IBMs Notebook mit TCPA

Schlüssel-suche

Lukas Grunwald

Als eines der ersten Notebooks, das den TCPA-Standard erfüllen soll, bietet IBM sein Thinkpad T-30 an. Eine genaue Untersuchung zeigt, was der Krypto-Chip unter Sicherheitsaspekten bringt.

Recht kontrovers führen Fachleute die Diskussion um neue hardwaregestützte Verschlüsselungsverfahren: Zusätzlicher Schutz gegen das Ausspionieren von Daten auf der einen Seite, auf der anderen die berechtigte Sorge um den Schutz der individuellen Freiheit (siehe Kasten „Was hinter dem ‚T' steht").

Wer einen frisch gelieferten Thinkpad T-30 mit dem Trusted Platform Module (TPM) nach den Regeln der Trusted Computing Platform Alliance (TCPA) auspackt, findet zum Thema Verschlüsselung keine passende Software auf dem Rechner. IBM stellt sie auf Nachfrage zum Herunterladen auf seiner Site bereit und hat sie auf Bitte der Redaktion hin für den Test auf einer selbst gebrannten CD nachgeliefert. Bis dato gibt es das Programmpaket nur in Englisch, das Betriebssystem auf dem Laptop, Windows XP Professionell, ist aber in Deutsch vorinstalliert, was zumindest zu einem Sprachenmischmasch führt.

Anwendungen können für die TCPA-Verschlüsselung Microsofts Krypto-API und PKCS#11 nutzen. Um diese zu aktivieren, muss der Eigner des Rechners erst die Treiber für den SME-Bus und ATMELs Krypto-Chip AT97SC3201 installieren. Danach soll er das Verschlüsselungssubsystem einrichten und Keys direkt auf dem Chip des Notebooks „sicher" und TCPA-konform hinterlegen können.

Umbaumaßnahmen zur Absicherung

Beim Installieren der Krypto-Unterstützung für das Notebook ersetzt IBMs Software die Login-Prozedur von Windows durch eine eigene, die mit ihren neuen Passwortregeln neue Zugangsworte verlangt. Dafür muss der Administrator einen Schlüssel im Krypto-Subsystem erzeugen und im Chip speichern. Das Sichern dieses Admin-Key ist zwingend. Laut Aussagen von IBM soll der Chipsatz des T-30 sicher gegen Fremdzugriffe sein. Damit bei einer Dateiverschlüsselung deren Inhalt aber nicht unrettbar verloren geht, sollte der Systembetreuer beim Einrichten ein Backup-Verzeichnis anlegen. Bei diesem muss er den Key anschließend unbedingt von Hand entfernen. Das Dateisystem sollte auf keinen Fall solche Schlüssel enthalten, die außerdem nicht mit sich selbst verschlüsselt werden dürfen, denn wenn der Key verloren geht, etwa durch Löschen des Chips, sind die Daten ein für alle mal verloren.

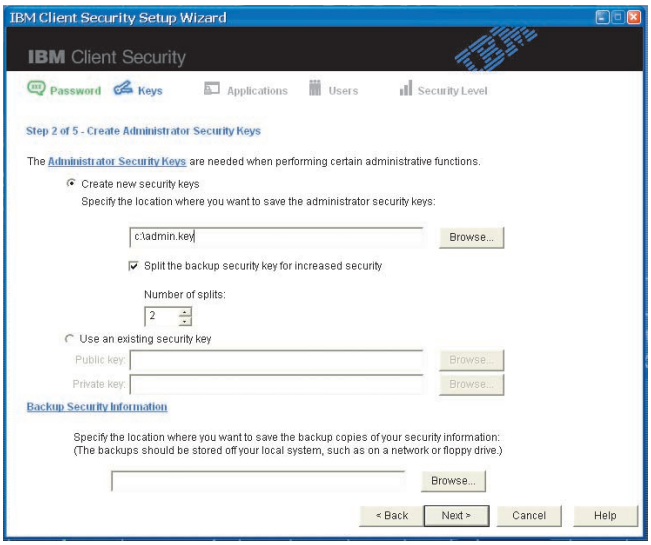
Um das Sicherheitsniveau zu erhöhen, kann der Administrator den Schlüssel in zwei Teile zerlegen und an zwei voneinander unabhängigen Orten hinterlegen. Es ist dann Sache eines passenden organisatorischen Konzeptes, dafür zu sorgen, dass keiner allein Zugriff auf den Admin-Key erhält.

