbesserung von *Spoofed Prompt*:
- Trojanisches Pferd stellt nach Eingabe des Nutzers den alten Zustand wieder her …
- … und bootet das System neu
- Ergebnis: Geheimnis des Nutzers kompromittiert


A problem has been detected and Windows has been shut down to prevent damage
to your computer.
The problem seems to be caused by the following file: SPCMDCON.SYS
PAGE_FAULT_IN_NONPAGED_AREA
If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:
Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.
If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.
Technical information:
*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)
*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c
Kann doch mal passieren, oder?

#5: Replace and Relay

- Zielsystem stehlen …
- … und durch äußerlich identisches Gerät ersetzen
- Nutzer gibt Geheimnis in das falsche Gerät ein
- Ergebnis:
  Bootfähiges System in der Hand des Angreifers

	Replace and relay	Plausible Recovery	Spoofed prompt	Tamper and revert	Preemptive modification	TPM reset
Passive TPM			X	X		X
No trusted path to user	X		X	X		
No context awareness	X					
Lack of system authentication			X	X		
History-bounded platform validation				X		X
Incomplete diagnostic information		X				
Lack of external reference		X			X	
TPM reset	X		X	X		X
Recovery mechanisms circumventing TPM	X	X	X	X		
Unprotected disk space		X	X	X		
Arbitrary sequence of partial attacks	?	?	?	?	?	?
The barn door property	?	?	?	?	?	?

Ein TPM kann physischen Schutz nicht ersetzen.

Schlussfolgerung

- BitLocker schützt Daten bei opportunistischem Diebstahl
  - Sofern das Gerät abgeschaltet ist
  - Aber das tut jede Verschlüsselung
- Gezielte Angriffe bleiben möglich
  - Aufwand kaum höher als ohne TPM
  - Können strikte Verhaltensregeln helfen?

Kontakt

Fraunhofer SIT
Testlabor IT-Sicherheit

Sven Türpe

Rheinstraße 75
D-64295 Darmstadt

+49-6151-869-238
tuerpe@sit.fraunhofer.de

http://testlab.sit.fraunhofer.de
http://erichsieht.wordpress.com

Fraunhofer SIT
Institut
Sichere Informations-
Technologie