idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

## Press release

### Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
### Oliver Küch

12/03/2009
http://idw-online.de/en/news347450

Research results, Transfer of Science or Research
Economics / business administration, Information technology, Social studies
transregional, national

# Sicherheitslücke trotz Trusted Computing

**Schwachstelle ermöglicht Skimming-Angriff auf die Windows-BitLocker-Festplattenverschlüsselung**

Mitarbeiter des Fraunhofer-Instituts SIT haben eine Sicherheitslücke in der Windows-Festplattenverschlüsselung "BitLocker" gefunden: Hat ein Angreifer die Möglichkeit, unbemerkt den Computerstart zu manipulieren, kann er an die geheime PIN der Festplattenverschlüsselung gelangen und die verschlüsselten Daten stehlen. Der Angriff verdeutlicht, dass die Verwendung von Trusted Computing nicht in allen Situationen vor Manipulationen schützt. Wie der Angriff konkret funktioniert, zeigt ein Video der Fraunhofer-Wissenschaftler im Internet unter http://testlab.sit.fraunhofer.de/bitlocker-skimming/ .

Vor kurzem erst ist ein Angriff auf den Boot-Vorgang des Festplattenverschlüsselungsprogramm TrueCrypt bekannt geworden. Die windowseigene BitLocker-Verschlüsselung galt jedoch noch als sicher, weil die Software zur Überprüfung des Boot-Vorgangs einen Hardware-Chip, das Trusted Computing Module (TPM) nutzt. Das Angriffsszenario des Fraunhofer SIT zeigt jedoch: Auch bei TPM-basierter Festplattenverschlüsselung können Angreifer die Passwörter ausspähen. Das Testlabor des Fraunhofer SIT hat den Angriff gegen die BitLocker-Festplattenverschlüsselung in Windows 7, 2008 Server und Vista praktisch durchgeführt. Der von den Forschern entwickelte Angriff umgeht die Sicherheitsfunktionen von BitLocker vollständig.