Das Notebook unterstützt nur das Speichern von Schlüsseln, aber keine Signaturprüfung oder andere Sicherheitsmethoden wie von TCPA vorgesehen, ganz zu schweigen von einem „Trusted Operating System", von dem bei Windows XP trotz IBMs Login-Erweiterung nicht die Rede sein kann.

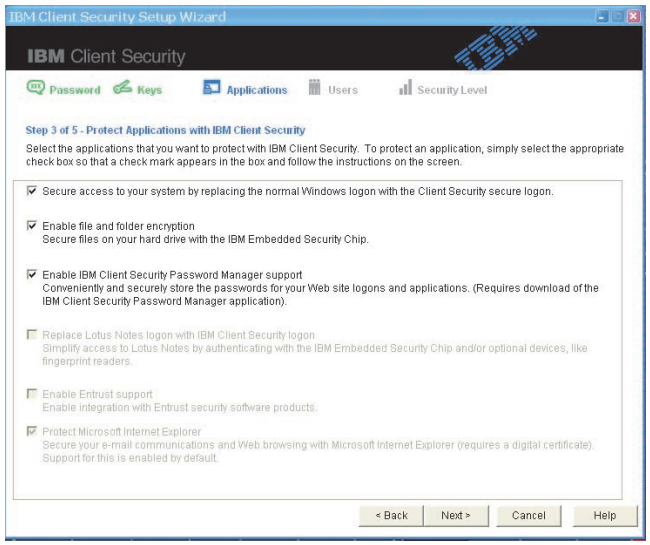
Die Software warnt zwar beim Installieren davor, dass sich Benutzer nicht mehr anmelden können, wenn jemand den Chipinhalt löscht, das gilt

iX-TRACT

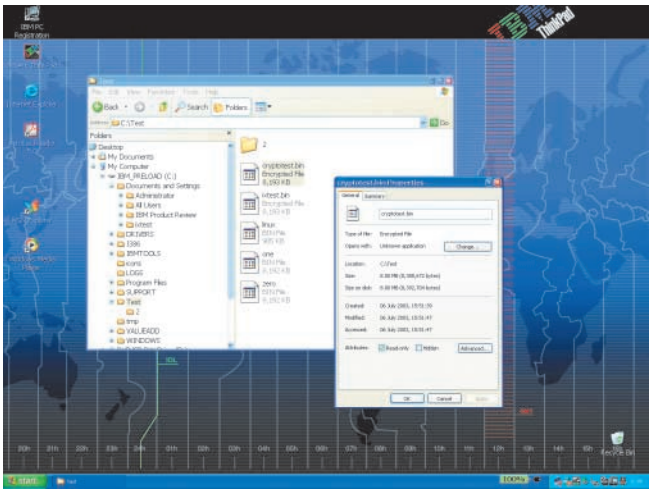
- Trusted Platform Modules verbauen IBM und HP bereits in mehreren Laptop- und Desktop-Modellen, ohne dies besonders herauszustellen.
- Eine solche hardwaregestützte Verschlüsselungstechnik nach den Vorschlägen der Trusted Computer Group birgt das Risiko einer ausufernden Fremdkontrolle.
- Außer einem veränderten Login und rudimentären Verschlüsselungswerkzeugen unter Windows und einem Experimentalpaket samt Quellen unter Linux gibt es derzeit keinerlei Anwendungen.



Zauberhaft: IBMs Installationsroutine für den Security Client erlaubt auf Wunsch ein Verteilen der Schlüsselteile (Abb. 1).



Fehlt was: Ein neues Anmeldeverfahren nebst strengen Passwortregeln und die Dateiverschlüsselung sorgen für ein erhöhtes Sicherheitslevel, doch Signaturprüfung und andere Verfahren fehlen (Abb. 2).



Gelbe Karte: An der Größe sieht man, dass das Verfahren keine Redundanzen eliminiert (Abb. 3).

aber nur für das von IBM ausgetauschte Login-Programm. Wer im per F8 erreichbaren Bootmanager von XP die Emergency Konsole oder den „Safe-Mode“ auswählt, landet wie gewohnt bei einer Shell, ohne dass die Krypto-Funktion eingreift.

Außerdem kann das BIOS jedes Betriebssystem booten und beliebigen Programmcode ausführen. Im Test fand hierfür ein Verkleinern der Windows-Partition gefolgt von einer Linux-Installation im frei gewordenen Bereich statt.

Hintertüren an allen Ecken

Ein weiterer Gegenstand der Untersuchung ist die Dateiverschlüsselung mit Hilfe spezieller Testdateien: eine mit 8 MByte Null-Bytes, eine weitere mit 8 MByte Einsen, eine gleich große Signaturdatei mit einer lesbaren Zeichenkette und ein Linux-Kernel.

Eine Überprüfung der verschlüsselten Dateien mit einem Forensik-Toolkit deckt auf, dass das Original nach einem Kopiervorgang noch in der Swap-Datei (Pagefile) zu finden ist. Die Krypto-Software sollte sämtliche Puffer von derartigen Überresten reinigen.

Windows löscht die Swap-Datei nicht, ebenso wenig die Software von IBM. Der Effekt: mit einem anderen Betriebssystem kann jeder deren Inhalt und damit die geheimen Informationen auslesen.

Gerade noch rechtzeitig vorm Redaktionsschluss tauchte ein brauchbares Linux-Paket in Version 1.1b für das TPM auf. Es handelt sich um ein ladbares Kernelmodul von Leendert van Doorn, tätig in IBMs Watson Research – Global Security Analysis Lab (siehe „Fundorte im Web“). Das Gzip-File enthält neben Readme-Dateien mit knapper

Qualitäten des Notebooks

IBMs Thinkpad T-30 hinterlässt als Notebook einen soliden Eindruck. Neben der akzeptablen Ausstattung (siehe Daten und Preise) gefällt der dicht schließende Deckel, der verhindert, dass das Display einstaubt oder bei Erschütterungen Tasten auf dem Display einen Abdruck hinterlassen, wie es bei so manch anderem Notebook der Fall ist, etwa bei Dells Inspiron und Apples Powerbook.

Für den Stromhunger der eingebauten Komponenten liefert der eingebaute Akku nicht lang genug Nahrung, sodass er bei normalem Arbeiten nach weniger mehr als 1,5 Stunden an die Nabelschnur des Stromnetzes muss. Wenn auf dem Thinkpad eine rechenintensive Applikation ohne Stromsparmodus werkelt, hält der Akku etwas unter einer Stunde, was für ein Notebook dieser Klasse eindeutig zu wenig ist.

Ungewohnte dürfte das eigenwillige Keyboard-Layout stören: Die Taste für die Sonderfunktionen (FN) liegt links außen neben der CTRL-Taste, was einen beim Wechseln vom Desktop zum Thinkpad zum Wahnsinn treiben kann, ebenso wie die über der F1- angebrachte ESC-Taste. Dieses Design erschwert geübten Keyboard-Schreibern trotz der qualitativ guten und druckgenauen Tastenmechanik das Leben.

aber gut nachvollziehbarer Anleitung ein 18-seitiges PDF-Dokument, die Quellen der *Libtpm.a*-Bibliothek und der API sowie einiger Beispielprogramme.

Nach dem Anpassen an die jeweilige Linux-Distribution – im Test war es Debian – sind noch ein paar Handgriffe zum Installieren notwendig. Abweichend von der Anleitung funktioniert die TPM-Schnittstelle erst nach einem *modprobe tpm*, *depmod –a* reicht nicht. Danach stehen Demo-Werkzeuge zur Verfügung, und zwar für das Auslesen der TPM-Informationen, die Personalisierung des Chips, das Ver- und Entschlüsseln von Dateien, das Erzeugen von Schlüsseln, das Signieren und Verifizieren von Dateien sowie zum Beseitigen der Schlüssel.

Irgendwelche Eingriffe in den Anmeldeprozess oder die Benutzerverwaltung finden bei der Version 1.1b unter Linux noch nicht statt. Im Unterschied zu Windows verändert das Verschlüsseln mit Nullen gefüllte Dateien in der Größe und entfernt sämtliche Redundanz.

Fazit

Das T-30 zählt zu den modernen Notebooks, wie es in der Preisklasse viele Mitbewerber anbieten. Wo der Mehrwert des fest eingebauten TPM-Chips liegen soll, ist wegen der kaum vorhandenen Anwendungen sowie der schlechten Integration in das Betriebssystem derzeit nicht zu erkennen. Kryptographiechips in mobilen Geräten wie in einem Notebook bringen wenig, denn sie schützen in keiner Weise vor Diebstahl und anschließendem Missbrauch, da sich das Verfahren leicht abschalten lässt.