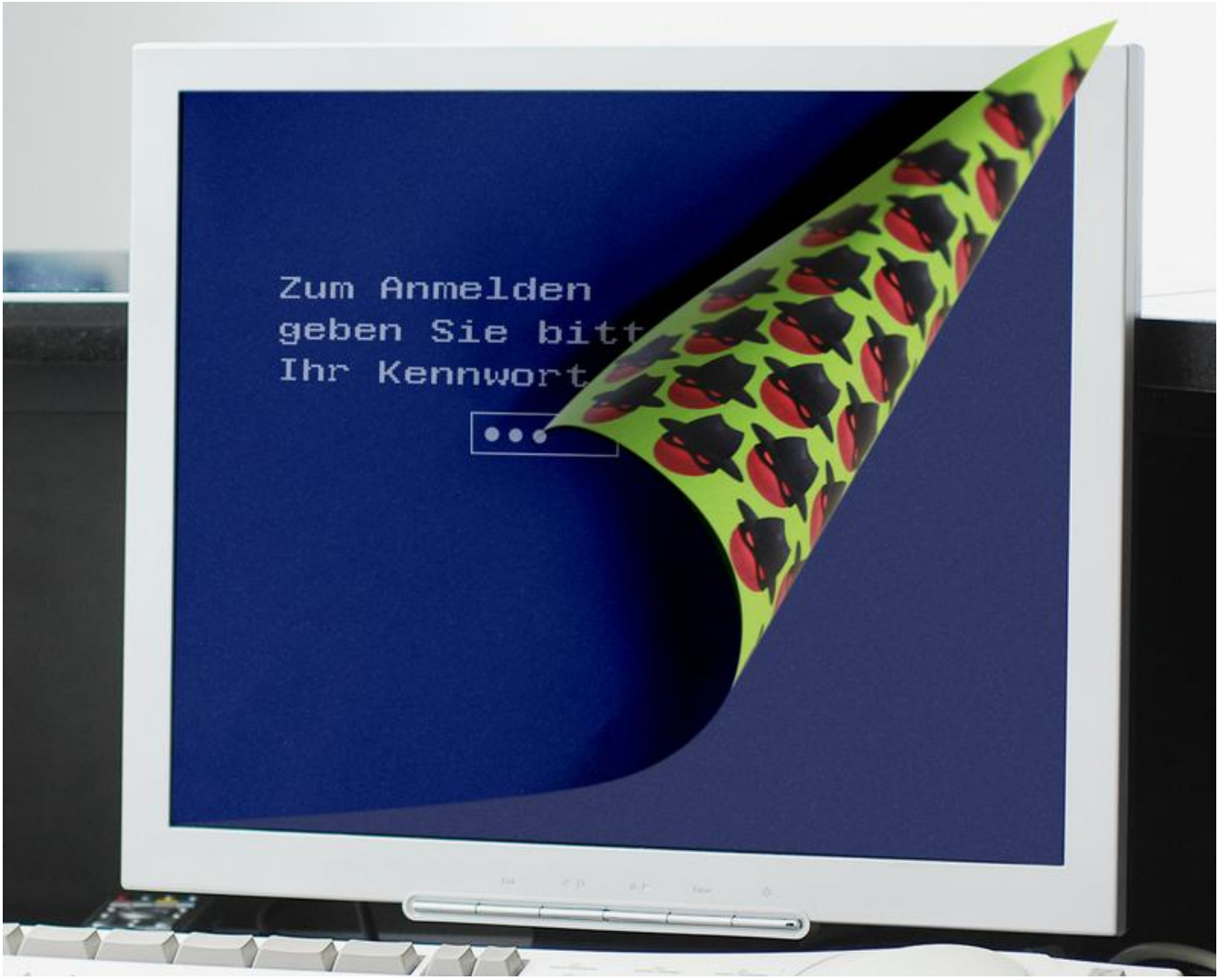
"Das Vorgehen ist vergleichbar mit Skimming-Angriffen an Geldautomaten", sagt Fraunhofer-Mitarbeiter Jan Steffan. "Erhält ein Angreifer kurz Zugang zum geschützten Computer, kann er die Startroutine von BitLocker durch ein eigenes Programm ersetzen, welches eine PIN-Abfrage vortäuscht. Wenn der Besitzer seinen Computer daraufhin startet, scheint dieser wie gewohnt nach der BitLocker-PIN zu fragen." Nun ist jedoch das Programm des Angreifers aktiv, das die geheime PIN im Klartext auf der Festplatte hinterlegt. Nach der PIN-Eingabe entfernt sich das Programm automatisch, stellt die BitLocker-Startroutine wieder her und startet den Rechner neu. BitLocker funktioniert jetzt wieder wie gewohnt - der Benutzer kann den Angriff, abgesehen vom Neustart des Computers, kaum erkennen. Der Angreifer verschafft sich jetzt ein zweites Mal Zugang zum Computer, liest die PIN von der Festplatte und entschlüsselt damit die geschützten Daten.

Im Gegensatz zu vielen anderen Festplattenverschlüsselungen nutzt BitLocker ein auf der Hauptplatine des Computers vorhandenes Trusted Platform Module (TPM). Damit prüft er die Unversehrtheit der zum Windows-Start notwendigen Software. "Wir haben einfach die Tatsache ausgenutzt, dass sich BitLocker dabei selbst mit Hilfe des TPM überprüft", sagt Jan Trukenmüller. "Ersetzt man BitLocker durch ein eigenes Programm, überprüft niemand mehr, ob die PIN-Eingabeaufforderung tatsächlich echt ist." Im Gegensatz zu den kürzlich auf der Blackhat-Konferenz veröffentlichen Angriff gegen die TrueCrypt-Festplattenverschlüsselung, benötigt der Angreifer jedoch zweimal Zugang zum verschlüsselten Computer.

Industriespione könnten mit dem Angriffsszenario in Unternehmen gezielt auf Datenfang gehen. "Trotz der Sicherheitslücke ist BitLocker eine gute Lösung zur Festplattenverschlüsselung", so Trukenmüller, "denn vor der häufigsten Bedrohung für sensible Daten auf Festplatten -- dem Verlust oder Diebstahl von Computern -- schützt

BitLocker gut."

URL for press release: http://testlab.sit.fraunhofer.de/bitlocker-skimming/




Optische Täuschung: Der Benutzer glaubt er sieht das Original.
Fraunhofer SIT