Mancher Consultant, der sein Notebook lieber im Hotelzimmer deponiert

QUELLEN IM WEB

TCPA-Spezifikation	www.trustedcomputing.org
TCG	www.trustedcomputing group.org
Kritik an TCPA	www.moon.hipjoint.de/ tcpa-palladium-faq-de.html
	www.againsttcpa.com
Lucky Green	www.cypherpunks.to/ TCPA_DEFCON_10.pdf
AEGIS	www.cis.upenn.edu/ ~waa/aegis.ps
Palladium	www.activewin.com/ articles/2002/pd.shtml
Linux-Tools	www.research.ibm.com/ gsal/tcpa/
ATML-Chip	www.atmel.com/ad/ TCG/default.asp

DATEN UND PREISE

IBMs Thinkpad T-30 mit TPM-Chip

Hardware: Pentium 4 Mobile Prozessor von Intel, 2,4 GHz; 256 MByte DDR-SDRAM; 30 GByte große Festplatte von Hitachi; ATI Randon Mobility 7500, 32 MByte VRAM; integrierte Wireless-Karte nach IEEE 802.11b; TPM-Chip

Software: Windows XP vorinstalliert; Verschlüsselungssoftware von IBM auf Nachfrage: Dateiverschlüsselung und Login-Prozedur mit schärferen Passwortregeln als bei Windows

Hersteller/Anbieter: IBM, www.ibm.de

Preis: 2220 €

und nur seine sensiblen Daten auf einer Wechselplatte oder seinem USB-Stick mitnimmt, würde durch den fest im Rechner integrierten Krypto-Chip eher behindert.

Zwar hat IBM gegenüber den vorherigen rudimentären Linux-Versionen mit der 1.1b ein Paket geschaffen, das einem Dank der vorliegenden Quellen einen ersten Eindruck von TPM verschaffen kann. Bei der Dateiverschlüsselung unter Windows bedarf es aber Nachbesserungen, da diese Implementierung reinen Softwarelösungen wie GPG (Gnu Privacy Guard) wegen der fehlenden Redundanzentfernung weit unterlegen ist. Aber es dürfte ohnehin eher um die stille Vorbereitung von Palladium & Co. gehen als um Datensicherheit für den Anwender. (rh)

LUKAS GRUNWALD

arbeitet als Consultant bei der DN Systems GmbH in Hildesheim und ist in diverse freie Softwareprojekte involviert.

Literatur

[1] Ute Roos; TCPA; Vertrauensfragen; Trusted-Computing-Symposium in Berlin; *iX* 9/2003, S. 20

[2] Klaus Schmeh; Kryptographie; dpunkt-Verlag 2001

[3] Reinhard Wobst; Abenteuer Kryptologie; Addison-Wesley 2001

Glossar

Fritz-Chip: Nach dem für vollständige Kontrolle plädierenden Senator Fritz Hollings benannter Coprozessor, der chiffrieren, Schlüssel generieren, digitale Signaturen überprüfen und identifizieren kann.

TCPA (Trusted Computing Platform Alliance): 1999 von Compaq, HP, IBM, Intel und Microsoft zur Entwicklung einer sicheren Hardwareplattform gegründetes Hersteller-Konsortium. Derzeit aktuelle TCPA-Spezifikation ist auf dem Stand 1.1b.

TCG (Trusted Computing Group): Im April von AMD, HP, IBM, Intel und Microsoft gegründeter TCPA-Nachfolger.

TPM (Trusted Platform Module): TCPA-Hardware („Fritz-Chip"), unter anderem hergestellt von Intel, Atmel, Infineon und NSC.

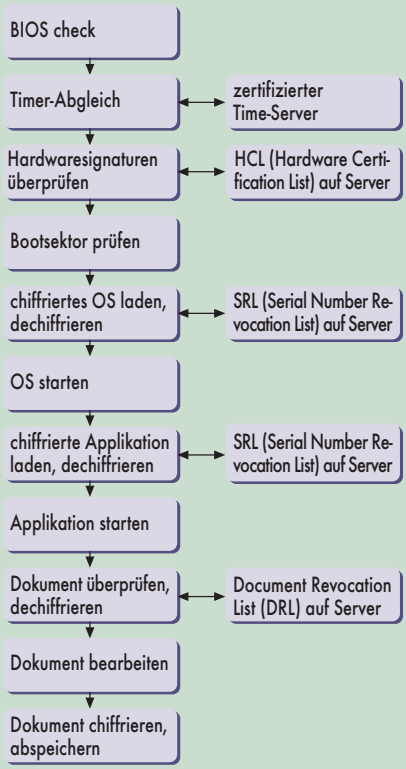
Palladium/NGSCB: TCPA-konforme Software von Microsoft, die voraussichtlich 2005 in das nächste Windows-Release mit dem Codenamen Longhorn integriert sein wird und TCPA teilweise implementiert.

Was hinter dem „T" steht

Im Jahr 1999 gründeten Compaq, HP, IBM, Intel und Microsoft die „Trusted Computing Platform Alliance" (TCPA) mit dem erklärten Ziel, eine höhere Computersicherheit zu erreichen. Hardwarekomponenten, so genannte Trusted Platform Modules (TPM), sollen durch Prüfen von Statusinformationen für sicheres Booten, Speichern sowie das Identifizieren von „vertrauenswürdiger" Soft- und Hardware sorgen. Die auf 180 Mitglieder angewachsene Liste umfasst unter anderem Adobe, Infineon, Motorola, NEC, RSA, Siemens und Toshiba. Die Trusted Computer Group (TCG), die im April die Rechtsnachfolge der TCPA angetreten hat, will offene, hersteller- und betriebssystemunabhängige Standards definieren.

Auf die bisher vorliegende 300 Seiten starke und ausgesprochen schwer verständliche TCPA-Spezifikation hat es kaum Reaktionen gegeben. Erst seit Microsoft über seine geplante Betriebssystemkomponente Palladium zu sprechen begonnen hat (die „mehr oder weniger" auf TCPA beruhe), findet eine heftige öffentliche Diskussion statt.

In einem TCPA-konformen System übernimmt eine spezielle Hardware, der nach Senator Fritz Hollings benannte „Fritz-Chip", die kryptograhische Kontrolle. Sie enthält unter anderem öffentliche Schlüssel zur Überprüfung digitaler Signaturen. Diese Schlüssel tragen Zertifikate, die der TCPA-Standard jedoch nicht beschreibt [2, 3]. Insbesondere ist ein eindeutiger, Mainboard-spezifischer (endorsement Key, EK) untergebracht, den der Hersteller signiert. Private Schlüssel behält der Chip für sich und arbeitet mit ihnen nur lokal: Der Anwender kann sie nicht auslesen.



Orwellsch: Die schematische Übersicht zeigt, wie viele Kontroll- und Freigabevorgänge „fremde Instanzen" erzwingen können.

Startet man den Computer im so genannten „Trusted Mode", überprüfen BIOS und Software mit Hilfe des Chips die Zertifikate und alle von den Herstellern erzeugten digitalen Signaturen in Hard- und Software. Bei Microsofts Sicherheitskonzept Palladium, das seit kurzem NGSCB (Next Generation Secure Computing Base) heißt und als fester Bestandteil des 2005 erscheinenden Windows mit Codenamen Longhorn geplant ist, sollen sogar Tastatur und Monitor mit einbezogen sein. Wer keine gültige Unterschrift vorzeigen kann, bleibt außen vor. Und nur Produkte, die von einer TCPA-Instanz zertifiziert sind, dürfen die begehrten Signaturen tragen.

TCPA liefert alle Voraussetzungen, dem Anwender die Kontrolle über seinen Rechner aus der Hand zu nehmen. Die TCG streitet zwar solche Intentionen ab [1], räumt aber ein, dass ein Missbrauchspotenzial vorhanden sei und man keinen Einfluss darauf habe, wie die einzelnen Hersteller letzten Endes die Standards in die Praxis umsetzten.

Den geplanten Einsatz von übers Internet aktualisierten Hardware Certification Lists (HCL), Serial Number Revocation Lists (SRL) und Document Revocation Lists (DCL), mit denen eine effektive Kontrolle der Hardwarekomponenten, Anwendungen und des Zugriffs auf gespeicherte Dokumente möglich wäre, bestreiten die beteiligten Hersteller.

Natürlich könne der Anwender einen TCPA-PC ebenso mit deaktiviertem Fritz-Chip starten und wie bisher nutzen (es steht aber nirgendwo, dass das für alle Zeiten gilt). In diesem so genannten Voluntary Mode gibt es jedoch keinen Zugriff auf die privaten Schlüssel. Wer seine geschützten Dokumente lesen will, muss im Trusted Mode booten und sich mit den zugelassenen Anwendungen begnügen.

IBM und HP liefern bereits Notebooks und Desktops mit TPM. In Bälde soll das Modul in die CPU integriert sein. Das betrifft die für 2003 angekündigten Intel-Prozessoren mit La-Grande-Technik ebenso wie zukünftige CPUs von AMD. Transmeta hat eine Firmware-Version des Moduls für den Crusoe TM5800 angekündigt. Das alles könnte schon 2004 Stand der Technik sein.

Reinhard Wobst